Pure and Applied Mathematics Quarterly
Volume 4, Number 4
(*Special Issue: In honor of
Jean-Pierre Serre, Part 1 of 2*)
1013—1031, 2008

Cusps of Minimal Non-compact Arithmetic Hyperbolic 3-orbifolds

Ted Chinburg, Darren Long and Alan W. Reid

To Jean-Pierre Serre for his eightieth birthday with admiration

Abstract: In this paper we count the number of cusps of minimal non-compact finite volume arithmetic hyperbolic 3-orbifolds. We show that for each N, the orbifolds of this kind which have exactly N cusps lie in a finite set of commensurability classes, but either an empty or an infinite number of isometry classes.

1. Introduction.

In this paper we count the number of cusps of minimal non-compact finite volume arithmetic hyperbolic 3-orbifolds. An orbifold of this kind is isometric to $\mathbf{H}^3/\Gamma$, where $\mathbf{H}^3$ is hyperbolic upper half space and Γ is a maximal discrete arithmetic subgroup in $\mathrm{PGL}_2(k)$ for some imaginary quadratic field k.

It is well known (cf. §3 below) that the cusps of the orbifold $\mathbf{H}^3/\Gamma$ correspond to Γ-equivalence classes of points of P^1_k under the action of $\mathrm{PGL}_2(k)$ on P^1_k. It was first noted by Bianchi [2] that $\mathbf{H}^3/\mathrm{PSL}_2(O_k)$ has h_k cusps where h_k is the class number of k. By work of Allan [1] and Shmidt [7], there is a unique maximal arithmetic subgroup $\Gamma_{\phi,\phi}$ of $\mathrm{PGL}_2(k)$ which contains $\mathrm{PSL}_2(O_k)$. Let $Cl(k)$ be the ideal class group of k, and let $h_{k,2}$ be the order of $Cl(k)/(2\cdot Cl(k))$. It follows from the work of Vinberg in [11, §2] that $\mathbf{H}^3/\Gamma_{\phi,\phi}$ has $h_k/h_{k,2}$ cusps. (Some closely related results are proved by Elstrodt, Grunewald and Mennicke in [4,

Received January 3, 2006.
1991 Mathematics Subject Classification. Primary 51M10; Secondary 20H15, 11R29.
Key words and Phrases. hyperbolic orbifolds, cusps, arithmetic groups.
All three authors were supported by N.S.F. Focused Research Group grant DMS01-39816 in addition to individual N.S.F. grants.

§7.2,7.4]). In particular, since there are only finitely many imaginary quadratic number fields of a fixed class number, for any given N there are only finitely orbifolds $\mathbf{H}^3/\Gamma_{\phi,\phi}$ as above which have N cusps.

The objective of this paper is to generalize the above result of Vinberg to an arbitrary maximal arithmetic subgroup Γ of $\mathrm{PGL}_2(k)$. To state the main theorem, recall that in [3], Borel described for each pair (S, S') of finite disjoint sets of finite places of k a discrete finite covolume subgroup $\Gamma_{S,S'}$ of $\mathrm{PGL}_2(k)$. We recall the definition of $\Gamma_{S,S'}$ in §2. Borel showed that each maximal finite covolume discrete subgroup of $\mathrm{PGL}_2(k)$ is conjugate to $\Gamma_{S,S'}$ for some (S, S').

The main result of this paper is:

Theorem 1.1. *Let $Cl(k)$ be the ideal class group of k. The number of cusps of $\mathbf{H}/\Gamma_{S,S'}$ is*

$$2^n \frac{h_k}{h_{k,2}}$$

where h_k is the class number of k, $h_{k,2}$ is the order of $Cl(k)/(2 \cdot Cl(k))$, $0 \leq n \leq \#S$ and 2^n is the order of the subgroup of $Cl(k)/(2 \cdot Cl(k))$ generated by the classes of prime ideals determined by the places in S.

This Theorem and work of Siegel in [8] leads to a proof of the following Corollary.

Corollary 1.2. *Let N be a positive integer, and let $C(N)$ be the set of isometry classes of minimal finite volume arithmetic hyperbolic three-orbifolds which have exactly N cusps.*

a. *Only finitely many commensurability classes are represented by the elements of $C(N)$.*
b. *If $C(N)$ is not empty, there are infinitely many elements of $C(N)$ which are commensurable to each element of $C(N)$.*

The proof of part (a) of this Corollary is not effective, though it can be made effective up to at most one exceptional commensurability class using work of Tatuzawa in [9]. Finding an effective proof is equivalent to the problem of showing that there are only finitely many imaginary quadratic fields k such that $h/h_{k,2}$ is bounded above by a given constant. Such a proof appears to be beyond present methods.

This paper is organized in the following way. In §2 we recall Borel's definition of $\Gamma_{S,S'}$. In §3 we recall some well-known facts concerning cusps of non-compact arithmetic three-orbifolds. In §4 and §5 we analyze the cusps of certain orbifolds defined by congruence subgroups of $\Gamma_{S,S'}$. This leads to the proof of Theorem 1.1 in §6 - §8. The main techniques used in §4 - §8 are Borel's work, the Strong Approximation Theorem for SL_2, and an argument of Swan [10] for constructing matrices satisfying various congruence conditions which send a prescribed point of P^1_k to another prescribed point. Corollary 1.2 is proved in §9.

Acknowledgements: We would like to thank the referee for helpful comments and references.

2. Borel's subgroups.

Let k be an imaginary quadratic field, with ring of integers $O = O_k$. Let S and S' be finite disjoint subsets of the set of all finite places v of k. For each such v, let k_v be the completion of k at v. Let π_v be a uniformizer in the ring of integers O_v of k_v. Define $\mathcal{D}_v = \mathrm{Mat}_2(O_v)$, and let $\mathcal{D}'_v$ be the maximal O_v-order of all matrices of the form

$$M = \begin{pmatrix} a & \pi_v b \\ \pi_v^{-1} c & d \end{pmatrix} \tag{2.1}$$

in which $a, b, c, d \in O_v$. Define $K_{1,v} = \mathrm{PGL}_2(O_v)$, so that $K_{1,v}$ is the image of $\mathcal{D}_v^*$ in $\mathrm{PGL}_2(k_v)$. Let $K'_{1,v}$ to be the image of $\mathcal{D}'^*_v$ in $PGL(2, k_v)$. Finally, let $K_{2,v}$ be the group generated by $K_{1,v} \cap K'_{1,v}$ together with image in $\mathrm{PGL}_2(k_v)$ of the element

$$w_v = \begin{pmatrix} 0 & \pi_v \\ 1 & 0 \end{pmatrix} \tag{2.2}$$

Then $K_{1,v}$ and $K'_{1,v}$ are the stabilizers in $\mathrm{PGL}_2(k_v)$ of adjacent vertices of the Bruhat-Tits building of $\mathrm{SL}_2(k_v)$, and $K_{2,v}$ is the stabilizer the edge joining these vertices. In [3] Borel defines $\Gamma_{S,S'}$ to be the group

(2.3)

$$\{g \in \mathrm{PGL}_2(k) : g \in K_{2,v} \text{ (resp. } K'_{1,v}, \text{ resp. } K_{1,v}) \text{ if } v \in S \text{ (resp. } v \in S', v \notin S \cup S')\}$$

It is shown in [3, Prop. 4.4] that every maximal arithmetic discrete subgroup of $\mathrm{PGL}_2(k)$ is conjugate to $\Gamma_{S,S'}$ for some S and S'. Not all of the $\Gamma_{S,S'}$ need be maximal (cf. [3, §4.4]). By [3, Prop. 4.10, Thm. 4.6], the groups $\Gamma_{S,S'}$ for a fixed S lie in finitely many conjugacy classes inside $\mathrm{PGL}_2(k)$, while as S varies these groups lie in infinitely many distinct conjugacy classes.

3. Cusps.

Suppose Γ is any discrete arithmetic subgroup of $\mathrm{PGL}_2(k)$ having finite covolume. An element $\sigma \in \Gamma$ is parabolic if it fixes a unique point of $\mathrm{P}^1_{\mathbf{C}}$, and such a fixed point is called a cusp of Γ (compare [6, p. 7-8]). The cusps of the orbifold $\mathbf{H}^3/\Gamma$ are the Γ-equivalence classes of cusps of Γ.

Lemma 3.1. *The cusps of* Γ *are the points in* $P^1_k = k \cup \{\infty\}$*, so that the cusps of* $\mathbf{H}^3/\Gamma$ *are the orbits of* Γ *acting on* P^1_k*.*

Proof: We first show that Γ has the same cusps as any group Γ' commensurable to Γ. For this, it will suffice to consider the case in which Γ' has finite index in Γ. Clearly the cusps of Γ' are cusps for Γ. Conversely, suppose z is a cusp of Γ, so z is the only point of $\mathrm{P}^1_{\mathbf{C}}$ fixed by a parabolic element $\sigma \in \Gamma$. Then σ^n is a parabolic element of Γ' fixing z when $n = [\Gamma : \Gamma']$, so z is also a cusp of Γ'. We can thus reduce to the case in which $\Gamma = \Gamma_{S,S'}$ for some S and S'.

Suppose z is a cusp of $\Gamma_{S,S'} \subset \mathrm{PGL}_2(k)$. Since z is the only fixed point of some $M \in GL_2(k)$ acting on $\mathrm{P}^1_{\mathbf{C}}$, the quadratic formula implies that z must lie in P^1_k. Thus we now must show each $z \in \mathrm{P}^1_k$ is a cusp.

If b is a sufficiently divisible non-zero element of O, the matrix

$$M = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \tag{3.1}$$

defines a parabolic element of $\Gamma_{S,S'}$ which fixes ∞, so ∞ is a cusp of $\Gamma_{S,S'}$. Suppose now that $z \in k \subset \mathrm{P}^1_k$. There is then a matrix T in $\mathrm{GL}_2(k)$ such that $T \cdot \infty = z$. This implies z is a cusp of the discrete group $T\Gamma_{S,S'}T^{-1}$, since TMT^{-1} defines a parabolic element of this group fixing z. However, $T\Gamma_{S,S'}T^{-1}$ and $\Gamma_{S,S'}$ are commensurable, so they have the same cusps, which proves the Lemma.

In the following sections we analyze equivalence classes of cusps under the action of various subgroups Γ of $\Gamma_{S,S'}$.

4. The principal congruence subgroup of $\Gamma_{S,S'}$.

We consider in this section the following subgroup of $\Gamma_{S,S'}$.

Definition 4.1. Let I be the two-by-two identity matrix. Define $\Gamma(S, S')$ to be the subgroup of elements of $\Gamma_{S,S'} \subset \mathrm{PGL}_2(k)$ which are the images of matrices $M \in \mathrm{GL}_2(k)$ such that $M - I \in \pi_v \mathrm{Mat}_2(O_v)$ for $v \in S$, $M \in \mathcal{D}'^{*}_v$ for $v \in S'$ and $M \in \mathrm{GL}_2(O_v)$ for $v \notin S \cup S'$.

We will first describe the $\Gamma(S, S')$-equivalent cusps of $\Gamma(S, S')$. By Lemma 3.1, this is the same as describing the cusps of $\mathbf{H}^3/\Gamma(S, S')$, and the orbits of $\Gamma(S, S')$ acting on P^1_k.

Define $\mathcal{I}(k)$ to be the multiplicative group of fractional ideals of k. For v a finite place of k, let $\mathcal{P}(v)$ be the prime ideal of O determined by v. If T is a finite set of finite places of k, define $\mathcal{P}(T) = \prod_{v \in T} \mathcal{P}(v)$. Define $L'(S)$ to be the set of triples (J, α_0, α_1) in which $J \in \mathcal{I}(k)$ and α_0 and α_1 are generators of $J/(\mathcal{P}(S) \cdot J)$

as a finite O-module. An element $\lambda \in k^*$ acts on $L'(S)$ by sending (J, α_0, α_1) to $(\lambda \cdot J, \lambda \cdot \alpha_0, \lambda \cdot \alpha_1)$. Define $L(S) = L'(S)/k^*$ to be the set of orbits in $L'(S)$ under this action of k^*.

Definition 4.2. Define a map $\Psi : P^1_k \to L(S)$ in the following way. Fix an element $t(S, S') \in \mathcal{P}(S')$ such that the ideal $t(S, S')O$ equals $\mathcal{P}(S') \cdot \mathcal{A}$ for some ideal $\mathcal{A}$ prime to $\mathcal{P}(S \cup S')$. Suppose $(x_0 : x_1)$ are homogeneous coordinates for a point of P^1_k. Define J to be the fractional O-ideal $O \cdot x_0 + \mathcal{P}(S') \cdot x_1$ of k. Let $\beta_0 = x_0$ and $\beta_1 = t(S, S')x_1$, so that β_0 and β_1 are elements of J. Define α_i to be the image of β_i in $J/(\mathcal{P}(S) \cdot J)$ for $i = 0, 1$. Define

$$\Psi((x_0 : x_1)) = [(J, \alpha_0, \alpha_1)] \tag{4.1}$$

to be the class of (J, α_0, α_1) in $L(S)$. The other homogeneous coordinates for $(x_0 : x_1)$ have the form $(\lambda \cdot x_0 : \lambda \cdot x_1)$ for some $\lambda \in k^*$, so Ψ is well-defined.

Proposition 4.3. *The map Ψ is surjective, and its fibers are exactly the $\Gamma(S, S')$-equivalent cusps of $\Gamma(S, S')$.*

Proof: Let us first check surjectivity. Suppose $(J, \alpha_0, \alpha_1) \in L'(S)$. We first claim that there is an $x_1 \in k^*$ such that $\mathcal{P}(S') \cdot x_1 \subset J$ and $t(S, S')x_1 \in J$ has class α_1 in $J/(\mathcal{P}(S) \cdot J)$. Such an x_1 exists because we can find an $x_1 \in \mathcal{P}(S')^{-1}J$ satisfying the appropriate congruence conditions at the places in S because S and S' are disjoint. Choose $x_0 \in J$ to have class α_0 in $J/(\mathcal{P}(S) \cdot J)$, and so that $O_v \cdot x_0 = O_v \cdot J$ for the finitely many finite places v of k which are not in S where $O_v \cdot \mathcal{P}(S')x_1$ is not equal to $O_v \cdot J$. We can find such an x_0 since these conditions amount to congruence conditions at a finite set of finite places of k. We show $\Psi((x_0 : x_1))$ is the class of (J, α_0, α_1) in $L(S)$. By construction, x_0 has class α_0 in $J/\mathcal{P}(S)J$, while $t(S, S')x_1$ has class α_1 in $J/(\mathcal{P}(S) \cdot J)$. Hence we only have to check that $J' = O \cdot x_0 + \mathcal{P}(S')x_1$ is equal to J. Clearly $J' \subset J$. Since $\alpha_0 \equiv x_0$ and $\alpha_1 \equiv t(S, S')x_1$ together generate $J/(\mathcal{P}(S) \cdot J)$ as an O-module, we have $O_v \cdot J' = O_v \cdot J$ if $v \in S$. However, for $v \notin S$, we chose x_0 so that $O_v \cdot x_0 = O_v \cdot J$ if $O_v \cdot \mathcal{P}(S')x_1$ is not equal to $O_v \cdot J$. Thus $O_v \cdot J' = O_v \cdot J$ for all such v, and we conclude $J' = J$.

We now consider the fibers of Ψ. Suppose $(x_0 : x_1)$ and $(x'_0 : x'_1)$ are two points having the same image under Ψ. After multiplying x'_0 and x'_1 by a suitable $\lambda \in k^*$, we can assume the following is true:

$$J = Ox_0 + \mathcal{P}(S')x_1 = Ox'_0 + \mathcal{P}(S')x'_1 \tag{4.2}$$

$$x_0 \equiv x'_0 \equiv \alpha_0 \bmod \mathcal{P}(S)J \tag{4.3}$$

and

$$t(S, S')x_1 \equiv t(S, S')x'_1 \equiv \alpha_1 \bmod \mathcal{P}(S)J. \tag{4.4}$$

We wish to show that there is a matrix $M \in \mathrm{GL}_2(k)$ such that

$$M \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} x'_0 \\ x'_1 \end{pmatrix} \tag{4.5}$$

and

$$M - I \in \pi_v \mathrm{Mat}_2(O_v) \quad \text{for} \quad v \in S, \tag{4.6}$$

$$M \in \mathcal{D}'^{*}_v \quad \text{for} \quad v \in S', \tag{4.7}$$

$$M \in \mathrm{GL}_2(O_v) \quad \text{for} \quad v \notin S \cup S' \tag{4.8}$$

We adapt an argument of Swan in [10, Prop. 3.10] to construct M. There are two exact sequences of O-modules

$$0 \longrightarrow \mathcal{B} \longrightarrow O \oplus \mathcal{P}(S') \xrightarrow{l'} J \to 0 \tag{4.9}$$

$$0 \longrightarrow \mathcal{C} \longrightarrow O \oplus \mathcal{P}(S') \xrightarrow{l} J \to 0 \tag{4.10}$$

in which l and l' are defined for $(a,b) \in O \oplus \mathcal{P}(S')$ by

$$l(a,b) = ax_0 + bx_1 \quad \text{and} \quad l'(a,b) = ax'_0 + bx'_1. \tag{4.11}$$

Since J is a projective O-module, these sequences split, giving isomorphisms

$$O \oplus \mathcal{P}(S') = J \oplus \mathcal{B} \quad \text{and} \quad O \oplus \mathcal{P}(S') = J \oplus \mathcal{C}. \tag{4.12}$$

Again using the fact that O is a Dedekind ring, these isomorphisms imply that there is an isomorphism $\phi : \mathcal{B} \to \mathcal{C}$ of projective rank one O-modules.

Let s be a unit of O, and suppose $W \in \mathrm{Hom}_O(J, \mathcal{C})$. We define an O-linear map

$$\theta_{s,W} : O \oplus \mathcal{P}(S') = J \oplus \mathcal{B} \to J \oplus \mathcal{C} = O \oplus \mathcal{P}(S') \tag{4.13}$$

by

$$\theta_{s,W}(j \oplus a) = j \oplus (s\phi(a) + W(j)) \tag{4.14}$$

for $j \in J$ and $a \in \mathcal{B}$. Then $\theta_{s,W}$ fits into a commutative diagram

$$\begin{array}{ccccccccc} 0 \longrightarrow & \mathcal{B} & \longrightarrow & O \oplus \mathcal{P}(S') & \xrightarrow{l'} & J & \longrightarrow 0 \\ & {\scriptstyle s\phi}\downarrow & & \downarrow{\scriptstyle \theta_{s,W}} & & \downarrow{\scriptstyle 1} & \\ 0 \longrightarrow & \mathcal{C} & \longrightarrow & O \oplus \mathcal{P}(S') & \xrightarrow{l} & J & \longrightarrow 0 \end{array} \tag{4.15}$$

Since $s\phi$ is an isomorphism, and $1 : J \to J$ is the identity map, we conclude that $\theta_{s,W}$ in an automorphism. Furthermore, $\det_O(\theta_{s,W}) = s \cdot \det_O(\theta_{1,W}) = s \cdot \det_O(\theta_{1,0})$ is independent of the choice of W, so we can choose s (depending on ϕ) so that $\det(\theta_{s,W}) = 1$ for all W.

Define

$$M_{s,W} = \begin{pmatrix} \alpha\,\beta \\ \gamma\,\delta \end{pmatrix} \tag{4.16}$$

to be the matrix of $\theta_{s,W}$ when we view elements of $O \oplus \mathcal{P}(S') \subset k \oplus k$ as column vectors. Here

$$\begin{aligned} \alpha &\in \mathrm{Hom}_O(O, O) = O, \\ \beta &\in \mathrm{Hom}_O(\mathcal{P}(S'), O) = \mathcal{P}(S')^{-1}, \\ \gamma &\in \mathrm{Hom}_O(O, \mathcal{P}(S')) = \mathcal{P}(S') \\ \delta &\in \mathrm{Hom}_O(\mathcal{P}(S'), \mathcal{P}(S')) = O. \end{aligned} \tag{4.17}$$

Thus the transpose $M^{tr}_{s,W}$ of $M_{s,W}$ is an element of $\mathrm{SL}_2(k)$ satisfying conditions (4.7) and (4.8), while $M^{tr}_{s,W} \in \mathrm{SL}_2(O_v)$ for $v \in S$. The commutativity of (4.15) shows

$$x_0' = l' \begin{pmatrix} 1 \\ 0 \end{pmatrix} = l\left(M_{s,W} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = l\begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \alpha x_0 + \gamma x_1 \tag{4.18}$$

and

(4.19)

$$t(S,S')x_1' = l\left(M_{s,W} \cdot \begin{pmatrix} 0 \\ t(S,S') \end{pmatrix}\right) = l\begin{pmatrix} \beta \cdot t(S,S') \\ \delta \cdot t(S,S') \end{pmatrix} = \beta{\cdot}t(S,S'){\cdot}x_0 + \delta{\cdot}t(S,S'){\cdot}x_1$$

This gives the matrix equation

$$M^{tr}_{s,W} \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} \alpha\,\gamma \\ \beta\,\delta \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_0' \\ x_1' \end{pmatrix} \tag{4.20}$$

We now show that we can choose $W \in Hom_O(J, \mathcal{C})$ so that $M^{tr}_{s,W} = M$ will satisfy (4.6), i.e. so that $M - I \in \pi_v \mathrm{Mat}_2(O_v)$ for $v \in S$. This will complete the proof that cusps having the same image under Ψ are $\Gamma(S,S')$-equivalent.

For $v \in S$, let $k(v) = O/\mathcal{P}(v)$ and let J_v be the localization of J at v, Since $t(S,S') \in O_v^*$ and $t(S,S')x_1 \in J$, we have $x_1 \in J_v$ for $v \in S$. Define $\beta_{i,v}$ be the image of x_i in the one-dimensional $k(v)$-vector space $J(v) = J_v/\mathcal{P}(v)J_v$. From (4.20), (4.3) and (4.4) we know that for $v \in S$, $M^{tr}_{s,W} \in \mathrm{SL}_2(O_v)$ fixes the vector $\beta(v) = (\beta_{0,v}, \beta_{1,v})$ in $J(v) \oplus J(v)$. This $\beta(v)$ is not the zero vector, since α_0 and α_1 together generate $J/\mathcal{P}(S)J$ and $\alpha_0 = x_0 \bmod \mathcal{P}(S)J$ and $\alpha_1 = t(S,S')x_1 \bmod \mathcal{P}(S)J$. Thus the image $M^{tr}_{s,W,v}$ of $M^{tr}_{s,W}$ in $\mathrm{SL}_2(k(v))$ lies in the stabilizer of $\beta(v)$, and this stabilizer has order $\#k(v)$ since $\beta(v)$ is non-zero. Letting v range over S, we see that the image of $M^{tr}_{s,W}$ in $T = \prod_{v \in S} \mathrm{SL}_2(k(v))$ lies in a subgroup of matrices which has order $N = \prod_{v \in S} \#k(v)$. However, as W ranges over $\mathrm{Hom}(J, \mathcal{C})$, the image of $M^{tr}_{s,W}$ in T also ranges over a set of N matrices, since each of J and $\mathcal{C}$ are rank one projective O-modules. It follows that we can choose W so that $M^{tr}_{s,W}$ has image the identity element of T, as required.

The last statement we have to prove is that $\Gamma(S,S')$-equivalent cusps have the same image under Ψ. Suppose $M = M^{tr}_{s,W}$ satisfies (4.20) and has the properties described in Definition (4.1). It will suffice to show (4.2), (4.3) and (4.4) hold. For (4.2), observe that the containments in (4.17) show

$$(4.21)\quad Ox'_0+\mathcal{P}(S')x'_1 = O(\alpha\cdot x_0+\gamma\cdot x_1)+\mathcal{P}(S')(\beta\cdot x_0+\delta\cdot x_1) \subset Ox_0+\mathcal{P}(S')x_1$$

Since M^{-1} also satisfies the conditions in (4.1) and takes the cusp $(x'_0 : x'_1)$ back to $(x_0 : x_1)$, we can interchange $(x'_0 : x'_1)$ and $(x_0 : x_1)$ to conclude that (4.2) holds. The proof of (4.3) and (4.4) is similar using the properties of M in Definition (4.1).

5. The Borel congruence subgroup of $\Gamma_{S,S'}$.

We consider in this section the following subgroup of $\Gamma_{S,S'}$.

Definition 5.1. For v a finite place of k, let $B_v \subset \mathrm{GL}_2(O_v)$ be the subgroup of invertible matrices of the form

$$(5.1)\qquad \begin{pmatrix} a & \pi_v b \\ c & d \end{pmatrix}$$

in which $a,b,c,d \in O_v$. Define $\Gamma_0(S,S')$ to be the subgroup of elements of $\Gamma_{S,S'} \subset \mathrm{PGL}_2(k)$ which are the images of matrices $M \in \mathrm{GL}_2(k)$ such that that $M \in B_v$ for $v \in S$, $M \in \mathcal{D}'^{\,*}_v$ for $v \in S'$ and $M \in \mathrm{GL}_2(O_v)$ for $v \notin S \cup S'$.

Note that the image of B_v in $\mathrm{PGL}_2(k_v)$ is the group $K_{1,v} \cap K'_{1,v}$ defined in §2. Thus $\Gamma_0(S,S') \subset \Gamma_{S,S'}$, while $\Gamma(S,S') \subset \Gamma_0(S,S')$.

Definition 5.2. Define $L_0(S)$ to be the set of pairs $([J],\{\beta_v\}_{v\in S})$ in which $[J]$ is an element of the ideal class group of k, and for each $v \in S$, β_v is either 0 or 1. Define $r : L(S) \to L_0(S)$ to be the map which sends a triple $(J,\alpha_0,\alpha_1) \in L'(S)$ representing an element of $L(S)$ to $([J],\{\beta_v\}_{v\in S})$, where $[J]$ is the ideal class of $J \in I(k)$, and $\beta_v = 0$ (resp. 1) if $\alpha_0 \equiv 0 \bmod \pi_v J$ (resp. if $\alpha_0 \not\equiv 0 \bmod \pi_v J$).

Proposition 5.3. *Let $\Psi : \mathrm{P}^1_k \to L(S)$ be the map of Proposition 4.3. The composition $r\circ\Psi : \mathrm{P}^1_k \to L_0(S)$ is surjective, and the fibers of this map are the $\Gamma_0(S,S')$-equivalent cusps of $\Gamma_0(S,S')$.*

Proof: Recall that $L'(S)$ consists of the triples (J,α_0,α_1) in which $J \in I(k)$ and α_0 and α_1 are generators of $J/\mathcal{P}(S)J$. Since $\mathcal{P}(S) = \prod_{v\in S}\mathcal{P}(v)$, we see that we can choose α_0 and α_1 to have prescribed classes $\alpha_0(v), \alpha_1(v) \in J/\mathcal{P}(v)$ as v

ranges over S provided that for no such v are both $\alpha_0(v)$ and $\alpha_1(v)$ trivial. This implies r is surjective, so $r \circ \Psi$ is surjective by Proposition 4.3.

Consider now the action of a matrix $M \in \mathrm{GL}_2(k)$ satisfying the hypotheses of Definition 5.1 on $\Psi(x_0 : x_1) = [(J, \alpha_0, \alpha_1)] \in L(S)$, where $(J, \alpha_0, \alpha_1) \in L'(S)$ is as in Definition 4.2 and $[(J, \alpha_0, \alpha_1)]$ is the class of (J, α_0, α_1) in $L(S)$. From $J = O \cdot x_0 + \mathcal{P}(S') \cdot x_1$ and the hypotheses on M we see that $J = O \cdot x_0' + \mathcal{P}(S') \cdot x_1'$ when

$$\begin{pmatrix} x_0' \\ x_1' \end{pmatrix} = M \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \tag{5.2}$$

Recall that α_0 (resp. α_1) is the image in $J/\mathcal{P}(S)$ of x_0 (resp. $t(S, S')x_1$). Suppose

$$M = \begin{pmatrix} a\, b \\ c\, d \end{pmatrix} \tag{5.3}$$

Define

$$M' = \begin{pmatrix} a & b \cdot t(S, S')^{-1} \\ t(S, S')c & d \end{pmatrix} \tag{5.4}$$

We find from (5.2) that $\Psi(x_0' : x_1') = (J, \alpha_0', \alpha_1')$, where α_0' and α_1' are elements of $J/\mathcal{P}(S)$ given by the following residue classes $\alpha_0'(v), \alpha_1'(v) \in J_v/\mathcal{P}(v)J_v = J/\mathcal{P}(v)J$ for $v \in S$:

$$\begin{pmatrix} \alpha_0'(v) \\ \alpha_1'(v) \end{pmatrix} = M' \cdot \begin{pmatrix} \alpha_0(v) \\ \alpha_1(v) \end{pmatrix}. \tag{5.5}$$

The number $t(S, S') \in k$ is a unit at each $v \in S$, so $M' \in B_v$ for such v because $M \in B_v$. Thus

$$a, d \in O_v^*, \quad bt(S, S')^{-1} \in \pi_v O_v \quad \text{and} \quad t(S, S')c \in O_v \tag{5.6}$$

This implies $\alpha_0'(v) = 0$ if and only if $\alpha_0(v) = 0$. It follows that $r \circ \Psi(x_0 : x_1) = r \circ \Psi(x_0' : x_1')$, so $\Gamma_0(S, S')$-equivalent cusps have the same image under $r \circ \Psi$.

To complete the proof of Proposition 5.3, we have to show that two points $(x_0 : x_1)$ and $(x_0' : x_1')$ with the same image under $r \circ \Psi$ are $\Gamma_0(S, S')$-equivalent. After multiplying x_0' and x_1' by a suitable scalar, we can assume

$$J = O \cdot x_0 + \mathcal{P}(S') \cdot x_1 = O \cdot x_0' + \mathcal{P}(S') \cdot x_1' \tag{5.7}$$

Furthermore, on defining $\alpha_0(v)$, $\alpha_1(v)$, $\alpha_0'(v)$ and $\alpha_1'(v)$ to be the images of x_0, $t(S, S')x_1$, x_0' and $t(S, S')x_1'$ in $J/\mathcal{P}(v)J$, we see that $\alpha_0(v) = 0$ if and only if $\alpha_0'(v) = 0$ for $v \in S$, since $r \circ \Psi(x_0 : x_1) = r \circ \Psi(x_0' : x_1')$. Furthermore, $\alpha_1(v) \neq 0$ if $\alpha_0(v) = 0$, and similarly $\alpha_1'(v) \neq 0$ if $\alpha_0'(v) = 0$. This implies there is a lower triangular matrix $m_v \in \mathrm{SL}_2(O_v/\pi_v O_v)$ such that

$$\begin{pmatrix} \alpha_0'(v) \\ \alpha_1'(v) \end{pmatrix} = m_v \cdot \begin{pmatrix} \alpha_0(v) \\ \alpha_1(v) \end{pmatrix} \tag{5.8}$$

We now use the Strong Approximation Theorem for SL_2 to conclude that there is $M \in \mathrm{SL}_2(k)$ which satisfies the hypotheses of Definition 5.1 such that when we write M in the form (5.3) and let M' be as in (5.4), then $M' \in \mathrm{SL}_2(O_v)$ for $v \in S$ satisfies the congruence $M' \equiv m_v \bmod \pi_v \mathrm{Mat}_2(O_v)$. We conclude from this that

$$\Psi(M \cdot (x_0 : x_1)) = \Psi(x_0' : x_1')$$

so that $M \cdot (x_0 : x_1)$ and $(x_0' : x_1')$ are $\Gamma(S, S')$-equivalent cusps by Proposition 4.3. Since $\Gamma(S, S') \subset \Gamma_0(S, S')$ and $M \cdot (x_0 : x_1)$ is $\Gamma_0(S, S')$ equivalent to $(x_0 : x_1)$ by our construction of M, this proves $(x_0 : x_1)$ and $(x_0' : x_1')$ are $\Gamma_0(S, S')$-equivalent cusps.

Corollary 5.4. *The number of* $\Gamma_0(S, S')$*-equivalence classes of cusps of* $\Gamma_0(S, S')$ *is* $2^{\#S} h_k$*, where* h_k *is the class number of* k*.*

6. $\Gamma_{S,S'}$-inequivalent cusps.

In this section we will prove Theorem 1.1. The proof is based on the following two results, which will be proved in §7 and §8, respectively.

Proposition 6.1. *Let* $C_0(S, S')$ *be the set of* $\Gamma_0(S, S')$*-equivalence classes of points of* P^1_k*. Since* $\Gamma_0(S, S') \subset \Gamma_{S,S'}$*, the group* $\Gamma_{S,S'}$ *acts on* $C_0(S, S')$*. Each* $\Gamma_{S,S'}$*-orbit in* $C_0(S, S')$ *has* $[\Gamma_{S,S'} : \Gamma_0(S, S')]$ *elements.*

Proposition 6.2. *Define* $h_{k,2}$ *to be the order of* $Cl(k)/(2Cl(k))$ *where* $Cl(k)$ *is the class group of* k*. Define* 2^n *to be the order of the subgroup of* $Cl(k)/(2 \cdot Cl(k))$ *generated by the classes of primes ideals determined by the places in* S*. Then* $0 \le n \le \#S$ *and*

$$[\Gamma_{S,S'} : \Gamma_0(S, S')] = 2^{\#S-n} h_{k,2}. \tag{6.1}$$

Theorem 1.1 is a consequence of these results in the following way. By Lemma 3.1 the set of $\Gamma_{S,S'}$-orbits in $C_0(S, S')$ is the set of $\Gamma_{S,S'}$-equivalence classes of cusps of $\Gamma_{S,S'}$. Corollary 5.4 together with Propostions 6.1 and 6.2 show this number is

$$\frac{2^{\#S} h_k}{2^{\#S-n} h_{k,2}} = 2^n \frac{h_k}{h_{k,2}} \tag{6.2}$$

as stated in Theorem 1.1.

7. Proof of Proposition 6.1.

We will need several Lemmas.

Lemma 7.1. *To prove Proposition 6.1, it will suffice to show the following. Suppose*

(7.1)

$$\sigma \in \Gamma_{S,S'}, \quad (x_0 : x_1) \in \mathrm{P}^1_k, \quad (x_0' : x_1') = \sigma\cdot(x_0 : x_1) \quad \text{and} \quad r\circ\Psi(x_0 : x_1) = r\circ\Psi(x_0' : x_1').$$

Then σ *lies in* $\Gamma_0(S, S')$.

Proof: This is clear from Proposition 5.3, which showed that the map $r \circ \Psi : \mathrm{P}^1_k \to L_0(S)$ has fibers equal to the elements of $C_0(S, S')$.

We will assume from now on that hypothesis (7.1) holds.

Definition 7.2. Let (J, α_0, α_1) be the triple associated in Definition 4.2 to the ordered pair (x_0, x_1) of elements of k which are not both 0. Thus $J = Ox_0 + \mathcal{P}(S')x_1$, and α_0 and α_1 are the classes of x_0 and $t(S, S')x_1$ in $J/\mathcal{P}(S)J$. The class $[(J, \alpha_0, \alpha_1)]$ of (J, α_0, α_1) in $L(S)$ is equal to $\Psi(x_0 : x_1)$. Write

$$\begin{pmatrix} x_0' \\ x_1' \end{pmatrix} = M \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

for some matrix $M \in \mathrm{GL}_2(k)$ with image $\sigma \in \Gamma_{S,S'}$ in $\mathrm{PGL}_2(k)$. Let $(J', \alpha_0', \alpha_1')$ be the triple associated to (x_0', x_1').

Lemma 7.3. *The element* σ *must be even at each* $v \in S$*, in the sense that* $\det(M)$ *has even valuation at each* $v \in S$.

Proof: Suppose to the contrary that σ is odd at some place $v \in S$. From the definition of $\Gamma_{S,S'}$ in §2, this implies that

(7.2)
$$M = \lambda_v \cdot w_v \cdot M_v$$

where $\lambda_v \in k_v^*$, w_v is the matrix

(7.3)
$$w_v = \begin{pmatrix} 0 & \pi_v \\ 1 & 0 \end{pmatrix}$$

and

(7.4)
$$M_v = \begin{pmatrix} a & \pi_v b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(O_v)$$

for some $a, b, c, d \in O_v$. Consider the localization J_v of J at v. Since $\mathcal{P}(S')$ is prime to $\mathcal{P}(v)$, we have

(7.5)
$$J_v = O_v x_0 + O_v x_1 \subset k_v \quad \text{and} \quad J_v' = O_v x_0' + O_v x_1'.$$

Since

(7.6)
$$\begin{pmatrix} x_0' \\ x_1' \end{pmatrix} = M \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \lambda_v \cdot w_v \cdot M_v \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

we see from (7.3) and (7.4) that

$$x_0' = \lambda_v \cdot \pi_v \cdot (cx_0 + dx_1) \quad \text{and} \quad x_1' = \lambda_v \cdot (ax_0 + \pi_v b x_1). \tag{7.7}$$

Here $a, d \in O_v^*$, since M_v in (7.4) is in $\mathrm{GL}_2(O_v)$. We claim

$$J_v' = \lambda_v \cdot (\pi_v O_v x_1 + O_v x_0). \tag{7.8}$$

To show this, let $\mathrm{ord}_v : k_v \to \mathbf{Z} \cup \{\infty\}$ be the discrete valuation at v, normalized so that $\mathrm{ord}_v(\pi_v) = 1$. From (7.7) and (7.5) we have

$$J_v' = O_v x_0' + O_v x_1' \subset \lambda_v \cdot (\pi_v O_v x_1 + O_v x_0)$$

since $a, b, c, d \in O_v$. This containment must be an equality since (7.2) shows $\mathrm{ord}_v(\det(M)) = \mathrm{ord}_v(\lambda_v^2) + 1$, and this integer is the power of $\#O_v/\pi_v O_v$ appearing in the generalized index

$$[O_v x_0 + O_v x_1 : \lambda_v \cdot (\pi_v O_v x_1 + O_v x_0)].$$

The first case we now must consider is when $\mathrm{ord}_v(x_0) \le \mathrm{ord}_v(x_1)$. In this case, (7.5) and (7.8) show

$$J_v = O_v x_0 \quad \text{and} \quad J_v' = \lambda_v \cdot O_v x_0 \tag{7.9}$$

Thus $x_0 \not\equiv 0 \bmod \pi_v J_v$, while (7.7) shows $x_0' \equiv 0$ in $J_v'/\pi_v J_v'$. This proves $\alpha_0(v) \neq 0$ but $\alpha_0'(v) = 0$. In view of the description of the map $r : L(S) \to L_0(S)$ in Definition 5.2, this forces $r([(J, \alpha_0, \alpha_1)]) = r \circ \Psi(x_0 : x_1)$ to be different from $r[(J', \alpha_0', \alpha_1')] = r \circ \Psi(x_0' : x_1')$. This contradicts hypothesis (7.1), so we conclude that this hypothesis forces $\mathrm{ord}_v(x_0) > \mathrm{ord}_v(x_1)$. In this case (7.5) and (7.8) imply

$$J_v = O_v x_1 \quad \text{and} \quad J_v' = \lambda_v \cdot \pi_v \cdot O_v x_1. \tag{7.10}$$

Since $\mathrm{ord}_v(x_0) > \mathrm{ord}_v(x_1)$, we find that $x_0 \equiv 0 \bmod \pi_v J_v$, while (7.7) implies $x_0' \not\equiv 0 \bmod \pi_v J_v'$. Thus we get $\alpha_0(v) = 0$ but $\alpha_0'(v) \neq 0$, again contradicting hypothesis (7.1). This contradiction proves Lemma 7.3.

Corollary 7.4. *The element $\sigma \in \Gamma_{S,S'}$ is represented by a matrix $M \in \mathrm{GL}_2(k)$ having the following properties. For each finite place v of k, there is an element $x_v \in k_v^*$ together with elements $a = a_v$, $b = b_v$, $c = c_v$ and $d = d_v$ of O_v such that*

$$M = x_v \cdot M_v \quad \text{and} \quad \det(M_v) \in O_v^*, \tag{7.11}$$

$$x_v \in O_v^* \quad \text{for all but finitely many places} \quad v \tag{7.12}$$

$$M_v = \begin{pmatrix} a & \pi_v b \\ c & d \end{pmatrix} \quad \text{if} \quad v \in S \tag{7.13}$$

$$M_v = \begin{pmatrix} a & \pi_v b \\ \pi_v^{-1} c & d \end{pmatrix} \quad \text{if} \quad v \in S' \tag{7.14}$$

(7.15) $$M_v = \begin{pmatrix} a\,b \\ c\,d \end{pmatrix} \quad \text{if} \quad v \notin S \cup S'$$

Proof: By [3, Prop. 4.4(iii)], if v is a finite place of k such that $\Gamma_{S,S'}$ contains an element which is odd at v, then $v \in S$. We proved in Lemma 7.3 that σ must be even at each $v \in S$. Hence for each finite place v, there is an element $x_v \in k_v^*$ such that $2 \cdot \text{ord}_v(x_v) = \text{ord}_v(\det(M))$. On defining $M_v = x_v^{-1} \cdot M$, it now follows from the definition of $\Gamma_{S,S'}$ in (2.3) that M_v has properties (7.11) - (7.15).

Corollary 7.5. *With the notation of Corollary 7.4, let* $\mathcal{B} = \prod_v \mathcal{P}(v)^{\text{ord}_v(x_v)}$. *Then with the notation of (7.1), we have*

(7.16) $$J' = Ox_0' + \mathcal{P}(S')x_1' = \mathcal{B} \cdot J = \mathcal{B} \cdot (Ox_0 + \mathcal{P}(S')x_1)$$

as fractional k-ideals.

Proof: Define

(7.17) $$\begin{pmatrix} x_{v,0} \\ x_{v,1} \end{pmatrix} = M_v \cdot \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

for all v. Since $M = x_v \cdot M_v$, the localization J_v' at v satisfies

(7.18) $$J_v' = (O_v x_0' + \mathcal{P}(S')_v x_1') = x_v \cdot (O_v x_{v,0} + O_v \mathcal{P}(S')_v x_{v,1})$$

However, the fact that $\det(M_v) \in O_v^*$ together with the form of M_v in (7.13) - (7.13) ensures that

(7.19) $$O_v x_{v,0} + O_v \mathcal{P}(S')_v x_{v,1} = O_v x_0' + \mathcal{P}(S')_v x_1' = J_v$$

Combining (7.18) and (7.19) shows (7.16).

Completion of the proof of Proposition 6.1.

In hypothesis (7.1) we supposed $r \circ \Psi(x_0 : x_1) = r \circ \Psi(x_0' : x_1')$. This forces J and $J' = \mathcal{B} \cdot J$ to have the same ideal class as fractional k-ideals. Hence $\mathcal{B} = O \cdot \lambda$ is a principal ideal for some $\lambda \in k^*$. With the notation of Corollaries 7.4 and 7.5, we now see that if we choose $x_v = \lambda$ for all places v, then the matrix $M' = \lambda^{-1} \cdot M \in \text{GL}_2(k)$ has image M_v in $\text{GL}_2(k_v)$ for all v. This implies $M' \in \Gamma_0(S, S')$. Since M and M' have the same image σ in $\text{PGL}_2(k)$, we have $\sigma \in \Gamma_0(S, S')$, which completes the proof of Proposition 6.1 by Lemma 7.1.

8. Proof of Proposition 6.2.

Let $\mathcal{D}'$ be the maximal O-order $\cap_{v \notin S'} \mathcal{D}_v \cap_{v \in S'} \mathcal{D}_v'$ in $\text{Mat}_2(k)$, where $\mathcal{D}_v$ and ${\mathcal{D}'}_v$ are defined in §2. The set R_f of finite places of k which ramify in $\text{Mat}_2(k)$ is empty. Therefore the group Γ_{R_f} which Borel defines in [3, §8.4] is the image in $\mathrm{PGL}_2(k)$ of the group $B^*_{R_f}$ of elements $\tau \in \mathrm{GL}_2(k)$ such that $\det(\tau) \in O^*$. Define $\Gamma_{\mathcal{D}'^*}$ (resp. to $\Gamma_{\mathcal{D}'^1}$) to be the image in $\mathrm{PGL}_2(k)$ of $\mathcal{D}'^*$ (resp. the image of the group of $\tau \in \mathcal{D}'^*$ such that $\det(\tau) = 1$.) Borel shows in [3, Lemma 8.5] that $[\Gamma_{R_f} : \Gamma_{\mathcal{D}'^1}] = 2$, since in our case the unit group O^* is finite, cyclic and of even order and k has no real places. However, we also have $[\Gamma_{\mathcal{D}'^*} : \Gamma_{\mathcal{D}'^1}] = 2$, since $\mathcal{D}'^*$ contains a diagonal matrix whose diagonal entries are 1 and a generator of O^*. Since

$$\Gamma_{\mathcal{D}'^1} \subset \Gamma_{\mathcal{D}'^*} \subset \Gamma_{R_f}$$

we conclude that $\Gamma_{\mathcal{D}'^*} = \Gamma_{R_f}$. Hence Borel's result in the Lemma of [3, §8.6] shows

$$[\Gamma_{\mathcal{D}'} : \Gamma_{\mathcal{D}'^*}] = h_{2,k} \tag{8.1}$$

where $\Gamma_{\mathcal{D}'}$ is the image in $\mathrm{PGL}_2(k)$ of the normalizer $\mathrm{Norm}(\mathcal{D}')$ of $\mathcal{D}'$ in $\mathrm{GL}_2(k)$. For $v \in S$, let $k(v) = O_v/\pi_v O_v$, and let $b(v)$ be the subgroup of lower triangular matrices in $\mathrm{GL}_2(k(v))$. Definition 5.1 implies that $\Gamma_0(S, S')$ is the image in $\mathrm{PGL}_2(k)$ of the subgroup $\mathcal{D}'(S)^*$ of elements $M \in \mathcal{D}'^*$ such that the image of M in

$$\mathcal{D}'_v/\pi_v\mathcal{D}'_v = \mathcal{D}_v/\pi_v\mathcal{D}_v = \mathrm{Mat}_2(O_v/\pi_v O_v)$$

lies in $b(v)$ for each $v \in S$. Since each of the $1+\#k(v)$ cosets of $b(v)$ in $\mathrm{GL}_2(k(v))$ is represented by an element of $\mathrm{SL}_2(k(v))$, the Strong Approximation Theorem for SL_2 implies

$$[\mathcal{D}'^* : \mathcal{D}'(S)^*] = \prod_{v \in S}(1 + \#k(v)). \tag{8.2}$$

Clearly $\mathcal{D}'^* \cap k^* = \mathcal{D}'(S)^* \cap k^*$ when we identify these groups with the diagonal matrices inside $\mathcal{D}'^*$ and $\mathcal{D}'(S)^*$. Thus (8.2) gives

$$[\Gamma_{\mathcal{D}'^*} : \Gamma_0(S, S')] = \prod_{v \in S}(1 + \#k(v)). \tag{8.3}$$

The group $\Gamma_{\mathcal{D}'}$ is equal to $\Gamma_{\emptyset,S'}$ by [3, §4.9, eq. (4)]. Hence on letting

$$\Gamma_2 = \Gamma_{\mathcal{D}'} \cap \Gamma_{S,S'} = \Gamma_{\emptyset,S'} \cap \Gamma_{S,S'}$$

we have from [3, §5.3, eq. (7) and (8)] that

$$[\Gamma_{\mathcal{D}'} : \Gamma_2] = \prod_{v \in S}(1 + \#k(v)) \tag{8.4}$$

(Note that there is a misprint in [3, §5.3, eq. (4)], since the product in that equation should be over places in S.) Putting together (8.1), (8.3) and (8.4) gives the generalized index relation

$$[\Gamma_2 : \Gamma_0(S, S')] = [\Gamma_{\mathcal{D}'} : \Gamma_{\mathcal{D}'^*}] \cdot [\Gamma_{\mathcal{D}'^*} : \Gamma_0(S, S')]/[\Gamma_{\mathcal{D}'} : \Gamma_2] = h_{2,k}. \tag{8.5}$$

We now define a homomorphism

$$F : \Gamma_{S,S'} \to \prod_{v \in S} (\mathbf{Z}/2) \tag{8.6}$$

by sending $\sigma \in \Gamma_{S,S'}$ to the vector having component 0 at $v \in S$ if σ is even at v and component 1 if v is odd at v. The kernel of F is

$$\Gamma_2 = \Gamma_{\emptyset,S'} \cap \Gamma_{S,S'}$$

so

$$[\Gamma_{S,S'} : \Gamma_2] = \#\text{Image}(F) \tag{8.7}$$

Consider the homomorphism

$$T : \prod_{v \in S} (\mathbf{Z}/2) \to Cl(k)/(2Cl(k)) \tag{8.8}$$

which sends the vector having component 1 at v and component 0 at the other places in S to the class of the prime ideal $\mathcal{P}(v)$. We will show that

$$\text{Image}(F) = \text{Kernel}(T). \tag{8.9}$$

Before proving (8.9) note that in the statement of Proposition 6.2, Image(T) has order 2^n. Thus (8.7) and (8.9) will show

$$[\Gamma_{S,S'} : \Gamma_2] = \#\text{Image}(F) = \#\text{Kernel}(T) = 2^{\#S}/\#\text{Image}(T) = 2^{\#S-n} \tag{8.10}$$

Hence (8.5) and (8.10) prove (6.1), which will prove Proposition 6.2.

It remains to show (8.9). If $M \in \mathrm{GL}_2(k)$ represents $\sigma \in \Gamma_{S,S'}$, then $\det(M) \in k^*$ is even at all $v \notin S$, and $\mathrm{ord}_v(\det(M))$ is even (resp. odd) exactly if the component of $F(\sigma)$ at v is 0 (resp. 1). Since $\det(M)$ generates a principal ideal, it follows that the composition $T \circ F$ is trivial, so Image(F) $\subset$ Kernel(T).

To show equality in (8.9), it will now suffice to show the following. Suppose $\lambda \in k^*$ has $\mathrm{ord}_v(\lambda) \equiv 0 \mod 2\mathbf{Z}$ for $v \notin S$. Then we need to show there is an element $\sigma \in \Gamma_{S,S'}$ which for $v \in S$ is odd at v if and only if $\mathrm{ord}_v(\lambda)$ is odd. Without loss of generality, we can assume $\lambda \in O$. Fix a uniformizing element $\pi_v \in O_v$ for each place v. We can choose an element $c \in O$ satifying the following finite system of congruences:

$$\text{If} \quad \mathrm{ord}_v(\lambda) = 2a_v + 1 \quad \text{is odd, then} \quad c \equiv 0 \mod \pi_v^{a_v+1} O_v; \tag{8.11}$$

(8.12)

$$\text{If } \mathrm{ord}_v(\lambda) = 2a_v \text{ is even, and } a_v > 0 \text{ or } v \in S \cup S', \text{ then } c \equiv \lambda \cdot \pi_v^{-a_v} - \pi_v^{a_v} \mod \pi_v^{a_v+1} O_v.$$

We let σ' be the matrix

$$\sigma' = \begin{pmatrix} 0 & \lambda \\ 1 & c \end{pmatrix}. \tag{8.13}$$

Clearly $\det(\sigma') = -\lambda$ is odd at exactly the places v of k where $\mathrm{ord}_v(\lambda)$ is odd. We will show below that

$$\text{(8.14)} \qquad \sigma' \quad \text{fixes an edge of} \quad T_v \quad \text{if} \quad v \in S \cup S' \quad \text{or} \quad \mathrm{ord}_v(\lambda) \neq 0.$$

Let us first prove that (8.14) implies equality in (8.9), which we have already proved will complete the proof of Proposition 6.2. If $v \in S$, then (8.14) states that σ' fixes an edge of T_v. If $v \in S'$ or $\mathrm{ord}_v(\lambda) \neq 0$, then σ' must fix an edge of T_v pointwise, since (8.14) says σ' fixes an edge, and σ' is even at v. Finally, if $v \notin S \cup S'$ and $\mathrm{ord}_v(\lambda) \neq 0$, then σ' lies in $\mathrm{GL}_2(O_v)$, so σ' fixes the vertex of T_v that is fixed by every element of $\Gamma_{S,S'}$. The group $\mathrm{SL}_2(k_v)$ acts transitively on the edges of T_v. Hence we can conclude from the Strong Approximation Theorem that a conjugate σ of σ' by an element of $\mathrm{SL}_2(k)$ defines an element of $\Gamma_{S,S'}$. Since $\det(\sigma) = \det(\sigma')$ has odd valuation at exactly those v where $\mathrm{ord}_v(\lambda)$ is odd, this implies equality holds in (8.9).

We now prove (8.14). Suppose first that v is a place for which $\mathrm{ord}_v(\lambda) = 2a_v+1$ is odd, so that v lies in S. Condition (8.11) implies that σ' acts in the following way on the lattices $\pi_v^{a_v} O_v \oplus O_v$ and $\pi_v^{a_v+1} O_v \oplus O_v$ in $k_v \oplus k_v$.

$$\text{(8.15)} \qquad \sigma' \begin{pmatrix} \pi_v^{a_v} O_v \\ O_v \end{pmatrix} = \begin{pmatrix} 0 & \lambda \\ 1 & c \end{pmatrix} \cdot \begin{pmatrix} \pi_v^{a_v} O_v \\ O_v \end{pmatrix} = \begin{pmatrix} \lambda O_v \\ \pi_v^{a_v} O_v \end{pmatrix} = \pi_v^{a_v} \begin{pmatrix} \pi_v^{a_v+1} O_v \\ O_v \end{pmatrix}.$$

(8.16)
$$\sigma' \begin{pmatrix} \pi_v^{a_v+1} O_v \\ O_v \end{pmatrix} = \begin{pmatrix} 0 & \lambda \\ 1 & c \end{pmatrix} \cdot \begin{pmatrix} \pi_v^{a_v+1} O_v \\ O_v \end{pmatrix} = \begin{pmatrix} \lambda O_v \\ \pi_v^{a_v+1} O_v \end{pmatrix} = \pi_v^{a_v+1} \begin{pmatrix} \pi_v^{a_v} O_v \\ O_v \end{pmatrix}.$$

These equalities show that σ' interchanges the homothety classes of $\pi_v^{a_v} O_v \oplus O_v$ and $\pi_v^{a_v+1} O_v \oplus O_v$. Hence σ' fixes the edge of T_v between these homothety classes (though it clearly does not fix this edge pointwise).

Now suppose that $\mathrm{ord}_v(\lambda) = 2a_v$ is even and $a_v > 0$ or $v \in S \cup S'$. In all cases we have $a_v \geq 0$, since $\lambda \in O$. Condition 8.12 implies $c \equiv 0 \bmod \pi_v^{a_v} O_v$. Hence

$$\text{(8.17)} \qquad \sigma' \begin{pmatrix} \pi_v^{a_v} O_v \\ O_v \end{pmatrix} = \begin{pmatrix} 0 & \lambda \\ 1 & c \end{pmatrix} \cdot \begin{pmatrix} \pi_v^{a_v} O_v \\ O_v \end{pmatrix} = \begin{pmatrix} \lambda O_v \\ \pi_v^{a_v} O_v \end{pmatrix} = \pi_v^{a_v} \begin{pmatrix} \pi_v^{a_v} O_v \\ O_v \end{pmatrix}.$$

Thus σ' fixes the homothety class of $\pi_v^{a_v} O_v \oplus O_v$, so it will now suffice to show σ' fixes the homothety class of an O_v lattice L containing $\pi_v^{a_v} O_v \oplus O_v$ for which $L/(\pi_v^{a_v} O_v \oplus O_v)$ is O_v-isomorphic to $k(v) = O_v/\pi_v O_v$. We now compute

$$\text{(8.18)} \qquad \begin{aligned} \sigma' \begin{pmatrix} \pi_v^{a_v-1} \\ \pi_v^{-1} \end{pmatrix} &= \begin{pmatrix} 0 & \lambda \\ 1 & c \end{pmatrix} \cdot \begin{pmatrix} \pi_v^{a_v-1} \\ \pi_v^{-1} \end{pmatrix} = \begin{pmatrix} \lambda \pi_v^{-1} \\ \pi_v^{a_v-1} + c\pi_v^{-1} \end{pmatrix} \\ &= = \pi_v^{a_v} \cdot \begin{pmatrix} \lambda \pi_v^{-2a_v} \pi_v^{a_v-1} \\ (1 + c\pi_v^{-a_v}) \pi_v^{-1} \end{pmatrix} \\ &\equiv \pi_v^{a_v} \cdot \lambda \pi_v^{-2a_v} \cdot \begin{pmatrix} \pi_v^{a_v-1} \\ \pi_v^{-1} \end{pmatrix} \quad \mathrm{mod} \quad \pi_v^{a_v} \begin{pmatrix} \pi_v^{a_v} O_v \\ O_v \end{pmatrix}. \end{aligned}$$

where the last congruence results from the condition on c in (8.12). Here $\lambda \cdot \pi_v^{-2a_v}$ is a unit of O_v, so we can take the lattice L to be the one generated as an O_v-module by $\pi_v^{a_v} O_v \oplus O_v$ and the vector $(\pi_v^{a_v - 1}, \pi_v^{-1})$. This completes the proof of Proposition 6.2.

9. Cusps and class numbers.

We begin by giving an ineffective proof of part (1) of Corollary 1.2. Recall that $C(N)$ is the set of isometry classes of minimal finite covolume discrete arithmetic hyperbolic 3-orbifolds having exactly N cusps. The finite covolume discrete arithmetic subgroups of $\mathrm{PGL}_2(k)$ are commensurable. Hence to show the elements of $C(N)$ represent only finitely many distinct commensurability classes, it will suffice by Theorem 1.1 to show that there are only finitely many imaginary quadratic fields k such that $h_k/h_{k,2} \leq N$. Siegel proved in [8] that for each $\epsilon > 0$, there is an ineffective constant $c(\epsilon) > 0$ such that

$$h_k > c(\epsilon)|d_k|^{\frac{1}{2}-\epsilon} \tag{9.1}$$

where d_k is the discriminant of k. By a result of Tatuzawa, the constant $c(\epsilon)$ can be made effective except for at most one exceptional field k; see [9] and [5]. Let n_k be the number of distinct prime factors of d_k. By genus theory, the two-rank of the ideal class group of k is equal to $2^{n_k - 1}$. Thus $h_{2,k} = 2^{n_k - 1}$ and we get

$$\frac{h_k}{h_{k,2}} > c(\epsilon)\frac{|d_k|^{\frac{1}{2}-\epsilon}}{2^{n_k - 1}} > c(\epsilon)\prod_{p|d_k}\frac{p^{\frac{1}{2}-\epsilon}}{2}. \tag{9.2}$$

The fact that there are only finitely many k for which $h_k/h_{k,2} < N$ is clear from (9.2), since $-d_k$ is either a square-free positive integer or 4 times such an integer, and if $\epsilon < 1/2$ then there are only finitely many primes p for which $\dfrac{p^{\frac{1}{2}-\epsilon}}{2} < 2$.

Suppose now that X is an element of $C(N)$. To show part (2) of Corollary 1.2, we must show that there are infinitely many elements of the commensurability class of X which also lie in $C(N)$. By Borel's work, $X = \mathbf{H}^3/\Gamma_{S,S'}$ for some imaginary quadratic field k and some maximal discrete subgroup $\Gamma_{S,S'} \subset \mathrm{PGL}_2(k)$. Theorem 1.1 shows

$$2^n \frac{h_k}{h_{k,2}} = N \tag{9.3}$$

where 2^n is the order of the subgroup of $Cl(k)/2Cl(k)$ generated by the places in S. We now let S_0 be a set of n places whose images in $Cl(k)/2Cl(k)$ generate a subgroup of order 2^n; such an S_0 exists by the Cebotarev density theorem. Let W be the set of finite places v of k such that

$$\mathcal{P}(v) \cdot \mathcal{P}(S_0) = \mathcal{P}(S_0 \cup \{v\}) \tag{9.4}$$

is principal. The Cebotarev density theorem also implies W is infinite. We claim that for $v \in \mathrm{W}$, the group $\Gamma_{S_0 \cup \{v\}, \emptyset}$ contains an element σ_v which is odd at $S_0 \cup \{v\}$. To construct σ_v, let λ_v be a generator for the ideal in (9.4). We can then take σ_v to be

$$\sigma_v = \begin{pmatrix} 0 & \lambda_v \\ 1 & 0 \end{pmatrix}. \tag{9.5}$$

We now see from [3, Prop. 4.4(iii)] that if $\Gamma_{S_0 \cup \{v\}, \emptyset}$ is not maximal, then it is conjugate to subgroup of a maximal discrete subgroup of the form $\Gamma_{S_0 \cup \{v\}, S'(v)}$ for some finite set of places $S'(v)$ which is disjoint from $S_0 \cup \{v\}$. We conclude that for each $v \in \mathrm{W}$, there is a maximal discrete group $\Gamma_{S_0 \cup \{v\}, S'(v)}$ which contains an element which is odd at v. Furthermore, the fact that (9.4) is principal implies that $\{\mathcal{P}(v') : v' \in S_0\}$ and $\{\mathcal{P}(v') : v' \in S_0\} \cup \{\mathcal{P}(v)\}$ generate the same subgroup of $Cl(k)/2Cl(k)$, which by hypothesis has order 2^n. Thus Theorem 1.1 shows $\mathbf{H}^3/\Gamma_{S_0 \cup \{v\}, S'(v)}$ has exactly N cusps, were N is as in (9.3). The orbifolds $\mathbf{H}^3/\Gamma_{S_0 \cup \{v\}, S'(v)}$ and $\mathbf{H}^3/\Gamma_{S_0 \cup \{v'\}, S'(v')}$ are not isometric for distinct v and v' in $\mathrm{W} - S_0$, since the group $\Gamma_{S_0 \cup \{v\}, S'(v)}$ contains no elements which are odd at v' and similarly with the roles of v and v' reversed (cf. [3, Prop. 4.4(ii)]). This completes the proof that $C(N)$ contains infinitely many elements which are commensurable to X.

References

[1] N. D. Allan, The problem of the maximality of arithmetic groups, Proc. Symp. Pure Math, Vol. 9 (1966), p. 104 - 109.

[2] L. Bianchi, Sui gruppi di sostituzioni lineari con coefficienti appartenenti a corpi quadratici immaginari, Math. Ann., Vol 40, p. 332 - 412.

[3] A. Borel, Commensurability classes and volumes of hyperbolic 3-manifolds, Ann. Scuola Normale Pisa, ser. 4 Vol. 8 (1981), p. 1 - 33.

[4] J. Elstrodt, F. Grunewald and J. Mennicke, Groups acting on hyperbolic space: Harmonic analysis and number theory, Springer Monographs in Mathematics, Springer, Berlin (1998).

[5] D. Goldfeld, Gauss's class number problem for imaginary quadratic fields, Bull. of the A.M.S. , Vol. 13, no. 1 (1985), p. 23 - 37.

[6] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Princeton Univ. Press, 1971.

[7] R. A. Shmidt, On subgroups of reflections in Bianchi groups (in Russian), Problems of group theory and homological algebra, Yaroskavi State University (1987), p. 121 - 127.

[8] C. L. Siegel, Über die Klassenzahl quadratischer Zahlkörper, Acta Arith. 1 (1935), p. 83 - 86.

[9] T. Tatuzawa, On a theorem of Siegel, Japan J. Math. 21 (1951), p. 163 - 178.

[10] R. Swan, Generators and Relations for certain Special Linear Groups, Advances in Math. 6 (1971), p. 1 - 77.

[11] E. B. Vinberg, Reflective subgroups in Bianchi groups, Selecta Math. Soviet, Vol. 9 (1990), p. 309 - 314.

Ted Chinburg
T.C.: Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
E-mail: ted@math.upenn.edu

Darren Long
D.L.: Department of Mathematics
University of California
Santa Barbara, California 93106
E-mail: long@math.ucsb.edu

Alan W. Reid
A.R.: Department of Mathematics
University of Texas
Austin, Texas 78712
E-mail: areid@math.utexas.edu