1. Introduction

Arithmetic groups are a rich class of groups where connections between topology and number theory are showcased in a particularly striking way. One construction of these groups is motivated by the modular group, PSL$_2(\mathbb{Z})$. The group of orientation preserving isometries of the hyperbolic upper half plane, $\mathbb{H}^2$, is isomorphic to PSL$_2(\mathbb{R})$. Since $\mathbb{Z}$ is a discrete subgroup of $\mathbb{R}$ it follows that PSL$_2(\mathbb{Z})$ is discrete in PSL$_2(\mathbb{R})$. The modular group acts on $\mathbb{H}^2$ by linear fractional transformations, and the quotient $\mathbb{H}^2$/PSL$_2(\mathbb{Z})$ is a finite volume hyperbolic orbifold.

The modular group has deep connections to many branches of mathematics and to number theory in particular. The modular group encodes the moduli space of elliptic curves. Modular forms, which are analytic functions on $\mathbb{H}^2$ satisfying a functional equation with respect to the modular group, have far-reaching connections between geometry, number theory, and analysis. In particular, Wiles’ proof of the Taniyama Shimura conjecture (the modularity theorem) established a proof of Fermat’s Last Theorem, one of the most famous conjectures of our time.

The geometry of the action of the modular group on $\mathbb{H}^2$ can also be used to provide a proof of Roth’s theorem (the Thue-Siegel-Roth theorem). This theorem essentially says that an algebraic integer (which is not in $\mathbb{Z}$) does not have many ‘good’ rational approximations. Precisely, Roth’s theorem says that if $\alpha$ is an irrational algebraic integer, then for any $\epsilon > 0$

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\epsilon}}$$

has only finitely many solutions where $p, q \in \mathbb{Z}$ are co-prime.

Arithmetic groups are essentially subgroups of matrix groups defined over integer rings. For example, the groups SL$_n(\mathcal{O}_K)$ are arithmetic, where $\mathcal{O}_K$ is the ring of integers of a number field $K$. The arithmetic groups we will concentrate on in the manuscript are a class of arithmetic groups which generalize the modular group, and act on (products of) hyperbolic spaces. There are many similarities between these arithmetic groups and the modular group, but there are also many difference. These differences showcase the dichotomy between lattices of low rank and higher-rank lattices. Some of this behavior can be seen algebraically, for example by the congruence subgroup property, and Kazhdan’s property (T).

One interesting connection between the underlying number theory of these groups and the topology of their quotients is that through the distance formula, lengths of geodesics correspond traces of matrices. Because of the arithmeticity, these traces correspond to special kinds of algebraic integers. As we discuss in §9 in the case of arithmetic Fuchsian groups, these algebraic integers are Salem numbers. We will outline a proof of the equivalence of the Salem conjecture and the short geodesic
conjecture for arithmetic hyperbolic surfaces. See [11] for this and other connections between Salem numbers and geometry.

The purpose of this manuscript is to provide an introduction to this class of arithmetic groups motivated by the modular group, and outline the proof of this correspondence between the geodesic length and the Mahler measure.

2. The Modular Group

One way to deconstruct the modular group is as follows. From a geometric viewpoint, we wish to construct a discrete subgroup of $\text{PSL}_2(\mathbb{R})$; such a group will be discrete in $\text{Isom}(\mathbb{H}^2)$ and act on $\mathbb{H}^2$ by linear fractional transformations. The quotient by this action will be an orbifold, a manifold with some well behaved singularities. (If the subgroup is torsion free, it will be a manifold.) We also want to ensure that the subgroup is large enough, so that the quotient has finite volume.

We begin with $M_2(\mathbb{Q})$, the $2 \times 2$ matrices with rational coefficients; the field $\mathbb{Q}$ introduces the arithmeticity since it is the quotient field of $\mathbb{Z}$. We then take $M_2(\mathbb{Z})$ which is discrete in $M_2(\mathbb{Q})$. We require a subgroup of $\text{PSL}_2(\mathbb{R})$, so we take the norm one elements, $\text{SL}_2(\mathbb{Z})$ and then projectivize. Happily, the resulting group $\text{PSL}_2(\mathbb{Z})$ is a discrete subgroup of $\text{PSL}_2(\mathbb{R})$; this follows from the fact that $M_2(\mathbb{Z})$ is discrete in $M_2(\mathbb{R})$, which is due to the discreteness of $\mathbb{Z}$ in $\mathbb{R}$. As a result, the quotient $\mathbb{H}^2/\text{PSL}_2(\mathbb{Z})$ is a finite volume orbifold. We will generalize the construction $M_2(\mathbb{Q}) \rightarrow M_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}) \rightarrow \text{PSL}_2(\mathbb{Z})$ to produce more discrete subgroups in $\text{PSL}_2(\mathbb{R})$, and then further generalize this to produce discrete groups in $\text{PSL}_2(\mathbb{C})$ and products of $\text{PSL}_2(\mathbb{R})$ and $\text{PSL}_2(\mathbb{C})$.

3. Quaternion Algebras

Let $K$ be a number field with $r_1$ real places and $r_2$ complex places, so $[K : \mathbb{Q}] = r_1 + 2r_2$. We will label the real embeddings as $\sigma_1, \ldots, \sigma_{r_1}$ and the complex embeddings as $\tau_1, \tau_1, \ldots, \tau_{r_2}, \tau_{r_2}$. Let $O_K$ be the ring of integers in $K$, elements in $K$ which are roots of a monic polynomial in $\mathbb{Z}[x]$.

3.1. Hilbert Symbols. Let $\mathcal{Q}$ be a quaternion algebra over a field $F$. That is, $\mathcal{Q}$ is a four dimensional central simple algebra over $F$. If $F$ does not have characteristic two, we can encode the data defining $\mathcal{Q}$ using a Hilbert symbol. We now assume that $\text{char}(F) \neq 2$. For non-zero elements $a, b \in F$ the Hilbert symbol $\left(\frac{a, b}{F}\right)$ defines the quaternion algebra

$$\left(\frac{a, b}{F}\right) = \{r_1 + r_2i + r_3j + r_4k : i^2 = a, j^2 = b, ij = -ji = k\}$$

where $r_1, r_2, r_3,$ and $r_4$ are elements of $F$. It follows that $k^2 = -ab$. Using this notation, Hamilton’s quaternions are

$$\mathcal{H} = \left(\frac{-1, -1}{\mathbb{R}}\right).$$

The Hilbert symbol $\left(\frac{1, 1}{\mathcal{F}}\right)$ defines a quaternion algebra isomorphic to $M_2(F)$ as can be seen by the map

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$
The Hamiltonians and $M_2(\mathbb{R})$ are not isomorphic. In particular, the Hamiltonians are a division algebra, but $M_2(\mathbb{R})$ has zero divisors; the non-zero elements of determinant zero are all zero divisors. It is a consequence of the Wedderburn-Artin theorem that a quaternion algebra over $F$ is either isomorphic to $M_2(F)$ or is a division algebra. We say that $Q$ is ramified if it is isomorphic to a division algebra, and split if it is isomorphic to a matrix algebra. Frobenius showed that the Hamiltonians are the only ramified quaternion algebra over $\mathbb{R}$.

Different Hilbert symbols often define isomorphic quaternion algebras. In particular, for $Q = \left( \frac{a,b}{F} \right)$ and any non-zero $u \in F$, 

$Q \cong \left( b, a \frac{F}{F} \right) \cong \left( au^2, b \frac{F}{F} \right) \cong \left( a, -ab \frac{F}{F} \right).$

The isomorphisms between the last three algebras and $Q$ can be seen by switching the roles of $i$ and $j$, by $i \mapsto iu^{-1}$ and $j \mapsto j$, and by the map $i \mapsto i$, $j \mapsto k$, respectively. This shows that over $\mathbb{R}$ a quaternion algebra is isomorphic to $H$ exactly when $a$ and $b$ are negative, and that all quaternion algebras over $\mathbb{C}$ are isomorphic to $M_2(\mathbb{C})$.

If $[L : F] = 2$ one can often embed $L$ as a quaternion algebra over $F$. For example, if $L = F(\sqrt{a})$ then $L \hookrightarrow \left( \frac{a,b}{F} \right)$ identifying $i$ with $\sqrt{a}$.

3.2. Norm and Trace. For $q = r_1 + r_2i + r_3j + r_4k \in Q = \left( \frac{a,b}{F} \right)$, define the conjugate of $q$ to be $\overline{q} = r_1 - r_2i - r_3j - r_4k$. This is well-defined independent of the choice of basis since the center of $Q$ is $F$. We define the reduced norm of $q$ to be

$n(q) = q \cdot \overline{q} = r_1^2 - ar_2^2 - br_3^2 + abr_4^2.$

Similarly, the reduced trace is $t(q) = q + \overline{q}$. Let the superscript one denote elements of norm one. The norm is preserved by homomorphism, so if $Q \cong M_2(F)$ then the image of $Q^1$ is $SL_2(F)$.

We extend this discussion to the following classification lemma.

**Lemma 3.1.** For the quaternion algebra $Q = \left( \frac{a,b}{F} \right)$, the following are equivalent:

1. $Q \cong \left( \frac{1,1}{F} \right) \cong M_2(F)$.
2. $Q$ is not a division algebra.
3. The quadratic form $ax^2 + by^2 = 1$ has a solution $(x, y) \in F \times F$.

**Proof.** It suffices to show the equivalence of the third. An element $q \in Q$ is invertible exactly when $n(q) \neq 0$. Consider $q_1 = r_1 + r_2i + r_3j + r_4k$.

If $r_1 \neq 0$ then letting $q_2 = b_2i + b_3j + b_4k$ with

$b_2 = b(r_1r_4 + r_2r_3), \quad b_3 = a(r_2^2 - br_4^2), \quad b_4 = (r_1r_2 + br_3r_4)$

we see that if $n(q_1) = 0$ then $n(q_2) = 0$ as well. The norm of $q_2$ is

$-ar_2^2 - br_3^2 + abr_4^2 = 0.$

Therefore, $Q$ is not a division algebra exactly when there is some non-zero element $0 \neq q = b_2i + b_3j + b_4k$ with zero norm.

Assume that $Q$ is not a division algebra. If any two of $b_2, b_3,$ and $b_4$ are zero then $q = 0$. If $b_4 \neq 0$ then let $x = b_3/ab_4$, $y = b_2/ab_4$. If $b_4 = 0$ then let $x = (1 + a)/2a$, $y = b_3(1 - a)/2ab_2$. Hence we have solutions to $ax^2 + by^2 = 1$. 


Assume there is a solution to \( ax^2 + by^2 = 1 \). If \( x = 0 \) then \( b = c^2 \) for some \( c \in F \). Then \( (c+j)(c-j) = 0 \) and \( Q \) is not a division algebra. If \( x \neq 0 \) then \( a + b(y/x)^2 = (1/x)^2 \), so \( a = (1/x)^2 - b(y - x)^2 \) and it follows that the norm of \((1/x) + i + (y/x)j\) is zero, so \( Q \) is not a division algebra.

\[ \square \]

3.3. Extension of Scalars. In our construction, we begin with \( Q = \left( \frac{a,b}{K} \right) \) a quaternion algebra over a number field \( K \). To create a Fuchsian group, the goal is to construct a discrete subgroup of \( \text{SL}_2(\mathbb{R}) \), so we need a well behaved map to \( M_2(\mathbb{R}) \).

If \( F \subset F' \) we can extend the scalars of \( Q = \left( \frac{a,b}{F} \right) \) by

\[
\left( \frac{a,b}{F} \right) \otimes_F F' \cong \left( \frac{a,b}{F'} \right).
\]

Similarly, if \( \iota : F \to F' \) is an injection then we define the quaternion algebra

\[
Q' = \left( \frac{\iota(a), \iota(b)}{\iota(F)} \right)
\]

by

\[
1 + 12i + 2j + 2k \mapsto \iota(1) + 12i + 2j + 2k'
\]

where \( 1, i, j, k \) are the the basis elements for \( Q \) and \( 1, i', j', k' \) are the basis elements for \( Q' \). If \( \nu \) is a place of \( K \) with completion \( K_\nu \) then we can extend scalars to \( K_\nu \) as

\[
Q'' = \left( \frac{a,b}{K} \right) \otimes_K K_\nu \cong \left( \frac{a,b}{K_\nu} \right).
\]

We say that \( Q \) is split at \( \nu \) if \( Q'' \) is isomorphic to \( M_2(K_\nu) \) and ramified if it is isomorphic to a division algebra. By the Hasse-Minkowski theorem a quaternion algebra \( Q = \left( \frac{a,b}{K} \right) \) is isomorphic to \( M_2(K) \) if and only if for all places \( \nu \) this extension by scalars is split. When \( \nu \) is an infinite place, this extension of scalars is isomorphic to either \( \left( \frac{a,b}{\mathbb{R}} \right) \) or \( \left( \frac{a,b}{\mathbb{C}} \right) \). We will use split extensions to produce maps from \( Q \) to \( M_2(\mathbb{R}) \) or \( M_2(\mathbb{C}) \). For discreteness, we need to be mindful of the other infinite places of \( K \). That is, if \( \sigma \) is an embedding of \( K \) into \( \mathbb{R} \) we need to understand the ramification of \( Q'' \cong \left( \frac{a,b}{\mathbb{R}} \right) \). (If \( \tau \) is a complex embedding \( Q'' \cong \left( \frac{a,b}{\mathbb{C}} \right) \) is always split.)

Let \( Q = \left( \frac{a,b}{K} \right) \). In view of Lemma 3.1 if \( K \subset L \) and \( Q \otimes_K L \) is split then there is an \( (x, y) \in L \times L \) such that \( ax^2 + by^2 = 1 \). If \( y = 0 \) then \( a \) is a square, so we can explicitly see the map to \( M_2(K) \) defined by

\[
1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ i \mapsto \sqrt{a} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ j \mapsto \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}.
\]

For any Galois automorphism \( \sigma \), \( \sigma(a) \) must also be a square. It follows that if \( \sigma(K) \subset L \), then \( Q'' \otimes_{\sigma(K)} L \) is also split and \( \sigma \) acts on the image of \( Q \) in \( M_2(L) \), sending it to the image of \( Q'' \subset M_2(L) \). Otherwise, if \( y \neq 0 \) then a map from \( Q \) to \( M_2(L) \) can explicitly be given by

\[
1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ i \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \ j \mapsto \begin{pmatrix} y^{-1} & -axy^{-1} \\ xy^{-1} & -y^{-1} \end{pmatrix}.
\]
If \( Q^c \otimes_{\sigma(K)} L \) is also split then there are \( x', y' \) in \( L \) such that \( \sigma(a)(x')^2 + \sigma(b)(y')^2 = 1 \) then the map between matrix groups can be seen by
\[
\begin{pmatrix}
  y^{-1} & -axy^{-1} \\
  xy^{-1} & -y^{-1}
\end{pmatrix} \mapsto \begin{pmatrix}
  (y')^{-1} & -\sigma(a)x'(y')^{-1} \\
  x'(y')^{-1} & -(y')^{-1}
\end{pmatrix}
\]
and extending the map on \( K \) by the Galois automorphism. We will use \( \rho \) to denote such a map from \( Q \) to \( M_2(K) \).

For a quaternion algebra \( Q \) over a number field \( K \), the number of places (finite and infinite) where \( Q \) is ramified is even. Moreover, for any even subset of places of \( K \) there is a quaternion algebra that is ramified at this set. This quaternion algebra is unique up to isomorphism.

3.4. Orders. In the construction of the modular group, we chose \( M_2(\mathbb{Z}) \subset M_2(\mathbb{Q}) \) to ensure discreteness and to get a quotient of finite volume; we generalize this idea using orders. Let \( Q \) be a quaternion algebra over the number field \( K \). For any vector space \( V \) over \( K \) an \( \mathcal{O}_K \) lattice \( L \) in \( V \) is a finitely generated \( \mathcal{O}_K \) module contained in \( V \). It is complete if \( L \otimes_{\mathcal{O}_K} K \cong V \). An order \( \mathcal{O} \) in the quaternion algebra \( Q \) is a complete \( \mathcal{O}_K \) lattice which is also a ring with unity. An order is called maximal if it is maximal with respect to inclusion. If \( \mathcal{O} \) is an order in \( Q \) defined over \( K \), then since it is a lattice if \( \alpha \in \mathcal{O} \) then both \( \text{tr}(\alpha) \) and \( n(\alpha) \) lie in \( \mathcal{O}_K \). (See [16] Lemma 2.2.4 page 83, for example.)

In the construction of the modular group \( K = \mathbb{Q} \), and \( \mathcal{O}_K = \mathbb{Z} \). If \( V = M_2(\mathbb{Q}) \) then since \( M_2(\mathbb{Z}) \otimes_{\mathbb{Q}} \mathbb{Q} \cong M_2(\mathbb{Q}) \) it is a complete lattice and we conclude that \( M_2(\mathbb{Z}) \) is an order. Similarly, for any number field \( K \), \( M_2(\mathcal{O}_K) \) is an order in \( M_2(K) \). The order \( \mathcal{O}' = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\left( \frac{1 + i + j + k}{2} \right) \) is contained in \( \mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k \) and so \( \mathcal{O}' \) is not maximal. By the Skolem-Noether theorem two isomorphic orders in \( Q \) are conjugate. The number of conjugacy classes of maximal orders is finite and called the type number of \( Q \). The type number of \( M_2(K) \) is finite and equals \( |\text{Cl}_K/\text{Cl}_K^{(2)}| \) where \( \text{Cl}_K \) is the class number of \( K \) and \( \text{Cl}_K^{(2)} \) is the subgroup generated by squares.

In the quaternion algebra \( Q = \left( \frac{-1,-11}{\mathbb{Q}} \right) \), define
\[
\tau = -1 + \frac{i + j}{2}, \quad z = \frac{i + j}{2}
\]
so that \( \tau^3 = 1 \) and \( z^2 - z + 3 = 0 \). The maximal orders
\[
\mathcal{O}_\tau = \mathbb{Z}[\tau] + j\mathbb{Z}[\tau] \quad \text{and} \quad \mathcal{O}_z = \mathbb{Z}[z] + i\mathbb{Z}[z]
\]
are not isomorphic. Regardless, the intersection of two maximal orders is an order, so we often focus on the order \( \mathcal{O}_K[1, i, j, k] \).

4. Construction of Arithmetic Fuchsian Groups

Let \( Q \) quaternion algebra over a number field \( K \) with a maximal order \( \mathcal{O} \). Assume that \( Q \) is split at at least one real embedding of \( K \). (In fact, for ease we often call this the identity embedding.) Next, take the norm one elements of \( \mathcal{O} \), \( \mathcal{O}^1 \). The set \( \mathcal{O}^1 \) is a maximal discrete group of norm one elements in our quaternion algebra, and the split place produces a mapping from this group to \( \text{SL}_2(\mathbb{R}) \) as seen by the extension of scalars. It remains to show that the image is discrete in \( \text{SL}_2(\mathbb{R}) \) and has finite co-area.
To ensure discreteness of the image, we impose the condition that all other infinite places are real and \( \mathcal{Q} \) is ramified at these places. Recall that the standard isomorphism from \( \mathcal{Q} \) to \( M_2(\mathbb{R}) \) is denoted as \( \rho \). We will use \( \rho \) to denote this map restricted to \( O^1 \) as well. We now sketch a proof that \( \rho(O^1) \) is a discrete subgroup of \( SL_2(\mathbb{C}) \). This will follow from the following two results.

**Lemma 4.1.** The norm one elements in the Hamiltonians, \( H^1 = \left( \frac{-1-1}{R} \right)^1 \) are a compact set.

**Proof.** The norm of \( q = (r_1 + r_2i + r_3j + r_4k) \in H \) is

\[ n(q) = q\overline{q} = r_1^2 + r_2^2 + r_3^2 + r_4^2. \]

It follows that \( H^1 \) is isomorphic to \( S^3 \) and is compact. \( \square \)

**Lemma 4.2.** Let \( C \subset \mathbb{C} \) be a compact set, and \( K \) a number field. Then there are only finitely many algebraic integers \( \alpha \in O_K \) such that \( \alpha \) and all of its conjugates lie in \( C \).

**Proof.** If \( \sigma_1, \ldots, \sigma_r \) are all real places of \( K \) and \( \tau_1, \ldots, \tau_s \) are all complex places of \( K \), then the injection \( \phi : O_K \to \mathbb{R}^r \times \mathbb{C}^s \) defined by

\[ \alpha \in K \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \tau_1(\alpha), \ldots, \tau_s(\alpha)) \]

sends \( O_K \) to a lattice. Any compact subset of \( \mathbb{R}^r \times \mathbb{C}^s \) can contain only finitely many lattice points, and therefore its preimage under \( \phi \) contains only finitely many integers \( \alpha \) such that \( \alpha \) and all of its conjugates are in the set. \( \square \)

The quaternion algebra \( \mathcal{Q} \) is defined over the totally real number field \( K \) which is split at the identity embedding. Therefore, \( \mathcal{Q} \otimes_K \mathbb{R} \) is isomorphic to \( M_2(\mathbb{R}) \). Call this isomorphism \( \rho \). Consider a convergent sequence \( \{q_n\} \subset O^1 \subset \mathcal{Q} \). Under the mapping \( \rho \) we can assume that

\[ \rho(q_n) \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \]

To show discreteness, it suffices to show that for \( n \) large enough the \( q_n \) are all equal. Let \( q_n = r_{1,n} + r_{2,n}i + r_{3,n}j + r_{4,n}k \). The images \( \rho(q_n) \) converge to the identity, and since \( \rho \) is a homomorphism, \( q_n \to 1 \), the identity in \( \mathcal{Q} \). Therefore

\[ r_{1,n} \to 1, \quad r_{2,n} \to 0, \quad r_{3,n} \to 0, \quad r_{4,n} \to 0, \]

and so there is an \( N_0 \) such that for all \( n > N_0 \), \( r_{2,n}, r_{3,n} \), and \( r_{4,n} \) are within \( \epsilon \) of 0, and \( r_{1,n} \) is within \( \epsilon \) of 1.

The number field \( K \) is totally real, and the quaternion algebra \( \mathcal{Q} \) is ramified at all non-identity places \( \sigma \) of \( K \). Therefore \( \mathcal{Q}^\sigma \otimes_K \mathbb{R} \cong \mathcal{H} \) for all of these places. It follows that if \( \sigma \) is a ramified real place the induced map takes \( \mathcal{O}^1 \) into \( \mathcal{H}^1 \), the norm one elements of the Hamiltonians. Since \( \mathcal{H}^1 \) is compact by Lemma 4.1, all of these conjugates of \( r_{1,n}, r_{2,n}, r_{3,n}, \) and \( r_{4,n} \) are all bounded. The numbers \( r_{1,n}, r_{2,n}, r_{3,n}, \) and \( r_{4,n} \) are bounded by the above discussion of the identity place. Therefore, discreteness follows by Lemma 4.2. For a general maximal order the values \( r_{1,n}, r_{2,n}, r_{3,n}, \) and \( r_{4,n} \) may not be algebraic integers, but they are ‘almost’ algebraic integers and discreteness follows.

This construction yields what is called a Fuchsian group derived from a quaternion algebra. For a broader family of groups, we introduce the notion of commensurability.
5. Commensurability

If $A$ and $B$ are both subgroups of a group $G$ we say that $A$ and $B$ are commensurable if the intersection $A \cap B$ has finite index in both $A$ and $B$. We say that $A$ and $B$ are commensurable in the wide sense if a conjugate of $A$ is commensurable with $B$. This parallels the notion of commensurability of manifolds (or orbifolds). Two manifolds $M$ and $N$ are commensurable if they share a finite sheeted cover.

**Definition 5.1.** A Fuchsian group derived from a quaternion algebra is a finite index subgroup of $\rho(O^1)$ where $O$ is a maximal order in a quaternion algebra over a totally real number field which is unramified in exactly one place. An arithmetic Fuchsian group is a subgroup of $\text{PSL}_2(\mathbb{R})$ which is commensurable (in the wide sense) to a Fuchsian group derived from a quaternion algebra.

There is a precise relationship between arithmetic and derived groups. Define $\Gamma^{(2)}$ as $\langle \gamma^2 : \gamma \in \Gamma \rangle$, so $\Gamma^{(2)}$ is a (finite index) subgroup of $\Gamma$. The group $\Gamma$ is arithmetic if and only if $\Gamma^{(2)}$ is derived (see [16] Corollary 8.3.5).

As we have seen, $\text{PSL}_2(\mathbb{Z})$ is an arithmetic Fuchsian group with torsion. For example $\pm \left( \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right)$ has order two. Therefore, the quotient is an orbifold. By Selberg’s Lemma, such an orbifold has a finite sheeted (branched) cover which is a manifold. That is, an arithmetic Fuchsian group with torsion has a finite index subgroup which is torsion free.

**Example 5.2.** Let $K$ be the splitting field of the biquadratic polynomial $p(x) = x^4 - 5x^2 + 2$. Then $p(x)$ has four real roots,

$$\pm \sqrt{\frac{5 \pm \sqrt{17}}{2}}.$$

Consider the quaternion algebra

$$Q = \left( \frac{\sqrt{5 + \sqrt{17}} - 2, -1}{K} \right).$$

The integer $-1$ is fixed by all elements of the Galois group of $K$. The other conjugates of $\sqrt{5 + \sqrt{17}} - 2$ are $-\sqrt{5 + \sqrt{17}} - 2$, $-\sqrt{5 - \sqrt{17}} - 2$ and $\sqrt{5 - \sqrt{17}} - 2$. All four of these conjugates are real; $\sqrt{5 + \sqrt{17}} - 2$ is positive, but the other conjugates are negative. Therefore the quaternion algebra is split at the identity embedding, but is ramified at all three non-identity embeddings. It follows that if $O$ is a maximal order, $\rho(O^1) \subset \text{PSL}_2(\mathbb{C})$ is a Fuchsian group derived from a quaternion algebra. Specifically, $\rho(O_K[1, i, j, k])$ is such a group. In fact (see Theorem 2) this is a co-compact group.

6. Arithmetic Kleinian Groups

The construction of arithmetic Kleinian groups is very similar to the construction of the arithmetic Fuchsian groups. In this case, we begin with $K$, a number field with exactly one complex place. If $Q$ is a quaternion algebra over $K$ then $Q \otimes_K \mathbb{C} \cong M_2(\mathbb{C})$. Denote this map to $M_2(\mathbb{C})$ as $\rho$ as above. If $Q$ is unramified at all real places, then for any (maximal) order $O \subset Q$ the proof that $\rho(O^1)$ is a finite covolume discrete subgroup of $\text{SL}_2(\mathbb{C})$ is analogous to the Fuchsian case.
Definition 6.1. A Kleinian group derived from a quaternion algebra is a finite index subgroup of $P\rho(O^1)$ where $O$ is a maximal order in a quaternion algebra over a number field with exactly one complex place which is ramified in all real places. An arithmetic Kleinian group is a subgroup of $PSL_2(\mathbb{C})$ which is commensurable (in the wide sense) to a Kleinian group derived from a quaternion algebra.

The Bianchi groups are natural analogs of the modular group in the Kleinian setting. Let $K$ be an imaginary quadratic number field. Then $O = O_K[1, i, j, k]$ is an order in the quaternion algebra $\left(\frac{1}{\mathcal{R}}\right)$. Under the map $\rho: O \subset M_2(O_K)$ and the image of the norm one elements is contained in $SL_2(O_K)$. As there is just one (complex) place and $M_2(O_K)$ is unramified at the identity place we see that $SL_2(O_K)$ is a discrete subgroup of $SL_2(\mathbb{C})$. (In fact, discreteness directly follows from the fact that $O_K$ is discrete is $\mathbb{C}$.) The groups $PSL_2(O_K)$ are called the Bianchi groups. The quotient $Q_K = \mathbb{H}^3/PSL_2(O_K)$ is a cusped hyperbolic 3-orbifold. Hurwitz showed that the number of cusps is equal to the class number of $Q_K$. The figure-8 knot complement can be realized as $\mathbb{H}^3/\Gamma$ where $\Gamma < PSL_2(\mathbb{C})$ is generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & -\omega \\ 0 & 1 \end{pmatrix}$$

with $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. The group $\Gamma$ is an index 12 subgroup of the Bianchi group $PSL_2(O_{\mathbb{Q}(\sqrt{-3})})$. Reid [22] proved that the figure-8 is the only arithmetic knot complement (in $S^3$). Cuspidal cohomology computations show that any arithmetic link complement in $S^3$ must be of the form $\mathbb{H}^3/\Gamma$ where $\Gamma$ is commensurable with the Bianchi group $PSL_2(O_{\mathbb{Q}(\sqrt{-1})})$ for

$$d \in \{1, 2, 3, 5, 6, 7, 11, 15, 19, 23, 31, 39, 47, 71\}.$$  

The Whitehead link is arithmetic, and the fundamental group of the complement is a finite index subgroup of $PSL_2(O_{\mathbb{Q}(\sqrt{-1})})$. In fact, Baker [1] showed that all links are sub links of arithmetic links.

7. Properties of Arithmetic Fuchsian and Kleinian groups

An alternate definition of arithmetic groups, due to Margulis, is that a Kleinian group $\Gamma$ is arithmetic if it has infinite index in its commensurator. The commensurator of $\Gamma$ is

$$\text{Comm}(\Gamma) = \{x \in PSL_2(\mathbb{C}) : x^{-1}\Gamma x \text{ is commensurable with } \Gamma\}.$$  

A similar statement is true for Fuchsian groups.

For any Fuchsian or Kleinian group $\Gamma$, the field $\mathbb{Q}(\text{tr}(\gamma) : \gamma \in \Gamma)$ is a number field. In the arithmetic case, if $\Gamma = P\rho(O^1)$ where $O$ is an order in a quaternion algebra defined over $K$, then $\mathbb{Q}(\text{tr}(\gamma)) = K$. In the general setting the invariant trace field $\mathbb{Q}(\text{tr}^2(\gamma))$ is an invariant of the commensurability class. (For arithmetic groups these fields coincide.) For any Fuchsian or Kleinian group, one can construct a quaternion algebra as well. One distinguishing characteristic of the arithmetic Fuchsian and Kleinian groups is that all traces are algebraic integers, since they correspond to traces of elements in an order. In fact, a Kleinian group $\Gamma$ is arithmetic if and only if the invariant trace field is a number field with one complex place, the traces are all algebraic integers, and the associated quaternion algebra is
ramified at all real places. A similar statement is true in the Fuchsian case. (See [16] for details.)

If $\mathcal{O}$ is a maximal order, the co-area of the derived Fuchsian group $P\rho(\mathcal{O}^1)$, the area of $\mathbb{H}^2/P\rho(\mathcal{O}^1)$, is given by

$$
\frac{8\pi \Delta_K^2 \zeta_K(2)}{(4\pi^2)|K:Q|} \prod_{P|\Delta(\mathcal{Q})} (N(P) - 1)
$$

where $\Delta_K$ is the absolute discriminant of $K$, $\Delta(\mathcal{Q})$ is the (reduced) discriminant of $\mathcal{Q}$, and $\zeta_K$ is the Dedekind zeta function of $K$ [5]. Similar to the Fuchsian case, if $\mathcal{O}$ is a maximal order in the quaternion algebra $\mathcal{Q}$ over $K$, the co-volume of the derived group $P\rho(\mathcal{O}^1)$ is

$$
\frac{4\pi^2|\Delta_K|^2 \zeta_K(2)}{(4\pi^2)|K:Q|} \prod_{P|\Delta(\mathcal{Q})} (N(P) - 1).
$$

### 7.1. Co-compactness

Co-compactness. The modular group and the Bianchi groups are non-co-compact. That is, the quotients are non compact 2- and 3-orbifolds. One way to see this is that each contains the parabolic element $\pm \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, the image of the norm one element $1 + i + j$. In fact, the commensurability classes containing these groups are precisely the non-co-compact arithmetic Fuchsian and Kleinian groups.

It is not difficult to determine which arithmetic Fuchsian and Kleinian groups are co-compact, and which are not. (See [16] Theorem 8.2.3.)

**Theorem 1.** Let $\Gamma$ be an arithmetic Kleinian group commensurable with the derived Kleinian group $P\rho(\mathcal{O}^1)$, where $\mathcal{O}$ is an order in the quaternion algebra $\mathcal{Q}$ defined over $K$. Then the following are equivalent.

1. $\Gamma$ is non-co-compact.
2. $K = \mathbb{Q}(\sqrt{-d})$ and $\mathcal{Q} \cong M_2(K)$
3. $\Gamma$ is commensurable with a Bianchi group, $\text{PSL}_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})})$.

**Proof.** Since $\Gamma$ is a Kleinian group, $G = P\rho(\mathcal{O}^1)$ is as well, and we must have that for $Q = \left\langle \frac{a,b}{R} \right\rangle$ that $K$ has exactly one complex place, $\tau$, and if $\sigma_1, \ldots, \sigma_r$ are the real places, $Q^{\sigma_1} \otimes_{\sigma(r(K))} \mathbb{R} \cong \mathcal{H}$.

Co-compactness is a commensurability invariant, so $\Gamma$ is non-co-compact exactly when $G = P\rho(\mathcal{O}^1)$ is compact. Therefore, if $\gamma$ is not co-compact $G$ contains a parabolic element which is conjugate to some $\pm \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ for $x \neq 0$ and can be written as

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

Since the identity is in the quaternions algebra $\mathcal{Q}$, and maps to the identity matrix, we see that up to an isomorphism, $x \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is in $\mathcal{Q}$. This element has norm 0 and corresponds to a zero divisor. Therefore, $\mathcal{Q}$ is not a division algebra and must be isomorphic to $M_2(K)$. It follows that $K$ has no real places. Therefore, 1 implies 2.
Assuming 2, notice that \( M_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}) \) is an order in \( \mathcal{O} = M_2(\mathbb{Q}(\sqrt{-d})) \). The intersection of a maximal order \( \mathcal{O} \) with \( M_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}) \) is an order in \( \mathcal{O} \) and it follows that the subgroups containing norm one elements are commensurable.

Assuming 3, notice that any Bianchi group contains the element \( \pm \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \) and therefore the quotient is not co-compact. Compactness is a commensurability invariant. Therefore, 3 implies 1.

\[ \square \]

Similarly, we have the following for Fuchsian groups.

**Theorem 2.** Let \( \Gamma \) be an arithmetic Fuchsian group commensurable with the derived Fuchsian group \( P\rho(\mathcal{O}^1) \), where \( \mathcal{O} \) is an order in the quaternion algebra \( Q \) defined over \( K \). Then the following are equivalent.

1. \( \Gamma \) is non-cocompact.
2. \( K = \mathbb{Q} \) and \( Q \cong M_2(\mathbb{K}) \)
3. \( \Gamma \) is commensurable with the Modular group, \( \text{PSL}_2(\mathbb{Z}). \)

**Example 7.1.** Consider the quaternion algebra

\[
Q = \left( \frac{-t, t^2 - 7}{\mathbb{Q}(t)} \right)
\]

where \( t \) is a root of \( x^3 - 7 \). The field \( \mathbb{Q}(t) \) has one real place, corresponding to the real root \( \sqrt[3]{7} \) and one complex place corresponding to the conjugate roots \( \omega \sqrt[3]{7} \) and \( \omega^2 \sqrt[3]{7} \) where \( \omega = (-1 + \sqrt{-3})/2 \) is a primitive third root of unity. Therefore \( Q \) is split at the complex place, but is ramified at the real place since \( -\sqrt[3]{7} \) and \( \sqrt[3]{7} - 7 \) are both negative. It follows that if \( \mathcal{O} \) is a maximal order in \( Q, P\rho(\mathcal{O}^1) \) is a finite co-volume derived Kleinian group. By Theorem 1 this is a co-compact group.

8. General Construction

The construction of the derived Fuchsian and Kleinian groups are special cases of a more general construction. Let \( a \) and \( b \) be non-negative integers, with at least one positive. The product \( \mathbb{H}^2 \times \mathbb{H}^3 \) carries a metric inherited from the metric on \( \mathbb{H}^2 \) and \( \mathbb{H}^3 \). It follows that the group

\[
[\text{PSL}_2(\mathbb{R})]^a \times [\text{PSL}_2(\mathbb{C})]^b
\]

is a subgroup of the group of orientation preserving isometries of \( \mathbb{H}^2 \times \mathbb{H}^3 \).

Let \( K \) be a number field with \( r_1 \) real places and \( r_2 \) complex places. Let \( Q \) be a quaternion algebra over \( K \). Let \( \sigma_1, \ldots, \sigma_l \) be the real places where \( Q \) is unramified, and \( \sigma_{l+1}, \ldots, \sigma_{r_1} \) be the real places where \( Q \) is ramified. Let \( \tau_1, \ldots, \tau_{r_2} \) be the complex places. Assume that there is some infinite place where \( Q \) is ramified. (This is called the *Eichler condition.* The quaternion algebras \( \left( \frac{-1,-1}{K} \right) \) and \( \left( \frac{\sqrt{-4} - 1}{Q(\sqrt{-2})} \right) \) do not satisfy the Eicher condition, for example.) Then for \( \ell = 1, \ldots l \)

\[
Q^{\sigma_{\ell}} \otimes_{\sigma_{\ell}(K)} \mathbb{R} \cong M_2(\mathbb{R})
\]

and for \( \ell = l + 1, \ldots r_1 \)

\[
Q^{\sigma_{\ell}} \otimes_{\sigma_{\ell}(K)} \mathbb{R} \cong \mathcal{H}
\]

and for \( \ell = 1, \ldots r_2 \)

\[
Q^{\sigma_{\ell}} \otimes_{\sigma_{\ell}(K)} \mathbb{C} \cong M_2(\mathbb{C}).
\]
Using the explicit maps in §3.3 this gives a map $\rho : \mathcal{Q} \to M_2(\mathbb{R})^l \times M_2(\mathbb{C})^{r_2}$. Choose a maximal order $\mathcal{O}$ in $\mathcal{Q}$ and take the norm one elements, $\mathcal{O}^1$ in $\mathcal{O}$. The restriction of $\rho$ is the map (which we will also call $\rho$)

$$\rho : \mathcal{O}^1 \to [\text{SL}_2(\mathbb{R})]^l \times [\text{SL}_2(\mathbb{C})]^{r_2}$$

defined in each coordinate by $q$ mapping to the image in $M_2(\mathbb{R})$ or $M_2(\mathbb{C})$ by the above. The fact that the image is full rank (finite co-volume) follows from the fact that the order $\mathcal{O}$ in $\mathcal{Q}$ was chosen to be full rank. It remains to address discreteness. This is similar to the Fuchsian case.

Consider a convergent sequence $\{q_n\}_{n=1}^{\infty}$ where $q_n = r_{1,n} + r_{2,n}i + r_{3,n}j + r_{4,n}k \in \mathcal{O}^1$ and $\rho(q_n) = (M_{n,1}, \ldots, M_{n,l+r_2}) \in [\text{SL}_2(\mathbb{R})]^l \times [\text{SL}_2(\mathbb{C})]^{r_2}$. By composition, we may assume that this sequence converges to the product of identity matrices. Since the map to matrices is defined by sending each $(\mathcal{O}^1)^{r_2}$ $(1 \leq \ell \leq l)$ to one $\text{SL}_2(\mathbb{R})$ in the product, and each $(\mathcal{O}^1)^{r_2}$ $(1 \leq \ell \leq r_2)$ to one $\text{SL}_2(\mathbb{C})$ in the product, we conclude that for each of these places, the image $M_{n,\ell} \in \text{SL}_2(\mathbb{R})$ or $\text{SL}_2(\mathbb{C})$ is converging to the identity matrix. That is, for all such embeddings $\psi$, we have

$$\psi(q_n) = \psi(r_{1,n}) + \psi(r_{2,n})i + \psi(r_{3,n})j + \psi(r_{4,n})k \to 1.$$ 

(These $i$, $j$, and $k$ correspond to the basis elements for the quaternion algebra $\mathcal{Q}^\psi$.) We conclude that

$$\psi(r_{1,n}) \to 1, \quad \psi(r_{2,n}), \psi(r_{3,n}), \psi(r_{4,n}) \to 0.$$ 

Therefore, for all split places, the conjugate of $r_{1,n}$ is a bounded distance from 1 and the conjugates of $r_{2,n}$, $r_{3,n}$ and $r_{4,n}$ are a bounded distance from 0.

Now, consider a ramified (real) place $\sigma$. The extension of scalars of $\mathcal{Q}^\sigma$ is isomorphic to $\mathcal{H}_1$. Under this identification, the elements of norm one in $\mathcal{Q}^\sigma$ map to $\mathcal{H}_1$, the norm one elements of the Hamiltonians. This set is compact by Lemma 4.1

We conclude that the group $P\rho(\mathcal{O}^1)$ is discrete by Lemma 4.2.

Example 8.1. Let $K$ be the splitting field of the biquadratic polynomial $p(x) = x^4 - 5x^2 + 4$. Then the roots of $p(x)$ can be determined by the quadratic formula and are

$$\pm \sqrt{\frac{5 \pm \sqrt{11}}{2}}.$$ 

This has two real roots, $\pm \sqrt{\frac{5 + \sqrt{11}}{2}}$ and two complex conjugate roots, $\pm \sqrt{\frac{5 - \sqrt{11}}{2}}$. Any quaternion algebra is split at the complex place.

The quaternion algebra $\mathcal{Q}_1 = \left( \frac{1,1}{K} \right) \cong M_2(K)$ and order $\mathcal{O} = M_2(\mathcal{O}_K)$ correspond to $\text{PSL}_2(\mathcal{O}_K)$ embedded in $[\text{PSL}_2(\mathbb{R})]^2 \times [\text{PSL}_2(\mathbb{C})]$.

Alternately, the quaternion algebra $\mathcal{Q}_2 = \left( \frac{-1,-1}{K} \right)$ is ramified at both real places. Therefore, if $\mathcal{O}$ is a maximal order, $P\rho(\mathcal{O}^1)$ is a discrete subgroup of $\text{PSL}_2(\mathbb{C})$. In fact, since $K$ is not a quadratic number field, we conclude that this group is co-compact.

Now, consider the quaternion algebra $\mathcal{Q}_3 = \left( \frac{\sqrt{11},-7}{K} \right)$. At the identity embedding, the extension of scalars gives $\left( \frac{\sqrt{11},-7}{R} \right)$. The automorphism corresponding to the other real place, $\sigma_2$, sends $\sqrt{11}$ to $-\sqrt{11}$. Therefore the extension
of scalars corresponding to this place is
\[
\begin{pmatrix}
\sigma(\sqrt{\Pi - 7}), \sigma(\sqrt{\Pi}) \\
\end{pmatrix}
\begin{pmatrix}
\mathbb{R} \\
\end{pmatrix} =
\begin{pmatrix}
-\sqrt{\Pi - 7}, -\sqrt{\Pi} \\
\end{pmatrix}
\begin{pmatrix}
\mathbb{R} \\
\end{pmatrix}.
\]

The quaternion algebra is ramified at \(\sigma_2\) and split at the identity, \(\sigma_1\). As a result, if \(\mathcal{O}\) is a maximal order in \(\mathbb{Q}_2\) then \(P_\rho(\mathcal{O}^1)\) is a co-compact, finite co-volume discrete subgroup of \(\text{PSL}_2(\mathbb{R}) \times \text{PSL}_2(\mathbb{C})\).

8.1. The groups \(\text{PSL}_2(\mathcal{O}_K)\). The simplest examples of this construction are the groups \(\text{PSL}_2(\mathcal{O}_K)\) which correspond to the order \(M_2(\mathcal{O}_K)\) in the quaternion algebra \(M_2(K)\). If \(K\) has \(r_1\) real places and \(r_2\) complex places then the extension by scalars corresponding to each place is split. We obtain the mapping
\[
\begin{pmatrix}
a & b \\
c & d \\
\end{pmatrix}
\rightarrow \prod_{\psi}
\begin{pmatrix}
\psi(a) & \psi(b) \\
\psi(c) & \psi(d) \\
\end{pmatrix}
\]
where the product is over all infinite places of \(K\).

For any number field \(K\) with \(r_1\) real places and \(r_2\) complex places, the quotient
\[
[\text{PSL}_2(\mathbb{R})]^{r_1} \times [\text{PSL}_2(\mathbb{C})]^{r_2} / \text{PSL}_2(\mathcal{O}_K)
\]
is not co-compact. This is evident as \(\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \text{PSL}_2(\mathcal{O}_K)\). The quotient has a finite number of finite volume topological ends, called cusps. Each cusp cross section is a Euclidean co-dimension one manifold. It is not difficult to show that the number of cusps of \(\text{PSL}_2(\mathcal{O}_K)\) equals the class number of \(\mathcal{O}_K\).

To see this, first notice that the cusps are equivalence classes of elements of \((K \cup \infty) \subset \mathbb{C}\) under the action of \(\text{PSL}_2(\mathcal{O}_K)\). (Consider \(K \cup \infty\) corresponding to the identity place of \(K\) in the product.) Two elements \(p_1 = \alpha_1/\beta_1\) and \(p_2 = \alpha_2/\beta_2\) are equivalent if there is a \(M \in \text{SL}_2(\mathcal{O}_K)\) such that \(M(p_1) = p_2\).

The ideals \((\alpha_1, \beta_1)\) and \((\alpha_2, \beta_2)\) are equivalent in the class group if there is a \(\gamma \in K\) such that
\[
(\alpha_1, \beta_1) = (\gamma)(\alpha_2, \beta_2),
\]
so \((\alpha_1, \beta_1) = (\gamma \alpha_2, \gamma \beta_2) = I\). The whole number ring is \(\mathcal{O}_K = II^{-1}\), and so \(1 = \alpha_i I^{-1} + \beta_i I^{-1}\). That is, there are elements \(s_i\) and \(t_i\) in \(I^{-1}\) such that
\[
\alpha_i s_i - \beta_i t_i = 1.
\]

It follows that with
\[
M_i = \begin{pmatrix}
\alpha_i & t_i \\
\beta_i & s_i \\
\end{pmatrix}
\]
\(M_i(\infty) = p_i\). The matrix \(\pm M_2 M_1^{-1} \in \text{PSL}_2(\mathcal{O}_K)\) and takes \(p_1\) to \(p_2\). Conversely, if the two ideals are in different elements of the class group no such matrix exists. (See [27].)

There are some striking differences between the groups \(\text{PSL}_2(\mathcal{O}_K)\) when \(K\) is neither \(\mathbb{Q}\) nor an imaginary quadratic number field and the modular group and Bianchi groups. This is a specific manifestation of the difference between higher rank arithmetic groups and lower rank groups. For these groups, this difference can be tied to the existence of infinitely many units in \(\mathcal{O}_K\); by Dirichlet’s unit Theorem, the rank of the unit group of \(\mathcal{O}_K\) is \(r_1 + r_2 - 1\). One such difference involves the subgroup structure of these groups. Let \(I\) be a non-zero ideal of \(\mathcal{O}_K\). The reduction modulo \(I\) map defines a map from \(\text{PSL}_2(\mathcal{O}_K)\) to the finite group
PSL$_2(\mathcal{O}_K/I)$. The kernel of this map is called the principal congruence subgroup of level $I$, and is denoted $\Gamma(I)$. These are finite index subgroups of PSL$_2(\mathcal{O}_K)$. A finite index subgroup of PSL$_2(\mathcal{O}_K)$ is called a congruence subgroup if it contains some principal congruence subgroup. The group PSL$_2(\mathcal{O}_K)$ is said to have the congruence subgroup property (CSP) if all finite index subgroups are congruence subgroups. Frick [10] and Pick [21] showed that there are finite index subgroups of the Modular group which are not congruence subgroups. Serre [25] showed that PSL$_2(\mathcal{O}_K)$ has the CSP precisely when $K$ is not $\mathbb{Q}$ or an imaginary quadratic. In fact, this difference between the subgroup structure of PSL$_2(\mathcal{O}_K)$ depending on whether $K$ has positive unit rank can be seen topologically by looking at minimally cusped quotients [20, 18, 19].

9. Lehmer’s Conjecture and Geodesics

9.1. Geodesics and Systoles. One natural way to measure a manifold is by the lengths of its geodesics. The length spectrum of a manifold is the collection of lengths of all closed geodesics, including multiplicities. For non-cocompact manifolds we consider only the lengths of non-boundary parallel curves as the length of a boundary parallel curve is not well-defined. In some sense, this is akin to studying a number field by its zeta function, which encodes the norms of all ideals. If $M$ is a hyperbolic 3-manifold one uses the set of complex lengths (complex numbers encoding lengths and rotations for loxodromic elements). Surprisingly, there are isospectral manifolds which are not isometric [28], similar to the existence of number fields with the same zeta function. For arithmetic hyperbolic 2- or 3-manifolds, isospectrality is known to imply commensurability [24].

For a compact Riemannian manifold the spectrum of the Laplacian consists of the eigenvalues of the Laplace operator. For hyperbolic surfaces, via the Selberg trace formula (see [13, 14]), this spectrum and the length spectrum encode the same data (see [29]). One conjecture in this direction is Selberg’s eigenvalue conjecture which states that the first non-zero eigenvalue of a principal congruence subgroup (the kernel of the modulo $n$ map) of the modular group is bounded by $1/4$ [24].

The smallest non-zero term in the length spectrum corresponds to the length of the shortest geodesic, the systole. The length of the systole is connected to the overall geometry of the manifold. Notably, Gromov [12] showed that in each dimension $n$ there is a universal constant $C_n$ such that for any Riemannian $n$-manifold $M$

$$\text{length}(\text{systole}(M)) \leq C_n \text{volume}(M).$$

For general hyperbolic 2-manifolds it is not difficult to see that there are hyperbolic surfaces where the length of the shortest geodesic gets arbitrarily small, by constructing bar bell surfaces, for example. In fact, one can do this for any genus. However, it is conjectured that this length is universally bounded away from zero for the arithmetic Fuchsian and Kleinian groups.

Conjecture 9.1 (Short Geodesic Conjecture). The length of any geodesic in an arithmetic hyperbolic 2- or 3-manifold is universally bounded away from zero.

It is not difficult to see that this is true for the non-cocompact groups. If $\Gamma$ is a non-compact arithmetic hyperbolic 2- or 3-manifold it is enough to bound the length of the systole of $\Gamma^{(2)} < \Gamma$ which is derived. Therefore $\Gamma^{(2)}$ is either a subgroup of the modular group or a Bianchi group. As outlined below, the length
of a geodesic corresponds to the Mahler measure of the trace. In this case the trace is an algebraic integer in \( \mathbb{Q} \) or an imaginary quadratic number field. Using Dobrowolski’s bound \( [8] \) (for example) these Mahler measures are bounded, and so is the systole length. One can obtain sharper results (see [16] Theorem 12.3.6) by direct computation and show, for example, that if \( \mathbb{H}^3/\Gamma \) is a cusped hyperbolic 3-manifold with a systole of length less that 0.431277313 then \( \Gamma \) is not arithmetic.

9.2. Lehmer’s Conjecture. Let \( \alpha \) be an algebraic number with minimal polynomial
\[
p(x) = a(x - r_1) \ldots (x - r_n).
\]
The Mahler measure of \( \alpha \) is
\[
M(\alpha) = \frac{1}{2\pi} \int_0^{2\pi} \log |p(e^{i\theta})| \, d\theta = |a| \prod_{i=1}^n \max\{1, |r_i|\}.
\]
As the Mahler measure is an invariant of the polynomial, we often refer to the Mahler measure of a polynomial in \( \mathbb{Z}[x] \) as the Mahler measure of any of its roots and we write \( M(p) \). It is elementary to see that the Mahler measure of any product of cyclotomic polynomials is one. Conversely, Kronecker showed that any monic polynomial in \( \mathbb{Z}[x] \) all of whose roots lie on or inside the unit circle must be a product of cyclotomics and factors of \( x \).

In 1933 Lehmer [15] asked whether there was a universal bound \( \mu > 1 \) such that if \( p(x) \in \mathbb{Z}[x] \) is not a product of cyclotomics, then \( M(p) > \mu \). This is often called Lehmer’s conjecture, or Lehmer’s question. The polynomial with the smallest known Mahler measure bigger than one was discovered by Lehmer. It is known as Lehmer’s polynomial and is
\[
l(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1.
\]
The Mahler measure of Lehmer’s polynomial is
\[
M(l) = 1.176280818 \ldots
\]
(In fact, one can construct many polynomials with this Mahler measure.) A strong version of Lehmer’s conjecture is that this is the smallest Mahler measure amongst polynomials in \( \mathbb{Z}[x] \) which are not products of cyclotomics and powers of \( x \).

There are bounds for the Mahler measure which depend on the degree of the polynomial (see the papers by Blanksby and Montgomery [3] and Dobrowolski [8]). So, if Lehmer’s conjecture is not true, then the degrees of the polynomials with small Mahler measure must increase. Additionally, Lehmer’s conjecture has been proven for certain special types of polynomials. Smyth [26] showed that Lehmer’s conjecture is true for non-reciprocal polynomials. Reciprocal polynomials are those whose coefficients read the same forwards as backwards; a polynomial is reciprocal when if \( r \) is a root then \( 1/r \) is also a root. Borwein, Dobrowolski, and Mossinghoff [6] showed that the conjecture holds for a large class of polynomials which includes the Littlewood polynomials (those with coefficients in \( \{-1, 1\} \)). (See also, [7], [3], and [2].)

We say that a monic irreducible polynomial \( p(x) \in \mathbb{Z}[x] \) is a Salem polynomial if all but two roots of \( p \) lie off the unit circle, and these roots are real numbers \( r \) and \( 1/r \). Additionally, if \( r > 1 \) is a root of a Salem polynomial, we call \( r \) a Salem number. For the purposes of this note, we will call a monic irreducible polynomial \( p(x) \in \mathbb{Z}[x] \) a complex Salem number if exactly four roots of \( p \) are off the unit circle.
and these roots are complex numbers of the form \( z, 1/z, \frac{1}{z}, \frac{1}{z} \). We will call the numbers \( z, \frac{1}{z}, \frac{1}{z}, \frac{1}{z} \) complex Salem numbers. The Salem conjecture asserts that the Mahler measure of any Salem polynomial is uniformly bounded away from 1. In some sense, this is the simplest case of Lehmer’s conjecture. A complex Salem conjecture can be formulated similarly.

9.3. Lengths and Mahler Measure. A geodesic in \( \mathbb{H}^2/\Gamma \) corresponds to a hyperbolic element \( \gamma \in \Gamma \) since the axis of a hyperbolic element in \( \Gamma \) projects to a geodesic in \( \mathbb{H}^2/\Gamma \), and every non-peripheral closed curve is freely homotopic to a unique closed geodesic corresponding to one of these axes. Up to conjugation,

\[
\gamma^{\pm 1} = \pm \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}
\]

with \( \lambda > 1 \) so that \( \pm \text{tr}(\gamma) = \lambda + \lambda^{-1} \). It is a straightforward application of the hyperbolic distance formula that the translation length of \( \gamma \), \( \text{length}(\gamma) \), is related to \( \lambda \) by

\[
\text{length}(\gamma) = 2 \log |\lambda|
\]

so that

\[
\cosh\left(\frac{1}{2} \text{length}(\gamma)\right) = \frac{1}{2} |\lambda + \lambda^{-1}|.
\]

It follows that the length of the geodesic is bounded away from zero if and only if the (absolute value of the) trace of \( \gamma \) is bounded away from two. The 3-dimensional case is similar, using complex length.

Now we establish a correspondence between short geodesics and the Salem conjecture, due to Neumann and Reid [17].

**Theorem 3.** The short geodesic conjecture for arithmetic hyperbolic 2-manifolds is equivalent to Salem’s conjecture. The short geodesic conjecture for arithmetic hyperbolic 3-manifolds is equivalent to the complex Salem conjecture.

We sketch a proof Theorem 3 in the Fuchsian case. We refer the reader to [16] for a detailed treatment, especially in the Kleinian case.

We reduce to the case where \( M = \mathbb{H}^2/\Gamma \) and \( \Gamma \) is derived, since if \( \Gamma_1 \) is arithmetic then \( \Gamma_1^{(2)} \) is a finite index subgroup of a derived group. First we show that lengths of geodesics correspond to Salem numbers.

**Claim 9.2.** Let \( \Gamma \) be a derived Fuchsian group, and let \( \gamma \in \Gamma \) be a hyperbolic element. Then \( \text{tr}(\gamma) = \lambda + \lambda^{-1} \) where \( \lambda > 1 \) is a Salem number.

**Proof.** (sketch) By construction, \( \Gamma = P\rho(\mathcal{O}^1) \) where \( \mathcal{O} \) is an order in the quaternion algebra \( \mathcal{Q} = \left( \frac{a,b}{K} \right) \) and \( K \) is a totally real number field and \( \mathcal{Q} \) is ramified at all non-identity (real) places. Let \( \gamma \in \Gamma \) with \( \text{tr}(\gamma) = \lambda + \lambda^{-1} \). Let 

\[
p(x) = x^2 - (\lambda + \lambda^{-1})x + 1.
\]

The element \( (\lambda + \lambda^{-1}) \in \mathcal{O}_K \) because \( |\lambda + \lambda^{-1}| = \pm \text{tr}(\gamma) \) and corresponds to \( \text{tr}(\alpha) \) for some element \( \alpha \in \mathcal{O} \) and therefore lies in \( \mathcal{O}_K \) as remarked on earlier. Moreover, \( \lambda^{-1} \) is a conjugate of \( \lambda \) since both roots of the polynomial \( p(x) \in \mathcal{O}_K[x] \). Let \( L \) denote the quadratic extension of \( K \) determined by \( p(x) \) so that \( \lambda, \lambda^{-1} \in L \).

Let \( \psi \) be a non-trivial Galois automorphism of \( K \); \( \psi \) extends to automorphisms of \( L \). The automorphisms of \( L \) corresponding to the identity place are the identity and the map that exchanges \( \lambda \) and \( \lambda^{-1} \). Since \( K \) is real and \( \lambda + \lambda^{-1} \in K \) we
conclude that $\lambda$ is either real or on the unit circle. But $\gamma$ is hyperbolic and so $|\text{tr}(\lambda + \lambda^{-1})| > 2$, ensuring that $\lambda$ is real and not on the unit circle.

If $\psi$ is a non-identity automorphism, then $\psi$ induces a map from $\mathbb{Q}$ to $\mathcal{H}$ and by restriction $\mathcal{O}^1$ maps into $\mathcal{H}^1$, so the trace of $\psi(\lambda + \lambda^{-1})$ must have absolute value less than two. Extending $\psi$ to $L$,

$$
\psi(\lambda + \lambda^{-1}) = [\psi(\lambda)] + [\psi(\lambda)]^{-1}.
$$

Since $K$ is totally real, this is in $\mathbb{R}$ so that either $\psi(\lambda)$ is real or $\psi(\lambda)$ is on the unit circle. If $\psi(\lambda)$ were real, then $|\psi(\lambda + \lambda^{-1})| = |\psi(\lambda) + \psi(\lambda)^{-1}| < 2$, is equivalent to $(\psi(\lambda) - 1)^2 < 0$, which is impossible. Therefore, $\psi(\lambda)$ is on the unit circle.

Consider the case when $\lambda_n$ is a Salem number corresponding to the geodesic $\gamma_n$. By the above discussion on lengths and traces, the following are equivalent: a sequence of Salem numbers $\{\lambda_n\}$ is bounded away from one, the Mahler measure of each term in $\{\lambda_n\}$ is bounded away from one, the sequence $\{\lambda_n + \lambda_n^{-1}\}$ is bounded away from two, the geodesic lengths $\{\text{length}(\gamma_n)\}$ are all bounded away from zero.

It suffices to show that any Salem number $\lambda$ corresponds to a hyperbolic element $\gamma$ in some arithmetic Fuchsian group.

**Claim 9.3.** Let $\lambda$ be a Salem number. Then there is a derived Fuchsian group $\Gamma$ and a hyperbolic element $\gamma \in \Gamma$ so that $|\text{tr}(\gamma)| = \lambda + \lambda^{-1}$.

**Proof.** (sketch) The only conjugate of $\lambda$ which lies off the unit circle is $\lambda^{-1}$. It follows that the field $\mathbb{Q}(\lambda + \lambda^{-1}) = K$ is totally real and $L = \mathbb{Q}(\lambda)$ is a quadratic extension of $K$. We want to construct a quaternion algebra over $K$ which is split at exactly one place. Moreover, we need to ensure that $\lambda + \lambda^{-1}$ appears as a trace of a norm one element.

By controlling the ramification set, we can construct a quaternion algebra $\mathbb{Q}$ over $K$, which is ramified at all non-identity real places of $K$, in which $L$ embeds. The element $\lambda \in L$ is an algebraic integer since $|\lambda + \lambda^{-1}| = |\text{tr}(\gamma)|$ is an algebraic integer and $\lambda$ satisfies $x^2 - (\lambda + \lambda^{-1})x + 1$. Moreover, the relative trace and norm are $\text{tr}_{K/L}(\lambda) = \lambda + \lambda^{-1} \in \mathcal{O}_K$ and $N_{K/L} = \lambda\lambda^{-1} = 1$. In the embedding $L \hookrightarrow \mathbb{Q}$ these correspond to the reduced norm and trace of an element $q$. It suffices to take a maximal order $\mathcal{O}$ containing $q$.

\[
\square
\]

**References**

   (56 #11952)
10. R. Fricke, über die substitutionsgruppen welche zu den aus dem legendreschen integralmodul gezogenen wurzeln gehören, Math Annalen 28 (1886), 99–111.