ONE-CUSPED CONGRUENCE SUBGROUPS OF $\mathrm{SO}(d, 1; \mathbb{Z})$

A Dissertation
Submitted to
the Temple University Graduate Board

---

in Partial Fulfillment
of the Requirements for the Degree of
DOCTOR OF PHILOSOPHY

---

by
Benjamin D. Choi
December 2022

ABSTRACT

The classical spherical and Euclidean geometries are easy to visualize and correspond to spaces with constant curvature 0 and +1 respectively. The geometry with constant curvature −1, hyperbolic geometry, is much more complex. A powerful theorem of Mostow and Prasad states that in all dimensions at least 3, the geometry of a finite-volume hyperbolic manifold (a space with local d-dimensional hyperbolic geometry) is determined by the manifold's fundamental group (a topological invariant of the manifold).

A *cusp* is a part of a finite-volume hyperbolic manifold that is infinite but has finite volume (cf. the surface of revolution of a tractrix has finite area but is infinite). All non-compact hyperbolic manifolds have cusps, but only finitely many of them. In the fundamental group of such a manifold, each cusp corresponds to a *cusp subgroup*, and each cusp subgroup is associated to a point on the boundary of $\mathbb{H}^d$, which can be identified with the $(d-1)$-sphere. It is known that there are many one-cusped two- and three-dimensional hyperbolic manifolds. This thesis studies restrictions on the existence of 1-cusped hyperbolic d-dimensional manifolds for $d \geq 3$.

Congruence subgroups belong to a special class of hyperbolic manifolds called *arithmetic manifolds*. Much is known about arithmetic hyperbolic 3-manifolds, but less is known about arithmetic hyperbolic manifolds of higher dimensions. An important infinite class of arithmetic d-manifolds is obtained using $\mathrm{SO}(n,1;\mathbb{Z})$, a subset of the integer matrices with determinant 1. This is known to produce 1-cusped examples for small d. Taking special congruence conditions modulo a fixed number, we obtain *congruence subgroups* of $\mathrm{SO}(n,1;\mathbb{Z})$ which also have cusps but possibly more than one. We ask what congruence subgroups with one cusp exist in $\mathrm{SO}(n,1;\mathbb{Z})$.

We consider the prime congruence level case, then generalize to arbitrary levels. Covering space theory implies a relation between the number of cusps and the image of a cusp in the mod p reduced group $\mathrm{SO}(d+1,p)$, an analogue of the classical rotation Lie group. We use the sizes of maximal subgroups of

groups $\mathrm{SO}(d+1,p)$, and the maximal subgroups' geometric actions on finite vector spaces, to bound the number of cusps from below.

Let $\Omega(d,1;\mathbb{Z})$ be the index 2 subgroup in $\mathrm{SO}(d,1;\mathbb{Z})$ that consists of all elements of $\mathrm{SO}(d,1;\mathbb{Z})$ with spinor norm $+1$. We show that for $d=5$ and $d \geq 7$ and all q not a power of 2, there is no 1-cusped level-q congruence subgroup of $\Omega(d,1;\mathbb{Z})$. For $d=4,6$ and all q not of the form 2^a3^b, there is no 1-cusped level-q congruence subgroup of $\Omega(d,1;\mathbb{Z})$.

ACKNOWLEDGEMENTS

I humbly express my deepest gratitude to my advisor and committee chair, Professor Matthew Stover, for his generous patience and feedback. Neither would this endeavor have been possible without my advising committee, who provided knowledge and expertise. I am also grateful to my schoolmates, in particular Khánh Lê and Rebekah Palmer, for moral support and being my "rubber ducks". I would be remiss not to mention my friends from outside of school, who provided me motivation which has been essential throughout this process.

TABLE OF CONTENTS

Page

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Fundamental groups of hyperbolic manifolds have attracted much attention, since they are exactly those manifolds that have constant curvature -1. Most frequently, one studies a hyperbolic manifold through the algebraic properties of its fundamental group. In particular, in all dimensions at least 3, the fundamental group determines the geometry of a finite-volume hyperbolic manifold, by Mostow-Prasad Rigidity [7] [14]. More generally one studies hyperbolic orbifolds, which for the purposes of this thesis can be defined as the quotient of a hyperbolic manifolds by a group of self-symmetries.

The modular surface $\mathbb{H}^2/\operatorname{PSL}_2(\mathbb{Z})$ is the quintessential arithmetic hyperbolic orbifold. It is noncompact, with one point at infinity, or cusp, which corresponds to $\mathbb{Q}\cup\infty$ in the boundary of $\mathbb{H}^2$ viewed as the upper half plane. With this motivation, the following is the definition of 'cusp' we will use throughout.

Definition 1.1. *A **cusp** is a topological end of a finite-volume hyperbolic manifold or orbifold. In the fundamental group Γ of such a manifold or orbifold, a **cusp subgroup** is the stabilizer in Γ of a parabolic fixed point on the boundary of $\mathbb{H}^d$.*

It is already known that there are many one-cusped two- and three-dimensional hyperbolic manifolds of finite volume. Petersen found that a Bianchi group has finitely many maximal 1-cusped congruence subgroups (a Bianchi group

is a subgroup of the isometry group of $\mathbb{H}^3$ of the form $\mathrm{PSL}_2(\mathcal{O}_K)$ for K a quadratic number field and $\mathcal{O}_K$ the ring of algebraic integers of K) [10]. However, a Bianchi group has infinitely many 1-cusped noncongruence subgroups; see the introduction to [12] for specific examples.

Murty and Petersen found that if $K/\mathbb{Q}$ is Galois with unit rank greater than 3, then there are only finitely many maximal one-cusped congruence subgroups of the Bianchi groups [8] . (If a Bianchi group is higher-unit-rank, then it acts on a product of a power of $\mathbb{H}^2$ and a power of $\mathbb{H}^3$, not just $\mathbb{H}^3$ as in the unit-rank-1 case.) Our results are somewhat analogous, but we consider the prime level congruence subgroups of $\mathrm{SO}(d,1;\mathbb{Z})$ case for $d > 3$.

Define $\Omega(d,1;\mathbb{Z}) \leq \Gamma = \mathrm{SO}(d,1;\mathbb{Z})$ to be the image of $\mathrm{Spin}(d,1;\mathbb{Z})$ under the universal cover $\mathrm{Spin}(d,1;\mathbb{R}) \to \mathrm{SO}(d,1;\mathbb{R})$ (which is two-to-one, since $\pi_1(\mathrm{SO}(d,1;\mathbb{R})) = \pi_1(\mathrm{SO}(d;\mathbb{R})) \cong \mathbb{Z}/2\mathbb{Z}$).

Definition 1.2. *For $N \in \mathbb{Z}_{\geq 1}$, the **principal congruence subgroup of level N in Γ**, denoted $\Gamma(N)$, is the kernel of the mod N reduction map*

$$\mathrm{SO}(d,1;\mathbb{Z}) \to \mathrm{SO}(d,1;\mathbb{Z}/n\mathbb{Z}).$$

*The **principal congruence subgroup of level N in $\Omega(d,1;\mathbb{Z})$** is*

$$\Omega(d,1;\mathbb{Z})(N) = \Omega(d,1;\mathbb{Z}) \cap \Gamma(N).$$

Definition 1.3. *A **congruence subgroup in Γ** is a (proper) subgroup H of Γ that contains $\Gamma(N)$ for some $N \in \mathbb{Z}_{\geq 1}$. The **level** of a congruence subgroup H is the smallest N such that H contains $\Gamma(N)$.*

Much is already known about arithmetic hyperbolic 3-manifolds with one cusp. The fundamental group of the complement of the figure-eight knot in S^3 injects into $\mathrm{PSL}_2(\mathcal{O}_3)$ as an index 12 subgroup containing $\Gamma(4)$ [11]. The fundamental group of the sister of the figure-eight knot complement, a knot in the lens space $L(5,1)$, injects into $\mathrm{PSL}_2(\mathcal{O}_3)$ as an index 12 subgroup containing $\Gamma(2)$ [11]. Reid [16] has shown that the figure-eight knot complement is the only arithmetic knot complement in S^3. If $d = 2, 7, 11, 19, 43, 67,$ or

163 there are infinitely many maximal one-cusped subgroups of $\mathrm{PSL}_2(O_d)$, as there is a surjection onto $\mathbb{Z}$ with a parabolic element generating the image. In particular, if $d = 1$ or $d = 3$ there are infinitely many one-cusped subgroups, but only finitely many 1-cusped congruence subgroups.

In contrast, little is known about arithmetic hyperbolic manifolds of dimension 4 or higher. The isometry group of d-dimensional hyperbolic space $\mathbb{H}^d$ is $\mathrm{SO}(d,1;\mathbb{R})$, the set of nonsingular matrices that preserve the form $x_0x_d + x_1^2 + \cdots + x_{d-1}^2$. $\mathbb{H}^d$ can be thought of as the level set of $x_0x_d + x_1^2 + \cdots + x_{d-1}^2$ at -1 where $x_0 > 0$. The natural analogue to $\mathrm{PSL}_2(\mathbb{Z})$ is $\mathrm{SO}(d,1;\mathbb{Z})$; the group $\mathrm{SO}(2,1;\mathbb{Z})$ is commensurable with the modular group $\mathrm{PSL}_2(\mathbb{Z})$ and $\mathrm{SO}(3,1;\mathbb{Z})$ is commensurable with the Bianchi group $\mathrm{PSL}_2(\mathbb{Z}[i])$. We will investigate the possible existence of one-cusped congruence subgroups in these higher-dimensional arithmetic lattices.

Let $\Omega(d,1;\mathbb{Z})$ be the index 2 subgroup in $\mathrm{SO}(d,1;\mathbb{Z})$ that consists of all elements of $\mathrm{SO}(d,1;\mathbb{Z})$ with spinor norm $+1$. Our main result is:

Theorem 1.1. *1. Let $d = 5$ or $d \geq 7$. For all odd q, there is no 1-cusped level-q congruence subgroup of $\Omega(d,1;\mathbb{Z})$, the image of $\mathrm{Spin}(d,1;\mathbb{Z})$ under the double cover $\mathrm{Spin}(d,1;\mathbb{R}) \to \mathrm{SO}(d,1;\mathbb{R})$.*

2. Let $d \geq 4$. For all odd q not a power of 3, there is no 1-cusped level-q congruence subgroup of $\Omega(d,1;\mathbb{Z})$, the image of $\mathrm{Spin}(d,1;\mathbb{Z})$ under the double cover $\mathrm{Spin}(d,1;\mathbb{R}) \to \mathrm{SO}(d,1;\mathbb{R})$.

The theorem will be proven as follows: First we carefully reduce to the composite level q case to the prime level p case. Then we study the group action of $\Omega(d,1;\mathbb{Z})$ on the reduced vector space $\mathbb{F}_p^{d+1}$. Specifically, cusps of H/Γ correspond one-to-one to pairs $(\pm v_1, B^{\pm})$ where:

1. v_1 is an isotropic vector
2. $B^{\pm} = (\pm S_{n-2})^1(w_2, ..., w_{n-1})$ where $(w_2, ..., w_{n-1})$ is a positively oriented, orthonormal basis of the space $(v_1)^{\perp}/(\mathbb{F}_p v_1)$. Here S_{n-2} refers to the

group of permutation matrices acting on the vector space spanned by $w_2, ..., w_{n-1}$, $\pm$ is a constant multiplication by ± 1, and the superscript 1 refers to taking the subset with determinant 1.

A one-cusped subgroup of $\Omega(d, 1; \mathbb{Z})$ has to map to a subgroup of $\Omega(d + 1; \mathbb{Z})$. Note that if a maximal subgroup H does not act transitively on pairs $(\pm v_1, B^{\pm})$, none of its subgroups can. The maximal subgroups H fall into several classes, as presented in [2]. For most maximal subgroups, it will suffice to just consider the action on pairs $\{\pm v\}$ where v is an isotropic vector. Only in one case, namely the maximal subgroup $G_2(p) \subseteq \mathrm{SO}(d, 1; \mathbb{Z})$ in dimensions 6 and 7, do we need to consider the full information given by the pairs. Often we count an orbit of a group action by using Orbit-Stabilizer Theorem, and compare that to the known number of isotropic vectors, or number of vector-baiss pairs. When this counting does not suffice to rule out a maximal subgroup, we consider the geometric structure of the group action itself, i.e. what structure on the vector space the maximal group preserves.

In Chapter 2 we recall background information on hyperbolic manifolds, and present some known results about arithmetic hyperbolic manifolds; we also define our notation and study what the action of Γ on cusps corresponds to in the $\mathbb{F}_p$-vector space, for prime level p. In Chapter 3 we eliminate most prime level cases using the proof strategy summarized above. In Chapter 4 we reduce the composite level case to the prime level case (this part was done in collaboration with Matthew Stover). In Chapter 5 we enumerate some examples of one-cusped subgroups we have found using a computer. We give the full proof of our result by examining all the relevant cases.

CHAPTER 2

BACKGROUND

Hyperbolic space $\mathbb{H}^d$ is the simply connected, complete d-dimensional Riemannian manifold with constant curvature -1. Hyperbolic geometry is one of the most actively studied geometries. For example it is common for Coxeter groups to act on hyperbolic space (e.g. giving symmetry groups of tessellations of $\mathbb{H}^d$), and generalizations of hyperbolic Coxeter groups are important objects in geometric group theory.

In general, orientable hyperbolic manifolds can be written as the quotient of $\mathbb{H}^d$ by a *lattice*, a discrete subgroup of $\mathrm{SO}(d,1;\mathbb{R})$. Of these, a certain class of groups called arithmetic groups (corresponding to arithmetic hyperbolic manifolds) are easier to study because it is computationally feasible to search over them, as there are only finitely many arithmetic manifolds with volume below a given bound [1]. $\mathrm{SO}(d,1;\mathbb{Z})$ is the canonical example of an arithmetic group; when $d = 2$ this is commensurable with $\mathrm{PSL}(2;\mathbb{Z})$. Moreover, for $d \leq 18$, $\mathrm{SO}(d,1;\mathbb{Z})$ are reflection groups and their Coxeter diagrams are given in [13].

The following can be deduced from [17] and the computations in Section 9 of [6]. Thus we can assume that $d \leq 8$ for the present investigation.

Proposition 2.1. $\mathrm{SO}(d,1;\mathbb{Z})$ *is one-cusped only for* $d \leq 8$. *Thus the image* $\Omega(d,1;\mathbb{Z})$ *of* $\mathrm{Spin}(d,1;\mathbb{Z})$ *in* $\mathrm{SO}(d,1;\mathbb{Z})$ *can only be one-cusped for* $d \leq 8$.

2.1 Notation

This section states the notation we will use, as well as some general facts about hyperbolic geometry. Readers may refer to [15] for more information.

Throughout, unless stated otherwise we will use d for the dimension of the arithmetic hyperbolic manifold and $n = d + 1$. We denote $G = \mathrm{SO}(Q; \mathbb{R})$ for the quadratic form

$$Q = Q_n = x_1 x_n + x_2^2 + \cdots + x_{n-1}^2$$

over $\mathbb{R}$. As stated, $\mathbb{H}^d$ can be understood using the hyperboloid model, where the hyperboloid is one component of the level set

$$Q(x_1, ..., x_n) = x_1 x_n + x_2^2 + \cdots + x_{n-1}^2 = -1.$$

We use $\Gamma = \mathrm{SO}(Q; \mathbb{Z})$, which is isomorphic to $\mathrm{SO}(d, 1; \mathbb{Z})$ which corresponds to the quadratic form $x_1^2 + \cdots x_{d-1}^2 - x_d^2$. A point in the boundary $\partial\mathbb{H}^d$ can be seen as the subspace generated by a Q-isotropic vector in $\mathbb{R}^n$, i.e. a vector v such that $Q(v) = 0$. This isotropic vector will be asymptotic to the hyperboloid. We define ∞ as the subspace $\mathbb{R}e_1$ and $\Delta = \mathrm{Stab}_\Gamma(\infty)$. We denote by $\Omega(d, 1; \mathbb{Z})$ the image of $\mathrm{Spin}(d, 1; \mathbb{Z})$ under the double cover $\mathrm{Spin}(d, 1; \mathbb{R}) \to \mathrm{SO}(d, 1; \mathbb{R})$, and we denote with G_p the image of $\mathrm{SO}(n, 1; \mathbb{Z})$ under the reduction map $r_p : \Gamma \to G(\mathbb{F}_p)$ given by reducing matrix entries mod p. Then the principal congruence subgroup $\Gamma(p)$ is the kernel of r_p. We use Δ_p for $r_p(\Delta)$. We also use H for a subgroup of G which we wish to focus on, usually the image of a putative 1-cusped subgroup in Γ.

We use $N^Q(n, p)$ for the number of isotropic vectors in $\mathbb{F}_p^n$ under the quadratic form Q.

We use $\mathrm{Std}(n)$ for the n-dimensional quadratic space with the standard quadratic form $x_1^2 + \cdots + x_n^2$, and $\mathrm{Hyp}(2)$ for the 2-dimensional quadratic space with the quadratic form $x_1 x_2$. By abuse of notation we will sometimes conflate quadratic spaces with their corresponding quadratic forms.

2.2 The action of $\mathrm{SO}(d,1;\mathbb{Z})$ on cusps

Lemma 2.1. *The stabilizer $\Delta \subseteq \Gamma$ of ∞ consists of all matrices of the form*

$$\begin{bmatrix} \epsilon & * & * \\ 0 & B & v \\ 0 & 0 & \epsilon \end{bmatrix}$$

where $\epsilon \in \{+1,-1\}$, $B \in \mathrm{SO}(d-1,\mathbb{Z})$ is an integral isometry of the standard quadratic form, and $v \in \mathbb{Z}^{d-1}$. The remaining values are uniquely determined by the triple (B,v,ϵ).

Proof. Direct calculation with the $\mathbb{Z}$-equivalent form $x_0x_n + \sum_i x_i^2$. We write the matrix M_Q corresponding to the quadratic form Q and deduce what an element $A \in \Delta$ has to look like by using $AM_QA^T = M_Q$ and constraining entries of A. □

The following proposition will follow from Lemma 2.3 below.

Proposition 2.2 (Preliminary proposition)**.** *If $\Gamma = \mathrm{SO}(d,1;\mathbb{Z})$ and $\Delta = \mathrm{Stab}_\Gamma(\pm e_1)$ (thus stabilizing $\infty \in \partial\mathbb{H}^d$), then the image of Δ under the reduction map $r_p : \mathrm{SO}(d,1;\mathbb{Z}) \to \mathrm{SO}(n;\mathbb{F}_p)$ is a strict subset of $\mathrm{Stab}_{G_p}(\pm e_1)$, now considering $e_1 \in \mathbb{F}_p^n$. $\mathrm{Stab}_{G_p}(\pm e_1)$ is in turn contained in $\mathrm{Stab}_{G_p}(\mathbb{F}_p e_1)$, the stabilizer of an isotropic line in $\mathbb{F}_p^n$, which can be viewed as stabilizing a cusp of the principal congruence cover corresponding to $\Gamma(p)$ under its action by deck transformations on $\mathbb{H}^d/\Gamma(p)$. The image $r_p(\Delta)$ is a stabilizer of pairs $(\pm v, B_{v^\perp})$ where v is an isotropic vector and B is a positively oriented orthonormal basis of $v^\perp/\mathbb{F}_p v$.*

Lemma 2.2. *Cusps of $\mathbb{H}^d/\Gamma(p)$ are in one-to-one correspondence with cosets of Δ_p in G_p.*

Proof. Cusps of $\mathbb{H}^d/\Gamma(p)$ are in one-to-one correspondence with $\Gamma(p)$-orbits of isotropic lines in $\mathbb{Q}^{d+1}$. The isotropic line $\ell_0 = \mathbb{Q}e_1$ has stabilizer Δ in Γ.

Since Γ acts transitively, choose $\ell_1 = \gamma_1(\ell_0)$ and $\ell_2 = \gamma_2(\ell_0)$ isotropic lines.

Suppose ℓ_1 and ℓ_2 are in the same $\Gamma(p)$-orbit. Then there exists $\alpha \in \Gamma(p)$ such that $\alpha(\ell_2) = \ell_1$, so $\gamma_1^{-1}\alpha\gamma_2 \in \Delta$. Then $r_p(\gamma_1^{-1}\alpha\gamma_2) = r_p(\gamma_1) \in \Delta_p$, since $r_p(\alpha) = I$, so $r_p(\gamma_2) \in r_p(\gamma_1)\Delta_p$. Thus r_p induces a well-defined map

$$c_p : \{\text{cusps of } \mathbb{H}^d/\Gamma(p)\} \to \{\text{coset representatives of } \Delta_p \text{ in } G_p\}.$$

Since r_p is surjective, so is c_p. To check that c_p is injective, suppose that $r_p(\gamma_2) = r_p(\gamma_1)r_p(\delta)$ for some $\delta \in \Delta$. So there exists $\alpha \in \Gamma(p)$ such that $\gamma_2 = \alpha\gamma_1\delta$, so $\gamma_2(\ell_0) = \alpha\gamma_1(\ell_0)$. Hence the isotropic line associated with γ_2 is in the same $\Gamma(p)$-orbit as in the isotropic line associated with γ_1, showing that c_p is injective. □

Lemma 2.3. *If p is an odd prime, cusps of $\mathbb{H}^d/\Gamma(p)$ are in one-to-one correspondence with pairs $\{\pm v_1, B^{\pm}\}$ where:*

1. *v_1 is an isotropic vector*
2. *$B^{\pm} = (\pm S_{n-2})^1(w_2, ..., w_{n-1})$ where $(w_2, ..., w_{n-1})$ is a positively oriented, orthonormal basis of the space $(v_1)^{\perp}/(\mathbb{F}_p v_1)$. Here S_{n-2} refers to the group of permutation matrices acting on the vector space spanned by $w_2, ..., w_{n-1}$, $\pm$ is a constant multiplication by ± 1, and the superscript 1 refers to taking the subset with determinant 1.*

Proof. This lemma will follow from Lemma 2.2 once we define an action on pairs of this form and prove that Δ_p is the stabilizer of a well-chosen pair.

First, note that the standard basis for $\mathbb{F}_p^{n-1}$, $\{e_1, ..., e_{n-1}\}$, defines such a pair by $(\pm e_1, (\pm S_n)^1(e_2, ..., e_{n-1}))$, since $\text{span}(e_2, ..., e_{n-1}) \subseteq e_1^{\perp}$ and hence the image of $\{e_2, ..., e_{n-1}\}$ determines an orthonormal basis of $e_1^{\perp}/(\mathbb{F}_p e_1)$.

Call $(\pm e_1, (\pm S_{n-2})^1(e_2, ..., e_{n-1}))$ the *standard pair*. We now show that Δ_p is the stabilizer in G_p of the standard pair. By an analogue to Lemma 2.1, elements of Δ_p are of the form given in Lemma 3.1. Elements of $\text{SO}(n-2;\mathbb{Z})$ act on $\{e_2, ..., e_{n-1}\}$ precisely as $(\pm S_{n-2})^1$ over both $\mathbb{Z}$ and $\mathbb{F}_p$ since $p \neq 2$. Similarly, if an element of G_p that stabilizes $e_1^{\perp}$ acts on $e_1^{\perp}/\mathbb{F}_p e_1$ by the middle $(n-2) \times (n-2)$ block of its matrix representative, then Δ_p stabilizes the

standard pair. Conversely, an element of the stabilizer of the standard pair has the form

$$\begin{bmatrix} \epsilon & * & * \\ 0 & B & v \\ 0 & 0 & \epsilon \end{bmatrix}$$

where $\epsilon \in \{\pm 1\}$, $B \in \pm S^1_{n-2}$, $v \in \mathbb{F}_p^{n-2}$ and $*$ is determined by the other choices. This is precisely Δ_p. Every choice of v is possible: There is a matrix in Δ of the form

$$\begin{bmatrix} \epsilon & -v^T B & |v|^2/2 \\ 0 & B & v \\ 0 & 0 & \epsilon \end{bmatrix}$$

assuming $|v|^2 \in \mathbb{Z}$ is even; if $|v|^2$ is odd we use $(1+p)v$ instead of v (note p is odd). Hence Δ_p is the stabilizer we seek.

It remains to show that G_p is transitive on pairs. Given a pair

$$\{\pm v, (\pm S_{n-2})^1(w_1, ..., w_{n-1})\}$$

for lifts v_i of w_i to $v_1^\perp$, and let v_n be the unique solution to the system $q(v,v) = 1$, $q(v_i, v) = 0, i \neq 1$ of linear equations. Let g be the matrix with columns $v_1, ..., v_n$. Then by construction g takes the standard pair to this pair, and $\pm gQg$ equals $[q(v_i, v_j)] = Q$, by hypothesis. Thus $g \in G_p$. □

This next corollary follows from Proposition 2.2 by the orbit-stabilizer theorem.

Corollary 2.1. *The orbit for the action on $\mathbb{H}^d/\Gamma(p)$ by deck transformations of the image $H \subseteq G_p$ of any one-cusped level-p congruence subgroup Γ_H must have size equal to $|G_p : \Delta_p|$. In particular, the number of cusps in the cover corresponding to $\Gamma(p)$ is equal to the index $|G_p : \Delta_p|$.*

The following preposition will be used to rule out many subgroups of Γ from being one-cusped, by using the subgroup's image in $G(\mathbb{F}_p)$.

Proposition 2.3 (Organizing proposition)**.** *If $H \leq G(\mathbb{F}_p)$ is a maximal subgroup and H preserves a subspace $W \subseteq \mathbb{F}_p^n$ such that W and $\mathbb{F}_p^n \setminus W$ both contain a nonzero isotropic vector, then $L\backslash\mathbb{H}^{n-1}$ has > 1 cusp for all finite index subgroups $L \leq \Gamma$ such that $r_p(L) \leq H$.*

Proof. A cusp of the manifold for the congruence subgroup $\Gamma(p)$ corresponds to a $\Gamma(p)$-orbit of a rational point at infinity of $\mathbb{H}^d$. This action is equivariant with the action of $G(\mathbb{F}_p)$ on the projective space of W (W modulo $\mathbb{F}_p$-scalar multiplication), via reduction modulo p. But since $H(W) \subseteq W$, there is no element $h \in H$ that takes the isotropic line $w\mathbb{F}_p \subseteq W$ to the isotropic line $w'\mathbb{F}_p \subseteq \mathbb{F}_p^n \setminus W$. The same must hold for any subgroup $L' \subseteq H$. So the manifold in question must have more than one cusp by Lemma 2.3 □

CHAPTER 3

THE PRIME LEVEL CASE

Lemma 3.1. *The size of the stabilizer Δ_p of an isotropic vector in $\mathrm{SO}(n,p)$ is*

$$2p^{n-2}|\,\mathrm{SO}(n-2,p)|$$

where $\mathrm{SO}(n-2,p)$ is the special orthogonal group for the standard dot product. Of these, $p^{n-2}|\,\mathrm{SO}(n-2,\mathbb{Z})| = p^{n-2}2^{n-3}(n-2)!$ are in the image of the cusp subgroup in $\mathrm{SO}(n,p)$.

Proof. This is a direct count, using the matrix form

$$\begin{bmatrix} x & * & * \\ 0 & B & v \\ 0 & 0 & x^{-1} \end{bmatrix}$$

for elements of the cusp stabilizer, for $x \in \mathbb{F}_p^\times$, $v \in \mathbb{F}_p^{n-2}$, $B \in \mathrm{SO}(n-2,p)$, and where the other elements are determined uniquely by x, v, and B, as in the proof of 2.3. □

The following is taken from [2].

Proposition 3.1. *For odd n and for all $p > 2$, there is only one class of quadratic form on $\mathbb{F}_p^n$, and we have the formula*

$$|\Omega(n,p)| = \frac{1}{2}p^{(n-1)^2/4}(p^2-1)(p^4-1)\cdots(p^{n-1}-1).$$

For even n, there are two equivalence classes of quadratic forms, denoted $+$ and $-$, and the corresponding order of the group of special isometries of spinor norm $+1$ is

$$|\Omega^{\pm}(n,p)| = \frac{1}{2}p^{n(n-2)/4}(p^{n/2} \mp 1)(p^2-1)(p^4-1)\cdots(p^{n-2}-1).$$

Here Ω^+ is the subgroup of $\mathrm{SO}(\mathrm{Hyp}(2)^{n/2})$ with spinor norm $+1$ and Ω^- is the subgroup of $\mathrm{SO}(\mathrm{Hyp}(2)^{n/2-1} \oplus \mathrm{Std}(2))$ with spinor norm $+1$.

Lemma 3.2. *There are two equivalence classes of quadratic forms Q in dimension 2: hyperbolic (equiv. to $2xy$) and anisotropic (equiv. to x^2+y^2). The cases split depending on $p \bmod 4$: if $p \equiv 1 \bmod 4$, $\mathrm{Std}(2)$ is equivalent to $\mathrm{Hyp}(2)$; if $p \equiv 3 \bmod 4$, then $\mathrm{Std}(2)$ is not equivalent to $\mathrm{Hyp}(2)$.*

Proof. If $p \equiv 1 \bmod 4$ then x^2+y^2 can be rewritten as $(x+by)(x-by)$ where b is a square root of -1 in $\mathbb{F}_p$. After change of basis $X = x+by$, $Y = x-by$ the quadratic form $\mathrm{Std}(2)$ becomes XY.

Conversely, if $\mathrm{Std}(2)$ and $\mathrm{Hyp}(2)$ are equivalent then $\mathbb{F}_p$ must contain a square root of -1, thus $p \equiv 1 \bmod 4$. Thus $\mathrm{Std}(2)$ and $\mathrm{Hyp}(2)$ are not equivalent when $p \equiv 3 \bmod 4$. □

Lemma 3.3. *The standard quadratic form for $n \equiv 2 \bmod 4$ is equivalent to $\mathrm{Hyp}(2) \oplus \cdots \oplus \mathrm{Hyp}(2) \oplus \mathrm{Std}(2)$ if $p \equiv 1 \bmod 4$ and $\mathrm{Hyp}(2) \oplus \cdots \oplus \mathrm{Hyp}(2) \oplus \mathrm{Hyp}(2)$ if $p \equiv 3 \bmod 4$. For $n \equiv 0 \bmod 4$ the standard quadratic form is always equivalent to $\mathrm{Hyp}(2) \oplus \cdots \oplus \mathrm{Hyp}(2)$.*

Proof. The $p \equiv 1 \bmod 4$ case is immediate from Lemma 1.0.3.

The $p \equiv 3 \bmod 4$ case can be proven by induction with Witt's cancellation theorem.

For the base case, $\mathrm{Std}(2)$ is not equivalent to $\mathrm{Hyp}(2)$ because $\mathrm{Hyp}(2)$ is isotropic unlike $\mathrm{Std}(2)$. For the induction step, if $\mathrm{Std}(2) \oplus \mathrm{Std}(2) = \mathrm{Hyp}(2) \oplus \mathrm{Std}(2)$, by Witt's cancellation theorem $\mathrm{Std}(2) = \mathrm{Hyp}(2)$, a contradiction. Note that $\mathrm{Hyp}(2) \oplus \mathrm{Hyp}(2)$ is also not equivalent to $\mathrm{Hyp}(2) \oplus \mathrm{Std}(2)$, also by Witt's cancellation theorem. Since there are only two equivavlence classes

of nondegenerate quadratic forms, it must be the case that $\mathrm{Std}(2) \oplus \mathrm{Std}(2) = \mathrm{Hyp}(2) \oplus \mathrm{Hyp}(2)$. □

Corollary 3.1. *The standard quadratic form for even n corresponds to*

$$\begin{cases} \Omega^+ & n \equiv 0 \bmod 4 \\ \Omega^- & n \equiv 2 \bmod 4 \text{ and } p \equiv 3 \bmod 4 \\ \Omega^+ & n \equiv 2 \bmod 4 \text{ and } p \equiv 1 \bmod 4. \end{cases}$$

Proof. By Lemma 3.3 and the definition of $\Omega^{\pm}$ in Proposition 3.1. □

Proposition 3.2. *Consider the quadratic form $Q = x_1x_n + x_2^2 + \cdots + x_{n-1}^2$.*

- *for n odd, $\Omega(Q,p)$ is isomorphic to Ω.*
- *for $n \equiv 2 \bmod 4$, $\Omega(Q,p)$ is isomorphic to Ω^+.*
- *for $n \equiv 0 \bmod 4$,*
  - *if $p = 1 \bmod 4$, $\Omega(Q,p)$ is isomorphic to Ω^+.*
  - *if $p = 3 \bmod 4$, $\Omega(Q,p)$ is isomorphic to Ω^-.*

Proof. Q is equivalent to the direct sum of $\mathrm{Hyp}(2)$ and the standard dot product over $\mathbb{F}_p^{n-2}$. □

The following fact will be useful for eliminating possibilities for H.

Lemma 3.4. *If H is an image in G_p of a 1-cusped subgroup of $\Omega(d,1;\mathbb{Z})$, and $\widetilde{\Delta}_p$ is the image in $\Omega(Q,p)$ of $\Delta \cap \Omega(d,1;\mathbb{Z})$, then $\frac{1}{2}N^Q(n,p)$ divides*

$$\frac{|H|}{|H \cap \widetilde{\Delta}_p|} = \frac{|G_p|}{|\widetilde{\Delta}_p|}.$$

In particular, $\frac{1}{2}N^Q(n,p)$ divides $|H|$.

Proof. By the Orbit-Stabilizer Theorem on the action on isotropic lines. □

We note that it suffices to show that all maximal subgroups of $\Omega(n;p)$ are not transitive on cusps. Maximal subgroups of $\Omega(n;p)$ fall into several classes [2], which we will consider in the following case-by-case analysis. We assume that $5 \leq n \leq 9$, so below we let $p \geq 11$ (so that p does not divide $n!$, which simplifies computing the exponent of p that divides $N^Q(n,p)$). For now, we are only considering the subgroups present in groups of all dimensions. We will call these subgroups "nonexceptional".

Lemma 3.5. *Assume $p \geq 11$. Then*

$$N^Q(n,p) = \begin{cases} (p^{n-1}-1) & n \text{ odd} \\ (p^{n/2}-1)(p^{n/2-1}+1) & n \equiv 2 \bmod 4 \\ (p^{n/2}-1)(p^{n/2-1}+1) & n \equiv 0 \bmod 4 \text{ and } p \equiv 1 \bmod 4 \\ (p^{n/2}+1)(p^{n/2-1}-1) & n \equiv 0 \bmod 4 \text{ and } p \equiv 3 \bmod 4. \end{cases}$$

In particular, p does not divide $N^Q(n,p)$.

Proof. By direct computation using the orders of $\Omega(Q,p)$ and the order of the G_p-stabilizer of $\mathbb{F}_p$-isotropic vector from Lemma 3.1. □

3.1 $\mathcal{C}_1$: Reducible subgroups

The class $\mathcal{C}_1$ (in G_p) are the groups that stabilize a totally isotropic subspace W (with $1 \leq \dim W \leq n/2$, or $1 \leq \dim W \leq n/2-1$ in case Ω^-), or both a nondegenerate subspace W (with $1 \leq \dim W \leq n/2$) and its orthogonal complement U. In the case of finite classical groups of class **O**, stabilizers of the second kind are in essence of the form $\mathrm{O}^{\epsilon_1}_m(q) \times \mathrm{O}^{\epsilon_2}_{n-m}(q)$. See Table 2.3 of [2]. If we show that at least one of these spaces stabilized by the maximal subgroup contains some, but not all, of the isotropic vectors (for the quadratic form in question), it would follow that the action on pairs $\pm v$ for v an isotropic vector is not transitive.

First, suppose W is totally isotropic of dimension $1 \leq j \leq \lfloor n/2 \rfloor$. Then it contains $p^j - 1$ isotropic vectors. Since $x^j - 1$ is smaller than x^{n-1}, $(x^{n/2} -$

$1)(x^{n/2-2}+1)$ and $(x^{n/2}+1)(x^{n/2-2}-1)$ for all $x \geq 1$, Lemma 3.5 implies that W does not contain all isotropic vectors in $\mathbb{F}_p^n$. Therefore the maximal subgroup of G_p stabilizing W cannot act tarnsitively on pairs $\{\pm v\}$ for $v \in \mathbb{F}_p^n$ isotropic, hence it cannot determine a 1-cusped subgroup of $\mathrm{SO}(n,1;\mathbb{Z})$.

Now suppose W is nondegenerate and $\mathbb{F}_p^n = W \oplus U$. Any decomposition $W \oplus U$ must have at least one of W and U with dimension ≥ 3 when $n \geq 5$. In this case, at least one of W or U must contain some isotropic vector, since any quadratic form in at least 3 variables over any finite field is isotropic. Without loss of generality, suppose it is W and $\dim W \geq \dim U$. We claim that W has strictly fewer isotropic vectors than $\mathbb{F}_p^n$. It suffices to consider the worst case $\dim W = n-1$. Since $(x^{2m}-1) \geq (x^m \mp 1)(x^{m-1} \pm 1) \geq (x^{2m-2}-1)$ for all $x \geq 1$ and for all $m \geq 2$, Lemma 3.5 implies the claim. Thus the maximal subgroup of G_p stabilizing W cannot act transitively on pairs $\{\pm v\}$ for v isotropic, and so H cannot be associated with a 1-cusped subgroup of Γ.

Proposition 3.3. *For $p \geq 3$ there are no 1-cusped level p congruence subgroups of $\mathrm{SO}(d,1;\mathbb{Z})$ whose reduction mod p is a maximal subgroup of G_p of type $\mathcal{C}_1$.*

3.2 $\mathcal{C}_2$: Imprimitive subgroups

These maximal subgroups stabilize decompositions of V into direct sums of subspaces of equal dimension, so $V = V_1 \oplus \cdots \oplus V_t$ where V_i is nondegenerate except possibly in the case $t = 2$; see Table 2.4 in [2]. Note that $n = \dim V$ is then divisible by t. In particular the maximal subgroup consists of the stabilizers of the subspaces themselves, with an S_t action between them given by the wreath product. In the case of **O** type groups these are of the form $\mathrm{O}^{\ell}_{n/t}(q) \wr S_t$, or they are of the form $2.S_n$ or $2.A_n$ when $t = n$ (i.e. these contain S_n or A_n as an index-2 subgroup; the 2 corresponds to scalar multiplication by -1).

Lemma 3.6. *If $n/t = 4$, which is only possible for $n = 8$, then the number of*

nonzero isotropic vectors in $V_1 \cup \cdots \cup V_t$ is nonzero and strictly smaller than the number of isotropic vectors in $\mathbb{F}_p^n$.

Proof. Since $\dim(V_i) = 4$, it contains isotropic vectors. Then $V_1 \cup V_2$ contains at most $2(p^4 - 1)$ nonzero isotropic vectors. Since $2(x^4 - 1) < (x^4 \mp 1)(x^3 \pm 1)$ for all $x \geq 2$, $\mathbb{F}_p^n$ contains isotropic vectors not in $V_1 \cup V_2$. This proves the lemma. □

Lemma 3.7. *If $n/t = 3$ (possible when $n = 6, t = 2$ or $n = 9, t = 3$), the number of nonzero isotropic vectors in the union of the V_i is strictly smaller than the number of isotropic vectors in $\mathbb{F}_p^n$.*

Proof. When $n = 6$ and $t = 2$, the worst case is when V_i is totally isotropic, and hence $V_1 \cup V_2$ contains $2(p^3 - 1)$ nonzero isotropic vectors, which is less than $(p^3 \mp 1)(p^2 \pm 1)$ for all $p \geq 3$. For $n = 9$, V_i is nondegenerate, and thus $V_1 \cup V_2$ contains $3(p^2 - 1) < (p^8 - 1)$ isotropic vectors. This proves the lemma. □

Lemma 3.8. *If $n/t = 2$ (possible when $n = 6, t = 3$ or $n = 8, t = 4$) and V_i contains a nonzero isotropic vector, then $\mathbb{F}_p^n$ contains an isotropic vector not in the union of the V_i.*

Proof. In all relevant cases for $n/t = 2$, $t > 2$, so V_i is nondegenerate of dimension 2. When it contains isotropic vectors, it contains $2(p - 1)$ isotropic vectors. Then $6(p - 1) < (p^3 \mp 1)(p^2 \pm 1)$ and $8(p - 1) < (p^4 \mp 1)(p^3 \pm 1)$, so $\mathbb{F}_p^n$ contains isotropic vectors not containsed in the union of the V_i. □

Lemma 3.9. *If $p \geq 3$, $n/t = 2$, and V_i contains no isotropic vectors, then the stabilizer H of $V_1 \cup V_2$ in G_p does not act transitively on pairs $\{\pm v\}$ for v isotropic.*

Proof. In this case, H is of type $\Omega_2^-(p) \wr S_{n/2}$, which has order at most $24(p+1)^3$ for $n = 6$ and $192(p + 1)^4$ for $n = 8$ (including the case that $G_p = \mathrm{SO}(Q; \mathbb{F}_p)$ which doubles the order). Then $24(x+1)^3 < \frac{1}{2}(x^3 \mp 1)(x^2 \pm 1)$ and $192(x^4+1)^4 < \frac{1}{2}(x^4 \mp 1)(x^3 \pm 1)$ for all $x \geq 9$, so this group cannot possibly act transitively on

pairs $\{\pm v\}$ for v isotropic for $p > 11$. Direct computation shows for $p = 3, 5, 7$ that $\frac{1}{2}N^Q(n,p)$ does not divide $24(p+1)^3$ for $n = 6$ or $192(p+1)^4$ for $n = 8$, which eliminates all possible cases. □

Now consider the case $n/t = 1$, so H is $(\mathbb{Z}/2) \wr S_n$ or $(\mathbb{Z}/2) \wr A_n$.

Lemma 3.10. *If $p \geq 3$ and $H \geq G_p$ is a maximal subgroup of type C_2 with $n/t = 1$ that is associated with a one-cusped congruence subroup of $\mathrm{SO}(n, 1; \mathbb{Z})$ then $n = 5$ and $p = 3$.*

Proof. If H acts transitively on pairs $\{\pm v\}$ for v isotropic, then

$$\frac{1}{2}N^Q(n,p) \mid 2^n n!$$

by Lemma 3.4. In particular, we have

$$2^n n! > \frac{1}{2}N^Q(n,p).$$

Then, using Lemma 3.5,

$$\begin{aligned}
\frac{1}{2}(x^4 - 1) &\geq 2^5 \cdot 5! \text{ for } x \geq 10 \\
\frac{1}{2}(x^3 \mp 1)(x^2 \pm 1) &\geq 2^6 \cdot 6! \text{ for } x \geq 10 \\
\frac{1}{2}(x^6 - 1) &\geq 2^7 \cdot 7! \text{ for } x \geq 11 \\
\frac{1}{2}(x^4 \mp 1)(x^3 \pm 1) &\geq 2^8 \cdot 8! \text{ for } x \geq 12 \\
\frac{1}{2}(x^8 - 1) &\geq 2^9 \cdot 9! \text{ for } x \geq 12
\end{aligned}$$

This only leaves the possibilities $p \geq 7$ for $n = 5, 6$, and $p \geq 11$ for $n = 7, 8, 9$. Checking for actual divisibility among the finite list of remaining cases, we are left with only $n = 5, p = 3$ and $n = 8, p = 3$.

Further, to obtain a 1-cusped congruence subgroup, $2^n n!$ must be divisible by the number of cusps of the full congruence subgroup of level p. For $n = 8$ and $p = 3$, there are 1208844 cusps (which can be computed using the code in Section 3.9), and this does not divide $2^8 \cdot 8!$, hence the relevant maximal subgroup of G_p cannot be associated with a 1-cusped congruence subgroup. Thus only $n = 5, p = 3$ remains. □

We have proven:

Proposition 3.4. *For $p \geq 3$ there are no 1-cusped level p congruence subgroups of $\mathrm{SO}(d,1;\mathbb{Z})$ whose reduction mod p is a maximal subgroup of G_p of type $\mathcal{C}_2$, except possibly in the exceptional case $n = 5, p = 3$.*

We will see later, with the aid of the computer, that the exceptional case does produce examples of one-cusped congruence subgroups.

3.3 $\mathcal{C}_3$: Field extension subgroups

Let E be a field extension of $F = \mathbb{F}_q$ of degree $r > 1$, where $r \mid n$. (Thus the $\mathcal{C}_3$ case is not relevant when n is prime.) Then V can be viewed as an E-vector space with a new quadratic form $\kappa_\sharp$ so that $\kappa = T\kappa_\sharp$ where T is the trace map for the field extension E/F.

These maximal subgroups preserve the E vector space structure of V, so we just need to find two isotropic vectors that are different according to E (analogous to the real and imaginary parts of complex numbers).

These groups act as E-linear maps (for the field extension E/F), but the exact type of these groups might differ. Notably, for odd prime q, these groups only exist for even n ($n = 6$ or $n = 8$) and $r = 2$, or $n = 9$ and $r = 3$. In our case, the C_3 subgroup may be of the form GO or of the form GU. If the subgroup is a GO, then we have an extension analogous to a real extension of $\mathbb{Q}$; if the subgroup is of the form GU, then the subgroup acts in a way that preserves a Hermitian form, analogously to the vector space over the complex numbers.

For example, suppose the $\mathcal{C}_3$ group H is of type **O**. Then there is a unique extension $\mathbb{F}_{p^2}/\mathbb{F}_p$.

We compute the orders of the maximal subgroups (for $r \mid n$), then conclude by Lemma 3.5 and Orbit-Stabilizer Theorem to conclude that the growth of the number of isotropic vectors with p forbids transitivity on pairs $\{\pm v\}$ with

v an isotropic vector for all p but finitely many. To do the comparison we compare $\frac{1}{2}N^Q(n,p)$ with the order of H with powers of p removed.

Lemma 3.11. *For $n=6$, $r=2$, a maximal $\mathcal{C}_3$-subgroup of type* **O** *has order (dividing out powers of p) divisible by $c(p^4-1)$ where $c \leq 8$.*

Proof. Using Lemma 3.5, we see that such a subgroup fails to be transitive on isotropic vectors for all $p \geq 3$. We use Tables 8.31 and 8.33 in [2]:

$$8(x^4-1) < \frac{1}{2}(x^3 \mp 1)(x^2 \pm 1) \text{ for all } x \geq 16.$$

Direct inspection rules out the required divisibility for $3 \leq p \leq 13$. □

Lemma 3.12. *For $n=8$, $r=2$, and $\epsilon = \pm$, a maximal $\mathcal{C}_3$-subgroup of type* **O** *has order (dividing out powers of p) divisible by $c(p^2 \mp 1)(p^4-1)$ where $c \leq 4$. Using Lemma 3.5, we compute that such a subgroup fails to be transitive on isotropic vectors for all $p \geq 3$.*

Proof. Using Lemma 3.5 and Tables 8.50 and 8.52 in [2], the same analysis as in the proof of 3.11 rules out $p \geq 11$ by order and $3 \leq p \leq 7$ by divisibility. □

Lemma 3.13. *For $n=9$ and $r=3$, a maximal $\mathcal{C}_3$-subgroup of type* **O** *has order (dividing out powers of p) divisible by $c(p^6-1)$ where $c \leq 3$.*

Proof. Using Lemma 3.5 and Table 8.58 in [2], the same analysis as in the proof of 3.11 rules out all $p \geq 3$ by order. □

Lemma 3.14. *Suppose a maximal $\mathcal{C}_3$-subgroup $H < G_p$ is of type* **U**. *Then H cannot be associated with a one-cusped subgroup of* $\mathrm{SO}(d,1;\mathbb{Z})$.

Proof. Given the assumptions, by tables in Chapter 8 of [2] H must be of the form $\mathrm{SU}_4(p).\frac{p+1}{2}.2$. Set $E = \mathbb{F}_p(\tau)$ with $\tau^2 \in \mathbb{F}_p$, and let $z \to \bar{z}$ be the Galois involution for $E/\mathbb{F}_p$, and interpret V as an E-vector space W. Take h to be the Hermitian form on $E^{n/2}$ with the same matrix as our quadratic form Q. Then $v = (1,0,...,0)$ and $w = (\tau,0,...,0)$ are isotropic for h. A map $W \to W$ sending v to v is $\mathbb{F}_p$-linear, but *not* E-linear, hence it cannot be an element of the unitary group of h. Hence H cannot be transitive on pairs $\{\pm v\}$ for v isotropic, which proves the lemma. □

The foregoing lemmas prove:

Proposition 3.5. *For all $p \geq 3$, there are no 1-cusped level p congruence subgroups of $\mathrm{SO}(n,1;\mathbb{Z})$ whose reduction mod p is a maximal subgroup of G_p of type $\mathcal{C}_3$.*

3.4 $\mathcal{C}_4$: Tensor product subgroups

Subgroups of type $\mathcal{C}_4$ are groups that preserve a tensor product decomposition, i.e. there is a decomposition $V = V_1 \otimes V_2$ such that for all g in such a subgroup there exist g_1 and g_2 with

$$(v_1 \otimes v_2)g = v_1 g_1 \otimes v_2 g_2.$$

We need only show that in any given quadratic space, we have both isotropic vectors that are pure tensors and isotropic vectors that are mixed tensors. Only the $\Omega^+(8,p)$ case has $\mathcal{C}_4$ subgroups, by the tables in Chapter 8 of [2].

Lemma 3.15. *If a maximal subgroup $H < G_p$ is in class $\mathcal{C}_4$ then $n = 8$, $\epsilon = +$ then H is not associated with a 1-cusped subgroup of $\mathrm{SO}(d,1;\mathbb{Z})$.*

Proof. By Table 8.50 in [2], H must have the form $(\mathrm{Sp}_2(p) \circ \mathrm{Sp}_4(p)).2$. Let v_1 be a nonzero isotropic vector for the 2-dimensional symplectic form, v_2 be a non-isotropic vector, and $v = v_1 \otimes v_2$. Similarly, let $w = w_1 \otimes w_2$ where w_1 is non-isotropic and w_2 is isotropic. There is no element of $\mathrm{Sp}_2(p)$ taking v_1 to w_1, hence H cannot send v to w and cannot be transitive on pairs $\{\pm v\}$ for v isotropic. □

Proposition 3.6. *For all $p \geq 3$, there are no 1-cusped level p congruence subgroups of $\mathrm{SO}(n,1;\mathbb{Z})$ whose reduction mod p is a maximal subgroup of G_p of type $\mathcal{C}_4$.*

3.5 $\mathcal{C}_6$: Symplectic-type subgroups

This case is relevant for $n = 8$ and $\epsilon = +$. However, the $\mathcal{C}_6$ groups in $n = 8$ are of type $2^7.S_8$ or $2^7.A_8$, which is of constant size, $2^8 8!$ or $2^7 8!$. We again use Lemma 3.5 to conclude

Lemma 3.16. *All $\mathcal{C}_6$ maximal subgroups are non-transitive on cusps of $\Gamma(p)$ for all $p \geq 3$.*

Proof. For $p \geq 13$ the number of cusps is too large for a transitive action. The cases $p = 3, 7, 11$ are ruled out since G_p has type $-$, and $p = 5$ is ruled out because $|H|$ is not divisible by $\frac{1}{2}N^Q(n, p)$. □

3.6 $\mathcal{C}_7$: Tensor product subgroups

This case is similar to the $\mathcal{C}_4$ case, but we have $n = m^t$, and a decomposition into isomorphic subspaces giving a wreath product by S_t. The only relevant cases are $n = 8 = 2^3$ and $n = 9 = 3^2$. But $\Omega^{\pm}(8, p)$ does not have $\mathcal{C}_7$ subgroups, and $\Omega(9, p)$ has one class of $\mathcal{C}_7$ subgroup, $\Omega_3(p)^2.[4]$, which has order $4p^2(p^2-1)^2$. Removing powers of p, the largest possible orbit cardinality is $8(p^2-1)^2$, which using Lemma 3.5 is smaller than $\frac{1}{2}N(9, p) = \frac{1}{2}(p^8 - 1)$ for all $p \geq 3$. This proves:

Lemma 3.17. *All $\mathcal{C}_7$ maximal subgroups are non-transitive on cusps of $\Gamma(p)$ for $p \geq 3$.*

3.7 Maximal subgroups of class $\mathscr{S}$

$\mathrm{SO}(n, p)$ has the subgroups of class $\mathscr{S}$ for $p \geq 11$ (the following table is adapted from Chapter 8 of [2]) ($b = 1$ or 2 depending on p) listed in Table 3.1.

For $n = 5$, all groups are ruled out by size considerations.

n, ϵ	Maximal subgroup	Conditions on $p \geq 3$
5	A_6	$p \equiv 5, 7 \bmod 12$
	S_6	$p \equiv 1, 11 \bmod 12$
	$L_2(p)$	$p \geq 7$
$6, \pm$	$b \times L_2(7)$	$p \equiv 1, 2, 4 \bmod 7$ for Ω^+; $p \equiv 3, 5, 6 \bmod 7$ for Ω^-
	$b \times A_7$	$p \equiv 1, 2, 4 \bmod 7$ for Ω^+; $p \equiv 3, 5, 6 \bmod 7$ for Ω^-
	$b \times U_4(2)$	$p \equiv 1 \bmod 6$
7	$S_6(2)$	any $p \geq 3$
	$G_2(p)$	any $p \geq 3$
$8, +$	$b \times L_3(q).3$	$p \equiv 1 \bmod 3$
	$b \times U_3(q).3$	$p \equiv 2 \bmod 3$
	$2^\bullet\Omega_8^+(2)$	any $p \geq 3$
$8, -$	$L_3(q)$	$p \equiv 2 \bmod 3$
	$U_3(q)$	$p \equiv 1 \bmod 3$
9	$L_2(8)$	$p \equiv \pm 1 \bmod 7$
	$L_2(17)$	$p \equiv \pm 1, \pm 2, \pm 4, \pm 8 \bmod 17$
	A_{10}	$p \equiv \pm 2 \bmod 5$
	S_{10}	$p \equiv \pm 1 \bmod 5, p \neq 11$
	S_{11}	$p = 11$
	$L_2(q).2$	any $p \geq 3$
	$L_2(q^2).2$	any $p \geq 3$

Table 3.1: Nonexceptional maximal subgroups of type $\mathscr{S}$ of G_p

For $n = 6$, all groups are ruled out by order considerations (note that $b \leq 2$), except for $b \times L_2(7)$ and $b \times A_7$ for Ω^- and $p = 3$. But $G_p = \Omega^+$ for $p = 3$, so all cases are eliminated.

For $n = 7$, $S_6(2)$ is eliminated for order reasons for $p \geq 13$ and for divisibility reasons for $3 \leq p \leq 11$.

For $n = 8$, all cases in Table 3.1 are ruled out by order and divisibility. The exceptional cases $2^\bullet\Omega_8^+(2)$, $2 \times A_{10}$ and $2^\bullet A_{10}$ for $p = 5$, $\epsilon = +$ are ruled out by divisibility.

For $n = 9$, all groups are ruled out by order, and divisibility in certain small cases.

We have proven:

Lemma 3.18. *Except possibly $G_2(p)$, all maximal subgroups of type $\mathscr{S}$ fail to*

be transitive on isotropic vectors of V for $p \geq 11$.

3.7.1 On maximal subgroups of type $G_2(p)$

We now consider the maximal subgroup $G_2(p)$ in the following. The only cases that have $G_2(p)$ as a maximal subgroup are $\mathrm{SO}_7(p)$ and $\mathrm{SO}_8^+(p)$. $G_2(p)$ is the group of algebra automorphisms of the the standard octonion algebra over $\mathbb{F}_p$. In the 7-dimensional case G_2 acts on V by treating it as the subspace of pure imaginary octonions in the 8-dimensional octonion algebra over $\mathbb{F}_p$ (under some choice of basis the basis can be seen as the octonions i, j, k, l, li, lj, lk). In the 8-dimensional case the action treats V as the whole octonion algebra.

In the 8-dimensional case, $G_2(p)$ must stabilize the space of pure octonions. Thus the isotropic vector that corresponds to $a1 + bj + ck + dl$ (for $a^2 + b^2 + c^2 + d^2 = 0$) is not $G_2(p)$-equivalent to the isotropic vector corresponding to $ai + bj + ck + dl$.

However, the group $G_2(p)$ is transitive on isotropic vectors of the pure octonions (see p. 127 of [18]), so the $d = 6$ case requires further argument. For this case, since $G_2(p)$ is already transitive on isotropic vectors, we can fix an isotropic vector v_0 and consider if $G_2(p)$ is transitive on oriented bases of the isotropic complement $W = (v_0)^\perp$.

We consider $\Delta_p \cap G_2$ (Δ_p is the image of $\Delta < \mathrm{SO}(d, 1; \mathbb{Z})$ in $G_p = \mathrm{SO}(7, p)$).

Now the order of $G_2(p)$ is $p^6(p^6 - 1)(p^2 - 1)$. Since $G_2(p)$ is transitive on isotropic vectors, together with Lemma 3.5 this implies that the order of the G_2-stabilizer of an isotropic vector is

$$|\operatorname{Stab}_{G_2}(v)| = \frac{|G_2|}{N^Q(7,p)} = \frac{p^6(p^6-1)(p^2-1)}{(p^6-1)} = p^6(p^2-1).$$

(recall that $p \equiv 1 \bmod 4$).

Lemma 3.19. *Assume the isotropic vector is $v = (1, 0, 0, 0, 0, 0, 0)$. The orthogonal complement of v is 6-dimensional and includes v.*

It follows that the number of positively oriented orthonormal bases of

$v^\perp/\mathbb{F}_p v$ is $\#\,\mathrm{SO}(5,p) = p^4(p^2-1)(p^4-1)$ for all $p \geq 5$: by Lemma 3.1, this is too large for $p > 43$. Divisibility rules out $5 \leq p \leq 43$.

We have proven:

Proposition 3.7. *For all $p \geq 5$ when $d = 6$ and for all $p \geq 3$ when $d = 7$, there are no 1-cusped level p congruence subgroups of $\Omega(d,1;\mathbb{Z})$ whose reduction mod p is a maximal subgroup of G_p of type $\mathscr{S}$.*

As we will see in Chapter 5, for $p = 3$, there is a one-cusped subgroup of $\mathrm{SO}(6,1;\mathbb{Z})$ associated with $G_2(3)$.

CHAPTER 4

THE COMPOSITE LEVEL CASE

Recall from Chapter 1 that $\Omega(d,1;\mathbb{Z})$ is index 2 in $\mathrm{SO}(d,1;\mathbb{Z})$ and consists of all elements of $\mathrm{SO}(d,1;\mathbb{Z})$ with spinor norm $+1$. This chapter and the next chapter will prove the main theorem:

Theorem. *For $d = 5$ and $d \geq 7$ and all q not a power of 2, there is no 1-cusped level-q congruence subgroup of $\Omega(d,1;\mathbb{Z})$. For $d = 4, 6$ and all q not of the form $2^a 3^b$, there is no 1-cusped level-q congruence subgroup of $\Omega(d,1;\mathbb{Z})$.*

The strategy is to assign an action of $\Omega(Q,q)$ on the cusps and show that the maximal subgroups of $\Omega(Q,q)$ cannot be transitive on the cusps. The current chapter will examine to what extent the composite case reduces to the prime case.

Throughout this chapter, let $\widetilde{G}$ be the absolutely almost simple, simply connected $\mathbb{Q}$-algebraic group such that $\widetilde{G}(\mathbb{Z}) = \mathrm{Spin}(d,1;\mathbb{Z})$ and $\widetilde{G}(\mathbb{Z}/q)$ will denote the image of $\widetilde{G}(\mathbb{Z})$ in $\Omega(Q;\mathbb{Z}/q) < M_n(\mathbb{Z}/q)$ obtained by reducing matrix entries modulo q.

4.1 Preliminary facts

Let p be an odd prime. Then Strong Approximation implies that $\widetilde{G}(\mathbb{Z}/p)$ is isomorphic to $\Omega(Q;\mathbb{F}_p)$. For all $r \geq 2$, there is an exact sequence

$$1 \to \mathfrak{g}_p \to \widetilde{G}(\mathbb{Z}/p^r) \to \widetilde{G}(\mathbb{Z}/p^{r-1}) \to 1$$

where $\mathfrak{g}_p$ is the Lie algebra of $\widetilde{G}(\mathbb{Z}/p)$ considered as an additive vector space, and hence it is an elementary abelian p-group. See, for example, the proof of Lemma 16.4.5 of [5]. The conjugation action of $g \in \widetilde{G}(\mathbb{Z}/p^r)$ on $\mathfrak{g}_p$ is through the projection $\widetilde{G}(\mathbb{Z}/p^r) \to \widetilde{G}(\mathbb{Z}/p)$ followed by the adjoint representation of $\widetilde{G}(\mathbb{Z}/p)$ on $\mathfrak{g}_p$. Since the action of $\widetilde{G}(\mathbb{Z}/p)$ is irreducible, the same holds for any subgroup $H \leq \widetilde{G}(\mathbb{Z}/p^r)$ that projects onto $\widetilde{G}(\mathbb{Z}/p)$. Therefore if $H \leq \widetilde{G}(\mathbb{Z}/p^r)$ projects onto $\widetilde{G}(\mathbb{Z}/p^{r-1})$ then H acts irreducibly on $\mathfrak{g}_p$. We also need to know that our exact sequence does not split.

Lemma 4.1. *The exact sequence*

$$1 \to \mathfrak{g}_p \to \widetilde{G}(\mathbb{Z}/p^r) \to \widetilde{G}(\mathbb{Z}/p^{r-1}) \to 1$$

does not split for any $r \geq 2$.

Proof. Suppose for a contradiction that $\widetilde{G}(\mathbb{Z}/p^r) \cong \mathfrak{g}_p \rtimes \widetilde{G}(\mathbb{Z}/p^{r-1})$. Fix $y \in (\mathbb{Z}/p^{r-1})^{n-2}$ nonzero with all entries in $\{0, ..., p-1\}$. Then y has additive order p^{r-1} hence so does the element

$$u = \begin{bmatrix} 1 & -y^t & -|y|^2/2 \\ 0 & I_{n-2} & y \\ 0 & 0 & 1 \end{bmatrix} \in \widetilde{G}(\mathbb{Z}/p^{r-1}).$$

Let $\tilde{y}$ be y considered as an element of $(\mathbb{Z}/p^r)^{n-2}$ (still with entries in $\{0, ..., p-1\}$). Let $\tilde{u}$ denote u, now considered as an element of $\widetilde{G}(\mathbb{Z}/p^r)$. Then any preimage of u in $\widetilde{G}(\mathbb{Z}/p^r)$ is of the form $\tilde{u} + p^{r-1}X$ for some $X \in M_n(\mathbb{F}_p)$, by expanding $(\tilde{u} + p^{r-1}X)^k$ by the binomial theorem and using the fact that y has additive order p^{r-1}. Since no preimage of u in $\widetilde{G}(\mathbb{Z}/p^r)$ has order p^{r-1} the exact sequence has no section and thus cannot split. □

Corollary 4.1. *If $r \geq 2$, $H \leq \widetilde{G}(\mathbb{Z}/p^r)$ is a proper subgroup, and*

$$\pi : \widetilde{G}(\mathbb{Z}/p^r) \to \widetilde{G}(\mathbb{Z}/p^{r-1})$$

is projection, then H is a proper subgroup of $\widetilde{G}(\mathbb{Z}/p^{r-1})$.

Proof. Suppose $H \leq \widetilde{G}(\mathbb{Z}/p^r)$ is a subgroup with $\pi(H) = \widetilde{G}(\mathbb{Z}/p^{r-1})$. Then $H \cap \mathfrak{g}_p = \{I\}$ implies $\widetilde{G}(\mathbb{Z}/p^r) = \mathfrak{g}_p \rtimes H \cong \mathfrak{g}_p \rtimes \widetilde{G}(\mathbb{Z}/p^{r-1})$. This is ruled out by Lemma 4.1. Thus $H \cap \mathfrak{g}_p$ is nontrivial hence is a nonzero linear subspace. Then $\pi(H) = \widetilde{G}(\mathbb{Z}/p^{r-1})$ implies H acts irreducibly on $\mathfrak{g}_p$ and $H \cap \mathfrak{g}_p \trianglelefteq H$ is H-invariant, so $H \cap \mathfrak{g}_p = \mathfrak{g}_p$. It follows that $H = \widetilde{G}(\mathbb{Z}/p^r)$. □

Before going further, we need a definition.

Definition 4.1. *If $q > 1$ is an integer then $H \leq \widetilde{G}(\mathbb{Z}/q)$ is **essential** if for all divisors d of q with $1 < d < q$, the kernel of the projection $\widetilde{G}(\mathbb{Z}/q) \to \widetilde{G}(\mathbb{Z}/d)$ is <u>not</u> contained in H.*

Note that for q prime $\widetilde{G}(\mathbb{Z}/q)$ is technically an essential subgroup of itself, but when q is composite an essential subgroup is necessarily proper.

4.2 The odd composite case

Proposition 4.1. *If $q = \prod_i p_i^{r_i}$ and $H < \widetilde{G}(\mathbb{Z}/q)$ is a maximal subgroup, then there is a prime factor p_i of q such that the image of H in $\widetilde{G}(\mathbb{Z}/p_i)$ is a maximal subgroup.*

Proof. We proceed by induction on the length of the decomposition of q into a product of primes. There is nothing to prove when q is prime. Again by induction it suffices to show that there is a divisor d of q with $1 < d < q$ such that the image of H in $\widetilde{G}(\mathbb{Z}/d)$ under the projection π_d is maximal.

Suppose not. Then H must map onto $\widetilde{G}(\mathbb{Z}/d)$ for all such d. Since H is a proper subgroup of $\widetilde{G}(\mathbb{Z}/q)$, $H \cap \ker \pi_d$ must be a proper subgroup of $\ker \pi_d$, so H is essential in $\widetilde{G}(\mathbb{Z}/d)$. However, Assertion 1.10 in [4] implies that $\pi_d(H)$

is essential in $\widetilde{G}(\mathbb{Z}/d)$ for all d. When some d is composite $\pi_d(H)$ is then a proper subgroup, and this contradiction proves the inductive step we need.

Therefore to prove the proposition it remains to consider the cases $q = p_1^2$ and $q = p_1 p_2$ for $p_1 \neq p_2$. When $q = p_1^2$ this is Corollary 4.1. Now suppose $q = p_1 p_2$, $H < \widetilde{G}(\mathbb{Z}/q) \cong \widetilde{G}(\mathbb{Z}/p_1) \times \widetilde{G}(\mathbb{Z}/p_2)$ is maximal and $\pi_j(H) = \widetilde{G}(\mathbb{Z}/p_j)$ for $j = 1, 2$ where π_j is projection of $\widetilde{G}(\mathbb{Z}/q)$ onto $\widetilde{G}(\mathbb{Z}/p_j)$. Set $K_i = \ker(\pi_i|_H) \trianglelefteq H$. Then $K_1 = H \cap \widetilde{G}(\mathbb{Z}/p_2)$ and $K_2 = H \cap \widetilde{G}(\mathbb{Z}/p_1)$. Moreover (with indices mod 2 in $\{1, 2\}$) π_j is onto hence $K_{j+1} \trianglelefteq \pi_j(H) = \widetilde{G}(\mathbb{Z}/p_j)$. However $\widetilde{G}(\mathbb{Z}/p_j)$ is almost simple, so every normal subgroup is either all of $\widetilde{G}(\mathbb{Z}/p_j)$ or is contained in the center which is either $\{I\}$ or $\mathbb{Z}/2$. The case $K_{j+1} = \widetilde{G}(\mathbb{Z}/p_j)$ means $H = \widetilde{G}(\mathbb{Z}/q)$ and thus is eliminated. Then $K_1 \cap K_2 = \{I\}$, so $K_1 \times K_2 \trianglelefteq H$ is central. Thus K_{j+1} maps to a central subgroup of $H/K_j \cong \widetilde{G}(\mathbb{Z}/p_j)$, hence $H/(K_1 \times K_2)$ is isomorphic to $(P)\Omega(Q; \mathbb{F}_{p_j})$ for $j = 1, 2$ (where the P appears when $K_{j+1} \cong \mathbb{Z}/2$, which is only possible for n even). Thus we obtain an isomorphism between distinct almost simple groups $(P)\Omega(Q; \mathbb{F}_{p_1}) \cong (P)\Omega(Q; \mathbb{F}_{p_2})$. These are classified e.g. on p. xv of [9], and there is no such exceptional isomorphism. This contradiction implies that $\pi_{p_j}(H)$ must be a proper subgroup of $\widetilde{G}(\mathbb{Z}/p_j)$ for at least one factor p_j. This was the last case to consider and thus completes the proof of the proposition. □

Corollary 4.2. *Suppose $q = \prod_i p_i$ is odd and that there is no one-cusped congruence subgroup of $\Omega(d, 1; \mathbb{Z})$ of level p_j for any prime factor p_j of q. Then there is no one-cusped congruence subgroup of $\Omega(d, 1; \mathbb{Z})$ of level q.*

Proof. It suffices to consider the case where $\Gamma < \Omega(d, 1; \mathbb{Z})$ is one-cusped for Γ_H with image $H < \widetilde{G}(\mathbb{Z}/q)$ maximal. Then Proposition 4.1 implies there is a factor p_j of q such that $\pi(H) < \widetilde{G}(\mathbb{Z}/p_j)$ is a maximal subgroup, for the projection $\pi : \widetilde{G}(\mathbb{Z}/q) \to \widetilde{G}(\mathbb{Z}/p_j)$. Then $\Gamma_H < \Gamma_{\pi(H)} < \Omega(d, 1; \mathbb{Z})$ where $\Gamma_{\pi(H)}$ is the preimage of $\pi(H)$ in $\Omega(d, 1; \mathbb{Z})$. However, $\Gamma_{\pi(H)}$ is then a one-cusped congruence subgroup of level p_j, which is a contradiction. □

The next corollary follows from the preceding corollary and the proof of

the main result in the prime level case.

Corollary 4.3. *If $d = 5$ or $d \geq 7$ there are no one-cusped congruence subgroups of $\Omega(d, 1; \mathbb{Z})$ of odd level. If $d = 4, 6$ there are no one-cusped congruence subgroups of $\Omega(d, 1; \mathbb{Z})$ of level q for $\gcd(q, 6) = 1$.*

4.3 The general case

Now suppose $q = ab$ for $b > 1$ where $a = 2^{s_2}3^{s_3}$ with $s_2 + s_3 > 0$ and $\gcd(a, b) = 1$ for $d = 4, 6$, and $a = 2^r$ with $r > 0$ and b odd for $d = 5, 7, 8$. Then $\widetilde{G}(\mathbb{Z}/q) \cong \widetilde{G}(\mathbb{Z}/a) \times \widetilde{G}(\mathbb{Z}/b)$. Decompose $b = \prod_i p_i$ as a product of distinct primes.

Theorem 4.1. *In the above notation suppose $H < \widetilde{G}(\mathbb{Z}/q)$ is a maximal subgroup such that $\pi_b(H) = \widetilde{G}(\mathbb{Z}/b)$ where π_b is the projection $\widetilde{G}(\mathbb{Z}/q) \to \widetilde{G}(\mathbb{Z}/b)$. Then there is a maximal subgroup $H_a < \widetilde{G}(\mathbb{Z}/a)$ such that $H = H_a \times \widetilde{G}(\mathbb{Z}/b)$.*

We need a preliminary lemma.

Lemma 4.2. *For p odd and $r > 0$ suppose l is a prime dividing $|\widetilde{G}(\mathbb{Z}/p)|$. If $l = p$, then $\widetilde{G}(\mathbb{Z}/p^r)$ is generated by elements of order a power of p. If $l \neq p$, then $\widetilde{G}(\mathbb{Z}/p^r)$ is generated by elements of order l.*

Proof. We induct on r. Let $\mathcal{G}$ be the candidate generating set for $\widetilde{G}(\mathbb{Z}/p)$, which is nonempty by Cauchy's theorem. Since order is preserved under conjugation, the subgroup generated by $\mathcal{G}$ is a nontrivial normal subgroup of $\widetilde{G}(\mathbb{Z}/p)$. By almost simplicity the only proper nontrivial normal subgroup of $\widetilde{G}(\mathbb{Z}/p)$ is possibly a central $\mathbb{Z}/2$ when n is even. Since $\mathbb{Z}/2$ contains no element of order l, the subgroup must be all of $\widetilde{G}(\mathbb{Z}/p)$, proving the base case.

Now suppose $r > 1$ and consider the exact sequence

$$1 \to \mathfrak{g}_p \to \widetilde{G}(\mathbb{Z}/p^r) \to \widetilde{G}(\mathbb{Z}/p^{r-1}) \to 1.$$

Again our candidate generating set $\mathcal{G}$ is nonempty by Cauchy's Theorem. Let G be the subgroup of $\widetilde{G}(\mathbb{Z}/p^r)$ generated by $\mathcal{G}$. We first consider the case $l = p$. Since $\mathfrak{g}_p$ is a p-group, $\mathfrak{g}_p \leq G$ by definition. Moreover, every element of $\widetilde{G}(\mathbb{Z}/p^{r-1})$ with order a power of p is $\pi(g)$ for some $g \in \widetilde{G}(\mathbb{Z}/p^r)$ with order a (possibly larger) power of p. Thus $\pi(G) = \widetilde{G}(\mathbb{Z}/p^{r-1})$, and thus $G = \widetilde{G}(\mathbb{Z}/p^r)$ as desired. If $l \neq p$ and $g \in \widetilde{G}(\mathbb{Z}/p^r)$ has order l, then $\pi(g)$ also has order l again, since $\mathfrak{g}_p$ is a p-group. Thus $\pi(G) = \widetilde{G}(\mathbb{Z}/p^{r-1})$. It follows by irreducibility of $\widetilde{G}(\mathbb{Z}/p^{r-1})$ acting on $\mathfrak{g}_p$ that either $G \cap \mathfrak{g}_p = I$, which is impossible by Lemma 4.1, or $G \cap \mathfrak{g}_p = \mathfrak{g}_p$. Therefore $\mathfrak{g}_p \leq G$ and $\pi(G) = \widetilde{G}(\mathbb{Z}/p^{r-1})$, hence $G = \widetilde{G}(\mathbb{Z}/p^r)$, which completes the proof. □

Proof of Theorem 4.1. Suppose $H < \widetilde{G}(\mathbb{Z}/q)$ is a maximal subgroup such that $\pi_b(H) = \widetilde{G}(\mathbb{Z}/b)$. We will prove that $\widetilde{G}(\mathbb{Z}/b) \leq H$, which proves that $H = H_2 \times \widetilde{G}(\mathbb{Z}/b)$ for $H_2 < \widetilde{G}(\mathbb{Z}/a)$ maximal. Recall that $b = \prod_i p_i$, so $\widetilde{G}(\mathbb{Z}/b) \cong \prod_i \widetilde{G}(\mathbb{Z}/p_i^{r_i})$ and it suffices to show that $\widetilde{G}(\mathbb{Z}/p_i^{r_i}) \leq H$ for all i. Since $\widetilde{G}(\mathbb{Z}/p^s)$ is an extension of $\widetilde{G}(\mathbb{Z}/p)$ by a p-group for all p, the case $p = 2$ following by inclusion into $\Omega(Q; \mathbb{F}_2)$, the only primes $l > 2$ dividing $\widetilde{G}(\mathbb{Z}/2^{s_2})$ are those dividing $|\widetilde{G}(\mathbb{Z}/2)|$ and the only primes $l \neq 3$ dividing $|\widetilde{G}(\mathbb{Z}/3^{s_3})|$ are those dividing $|\widetilde{G}(\mathbb{Z}/3)|$. Using this, the possible prime divisors of $|\widetilde{G}(\mathbb{Z}/a)|$ are given in Table 4.1. Note not all the primes need appear; e.g. 13 does not divide $|\widetilde{G}(\mathbb{Z}/a)|$ if $n = 7$ and $a = 2^{s_2}$.

n	Possible prime divisors
5	$2, 3, 5$
6	$2, 3, 5$
7	$2, 3, 5, 7, 13$
8	$2, 3, 5, 7$
9	$2, 3, 5, 7$

Table 4.1: Possible prime divisors of $|\tilde{G}(\mathbb{Z}/a)|$

Suppose p_j does not divide $|\widetilde{G}(\mathbb{Z}/a)|$. By Lemma 4.2 $\widetilde{G}(\mathbb{Z}/p_j^{r_j})$ is generated by elements of order a power of p_j. If $g \in \widetilde{G}(\mathbb{Z}/p_j^{r_j})$ is any such generator, we

claim that

$$(I, ..., I, g, I, ..., I) \in H \leq \widetilde{G}(\mathbb{Z}/q) = \widetilde{G}(\mathbb{Z}/a) \times \prod_i \widetilde{G}(\mathbb{Z}/p_i^{r_i}),$$

which implies $\widetilde{G}(\mathbb{Z}/p_j^{r_j}) \leq H$ as claimed. Since $\pi_b(H) = \widetilde{G}(\mathbb{Z}/b)$, there exists $g_a \in \widetilde{G}(\mathbb{Z}/a)$ such that H contains $h = (g_a, I, ..., I, g, I, ..., I)$. Since p_j is coprime to $|\widetilde{G}(\mathbb{Z}/a)|$, the order c of g_a is coprime to the order p_j^d of g there is an integer e such that $ce \equiv 1 \bmod p_j^d$. Then $h^{ce} = (I, I, ..., I, g, I, ..., I)$, proving the claim.

All that remains is to show that $\widetilde{G}(\mathbb{Z}/p_j^{r_j}) \leq H$ for p_j a prime in Table 4.1 with $p_j \geq 5$ for $n = 5, 7$ and $p_j \geq 3$ for $n = 6, 8, 9$. For each relevant prime one checks that there is an $l \geq p_j$ dividing $|\widetilde{G}(\mathbb{Z}/p_j^{r_j})|$ but not $|\widetilde{G}(\mathbb{Z}/a)|$:

- $l = 13$ works for $\Omega^+(6,3), \Omega^\pm(8,3), \Omega(9,3)$
- $l = 7$ works for $\Omega^-(6,3)$
- $l = 13$ works for $\Omega(5,5), \Omega^\pm(6,5), \Omega^\pm(8,5), \Omega(9,5)$
- $l = 31$ works for $\Omega(7,5)$
- $l = 19$ works for $\Omega(7,7), \Omega^\pm(8,7), \Omega(9,7)$
- $l = 17$ works for $\Omega(7,13)$

Then $\widetilde{G}(\mathbb{Z}/p_j^{r_j})$ is generated by elements of order l by Lemma 4.2. The same argument as in the case $l = p_j$ implies that $\widetilde{G}(\mathbb{Z}/p_j^{r_j}) \leq H$, completing the proof that $\widetilde{G}(\mathbb{Z}/b) \leq H$. This proves the theorem. □

Theorem 4.2. *If $p \geq 5$ for $d = 4, 6$ and $p \geq 3$ for $d = 5$ or $d \geq 7$, then there is no one-cusped level-p congruence subgroup of $\Omega(d, 1; \mathbb{Z})$.*

Proof. Proven in Chapter 3. □

Corollary 4.4. *Suppose $q = ab$ as in the statement of Theorem 4.1 and $H \leq \widetilde{G}(\mathbb{Z}/q)$ has preimage $\Gamma_H \leq \Omega(d, 1; \mathbb{Z})$ that is one-cusped. Then Γ_H has level dividing a. In other words, all one-cusped congruence subgroups of $\Omega(d, 1; \mathbb{Z})$ have level $2^{s_2}3^{s_3}$ for $d = 4, 6$ and level 2^s for $d = 5, 7, 8$.*

Proof. Since there is no one-cusped congruence subgroup of level p for p dividing b, Corollary 4.2 implies that $\pi_b(H)$ cannot be a proper subgroup of $\widetilde{G}(\mathbb{Z}/b)$. Indeed, the preimage of $\pi_b(H)$ in $\Omega(d, 1; \mathbb{Z})$ would be a proper one-cusped congruence subgroup of level b, which contradicts the combination of Theorem 4.2 and Corollary 4.2. Thus Theorem 4.1 implies that $H = H_a \times \widetilde{G}(\mathbb{Z}/b)$ for $H_a \leq \widetilde{G}(\mathbb{Z}/a)$. This implies that Γ_H contains the kernel of reduction mod a, hence Γ_H has level dividing a. □

Remark 4.1. *In terms of prime divisors of the level, Chapter 5 has examples showing that Corollary 4.4 is optimal.*

CHAPTER 5

REMAINING CASES

We check the remaining cases using the following Magma code to get the number of 1-cusped maximal subgroups in $\mathrm{SO}(d,1;\mathbb{Z})$. This code simply iterates over maximal subgroups of G_p and checks whether the associated hyperbolic orbifold is 1-cusped using Lemma 3.4. We use the matrix generators and Coxeter diagram relations for $\mathrm{SO}(d,1;\mathbb{Z})$ and generators for Δ taken from [3].

```
// DIMENSION 4

R := IntegerRing(q);

h1 := Matrix(R,5,5,
[0,1,0,0,0,
1,0,0,0,0,
0,0,1,0,0,
0,0,0,1,0,
0,0,0,0,1]);

h2 := Matrix(R,5,5,
[1,0,0,0,0,
0,0,1,0,0,
0,1,0,0,0,
0,0,0,1,0,
0,0,0,0,1]);

h3 := Matrix(R,5,5,
[1,0,0,0,0,
```

```
0,1,0,0,0,
0,0,0,1,0,
0,0,1,0,0,
0,0,0,0,1]);

h4 := DiagonalMatrix(R,5,[1,1,1,-1,1]);

h5 := Matrix(R,5,5,
[0,-1,-1,0,1,
-1,0,-1,0,1,
-1,-1,0,0,1,
0,0,0,1,0,
-1,-1,-1,0,2]);

H := MatrixGroup<5,R| [h1,h2,h3,h4,h5]>;

J := sub<H | h1*h2,h1*h3,h1*h4,h1*h5,
h2*h3,h2*h4,h2*h5,h3*h4,h3*h5,h4*h5>;

G<a1,a2,a3,a4,a5> := Group<a1,a2,a3,a4,a5|
a1^2,a2^2,a3^2,a4^2,a5^2,
(a1,a3),(a1,a4),(a1,a5),(a2,a4),(a2,a5),(a4,a5),
(a1*a2)^3,(a2*a3)^3,(a3*a4)^4,(a3*a5)^3>;

f := hom<G->H|a1->h1,a2->h2,a3->h3,a4->h4,a5->h5>;

D := sub<H|f(a2),f(a3),f(a4),f(a5)>;

E := D meet J;

GoodGps := [];

for A0 in MaximalSubgroups(J) do

A := A0`subgroup;

if Index(A, A meet E) eq Index(J, E) then

Append(~GoodGps, A);

end if;
```

```
end for;

#GoodGps;

for A in GoodGps do

Index(J, A);

end for;



// DIMENSION 5

R := IntegerRing(q);

h1 := Matrix(R,6,6,
[0,1,0,0,0,0,
1,0,0,0,0,0,
0,0,1,0,0,0,
0,0,0,1,0,0,
0,0,0,0,1,0,
0,0,0,0,0,1]);

h2 := Matrix(R,6,6,
[1,0,0,0,0,0,
0,0,1,0,0,0,
0,1,0,0,0,0,
0,0,0,1,0,0,
0,0,0,0,1,0,
0,0,0,0,0,1]);

h3 := Matrix(R,6,6,
[1,0,0,0,0,0,
0,1,0,0,0,0,
0,0,0,1,0,0,
0,0,1,0,0,0,
0,0,0,0,1,0,
0,0,0,0,0,1]);

h4 := Matrix(R,6,6,
[1,0,0,0,0,0,
```

```
0,1,0,0,0,0,
0,0,1,0,0,0,
0,0,0,0,1,0,
0,0,0,1,0,0,
0,0,0,0,0,1]);

h5 := DiagonalMatrix(R,6,[1,1,1,1,-1,1]);

h6 := Matrix(R,6,6,
[0,-1,-1,0,0,1,
-1,0,-1,0,0,1,
-1,-1,0,0,0,1,
0,0,0,1,0,0,
0,0,0,0,1,0,
-1,-1,-1,0,0,2]);

H := MatrixGroup<6,R| [h1,h2,h3,h4,h5,h6]>;

J := sub<H | h1*h2,h1*h3,h1*h4,h1*h5,h1*h6,
h2*h3,h2*h4,h2*h5,h2*h6,h3*h4,h3*h5,h3*h6,
h4*h5,h4*h6,h5*h6>;

G<a1,a2,a3,a4,a5,a6> := Group<a1,a2,a3,a4,a5,a6|
a1^2,a2^2,a3^2,a4^2,a5^2,a6^2,
(a1,a3),(a1,a4),(a1,a5),(a1,a6),
(a2,a4),(a2,a5),(a2,a6),(a3,a5),(a4,a6),(a5,a6),
(a1*a2)^3,(a2*a3)^3,(a3*a4)^3,(a3*a6)^3,(a4*a5)^4>;

f := hom<G->H|a1->h1,a2->h2,a3->h3,a4->h4,a5->h5,a6->h6>;

D := sub<H|f(a2),f(a3),f(a4),f(a5),f(a6)>;

E := D meet J;

GoodGps := [];

for A0 in MaximalSubgroups(J) do

A := A0`subgroup;

if Index(A, A meet E) eq Index(J, E) then
```

```
Append(~GoodGps, A);

end if;

end for;

#GoodGps;

for A in GoodGps do

Index(J, A);

end for;



// DIMENSION 6

R := IntegerRing(q);

h1 := Matrix(R,7,7,
[0,1,0,0,0,0,0,
1,0,0,0,0,0,0,
0,0,1,0,0,0,0,
0,0,0,1,0,0,0,
0,0,0,0,1,0,0,
0,0,0,0,0,1,0,
0,0,0,0,0,0,1]);

h2 := Matrix(R,7,7,
[1,0,0,0,0,0,0,
0,0,1,0,0,0,0,
0,1,0,0,0,0,0,
0,0,0,1,0,0,0,
0,0,0,0,1,0,0,
0,0,0,0,0,1,0,
0,0,0,0,0,0,1]);

h3 := Matrix(R,7,7,
[1,0,0,0,0,0,0,
0,1,0,0,0,0,0,
0,0,0,1,0,0,0,
```

```
0,0,1,0,0,0,0,
0,0,0,0,1,0,0,
0,0,0,0,0,1,0,
0,0,0,0,0,0,1]);

h4 := Matrix(R,7,7,
[1,0,0,0,0,0,0,
0,1,0,0,0,0,0,
0,0,1,0,0,0,0,
0,0,0,0,1,0,0,
0,0,0,1,0,0,0,
0,0,0,0,0,1,0,
0,0,0,0,0,0,1]);

h5 := Matrix(R,7,7,
[1,0,0,0,0,0,0,
0,1,0,0,0,0,0,
0,0,1,0,0,0,0,
0,0,0,1,0,0,0,
0,0,0,0,0,1,0,
0,0,0,0,1,0,0,
0,0,0,0,0,0,1]);

h6 := DiagonalMatrix(R,7,[1,1,1,1,1,-1,1]);

h7 := Matrix(R,7,7,
[0,-1,-1,0,0,0,1,
-1,0,-1,0,0,0,1,
-1,-1,0,0,0,0,1,
0,0,0,1,0,0,0,
0,0,0,0,1,0,0,
0,0,0,0,0,1,0,
-1,-1,-1,0,0,0,2]);

H := MatrixGroup<7,R| [h1,h2,h3,h4,h5,h6,h7]>;

J := sub<H | h1*h2,h1*h3,h1*h4,h1*h5,h1*h6,h1*h7,
h2*h3,h2*h4,h2*h5,h2*h6,h2*h7,
h3*h4,h3*h5,h3*h6,h3*h7,h4*h5,h4*h6,h4*h7,
h5*h6,h5*h7,h6*h7>;

G<a1,a2,a3,a4,a5,a6,a7> := Group<a1,a2,a3,a4,a5,a6,a7|
```

```
a1^2,a2^2,a3^2,a4^2,a5^2,a6^2,a7^2,
(a1,a3),(a1,a4),(a1,a5),(a1,a6),(a1,a7),
(a2,a4),(a2,a5),(a2,a6),(a2,a7),(a3,a5),(a3,a6),
(a4,a6),(a4,a7),(a5,a7),(a6,a7),
(a1*a2)^3,(a2*a3)^3,(a3*a4)^3,(a3*a7)^3,(a4*a5)^3,(a5*a6)^4>;

f := hom<G->H|a1->h1,a2->h2,a3->h3,a4->h4,a5->h5,a6->h6,a7->h7>;

D := sub<H|f(a2),f(a3),f(a4),f(a5),f(a6),f(a7)>;

E := D meet J;

GoodGps := [];

for A0 in MaximalSubgroups(J) do

A := A0`subgroup;

if Index(A, A meet E) eq Index(J, E) then

Append(~GoodGps, A);

end if;

end for;

#GoodGps;

for A in GoodGps do

Index(J, A);

end for;



// DIMENSION 7

R := IntegerRing(q);

h1 := Matrix(R,8,8,
[0,1,0,0,0,0,0,0,
```

```
1,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,
0,0,0,1,0,0,0,0,
0,0,0,0,1,0,0,0,
0,0,0,0,0,1,0,0,
0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,1]);

h2 := Matrix(R,8,8,
[1,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,
0,1,0,0,0,0,0,0,
0,0,0,1,0,0,0,0,
0,0,0,0,1,0,0,0,
0,0,0,0,0,1,0,0,
0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,1]);

h3 := Matrix(R,8,8,
[1,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,
0,0,0,1,0,0,0,0,
0,0,1,0,0,0,0,0,
0,0,0,0,1,0,0,0,
0,0,0,0,0,1,0,0,
0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,1]);

h4 := Matrix(R,8,8,
[1,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,
0,0,0,0,1,0,0,0,
0,0,0,1,0,0,0,0,
0,0,0,0,0,1,0,0,
0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,1]);

h5 := Matrix(R,8,8,
[1,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,
```

```
0,0,0,1,0,0,0,0,
0,0,0,0,0,1,0,0,
0,0,0,0,1,0,0,0,
0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,1]);

h6 := Matrix(R,8,8,
[1,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,
0,0,0,1,0,0,0,0,
0,0,0,0,1,0,0,0,
0,0,0,0,0,0,1,0,
0,0,0,0,0,1,0,0,
0,0,0,0,0,0,0,1]);

h7 := DiagonalMatrix(R,8,[1,1,1,1,1,1,-1,1]);

h8 := Matrix(R,8,8,
[0,-1,-1,0,0,0,0,1,
-1,0,-1,0,0,0,0,1,
-1,-1,0,0,0,0,0,1,
0,0,0,1,0,0,0,0,
0,0,0,0,1,0,0,0,
0,0,0,0,0,1,0,0,
0,0,0,0,0,0,1,0,
-1,-1,-1,0,0,0,0,2]);

H := MatrixGroup<8,R| [h1,h2,h3,h4,h5,h6,h7,h8]>;

J := sub<H | h1*h2,h1*h3,h1*h4,h1*h5,h1*h6,h1*h7,h1*h8,
h2*h3,h2*h4,h2*h5,h2*h6,h2*h7,h2*h8,
h3*h4,h3*h5,h3*h6,h3*h7,h3*h8,h4*h5,h4*h6,h4*h7,h4*h8,
h5*h6,h5*h7,h5*h8,h6*h7,h6*h8,h7*h8>;

G<a1,a2,a3,a4,a5,a6,a7,a8> := Group<a1,a2,a3,a4,a5,a6,a7,a8|
a1^2,a2^2,a3^2,a4^2,a5^2,a6^2,a7^2,a8^2,
(a1,a3),(a1,a4),(a1,a5),(a1,a6),(a1,a7),(a1,a8),
(a2,a4),(a2,a5),(a2,a6),(a2,a7),(a2,a8),
(a3,a5),(a3,a6),(a3,a7),(a4,a6),(a4,a7),(a4,a8),
(a5,a7),(a5,a8),(a6,a8),
(a1*a2)^3,(a2*a3)^3,(a3*a4)^3,(a3*a8)^3,(a4*a5)^3,(a5*a6)^3,(a6*a7)^4>;
```

```
f := hom<G->H|a1->h1,a2->h2,a3->h3,a4->h4,a5->h5,a6->h6,a7->h7,a8->h8>;

D := sub<H|f(a2),f(a3),f(a4),f(a5),f(a6),f(a7),f(a8)>;

E := D meet J;

GoodGps := [];

for A0 in MaximalSubgroups(J) do

A := A0`subgroup;

if Index(A, A meet E) eq Index(J, E) then

Append(~GoodGps, A);

end if;

end for;

#GoodGps;

for A in GoodGps do

Index(J, A);

end for;


// DIMENSION 8

R := IntegerRing(q);

h1 := Matrix(R,9,9,
[0,1,0,0,0,0,0,0,0,
1,0,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,0,
0,0,0,1,0,0,0,0,0,
0,0,0,0,1,0,0,0,0,
0,0,0,0,0,1,0,0,0,
```

```
0,0,0,0,0,0,1,0,0,
0,0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,0,1]);

h2 := Matrix(R,9,9,
[1,0,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,0,
0,0,0,1,0,0,0,0,0,
0,0,0,0,1,0,0,0,0,
0,0,0,0,0,1,0,0,0,
0,0,0,0,0,0,1,0,0,
0,0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,0,1]);

h3 := Matrix(R,9,9,
[1,0,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,0,
0,0,0,1,0,0,0,0,0,
0,0,1,0,0,0,0,0,0,
0,0,0,0,1,0,0,0,0,
0,0,0,0,0,1,0,0,0,
0,0,0,0,0,0,1,0,0,
0,0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,0,1]);

h4 := Matrix(R,9,9,
[1,0,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,0,
0,0,0,0,1,0,0,0,0,
0,0,0,1,0,0,0,0,0,
0,0,0,0,0,1,0,0,0,
0,0,0,0,0,0,1,0,0,
0,0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,0,1]);

h5 := Matrix(R,9,9,
[1,0,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,0,
0,0,0,1,0,0,0,0,0,
```

```
0,0,0,0,0,1,0,0,0,
0,0,0,0,1,0,0,0,0,
0,0,0,0,0,0,1,0,0,
0,0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,0,1]);

h6 := Matrix(R,9,9,
[1,0,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,0,
0,0,0,1,0,0,0,0,0,
0,0,0,0,1,0,0,0,0,
0,0,0,0,0,0,1,0,0,
0,0,0,0,0,1,0,0,0,
0,0,0,0,0,0,0,1,0,
0,0,0,0,0,0,0,0,1]);

h7 := Matrix(R,9,9,
[1,0,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,0,
0,0,0,1,0,0,0,0,0,
0,0,0,0,1,0,0,0,0,
0,0,0,0,0,1,0,0,0,
0,0,0,0,0,0,0,1,0,
0,0,0,0,0,0,1,0,0,
0,0,0,0,0,0,0,0,1]);

h8 := DiagonalMatrix(R,9,[1,1,1,1,1,1,1,-1,1]);

h9 := Matrix(R,9,9,
[0,-1,-1,0,0,0,0,0,1,
-1,0,-1,0,0,0,0,0,1,
-1,-1,0,0,0,0,0,0,1,
0,0,0,1,0,0,0,0,0,
0,0,0,0,1,0,0,0,0,
0,0,0,0,0,1,0,0,0,
0,0,0,0,0,0,1,0,0,
0,0,0,0,0,0,0,1,0,
-1,-1,-1,0,0,0,0,0,2]);

H := MatrixGroup<9,R| [h1,h2,h3,h4,h5,h6,h7,h8,h9]>;
```

```
J := sub<H | h1*h2,h1*h3,h1*h4,h1*h5,h1*h6,h1*h7,h1*h8,h1*h9,
h2*h3,h2*h4,h2*h5,h2*h6,h2*h7,h2*h8,h2*h9,
h3*h4,h3*h5,h3*h6,h3*h7,h3*h8,h3*h9,
h4*h5,h4*h6,h4*h7,h4*h8,h4*h9,h5*h6,h5*h7,h5*h8,h5*h9,
h6*h7,h6*h8,h6*h9,h7*h8,h7*h9,h8*h9>;

G<a1,a2,a3,a4,a5,a6,a7,a8,a9> := Group<a1,a2,a3,a4,a5,a6,a7,a8,a9|
a1^2,a2^2,a3^2,a4^2,a5^2,a6^2,a7^2,a8^2,a9^2,
(a1,a3),(a1,a4),(a1,a5),(a1,a6),(a1,a7),(a1,a8),(a1,a9),
(a2,a4),(a2,a5),(a2,a6),(a2,a7),(a2,a8),(a2,a9),
(a3,a5),(a3,a6),(a3,a7),(a3,a8),(a4,a6),(a4,a7),(a4,a8),(a4,a9),
(a5,a7),(a5,a8),(a5,a9),(a6,a8),(a6,a9),(a7,a9),(a8,a9),
(a1*a2)^3,(a2*a3)^3,(a3*a4)^3,(a3*a9)^3,(a4*a5)^3,(a5*a6)^3,(a6*a7)^3,\
(a7*a8)^4>;

f := hom<G->H|a1->h1,a2->h2,a3->h3,a4->h4,a5->h5,a6->h6,a7->h7,a8->h8,\
a9->h9>;

D := sub<H|f(a2),f(a3),f(a4),f(a5),f(a6),f(a7),f(a8),f(a9)>;

E := D meet J;

GoodGps := [];

for A0 in MaximalSubgroups(J) do

A := A0`subgroup;

if Index(A, A meet E) eq Index(J, E) then

Append(~GoodGps, A);

end if;

end for;

#GoodGps;

for A in GoodGps do

Index(J, A);
```

```
end for;
```

In Tables 5.1 and 5.2, each entry gives a list of values for $[\Gamma : H]$ for conjugacy classes of 1-cusped H that exist for the given p and d.

p	$d=4$	$d=5$	$d=6$	$d=7$	$d=8$
3	27	none	1080	none	none
5	none	none	none	none	none
7	none	none	none	none	none

Table 5.1: Maximal 1-cusped level p congruence subgroups of $\Omega(d,1;\mathbb{Z})$ for $p=3,5,7$, listed by index

r	4	5	6	7	8
1	6	6	40, 40	960, 120	1120, 1120, 960, 960, 120, 120
2	16, 16, 16, 16	none	none	none	none
3	none	none	none	?	none
4	none	none	?	?	none

Table 5.2: Maximal 1-cusped level 2^r congruence subgroups of $\Omega(d,1;\mathbb{Z})$ for $1 \leq r \leq 4$, listed by index

As listed in Table 5.1, the only 1-cusped subgroup in the $p=3,5$ cases is the subgroup of order 2 in $\mathrm{SO}(d,1;\mathbb{Z})$, which is $\Omega(d,1;\mathbb{Z})$, and there are no 1 cusped subgroups of $\mathrm{SO}(d,1;\mathbb{Z})$ for $p=7$, proving the main result.

REFERENCES

[1] Armand Borel and Gopal Prasad. Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups. Inst. Hautes Études Sci. Publ. Math., (69):119–171, 1989.

[2] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal. The Maximal Subgroups of the Low-Dimensional Finite Classical Groups. London Mathematical Society Lecture Note Series. Cambridge University Press, 2013.

[3] Brent Everitt, John G Ratcliffe, and Steven T Tschantz. Right-angled coxeter polytopes, hyperbolic six-manifolds, and a problem of siegel. Mathematische Annalen, 354(3):871–905, 2012.

[4] Alexander Lubotzky. Subgroup growth and congruence subgroups. Inventiones mathematicae, 119(1):267–295, 1995.

[5] Alexander Lubotzky and Dan Segal. Subgroup growth, volume 212. Springer, 2003.

[6] John Willard Milnor and Dale Husemoller. Symmetric bilinear forms, volume 73. Springer, 1973.

[7] G. Daniel Mostow. Strong Rigidity of Locally Symmetric Spaces.(AM-78), Volume 78. Princeton University Press, 2016.

[8] M. Ram Murty and Kathleen L. Petersen. The generalized Artin conjecture and arithmetic orbifolds. Groups and symmetries, 47:259–265, 2009.

[9] JH Conway-RT Curtis-SP Norton and RA Parker-RA Wilson. Atlas of finite groups. Clarendon Press, Oxford, 31:145–153, 1985.

[10] K. L. Petersen. One-cusped congruence subgroups of $\mathrm{PSL}_2(\mathcal{O}_k)$, 2005.

[11] K. L. Petersen. One-cusped congruence subgroups of Bianchi groups. Math. Ann., 338(2):249–282, 2007.

[12] K. L. Petersen. Counting cusps of subgroups of $\mathrm{PSL}_2(\mathcal{O}_\mathcal{K})$. Proceedings of the American Mathematical Society, 136(7):2387–2393, 2008.

[13] Leonid Potyagailo and Ernest Vinberg. On right-angled reflection groups in hyperbolic spaces. Commentarii Mathematici Helvetici, 80(1):63–73, 2005.

[14] Gopal Prasad. Strong rigidity of $\mathbb{Q}$-rank 1 lattices. Inventiones Mathematicae, 21(4):255–286, 1973.

[15] John G. Ratcliffe. Foundations of hyperbolic manifolds, volume 149 of Graduate Texts in Mathematics. Springer, 2019. Third edition.

[16] Alan W. Reid. Arithmeticity of knot complements. Journal of the London Mathematical Society, 2(1):171–184, 1991.

[17] Matthew Stover. On the number of ends of rank one locally symmetric spaces. Geometry & Topology, 17(2):905–924, 2013.

[18] Robert Wilson. The finite simple groups, volume 147. Springer, 2009.