

Eigenvalues of hyperbolic elements in Kleinian groups

D. D. Long* & A. W. Reid†

July 21, 2009

1 Introduction

Let Γ be a torsion-free Kleinian group, so that $M = \mathbf{H}^3/\Gamma$ is an orientable hyperbolic 3-manifold. The non-trivial elements of Γ are classified as either parabolic or hyperbolic. If $\gamma \in \Gamma$ is hyperbolic, then γ has an axis in \mathbf{H}^3 which projects to a closed geodesic g_γ in M (which depends only on the conjugacy class of γ in Γ). The element γ acts on its axis by translating and possibly rotating around the axis. In terms of eigenvalues, if $\gamma \in \Gamma$ is hyperbolic, we let

$$\lambda = \lambda_\gamma = r_\gamma e^{i\theta_\gamma}$$

be the eigenvalue of γ (more accurately of a pre-image of γ in $\mathrm{SL}(2, \mathbf{C})$) for which $|\lambda| > 1$. The angle θ_γ takes values in $[0, 2\pi)$, and is the rotation angle mentioned above. We will usually suppress the subscripts. A hyperbolic element is called *purely hyperbolic* if and only if $\theta = 0$, or equivalently, if $\mathrm{tr}(\gamma) \in \mathbf{R}$.

The length of the closed geodesic g_γ is given by $2 \ln |\lambda|$ and the collections of these lengths counted with multiplicities is a well-known important geometric invariant of the manifold M (see [3] and [4] and the references therein). On the other hand, little seems known about the “angle spectrum” for hyperbolic 3-manifolds. If Γ is not Fuchsian, then there must be hyperbolic elements that are not purely hyperbolic. However, the following question naturally arises as a first step beyond this.

Question 1: *Let $M = \mathbf{H}^3/\Gamma$ be a finite volume orientable hyperbolic 3-manifold, does Γ contain infinitely many conjugacy classes of hyperbolic elements, no power of which is purely hyperbolic?*

It is implicit in [3] (see the discussion in §4.1 below) that Question 1 has an affirmative answer for arithmetic Kleinian groups. The purpose of this note is to establish that this holds more generally. Namely we prove:

Theorem 1.1 *Let $M = \mathbf{H}^3/\Gamma$ be as in Question 1. Then Γ contains infinitely many conjugacy classes of primitive hyperbolic elements with the property that they have no power which is purely hyperbolic.*

The proof of Theorem 1.1 is given in §3 and proceeds by first establishing the existence of one primitive hyperbolic element for which no power is purely hyperbolic. The extension which shows that there are infinitely many conjugacy classes of such elements can be made either by an algebraic argument or a geometric argument, and we include both.

There is an obvious generalization of the previous discussion to higher dimensions, and in §5 we provide a proof of the following result.

*supported in part by the NSF

†supported in part by the NSF

Theorem 1.2 *Let $M = \mathbf{H}^n/\Gamma$ be an orientable hyperbolic n -manifold of finite volume, where $n > 3$. Then Γ contains infinitely many primitive hyperbolic elements with the property that they have no power which is purely hyperbolic.*

As in the proof of Theorem 1.1, the proof of Theorem 1.2 proceeds by first establishing the existence of one primitive hyperbolic element for which no power is purely hyperbolic. However, the method of proof is different to that given for dimension 3.

This paper is a revised version of a paper where we proved a more general version of Theorem 1.1. However, it was subsequently pointed out to us by Gopal Prasad, that the main results of that paper follow from very general results contained in his work with Rapinchuk ([12]). We have therefore decided to give a proof only in the case of finite volume hyperbolic manifolds so as to illuminate the ideas in that setting, and thereby avoiding some of the issues in the general case of [12].

Acknowledgments: We thank Mahan Mj for email correspondence on the “angle spectrum” that prompted us to write this down carefully, and Chris Leininger, Alex Lubotzky and Gopal Prasad for comments on the previous version of this paper. We also wish to thank Ted Chinburg and Emily Hamilton for many interesting conversations on matters related to this arising from [3]. We also thank the referee for their careful reading of the paper, and many very useful comments. The second author wishes to thank the Institute for Advanced Study for its hospitality whilst this paper was written.

2 Some preliminaries for the proof of Theorem 1.1

2.1

By a number field k we will mean a finite extension of \mathbf{Q} . The ring of integers of k will be denoted R_k , and $R_S = R_k[S]$ will denote a subring of k where a finite number of k -primes S are inverted. A place ν of k will be one of the canonical absolute values of k . The finite places of k correspond bijectively to the prime ideals of R_k . We denote by k_ν the local field obtained as the completion of k at a place ν . In the case of finite places we sometimes abuse notation and write the prime \mathcal{P} rather than the associated place ν when referring to the completions.

If \mathcal{A} is an ideal of R_k , the norm of \mathcal{A} is the cardinality of the quotient ring R_k/\mathcal{A} and is denoted by $N\mathcal{A}$. When \mathcal{A} is a prime ideal, then $N\mathcal{A} = p^t$ for some rational prime p , and R_k/\mathcal{A} is a finite field of characteristic p . We will denote this finite field by $\mathbf{F}_{\mathcal{A}}$; this is usually called the residue class field.

2.2

For convenience we record two well-known results about extensions of number fields. We refer the reader to [5] for example for more details.

The first of these follows from the fact that if $\zeta = e^{2\pi i/n}$ is a primitive n -th root of unity, then $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \phi(n)$ (where ϕ denotes the Euler ϕ -function) and $\phi(n)$ is well-known to go to infinity with n .

Proposition 2.1 *There are only finitely many roots of unity ζ for which $\mathbf{Q}(\zeta)$ has bounded degree over \mathbf{Q} .*

The second result we need requires some additional notation. Let k be a number field and L a proper subfield. Suppose that p is a rational prime, P is an L -prime lying over p , and \mathcal{P} is a k -prime lying over P . Then we get extensions of local fields,

$$\mathbf{Q}_p \subset L_P \subset k_{\mathcal{P}},$$

and extensions of finite fields

$$\mathbf{F}_p \subset \mathbf{F}_P \subset \mathbf{F}_{\mathcal{P}}.$$

Note that, even though L is a proper subfield of k , the field extensions shown above may all be equalities. With this we have the following standard consequence of the Chebotarev Density theorem (see for example [10] Chapter VII, 13.4). We sketch a proof for convenience.

Proposition 2.2 *In the notation above, there exist infinitely many rational primes p for which the field extension $\mathbf{F}_{\mathcal{P}}/\mathbf{F}_P$ has degree at least 2.*

Proof: Let K denote the Galois closure of k . Since L is a proper subfield of k there exists a Galois automorphism $\sigma \in \text{Gal}(K/L)$ such that σ is trivial on L and non-trivial on k . The Chebotarev density theorem provides a positive density set of primes of \mathcal{Q} in K for which the induced Galois automorphism $\bar{\sigma}$ of the Galois extension $\mathbf{F}_{\mathcal{Q}}/\mathbf{F}_P$ has order $|\sigma|$. In particular $\bar{\sigma}$ is trivial on \mathbf{F}_P but not on $\mathbf{F}_{\mathcal{P}}$; i.e. $\mathbf{F}_{\mathcal{P}}$ is a proper extension of \mathbf{F}_P as required. \square

2.3

We will also make use of the classification of elements in $\text{PSL}(2, \mathbf{F})$ where \mathbf{F} is a finite field. The following is easily deduced from [15] §6.23. We will exclude the prime 2 from all considerations and henceforth any prime p that is mentioned is odd.

Proposition 2.3 *Suppose that \mathbf{F} is a finite field of order p^t , and $x \in \text{PSL}(2, \mathbf{F})$ a non-trivial element. Then either x is unipotent and has order p , or the order of x is a divisor of $(p^t \pm 1)/2$. Moreover, for each divisor m of $(p^t \pm 1)/2$, there is an element of $\text{PSL}(2, \mathbf{F})$ of order m .*

3 Proof of Theorem 1.1

Before commencing with the proof we introduce some notation and make some preliminary comments. First observe that if $\gamma \in \Gamma$ is a primitive hyperbolic element, $\Delta < \Gamma$ a subgroup of finite index and $\gamma^n = \delta \in \Delta$ is a hyperbolic element for which no power is purely hyperbolic, then it is easy to see that γ also has the property that it has no power which is purely hyperbolic.

Also note that to prove Theorem 1.1, it suffices to establish Theorem 1.1 for a normal subgroup of finite index in Γ . Briefly, suppose that $\Delta < \Gamma$ of index N , and $\{\delta_j\}$ is a collection of non-conjugate (in Δ) of primitive (in Δ) hyperbolic elements with the property that no power of δ_j is purely hyperbolic. Let γ_j be primitive hyperbolic elements in Γ with $\gamma_j^{n_j} = \delta_j$. From the previous paragraph, no power of γ_j is purely hyperbolic. Thus it suffices to show that infinitely many of the elements γ_j are not conjugate in Γ . Therefore suppose to the contrary that infinitely many of the elements γ_j are conjugate, and fix one such element which we denote by γ with $\gamma^n = \delta \in \Delta$. Thus, there are elements $x_j \in \Gamma$ such that $x_j \gamma x_j^{-1} = \gamma_j$. Then we have, $x_j \gamma^N x_j^{-1} = \gamma_j^N$. Since Δ is a normal subgroup of index N , then N is divisible by n and n_j for each j . Hence we deduce that

$$x_j \delta^m x_j^{-1} = \delta_j^{m_j} \text{ for some integers } m, m_j \text{ bounded by } N.$$

Thus, the elements $\delta_j^{m_j}$ have bounded translation lengths, so the elements δ_j have bounded translation lengths, and therefore, infinitely many of the elements δ_j are conjugate in Δ (being of finite co-volume). However, this contradicts the assumption on $\{\delta_j\}$.

A well-known consequence of Mostow-Weil Rigidity is that the trace-field of Γ is a number field (see

[9] for example). In addition, this field is obviously not a subfield of \mathbf{R} , for if it were, then Γ would be conjugate into $\mathrm{PSL}(2, \mathbf{R})$, contradicting the hypothesis that M has finite volume. Let k denote the invariant trace-field of Γ ; i.e. the trace-field of the normal subgroup of finite index $\Gamma^{(2)} < \Gamma$ (see [9] for more). Given the discussion above, to prove Theorem 1.1 we may assume that $\Gamma = \Gamma^{(2)}$. As is well-known, and is discussed in [7] for example, for all but a finite number of k -primes ν , there are natural reduction homomorphisms

$$\pi_\nu : \Gamma \longrightarrow \mathrm{PSL}(2, \mathbf{F}_\nu).$$

Since Γ is a non-elementary Kleinian group, it is Zariski dense. Letting Ad denote the adjoint representation of $\mathrm{SL}(2, \mathbf{C})$, a theorem of Vinberg [17] shows that k coincides with the field $\mathbf{Q}(\mathrm{trAd}(\gamma) : \gamma \in \Gamma)$ and Strong Approximation in the form of [18] Theorem 10.5 applies (see [11], or [7] for a more elementary approach for $\mathrm{SL}(2)$ in the case of ν dividing a rational prime p which splits completely in k). More precisely, for infinitely many of the primes ν as above, the homomorphism π_ν is surjective. This is the reason for the passage to the group $\Gamma^{(2)}$.

We need to be more selective in the primes ν as we now discuss. The trace of a purely hyperbolic element is real, so such a trace will generate a real subfield of k , which by the remarks above, is a proper subfield of k . We will denote by $k_{\mathbf{R}}$ the maximal real subfield of k . Clearly, this contains all the fields $\mathbf{Q}(\mathrm{tr}(\gamma))$ where γ is a purely hyperbolic element of Γ . Applying Proposition 2.2 to the field extension $k/k_{\mathbf{R}}$, we can find infinitely many rational primes p such that if ν and ω denote a k -prime and $k_{\mathbf{R}}$ prime with $\nu|\omega|p$, then the extension of residue class fields $\mathbf{F}_\nu/\mathbf{F}_\omega$ has degree at least 2. We will denote by \mathcal{S} the set of such primes in k for which the homomorphism π_ν is surjective.

Completing the proof of Theorem 1.1:

We will first establish the following claim.

Claim 1: *There exists a primitive hyperbolic element in Γ with the property that no power is purely hyperbolic.*

Proof of Claim 1: We begin by noting that if $\gamma \in \Gamma$ is a hyperbolic element for which some power is purely hyperbolic, then $\lambda = re^{i\theta}$ and $e^{i\theta}$ is a root of unity. Given this, we have the following simple lemma.

Lemma 3.1 *Let Γ be as above. Then there is a positive integer N so that if $re^{i\theta}$ is an eigenvalue of a hyperbolic element of Γ with $e^{i\theta}$ a root of unity, then $e^{iN\theta} = 1$.*

Proof: Let d denote the degree of k over \mathbf{Q} . Hence the eigenvalue $\lambda = re^{i\theta}$ has degree at most $2d$ over \mathbf{Q} . Let $K = k(\lambda)$. The complex conjugate field \bar{K} has the same degree, so that the smallest field containing K and \bar{K} has degree at most $(2d)^2$. This field contains $\lambda/\bar{\lambda} = e^{2i\theta}$.

If now $e^{i\theta}$ is a root of unity, then the above paragraph shows that it lies in a field of degree at most $2(2d)^2$ over \mathbf{Q} , thus bounding the degree of the root of unity. Proposition 2.1 now shows there are only finitely many such roots of unity, and this provides the required N . \square

Thus to establish Claim 1, we need only show that there is a hyperbolic element for which γ^m is not purely hyperbolic for all $0 < m \leq N$, (where N is as in Lemma 3.1). To achieve this we argue as follows.

With N as in Lemma 3.1, we fix $\nu \in \mathcal{S}$ with $\nu|p$ and assume that $p \gg N$. Proposition 2.3 shows that the orders of the elements in $\mathrm{PSL}(2, \mathbf{F}_\nu)$ are either p , or divisors of $(|\mathbf{F}_\nu| \pm 1)/2$, and in the latter case, the maximal possible order is attained. Denote this maximal order by R_ν , and let

$\delta \in \mathrm{PSL}(2, \mathbf{F}_\nu)$ be an element of order R_ν . Note that δ is not unipotent, since these only have order p .

Using Proposition 2.3, observe that since $\mathbf{F}_\nu/\mathbf{F}_\omega$ is at least two, R_ν is around p times larger than the maximal possible order for any element of $\mathrm{PSL}(2, \mathbf{F}_\omega)$. Denote this maximal possible order by R_ω . We then have that R_ν is around $p \cdot R_\omega$. Notice that since traces control the order of an element, this implies that R_ν is around p times larger than the order of any element whose trace lies \mathbf{F}_ω .

Pick some $\gamma \in \Gamma$ lying in $\pi_\nu^{-1}(\delta)$. We claim that γ cannot have any power which is purely hyperbolic. The reason is this. If there is such a power, then γ^m is purely hyperbolic for some $0 < m \leq N$. It follows that γ^m now has real trace, so that the order of δ is bounded above by $m \cdot R_\omega$. However, we chose $p \gg N$, so that $R_\nu \sim p \cdot R_\omega \gg m \cdot R_\omega$, contradicting our choice of δ as an element of order R_ν .

Given such an element γ , then a primitive element in the cyclic subgroup containing γ finishes the proof of Claim 1. \square

Remark: This argument shows that *all* the elements γ in $\pi_\nu^{-1}(\delta)$ are hyperbolic and no power is purely hyperbolic.

We now complete the proof of the existence of infinitely many conjugacy classes of elements with no purely hyperbolic power. We give both an algebraic argument and a geometric one.

Algebraic argument: We argue as follows. Let α_1 be any primitive hyperbolic element that is produced via the method of Claim 1. Let $\Gamma_2 = \ker(\pi_\nu)$. Now we can choose a different prime $\nu' \in \mathcal{S}$ (with residue class field $\mathbf{F}_{\nu'}$) so that the reduction homomorphism

$$\pi_{\nu'} : \Gamma \longrightarrow \mathrm{PSL}(2, \mathbf{F}_{\nu'}),$$

restricted to Γ_2 is onto. Moreover, an easy argument (e.g. Theorem 4.6 of [6]) now shows that the homomorphism

$$\Gamma \longrightarrow \mathrm{PSL}(2, \mathbf{F}_\nu) \times \mathrm{PSL}(2, \mathbf{F}_{\nu'})$$

is also onto. Choose a $\gamma_2 \in \Gamma$ with the property that in the second coordinate it maps to an element of maximal order and in the first coordinate it maps to a unipotent element ξ . Notice that ξ has order precisely p and Proposition 2.3 shows that $\langle \xi \rangle$ is a maximal cyclic subgroup of $\mathrm{PSL}(2, \mathbf{F}_\nu)$.

Now choose the primitive element in Γ associated to the element γ_2 , and denote this element by α_2 . As above, consideration of the image of α_2 in the second factor shows that no power is pure hyperbolic. We claim that no power of α_1 is conjugate to any power of α_2 . The reason is this. Hyperbolic elements with this property must simultaneously conjugate into a single cyclic subgroup of Γ . Since the elements α_1 and α_2 are primitive in Γ , they must both be generators of this cyclic group, and this implies that they are conjugate (up to inverting one of them) before taking powers. However, α_2 has order p in the first factor and α_1 has maximal order in the first factor, and in particular much larger than p . Hence, these elements can never be conjugate.

The theorem is proved by repeating this argument making use of the infinitude of primes in the set \mathcal{S} . \square

Geometric argument: As in the previous setting, we fix one primitive element provided by the proof of Claim 1, $\alpha = \alpha_1$ say, so that $\pi_\nu^{-1}(\delta) = \alpha \cdot \ker(\pi_\nu)$. Now by construction, everything in this coset maps to an element of order R , and therefore all the primitive elements associated to such elements map to elements of maximal order too. Hence, as remarked above, they are all hyperbolic elements with no power being purely hyperbolic. To construct infinitely many non-conjugate primitive elements in this case we argue as follows. We will use ℓ to denote the hyperbolic length in the hyperbolic 3-manifold $M = \mathbf{H}^3/\Gamma$.

Fix a number $K \gg 10\ell(g_\alpha)$ say, and let $g \subset M$ be a closed geodesic with length $\ell(g) > K$. Now choose a point p on g and some small compact ball $B_1 \subset M = \mathbf{H}^3/\Gamma$ centered at p which is disjoint from all the primitive closed geodesics in M which have length at most K . Fix some lift of B_1 (still denoted B_1) and some lift of g (still denoted g) in \mathbf{H}^3 which passes through B_1 . We next choose very small open neighbourhoods N_+, N_- of the endpoints of this lift of g to the sphere at infinity, so that any geodesic in \mathbf{H}^3 with one endpoint in N_+ and one endpoint in N_- must run through B_1 .

Now $\ker(\pi_\nu)$ and Γ have limit sets the entire sphere-at-infinity. Thus, there exists an element $\beta \in \ker(\pi_\nu)$ with one fixed point in N_+ and one in N_- . By standard arguments, for k sufficiently large, the element $\beta^k \alpha \beta^k$ also has fixed points in those neighbourhoods. Let α_2 be the primitive hyperbolic element in the cyclic group containing $\beta^k \alpha \beta^k$. By construction, g_{α_2} runs through the ball B_1 in M , so that by choice of B_1 it has length $> K > 10\ell(\alpha)$ and in particular, α_2 is not conjugate to α . However α_2 is conjugate to $\alpha \beta^{2k}$ which lies in $\pi^{-1}(\delta)$, so that it has no power which is purely hyperbolic.

Now repeat this argument by choosing a small ball B_2 missing all geodesics of length at most $K_2 \gg 10\ell(\alpha_2)$. It is clear that repeating this construction provides infinitely many distinct primitive elements (up to conjugacy). \square

4 Comments on the case of arithmetic Kleinian groups

4.1

We begin by discussing the proof of Theorem 1.1 for arithmetic hyperbolic 3-manifolds that is implicit in [3]. It is convenient to work with arithmetic Kleinian groups derived from a quaternion algebra (i.e. those for which the invariant trace-field coincides with the trace-field). We refer the reader to [3] and [9] for more details. In the notation of §3, if k denotes the trace-field and $k_{\mathbf{R}}$ the maximal real subfield, then the analysis in [3] breaks into two cases: either $[k : k_{\mathbf{R}}] > 2$ or $[k : k_{\mathbf{R}}] = 2$.

The former case is straightforward to handle, since there are no purely hyperbolic elements in this case (see [9] Theorem 5.3.1).

The latter case is handled using Lemmas 4.3 and 5.2 of [3]. Briefly, Lemma 5.2 of [3] provides infinitely many hyperbolic elements for which the eigenvalue λ generates a field $\mathbf{Q}(\lambda)$ which is distinct from $\mathbf{Q}(\bar{\lambda})$. However, if λ is the eigenvalue of a hyperbolic element for which some power is purely hyperbolic it can be shown that $\mathbf{Q}(\lambda) = \mathbf{Q}(\bar{\lambda})$, and hence a contradiction.

4.2

More is implicit in [3] as we now discuss, and that we are unable to establish in general.

If $\lambda = re^{i\theta}$ is the eigenvalue for a hyperbolic element for which no power is purely hyperbolic, then $e^{i\theta}$ is an algebraic number that is not a root of unity. A stronger version of Question 1 to ask is:

Question 2: *For those eigenvalues associated to hyperbolic elements no power of which is purely hyperbolic, is the collection of fields $\mathbf{Q}(e^{i\theta})$ infinite?*

Claim 2: *Question 2 has an affirmative answer in the arithmetic case.*

Proof: As in §4.1, is convenient to work with arithmetic Kleinian groups derived from a quaternion algebra. Suppose that there are only finitely many such fields. Then there are only finitely many fields $\mathbf{Q}(e^{2i\theta}) = \mathbf{Q}(\lambda/\bar{\lambda})$. Now it is shown in [3] (see Lemma 5.2 and Proposition 4.4), that we can

find infinitely many distinct hyperbolic elements (no power of which is purely hyperbolic) such that the Galois closure $\mathbf{Q}(\lambda)^{\text{cl}}$ of $\mathbf{Q}(\lambda)$ over \mathbf{Q} coincides with $\mathbf{Q}(\lambda\bar{\lambda})^{\text{cl}}$ (the Galois closure of $\mathbf{Q}(\lambda\bar{\lambda})$ over \mathbf{Q}). Furthermore, the proof of Lemma 5.2 of [3] shows that these hyperbolic elements can be taken to be primitive and non-conjugate (since their respective eigenvalues generate distinct quadratic extensions of the invariant trace-field). Now for these λ , it can be shown that $\mathbf{Q}(\lambda\bar{\lambda})^{\text{cl}} = \mathbf{Q}(\lambda/\bar{\lambda})^{\text{cl}}$ (the Galois closure of $\mathbf{Q}(\lambda/\bar{\lambda})$ over \mathbf{Q}). Hence $\mathbf{Q}(\lambda)^{\text{cl}} = \mathbf{Q}(\lambda/\bar{\lambda})^{\text{cl}}$.

Consequently, if there are only finitely many fields $\mathbf{Q}(\lambda/\bar{\lambda})$, there are only finitely many fields arising as $\mathbf{Q}(\lambda)^{\text{cl}}$, and this implies that there are in fact only finitely many possibilities for λ , which is a contradiction. \square

5 The higher dimensional setting

Throughout this section, we shall always assume that $n \geq 4$. We begin with some preliminary discussion.

5.1

A hyperbolic element $\gamma \in \text{SO}_0(n, 1)$ is conjugate in $\text{SO}_0(n, 1)$ to an element of the form

$$\left(\begin{array}{c|c} \alpha_\gamma & 0 \\ \hline 0 & T_\gamma \end{array} \right),$$

where α_γ has real eigenvalues λ and $1/\lambda$ with $|\lambda| > 1$, and $T_\gamma \in \text{O}(n-1)$. In this case, a hyperbolic element is called purely hyperbolic if $T_\gamma = 1$. If γ is a hyperbolic element that has a purely hyperbolic power, then T_γ must have finite order.

Let $M = \mathbf{H}^n/\Gamma$ be orientable and have finite volume. As is well-known (see [13]), Γ can be conjugated in $\text{O}_0(n, 1)$ to have entries in a (real) number field. Furthermore, Vinberg [16] showed that there is a minimal field of definition for this number field. We will denote this by k in what follows. Using this number field, an argument similar to that used in Lemma 3.1 proves the following lemma.

Lemma 5.1 *Let Γ be as above. Then there is a positive integer N such that if $\gamma \in \Gamma$ has a purely hyperbolic power, then $T_\gamma^N = 1$.*

Remark: As is well-known there are infinitely rational primes that split completely in k (see [5]). We will denote by \mathcal{V} be the collection of such primes. As in the case of dimension 3, for convenience, we will exclude any prime from \mathcal{V} for which the residue class field has characteristic 2.

5.2

We will use some facts about the simple groups of orthogonal type (see [15] or [2] for more details).

Let f be an m -dimensional quadratic form over the finite field \mathbf{F} of cardinality q , where to simplify some of the discussion we assume q is an odd prime. In the case when m is also odd, there is a unique orthogonal group $\text{O}(m, q)$ up to isomorphism, and when m is even there are two $\text{O}_\pm(m, q)$ (see [15] p 377 Theorem 5.8). Let $\text{SO}(m, q)$ and $\text{SO}_\pm(m, q)$ denote the special orthogonal groups in these cases, and let $\Omega(m, q) = [\text{O}(m, q), \text{O}(m, q)]$ when m is odd (resp. $\Omega_\pm(m, q) = [\text{O}_\pm(m, q), \text{O}_\pm(m, q)]$ when m is even) where $[G, G]$ denotes the commutator subgroup of a group G . When m is even $\Omega_\pm(m, q)$ has index 2 in $\text{SO}_\pm(m, q)$ and has a center of order 1 or 2. Let $\text{P}\Omega_\pm(m, q)$ be the central quotient group.

We summarize the important facts for us in the following theorem (see [15] *loc. cit.* or [2] pp. 6-7 for a discussion):

Theorem 5.2

1. $\Omega(2m+1, q)$ is a simple subgroup of $O(2m+1, q)$ of index 4 and has order $\frac{1}{2}q^{m^2} \prod_1^m (q^{2i} - 1)$.
2. $\Omega(2m, q)$ is a subgroup of $O(2m, q)$ of index 4 and the central quotient groups $P\Omega_{\pm}(2m, q)$ are simple groups whenever $m \geq 3$. These groups have orders

$$\frac{1}{d}q^{m(m-1)}(q^m - 1) \prod_1^{m-1} (q^{2i} - 1), \text{ where } d = (4, q^m - 1), \text{ (in the case of +)}$$

and

$$\frac{1}{d}q^{m(m-1)}(q^m + 1) \prod_1^{m-1} (q^{2i} - 1), \text{ where } d = (4, q^m + 1), \text{ (in the case of -)}.$$

Remark: The cases of \pm are distinguished by the discriminant of the quadratic form. When the discriminant is a square in \mathbf{F}_q , we are in the case of $+$, and the non-square case corresponds to $-$.

As in §3 (using the minimal field of definition k), we will consider reduction homomorphisms

$$\pi_{\nu} : \Gamma \rightarrow \text{SO}(n, 1; q),$$

for $\nu \in \mathcal{V}$.

Strong Approximation in this case gives ([11], [18] or [8] for a discussion of the proof of the version stated below):

Theorem 5.3 *In the notation above, for all but a finite number of primes $\nu \in \mathcal{V}$, we have*

1. $\Omega(n+1, q) \leq \pi_{\nu}(\Gamma) \leq \text{SO}(n+1; q)$, when $n+1$ is odd.
2. $P\Omega_{\pm}(n+1, q) \leq P\pi_{\nu}(\Gamma) \leq \text{PSO}_{\pm}(n+1; q)$, when $n+1$ is even (where the notation indicates that only the correct sign is chosen in the subscript).

It is necessary for us to sharpen this discussion a little so as to better suit our needs. In particular we will pass to an infinite subset of primes $\mathcal{V}_0 \subset \mathcal{V}$ that have some additional constraints. (Actually we need only that \mathcal{V}_0 is nonempty.) Firstly, Lemma 5.1 provides an integer N such that if $\beta \in \Gamma$ is a hyperbolic element that has some power that is purely hyperbolic, then $T_{\beta}^N = 1$. Thus the eigenvalues of T_{β} are N -th roots of unity. Secondly, in the case when $(n+1)$ is even, we wish to restrict to those primes so as to ensure that -1 is a square in \mathbf{F}_q , and so the form of signature $(n, 1)$ determines a form over \mathbf{F}_q whose discriminant is a square (recall the Remark after Theorem 5.2).

Given the remarks of the previous paragraph, henceforth, we will restrict attention to those reduction homomorphisms arising from the (infinite) subset of primes $\mathcal{V}_0 \subset \mathcal{V}$ that divide rational primes that split completely in the field K obtained by adjoining to k the N -th roots of unity together with a square root of -1 . That \mathcal{V}_0 is still infinite is a well-known consequence of the Cebatorev Density theorem. In particular, we have arranged that when $n+1$ is even, we are in the case of $+$ in Theorems 5.2 and 5.3.

We prove the following rather general lemma:

Lemma 5.4 *Suppose in the notation established above, that T_{β} is the rotational part of some element of Γ which has finite order r_{β} (in particular, this order divides N).*

Then for any $\nu \in \mathcal{V}_0$ lying over a rational prime q , r_{β} divides $|\text{O}(n-1; q)|$.

Proof: Note that it suffices to construct *any* element of order r_β in $O(n-1; q)$.

Since by construction K contains all the relevant N -th roots of unity, it contains $c = \cos(2\pi/r_\beta)$ and $s = \sin(2\pi/r_\beta)$. Note that $c, s \in K$, and that $2c$ and $2s$ are algebraic integers. Consider the element

$$\left(\begin{array}{cc|c} c & s & 0 \\ -s & c & 0 \\ 0 & 0 & \text{Id} \end{array} \right) \in O(n-1; K),$$

where the orthogonal group is that of the standard positive definite quadratic form over \mathbf{R} of signature $(n-1, 0)$ with coefficients in K . Observe that for the primes q under consideration, the appropriate reduction homomorphism carries this element into $O(n-1; q)$.

The proof of the lemma is completed with the observation that the image of this element has order r_β in $O(n-1; q)$. This will follow from a theorem of Minkowski (see Lemma 2.4 of [8] for example).

Lemma 5.5 *Let L be a number field, S be a finite collection of prime ideals in R_L , and $\wp \subset R_S$ be a prime ideal lying over the rational prime $p \neq 2$. Then $\ker\{\pi_\wp : \text{GL}(n, R_S) \rightarrow \text{GL}(n, R_S/\wp)\}$ contains no q -torsion for any primes q not divisible by \wp .*

We will apply Lemma 5.5 with S the set of K -prime divisors of 2. Recall that we are considering a subset of those reduction homomorphisms associated to primes splitting completely in K . In addition, since a rational prime $t|N$ will be ramified in $\mathbf{Q}(\zeta_N)$, t cannot be divisible by any prime in the set \mathcal{V}_0 . That is to say, the above element must have order r_β in $O(n-1; q)$ as required. \square

5.3 Proof of Theorem 1.2.

We need one more ingredient before embarking on the proof of Theorem 1.2. As in the proof of Theorem 1.1, we need control on the orders of certain elements in the finite simple groups given in Theorem 5.2. To that end, for convenience we recall Zsigmondy's Theorem [19] (see also [14] for a short proof of this and some related results).

Theorem 5.6 *Let a and n be integers greater than 1. Exclude the cases (1) $a = 2^r - 1$, $r \geq 2$ and $n = 2$; and (2) $a = 2$ and $n = 6$.*

Then there exists a prime s such that $s|(a^n - 1)$, but for each $j < n$, s does not divide $a^j - 1$.

A prime divisor as in the conclusion of Theorem 5.6 is called a *primitive prime divisor* (or sometimes a *Zsigmondy prime*).

We now complete the proof of Theorem 1.2 by arguing as follows. Since the property of being a hyperbolic element having no power that is purely hyperbolic is preserved by passage to subgroups of finite index, we will assume that the reduction homomorphisms π_ν surject Γ onto the finite simple groups as given in Theorem 5.3. Since $n \geq 4$ is fixed, for convenience of notation, we will simply denote any of these finite simple groups by Ω_q .

Fix some such prime $\nu \in \mathcal{V}_0$ lying over the rational prime q , and let p be a primitive prime divisor of $q^{2^m} - 1$ (when $n = 2m$, i.e. $n+1$ is odd) or a primitive prime divisor of $q^{2^{(m-1)}} - 1$ (when $n = 2m - 1$, i.e. $n+1$ is even). Note that since we are always assuming $n \geq 4$, and q is odd we can apply Theorem 5.6. By Cauchy's theorem, there is an element $\delta \in \Omega_q$ of order p . Pick some $\gamma \in \Gamma$, with $\pi_\nu(\gamma) = \delta$. Then the proof is completed by the following claim.

Claim 3: No power of γ is purely hyperbolic.

Proof of Claim 3: To begin with, suppose that $\beta \in \Gamma$ is a hyperbolic element for which some power is purely hyperbolic. Then applying Lemma 5.4, we see that if we raise β to the power $|\mathrm{O}(n-1; q)|$, it becomes purely hyperbolic. Now since such any purely hyperbolic element is conjugate in $\mathrm{SO}_0(n, 1)$ to an element with rotational part being the identity, it follows that the image under the reduction homomorphism π_ν is an element whose order divides $q(q^2 - 1)/2$ (recall Proposition 2.3). Putting these two observations together we see that the image of the given β under π_ν is an element whose order divides $q(q^2 - 1)|\mathrm{O}(n - 1; q)|/2$.

We next claim that that p does not divide $|\mathrm{O}(n-1; q)|$. The reason is this: the order of $\mathrm{O}(n-1; q)$ differs from the order of the corresponding finite simple group of that orthogonal type by a factor of most 4 (cf. Theorems 5.2 and 5.3). As remarked above, we have arranged that when n is odd (by choice of q) that the finite simple group which arises is of $+$ type. Now it is visible from the formula of Theorem 5.2 that the property that p is a primitive prime divisor ensures it cannot divide the order of $|\mathrm{O}(n - 1; q)|$.

Finally, recall that we chose $\gamma \in \Gamma$ so that $\pi_\nu(\gamma) = \delta$, an element of order p . We claim that no power of γ is purely hyperbolic. The argument is that the above discussion shows that if it were, its order would divide $q(q^2 - 1)|\mathrm{O}(n - 1; q)|/2$. However note that p being a primitive prime divisor and the condition $n \geq 4$, means that p does not divide $q^2 - 1$ and we have already argued that p does not divide $|\mathrm{O}(n - 1; q)|$. This contradiction finishes the proof of Claim 3. \square

The proof of Theorem 1.2 is completed using the geometric argument provided in §3. Briefly, notice that the argument to produce one element given above, shows that any element γ in $\pi_\nu^{-1}(\delta)$ is hyperbolic and no power is purely hyperbolic. The argument now proceeds as before. \square

Remark: It was pointed out to us by Alex Lubotzky that the argument given above still works in dimension 3. In this case, running the arguments of §5.2 and 5.3, we have (in the notation above) $m = 2$, so the exponent is 2. Now the excluded values in Theorem 5.6(1) would be primes q of the form $2^r - 1$; i.e. Mersenne primes. It is still an open problem as to whether there are infinitely many Mersenne primes, however, even if this is the case, it is known that the density of Mersenne primes is small [1] and one can still therefore find a primitive prime divisor.

References

- [1] P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff Jr., *The new Mersenne conjecture*, Amer. Math. Monthly **96** (1989), 125–128.
- [2] R. Carter, *Simple groups of Lie type*, Pure and Applied Mathematics **XXVIII**, Wiley (1972).
- [3] T. Chinburg, E. Hamilton, D. D. Long and A. W. Reid, *Geodesics and commensurability classes of arithmetic hyperbolic 3-manifolds*, Duke Math. J **145** (2008), 25–44.
- [4] R. Gangolli, *The length spectra of some compact manifolds*, J. Diff. Geom. **12** (1977), 403–424.
- [5] G. J. Janusz, *Algebraic Number Fields*, Academic Press, (1973).
- [6] M. Lackenby, D. D. Long and A. W. Reid, *Covering spaces of arithmetic 3-orbifolds*. Int. Math. Res. Not. IMRN 2008, no. 12, Art. ID rnn036.
- [7] D. D. Long and A. W. Reid, *Simple quotients of hyperbolic 3-manifold groups*, Proc. A. M. S. **126** (1998), 877–880.

- [8] D. D. Long and A. W. Reid, *Constructing hyperbolic manifolds which bound geometrically*, Math. Research Letters **8** (2001), 443–456.
- [9] C. Maclachlan and A. W. Reid, *The Arithmetic of Hyperbolic 3-Manifolds*, Graduate Texts in Mathematics **219**, Springer-Verlag (2003).
- [10] J. Neukirch *Algebraic number theory*, Grundlehren der mathematischen Wissen. **322**, Springer-Verlag, (1999).
- [11] M. V. Nori, *On subgroups of $GL_n(\mathbf{F}_p)$* , Invent. Math. **88** (1987), 257–276.
- [12] G. Prasad and A. S. Rapinchuk, *Existence of irreducible \mathbf{R} -regular elements in Zariski-dense subgroups*, Math. Res. Lett. **10** (2003), 21–32.
- [13] M. S. Raghunathan, *Discrete Subgroups of Lie Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, **68** Springer-Verlag (1972).
- [14] M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc. **125** (1997), 1913–1919.
- [15] M. Suzuki, *Group Theory I*, Grundlehren der mathematischen Wissen. **247**, Springer-Verlag, (1982).
- [16] E. B. Vinberg, *Rings of definition of dense subgroups of semisimple linear groups*, Math. USSR Izvest. **5** (1972), pp. 45–55.
- [17] E. B. Vinberg, *The smallest field of definition of a subgroup of the group PSL_2* , Russian Acad. Sci. Sb. Math. **80** (1995), pp. 179–190.
- [18] B. Weisfeiler, *Strong approximation for Zariski dense subgroups of semi-simple algebraic groups*, Annals of Math. **120** (1984), 271 - 315.
- [19] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Für Math. Phys. **3** (1892), 265–284.

Department of Mathematics,
 University of California
 Santa Barbara, CA 93106, USA.
 Email: long@math.ucsb.edu

Department of Mathematics,
 University of Texas
 Austin, TX 78712, USA.
 Email: areid@math.utexas.edu