Math. Ann. 325, 299–321 (2003) **Mathematische Annalen**

Digital Object Identifier (DOI) 10.1007/s00208-002-0380-y

Integral points on character varieties

D.D. Long[⋆] **· A.W. Reid** [⋆⋆]

Received: 7 July 1999 / Revised version: 7 July 2002 /
Published online: 2 December 2002 – © Springer-Verlag 2002

1 Introduction

Let k be a number field and denote its ring of integers by R_k. If V is a complex algebraic variety defined over a number field k, and L a number field, by an **L-integral point** we mean a point P on V all of whose co-ordinates are in R_L. A good deal of attention has been devoted over the years to understanding L-integral points, most of which are rooted in the celebrated theorem of Siegel [26]:

Theorem 1.1. *Let k and L be number fields, and X be an algebraic curve defined over k with projective completion $\widehat{X}$. If the genus of X is at least one or if $\widehat{X}$ contains at least three points at infinity, then the collection of L-integral points on X is finite.*

The focus of this paper will be to show that one can prove even stronger results using topological methods for certain naturally occurring varieties. For example Siegel's theorem leaves open the question of whether, given a constant D, there are finitely many R_L points as we allow L to run over all number fields with $[L : \mathbf{Q}] < D$; we have a result in this direction for our varieties.

Before stating our results, we describe the setting in which we will work. Let M be a finite volume hyperbolic 3-manifold with a single cusp, and let $X(M)$ denote the character variety associated to representations $\pi_1(M) \to \mathrm{SL}(2, \mathbf{C})$ (see §2.1 for definitions). By an **algebraic curve** we will mean an irreducible algebraic curve unless otherwise stated. The work of Thurston [28] shows that the component of the character variety containing the character of the faithful discrete representation of $\pi_1(M)$ is an algebraic curve. Throughout this paper, this algebraic curve component will be denoted X_0. Work begun in [13] (and

D.D. Long
Department of Mathematics, University of California, Santa Barbara, CA 93106, USA

A.W. Reid
Department of Mathematics, University of Texas, Austin, TX 78712, USA

[⋆] This work was partially supported by the N. S. F.

[⋆⋆] This work was partially supported by the N. S. F., The Alfred P. Sloan Foundation and a grant from the Texas Advanced Research Program.

continued in [14], [15], [8], [9]) has shown that $X(M)$ carries much important topological information about M. However, beyond the fact that the algebraic curves in question can be very complicated, little is known about the algebro-geometric or arithmetic properties of components of $X(M)$ and how this reflects, and is reflected by, properties of M or the fundamental group.

In the case of a quadratic imaginary number field $\mathbf{Q}(\sqrt{-d})$, we denote the ring of integers by O_d. Our results concern the topological detection and obstruction of $\mathbf{Z}$-integral points and O_d-points. We show:

Theorem 1.2. *Let M be a 1-cusped finite volume hyperbolic 3-manifold.*

Then for each d the number of O_d-points on X_0 is finite. For large enough d there are no O_d-points on X_0 other than possibly $\mathbf{Z}$-points.

Note that typically the presence of L-integral points is not an invariant of birational equivalence. However, in our setting (a careful discussion is given in §2.1), since the birational equivalences on the character variety induced by change of systems generators is defined over $\mathbf{Z}$, all our results are invariant for certain (natural) models in the birational equivalence class.

Theorem 1.2 implies in particular

Corollary 1.3. *Let M be a 1-cusped finite volume hyperbolic 3-manifold.*

Then the total number of R_L-points on X_0, as L runs over all quadratic imaginary number fields is finite.

This seems to be the first result of its type. In fact, if we restrict to $\mathbf{Z}$-points we can say a good deal more, as we now describe.

Throughout the paper Σ will always denote an integral homology 3-sphere and the term **knot group** will be reserved for the fundamental group of a knot complement in an integral homology 3-sphere. In this case we denote the character variety by $X(K)$.

Theorem 1.4. *Let $K \subset \Sigma$ be a knot with hyperbolic complement, and suppose that X_0 contains a $\mathbf{Z}$-integral point.*

Then the integral point corresponds to a surjection of $\pi_1(\Sigma \setminus K)$ onto either Σ_3^* or A_4^*.

The groups Σ_3^* or A_4^* denote the central extensions obtained by lifting the symmetric group on three letters and alternating group on four letters from SO(3) to SU(2). We note that if G_K is the fundamental group of the complement of a knot in an integral homology 3-sphere, then $H^2(G_K; \mathbf{Z}_2) = 0$, so that such a knot group surjects onto Σ_3 or A_4 if and only if it surjects onto Σ_3^* or A_4^*. In particular, such representations are controlled completely by conditions on the Alexander polynomial of the knot group. (see §5.1)

In fact in this context one has results about all the components of $X(K)$:

Theorem 1.5. *Let $K \subset \Sigma$ be a knot with hyperbolic complement, and suppose a component of $X(K)$ contains a $\mathbf{Z}$-integral point corresponding to an irreducible representation. Then at least one of the following happens:*

- *$\pi_1(\Sigma \setminus K)$ surjects onto the fundamental group of the trefoil knot complement. In which case either there is an algebraic curve component of genus 0 which is the component of the character variety of the trefoil knot group containing an irreducible representation or there is a component of dimension at least* 2.
- *The integral point corresponds to a surjection of $\pi_1(\Sigma \setminus K)$ onto either Σ_3^* or A_4^*.*

It is easily shown (we sketch this in §4) that the character variety of the trefoil knot group cannot be an X_0 for any hyperbolic knot group, so 1.5 implies 1.4.

We remark that for a knot group, the abelian representations form a component (See Proposition 3.4 in [19]) and that this component always contains integral points. Thus we introduce the notation, **irreducible integral point** to mean an integral point on some component of $X(K)$ containing an irreducible representation.

Since the number of homomorphisms from a knot group to Σ_3^* and A_4^* is finite, we have the following version of Siegel's Theorem (we do not assume every component is an algebraic curve):

Corollary 1.6. *With K as above, the number of irreducible integral points on $X(K)$ is finite, unless $\pi_1(\Sigma \setminus K)$ surjects onto the trefoil knot group.* □

As further corollaries of Theorem 1.5 we have:

Corollary 1.7. *With K as above, assume that $X(K)$ has only algebraic curve components. If $\pi_1(\Sigma \setminus K)$ admits no homomorphism onto Σ_3 or A_4 then no component has an irreducible integral point. In particular if X_0 is the unique component of $X(K)$ containing an irreducible representation and $\pi_1(\Sigma \setminus K)$ admits no homomorphism onto Σ_3 or A_4 then X_0 has no integral point.*

Proof.. By the remarks above $\pi_1(\Sigma \setminus K)$ surjects onto Σ_3 or A_4 if an only if it surjects onto Σ_3^* or A_4^*. The proof now follows from the observation that since $\pi_1(\Sigma \setminus K)$ admits no homomorphism onto Σ_3, $\pi_1(\Sigma \setminus K)$ cannot surject onto the group of the trefoil. The reason being that the complement of the trefoil knot is a Seifert fiber space over the disk with 2 exceptional fibers of orders 2 and 3. The base orbifold therefore surjects onto the group Σ_3 (see §4 for more on the trefoil). □

The philosophy behind the proofs of Theorem 1.5 and Theorem 1.2 is that if k is a number field then a k-integral point on $X(M)$ corresponds to either a finite representation with special properties, or a representation into an "arithmetic group". In particular, the proofs of Theorem 1.5 and Theorem 1.2 rely on understanding finite subgroups of SL(2, **C**) with integral traces, arithmetic Fuchsian groups with integral traces and arithmetic Kleinian groups with traces in O_d.

The paper is organized as follows. §2 provides background material concerning character and representation varieties, the A-polynomial and quaternion algebras. Most of this is standard and included only to establish notation and for the sake of completeness. §3 contains the proof of Theorem 1.2 and §4 is devoted to the proof of 1.5. Related topics and computations are included in §5.

2 Preliminaries

2.1 Representation and character varieties

To begin, we recall some standard facts about the structure of the representation and character varieties. References for this material are [13], [15] and [8].

Let Γ be a finitely generated group with a generating set $\{\gamma_1, \dots, \gamma_n\}$. We denote by $\mathrm{Hom}(\Gamma)$ the set of all homomorphisms of Γ into SL(2, **C**). Then via the embedding

$$\mathrm{Hom}(\Gamma) \subset \mathrm{SL}(2, \mathbf{C})^n \subset \mathbf{C}^{4n},$$

$\mathrm{Hom}(\Gamma)$ inherits the structure of a complex affine algebraic set defined over **Q** (in fact over **Z**), where the polynomials defining the set arise from the relations in the γ_i's. Although it is not in general irreducible, $\mathrm{Hom}(\Gamma)$ is usually called the **representation variety** of Γ. A related algebraic set is the **character variety**. Recall that by a character of a representation $\rho \in \mathrm{Hom}(\Gamma)$ we mean a function $\chi_\rho : \Gamma \to \mathbf{C}$ with $\chi_\rho(\gamma) = \mathrm{tr}(\rho(\gamma))$. As discussed in [13], the space of characters denoted $X(\Gamma)$ also has the structure of a complex affine algebraic set defined over **Q** (see also [21]). When M is a 3-manifold and $\Gamma = \pi_1(M)$ we denote the character variety by $X(M)$. We briefly recall the definitions.

For each $\gamma \in \Gamma$, we can define a regular function $\tau_\gamma : \mathrm{Hom}(\Gamma) \to \mathbf{C}$ by

$$\tau_\gamma(\rho) = \chi_\rho(\gamma).$$

Also following [13] we denote by I_γ the regular function on $X(\Gamma)$ defined by $I_\gamma(\chi) = \chi(\gamma)$.

Let T be the ring generated by all such functions. As shown in [13] Proposition 1.4.1, T is finitely generated. Fixing a finite set of elements $\delta_1, \dots, \delta_m$ that generate T, the character variety $X(\Gamma)$ is described as the image of a map $t : \mathrm{Hom}(\Gamma) \to X(\Gamma)$, where

$$t(\rho) = (\tau_{\delta_1}(\rho), \dots, \tau_{\delta_m}(\rho)).$$

Hence the character χ_ρ is determined by $t(\rho)$. It is shown that the image of t is closed, so that $X(\Gamma)$ is an affine algebraic set.

Remark. The algebraic sets $\mathrm{Hom}(\Gamma)$ and $X(M)$ are computed with respect to a fixed generating set and changing the generating set induces a birational equivalence defined over $\mathbf{Z}$. In what follows, although some choice of generators is implicit, our results do not depend on this choice, and so L-integral point will therefore be an invariant of birational equivalence when restricted to the class of varieties $X(M)$ obtained in this way.

We shall also require some of the machinery associated to the **A-polynomial** [8]. We sketch the construction following [9].

Suppose that N is a compact 3-manifold with boundary a torus, T say. Pick a "meridian-longitude basis" for $\pi_1(T) =< m, \ell >$ and consider the subset of $\mathrm{Hom}(\pi_1(N))$ having the property that $\rho(m)$ and $\rho(\ell)$ are upper triangular. Denote this (algebraic) subset by $\mathrm{Hom}_U(\pi_1(N))$. There is a well-defined eigenvalue map

$$\xi \ : \ \mathrm{Hom}_U(\pi_1(N)) \to \mathbf{C}^2$$

defined by sending a representation ρ to the pair (L, M) where L and M are the eigenvalues (i.e. the upper left entries) of $\rho(\ell)$ and $\rho(m)$ respectively. If we take the Zariski closure we obtain a new complex affine algebraic set $\mathcal{V} \subset \mathbf{C}^2$. From [8] all the components of $\mathcal{V}$ have complex dimension zero or one. Discard the zero dimensional components. Each component of dimension 1 is the zero set of a single polynomial of two variables and so for each algebraic curve component $\mathcal{C}_i$ of $\mathcal{V}$ we may associate a two variable polynomial $c_i(L, M)$. We define

$$A_N(L, M) = \prod_i c_i(L, M)$$

where the product is taken over the polynomials associated to each algebraic curve component of $\mathcal{E}$. This algebraic set is defined over $\mathbf{Q}$ (indeed $\mathbf{Z}$), [8].

There is some ambiguity in A since one can regard it as the generator of an ideal, but it turns out that we may scale so that $A_N(L, M)$ is an integer polynomial and it is then defined up to $\pm L^\alpha M^\beta$. Furthermore, $A_N(L, M) = A_N(1/L, 1/M)$ to powers of L and M.

If N is hyperbolic, the component R_0 of $\mathrm{Hom}(\pi_1(N))$ where in the notation of the previous section $t(R_0) = X_0$ always contributes a factor of the A-polynomial.

A common construction in 3-dimensional topology is that of Dehn filling (or surgery). We have no need for the topology of this construction, only to remark that given N and T as above and a simple closed curve γ in T, one can form the **Dehn filled** manifold and that the fundamental group of the Dehn filled manifold is $\pi_1(M)$ with a single extra relation that says $\gamma = 1$. Somewhat more generally one might kill some *power* of γ to yield an **orbifold**; all the same considerations apply. If γ is the boundary of an incompressible, boundary incompressible surface properly embedded in M, then γ is called a *boundary slope*.

The A-polynomial carries number theoretic information associated to Dehn filling (see [11]). Let (p, q) be a coprime pair of integers, then we may take the filling curve to be $m^p\ell^q$, this is described as the p/q Dehn filling. The representations of the Dehn filled manifold correspond to representations of the original manifold which map the curve $m^p\ell^q$ to the identity. (In the orbifold case, they map the curve to an element of finite order). It follows that such a representation gives rise to a point on the curve $A(L, M) = 0$ where we have $M^pL^q = 1$. If we set $M = k^q$ and $L = k^{-p}$ we see that $0 = A(k^{-p}, k^q) = X(k)$ describes restrictions on the possibilities for eigenvalues which give rise to representations of the p/q-Dehn filled manifold. Notice that (after clearing denominators) the polynomial $X(k)$ is symmetric.

If the pair (r, s) satisfies $ps - qr = 1$, then the curve $m^r\ell^s$ is primitive and the pair $\{m^p\ell^q, m^r\ell^s\}$ is a basis for the free abelian group $\pi_1(T)$. We refer to this curve as a **core curve** for the representation. Moreover, at any representation corresponding to p/q Dehn filling we have that $m^r\ell^s$ has eigenvalue $(k^q)^r(k^{-p})^s = k^{-1}$, so that we may interpret the element k as an eigenvalue of a core curve.

This discussion is easily extended to pairs (p, q) that are not co-prime, and hence to orbifold Dehn fillings p/q on N. In this setting if $p = np_0$ and $q = nq_0$ with $(p_0, q_0) = 1$, then the orbifold filling yields a relation $(m^{p_0}\ell^{q_0})^n = 1$, and arguing as above, setting $M = k^{nq_0}$ and $L = k^{-np_0}$ gives an eigenvalue equation for the core curve (which is a dual curve to the curve $m^{p_0}\ell^{q_0}$ as defined above).

2.2 *Quaternion algebras, orders and arithmetic groups*

To prove Theorems 1.2 and 1.5 we shall require some of the theory of quaternion algebras, orders and arithmetic Fuchsian and Kleinian groups. In addition we include a description of how the groups Σ_3^* and A_4^* arise from quaternion algebras (see [29] for more details).

If k is a field by a **quaternion algebra** B defined over k we mean a four dimensional central simple algebra defined over k. When the characteristic of k is different from 2, a convenient description of a quaternion algebra is via the **Hilbert symbol** $(\frac{a,b}{k})$. This information encodes a basis, $\{1, i, j, ij\}$ with multiplicative relations $i^2 = a$, $j^2 = b$ and $ij = -ji$, with a and b non-zero elements of k.

The quaternion algebra B admits a canonical involution defined by

$$\overline{x_0 + x_1 i + x_2 j + x_3 ij} = x_0 - x_1 i - x_2 j - x_3 ij.$$

Via this, there is a norm and a trace defined on B which is a multiplicative (resp. additive) homomorphism from $B \to k$ defined by $x\overline{x}$ (resp. $x + \overline{x}$). We denote by B^* (resp. B^1) the invertible elements, ie those of non-zero norm (resp. norm one). If R is a subring of B we use these superscripts to indicate invertible or norm one elements in R.

The classification theorem for quaternion algebras implies that either B is a division algebra over k or is isomorphic to $M(2, k)$. In the case when k is a number field, the isomorphism type of B is completely determined by the **ramification set** of B (denoted herein by $\mathrm{Ram}(B)$). In the case where ν is an infinite place (i.e. associated to an embedding of k into $\mathbf{C}$), B is ramified at ν if and only if both ν is a real place and $B \otimes_k k_\nu \cong \mathcal{H}$. Here $\mathcal{H}$ is the Hamiltonian division algebra of quaternions. If ν is a finite place (i.e. associated to a prime of R_k) B is ramified at ν if and only if $B \otimes_k k_\nu$ is isomorphic to the unique division algebra of quaternions over k_ν.

The set $\mathrm{Ram}(B)$ is always finite of even cardinality. Furthermore given any set S of places of k of finite even cardinality there is a quaternion algebra over k with $\mathrm{Ram}(B) = S$.

Let B be a quaternion algebra over k, by an **order** of B we mean a subring of B containing 1 which is a finitely generated R_k-module, and which contains a k-basis of B. A maximal order is one which is not properly contained in any other order. B^* acts by conjugation on the set of maximal orders, and the number of equivalence classes is called **the type number** of B. The type number is always finite. All we shall require is the following theorem about quaternion algebras over $\mathbf{Q}$ (cf [29] Chapter 3),

Theorem 2.1. *If B is a quaternion algebra defined over $\mathbf{Q}$ which is unramified at the infinite place, the type number of B is one.*

We now give the definition of an arithmetic Fuchsian group arising from quaternion algebras over $\mathbf{Q}$, and an arithmetic Kleinian groups from quaternion algebras over $\mathbf{Q}(\sqrt{-d})$.

Let B be a quaternion algebra over $\mathbf{Q}$ unramified at the infinite place. Let ρ be an embedding of B into $M(2, \mathbf{R})$, $\mathcal{O}$ an order of A and $\mathcal{O}^1$ the elements of norm 1 in $\mathcal{O}$. Then $\rho(\mathcal{O}^1)$ is a discrete subgroup of $\mathrm{SL}(2, \mathbf{R})$ and its projection to $\mathrm{PSL}(2, \mathbf{R})$, $\mathrm{P}\rho(\mathcal{O}^1)$, is an **arithmetic Fuchsian group**.

For Kleinian groups we take a quaternion algebra over $\mathbf{Q}(\sqrt{-d})$ (necessarily unramified at the infinite place) and proceed exactly as above giving groups in $\mathrm{PSL}(2, \mathbf{C})$.

Torsion in groups $\mathrm{P}\rho(\mathcal{O}^1)$ arising in either case above, is controlled by the following, which is proved by consideration of the characteristic polynomial of elements of finite order in $\mathrm{PSL}(2, \mathbf{C})$ with integral trace (see [29] Chapters 3 and 4 for example).

Lemma 2.2. *Let B and $\mathcal{O}$ arise from either of the two cases above. Let $\gamma (\neq 1) \in \mathrm{P}\rho(\mathcal{O}^1)$ be an element of finite order. Then γ has order* 2 *or* 3. □

Remark. The general arithmetic Fuchsian (resp. Kleinian) group arises from a generalization of this construction. In this case, one starts with a certain kind of quaternion algebra over a totally real number field (resp. field with exactly one complex place), see [2], [27], and [23] for more details.

2.3 Finite subgroups

Omitted from consideration in the previous subsection were division algebras defined over $\mathbf{Q}$ ramified at the infinite place. In this case $\mathcal{H}^1$ is a compact Lie group, and the groups $\rho(\mathcal{O}^1)$ that we obtain are finite. The following examples will be relevant, and since this material seems not all that well known, we include a brief discussion. (see [29] Chapter 1 and [16] §9).

Let B denote the quaternion algebra with Hilbert Symbol $(\frac{-1,-1}{\mathbf{Q}})$ (so $\mathrm{Ram}(B) = \{\infty, 2\}$). Upon tensoring with $\mathbf{R}$, we induce $\rho : \mathcal{H}^1 \to \mathrm{SL}(2, \mathbf{C})$ given by

$$\rho(a_0 + a_1 i + a_2 j + a_3 ij) = \begin{pmatrix} a_0 + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_0 - a_1 i \end{pmatrix}.$$

If n denotes the norm on $\mathcal{H}$, then there is an epimorphism

$$\Phi : \mathcal{H}^1 \to \mathrm{SO}(3)$$

where SO(3) is represented as the orthogonal group of the quadratic subspace V of $\mathcal{H}$ spanned by $\{i, j, ij\}$, that is, the pure quaternions, equipped with the restriction of the norm form, so that $n(x_1 i + x_2 j + x_3 ij) = x_1^2 + x_2^2 + x_3^2$. The mapping Φ is defined by $\Phi(\alpha) = \phi_\alpha$ where

$$\phi_\alpha(\beta) = \alpha\beta\alpha^{-1} \quad \alpha \in \mathcal{H}^1 \quad \beta \in V.$$

The kernel of Φ is $\{\pm 1\}$. The binary tetrahedral group is a central extension of an element of order 2 by the tetrahedral group and can be faithfully represented in $\mathcal{H}$. More precisely, if the tetrahedron has its vertices at

$$i + j + ij, \quad i - j - ij, \quad -i + j - ij, \quad -i - j + ij,$$

then ϕ_{α_1} is a rotation of order 2 about the axis through the edge mid-point i if $\alpha_1 = i$, while ϕ_{α_2} is a rotation of order 3 about the axis through the vertex $i + j + ij$ when $\alpha_2 = (1 + i + j + ij)/2$. The binary tetrahedral group Γ_1 is thus generated by $\alpha_0 = -1, \alpha_1, \alpha_2$ in $\mathcal{H}^1$. The group $\mathrm{P}\rho(\Gamma_1)$ is therefore A_4. Notice in particular that the three generators of Γ_1 all have norm 1 and integral traces, and so Γ_1 is a subgroup of $\mathcal{O}$ for some maximal order $\mathcal{O}$ of B.

A similar discussion can be made for Σ_3. Using the fact that for quaternion algebras over $\mathbf{Q}$ ramified at the infinite place, $\mathcal{O}^* = \mathcal{O}^1$ (see [29] p. 145) a more precise statement of what happens as $\mathrm{Ram}(B)$ varies is (cf. [29] p. 145 Proposition 3):

Theorem 2.3. *Let B be a quaternion algebra over $\mathbf{Q}$ ramified at the infinite place and $\mathcal{O}$ a maximal order of B. Then $\mathcal{O}^1$ is cyclic of order 2, 4, or 6 unless:*

- $\mathrm{Ram}(B) = \{\infty, 2\}$ *and* $\mathcal{O}^1 \cong A_4^*$.
- $\mathrm{Ram}(B) = \{\infty, 3\}$ *and* $\mathcal{O}^1 \cong \Sigma_3^*$. □

We also record some further related information that we will use in §4.

If Σ_4 and A_5 (resp. Σ_4^* and A_5^*) denote the symmetric group on 4 letters and the alternating group on 5 letters (resp. the central extensions as discussed above), then these are also related to the unit groups of orders in quaternion algebras. We recall the following (cf. [29] Chapter 1 and [16] §9).

If the cube has its vertices at

$$\pm i \pm j \pm ij,$$

then ϕ_{α_3} is a rotation of order 4 about the axis through the mid-point i of a face when $\alpha_3 = (1+i)/\sqrt{2}$. Thus Σ_4^* is generated by $\alpha_0, \alpha_2, \alpha_3$.

If the regular dodecahedron has its vertices at

$$\pm i \pm j \pm ij, \quad \pm\tau i \pm \tau^{-1} j, \quad \pm\tau j \pm \tau^{-1} ij, \quad \pm\tau ij \pm \tau^{-1} i,$$

then ϕ_{α_4} is a rotation of order 5 about the axis through the mid-point of the face with vertices

$$i + i + ij, \quad i + j - ij, \quad \tau i + \tau^{-1} j, \quad \tau j + \tau^{-1} ij, \quad \tau j - \tau^{-1} ij,$$

where $\alpha_4 = (\tau + \tau^{-1} i + j)/2$ and $\tau = (\sqrt{5}+1)/2$. Then A_5^* is generated by $\alpha_0, \alpha_2, \alpha_4$.

Via this description we have that S_4^* is the normalizer of A_4^* in B^* where $\mathrm{Ram}(B) = \{\infty, 2\}$. In particular this gives a representation of Σ_4^* admitting a character value of $\sqrt{2}$. Similarly A_5^* can be described as the elements of norm 1 in a maximal order of the quaternion algebra $(\frac{-1,-1}{\mathbf{Q}(\sqrt{5})})$.

We also remark that all faithful representations of the groups Σ_3^*, Σ_4^*, A_4^*, and A_5^* in $\mathrm{SL}(2, \mathbf{C})$ are conjugate to the ones described (see [16], §9 for more details).

3 Proof of Theorem 1.2

The proof of Theorem 1.2 will involve two ingredients, the first is a special case of a result in [16]. Recall that a subgroup of $\mathrm{SL}(2, \mathbf{C})$ is called **reducible** if all its elements have a common fixed point in $\mathbf{C} \cup \{\infty\}$, otherwise a subgroup is called **irreducible**.

Theorem 3.1. *Let Γ be an irreducible subgroup of $\mathrm{SL}(2, \mathbf{C})$ such that $\mathrm{tr}(\gamma) \in O_d$ for all $\gamma \in \Gamma$.*

Then Γ is conjugate in $\mathrm{SL}(2, \mathbf{C})$ to a subgroup of $\rho(\mathcal{O}^1)$ for some order $\mathcal{O}$ in a quaternion algebra B over $\mathbf{Q}(\sqrt{-d})$ (as discussed in §2.2).

In particular $P\Gamma$ is conjugate to a subgroup of an arithmetic Kleinian group from a quaternion algebra defined over $\mathbf{Q}(\sqrt{-d})$.

Theorem 3.2. *Let M be an orientable hyperbolic 3-manifold of finite volume with a single cusp.*

Then given a positive integer D, there at most finitely many $\chi_\rho \in X_0$ with ρ discrete and $\mathrm{tr}(\rho(\pi_1(M))) \in k$ *with k a number field of degree at most D.*

Remark. Theorem 3.2 is a strong form of an observation due to Hodgson ([18]).

The proof of Theorem 1.2 now follows:

Proof of 1.2. If χ_ϕ is any character on X_0 with values in O_d, then by Theorem 3.1, the representation ϕ of $\pi_1(M)$ with this character is a discrete subgroup $\mathrm{SL}(2, \mathbf{C})$. Every such character values in quadratic imaginary number field, so by Theorem 3.2 there are can be only finitely many such characters. □

Proof of 3.1. Following Bass [1], we define:

$$A\Gamma = \{\sum a_i g_i : a_i \in \mathbf{Q}(\sqrt{-d}) \quad g_i \in \Gamma\}$$

Then Bass shows that $A\Gamma$ is a quaternion algebra over $\mathbf{Q}(\sqrt{-d})$. Additionally, if $\mathrm{tr}(\Gamma)$ consists of elements of O_d, then [1] also shows that

$$\mathcal{O}\Gamma = \{\sum a_i g_i \mid a_i \in O_d, \quad g_i \in \Gamma\}$$

is an order in $A\Gamma$.

By the Skolem-Noether Theorem ([29] Chapter 1) we deduce that Γ is conjugate into a group $\rho(\mathcal{O}^1)$ as discussed in §2.2. This completes the proof. □

To prove 3.2 we need some additional notation. The **Mahler measure** $M(f)$ of a polynomial

$$f(X) = a_n X^n + \ldots + a_1 X + a_0 = a_n(X - \alpha_1)\ldots(X - \alpha_n)$$

with $a_0 \neq 0$ and $a_i \in \mathbf{Z}$ is defined by

$$M(f) = |a_n| \prod_{i=1}^{d} \max(|\alpha_i|, 1).$$

It can also be defined by

$$M(f) = \exp(\int_0^1 \log |f(e^{2\pi i t})|\, dt).$$

A related measure of complexity of a polynomial f is the **length** $L(f)$ defined as:

$$L(f) = |a_0| + \ldots + |a_n|$$

The following lemma is standard, see [3] and [20], pp 7–8.

Lemma 3.3. *Let f_1 and f_2 be polynomials (as above). Then,*

1. $M(f_1 f_2) = M(f_1)M(f_2)$

2. $M(f) \leq L(f)$. □

With this lemma we can prove Theorem 3.2.

Proof of 3.2. Let $\Gamma = \pi_1(M)$, and $\Delta = \pi_1(\partial M) =< m, \ell >$ a fixed basis of the peripheral subgroup. All Dehn fillings on M will be coordinatized with respect to this basis.

If false, the hypothesis of Theorem 1.2 yields an infinite number of inequivalent irreducible representations ϕ_j, with traces in k_j where $[k_j : \mathbf{Q}] \leq D$. We shall derive a contradiction.

Note that for each j, either $\phi_j(\Delta)$ injects or it does not. Since the image groups are discrete, if $\phi_j(\Delta)$ injects, the image must consist of nonidentity parabolic elements. A key ingredient here is (cf. [15] Proposition 1.1.1, and [14]):

Lemma 3.4. *Let X_0 be the component containing the discrete faithful representation of a hyperbolic* 3*-manifold with a single cusp and let ξ be any element on ∂M.*

Then X_0 is an algebraic curve and the function $I_\xi : X_0 \to \mathbf{C}$ given by evaluation of the character on the nontrivial element ξ is nonconstant. □

Observe that the lemma implies that a given element on ∂M can take on any complex value at most a finite number of times so that in particular the element m in Δ can have trace taking on the values ± 2 at most a finite number of times. Thus we can assume that an infinite number of the representations ϕ_j do not inject Δ. A discrete, nonfaithful representation of $\mathbf{Z} \oplus \mathbf{Z}$ must be either a finite group, $\mathbf{Z}$ or $\mathbf{Z} \oplus \mathbf{Z}_n$.

Now there are only finitely many cyclotomic polynomials of any given degree. In our setting, traces of elements in $\phi_j(\Gamma)$ lie in number fields of bounded degree, so there are only a finite number of possible values of orders of torsion elements in $\phi_j(\Gamma)$. Thus if infinitely many of the representations had finite image on the boundary, we could extract an infinite subsequence of inequivalent representations whose restriction to ∂M was constant, contradicting Lemma 3.4. This argument also shows that the possibilities for n in the case $\mathbf{Z} \oplus \mathbf{Z}_n$ are bounded in number. It follows that we are finished unless the images of $\mathrm{P}\phi_j(\Delta)$ are all $\mathbf{Z}$ or $\mathbf{Z} \oplus \mathbf{Z}_n$. As in the argument above n also has bounded order.

To each ϕ_j there is an element $\beta_j \in \Delta$ such that $\phi_j(\beta_j) = 1$. We can assume that infinitely many of the β_j are distinct. For if not, denote by $\beta \in \Delta$ an element satisfying $\phi_j(\beta) = 1$ for infinitely many j. We therefore have infinitely many representations ϕ_j whose characters χ_j are distinct points on the component X_0 but whose character on the class β is constant. The element β may actually not be primitive, but 3.4 continues to apply and we still obtain a contradiction.

Thus we are reduced to the case where infinitely many of the β_j are distinct elements of Δ. For each such representation ϕ_j, it follows that Pϕ_j factors through the (possibly orbifold) β_j Dehn fillings on M.

To clarify this point of the argument, assume first that these β_j Dehn fillings are genuine topological Dehn fillings, that is to say, β_j represents a primitive class in ∂M. (The orbifold case is entirely analogous.)

As in §2.1, let us denote a core curve for the β_j Dehn filling by γ_j. As described in that section, this core curve has an eigenvalue λ_j which is a root of a **Z**-polynomial $X_j(t) = 0$. The length of the polynomials X_j is uniformly bounded by the sum of the absolute values of the coefficients of the A-polynomial. Hence by Lemma 3.3 the Mahler measures $M(X_j)$ are all bounded. It follows that the absolute values of all the roots of the X_j are bounded, by L say.

The coefficients of a polynomial are symmetric functions of the roots of the polynomial, so that for a *fixed* degree Q, there are at most a finite number of distinct polynomials with

1. **Z**-coefficients
2. Degree $\leq Q$
3. all the roots are less than L in modulus.

It follows that there are only finitely many possiblities for irreducible polynomial factors occuring in the sequence of X_j's.

Now each $\phi_j(\gamma_j)$ has trace in the number field k_j of degree at most D, and therefore the irreducible polynomial of the eigenvalue of this representation has degree at most $2D$ over **Q**. We therefore conclude, by passing to a subsequence if necessary, that we have an infinite sequence of inequivalent irreducible representations for which $\mathrm{tr}(\phi_j(\gamma_j)) = c$ is fixed.

Recall β_j and γ_j are dual curves, so they generate Δ. We have assumed that $\phi_j(\beta_j) = I$ for all j and we may conjugate the terms of the sequence to arrange $\phi_j(\gamma_j) = A$ for some fixed diagonal matrix A. Our previous reductions guarantee that A has infinite order and since this image group is discrete, it follows that the eigenvalues of A cannot be on the unit circle in **C**.

If we now write $\phi_j(m) = A^{a_j}$ and $\phi(\ell) = A^{b_j}$, we see that both sequences a_j or b_j must be unbounded, else we extract a subsequence which is constant on at least one of these curves and the usual contradiction to 3.4. However, since A does not have eigenvalues on the unit circle it follows that the traces of m or ℓ must be going to ∞.

Now the theory developed in [13] shows that a sequence of characters going to an ideal point of the character variety gives rise to a splitting of the group. One possibility for this kind of degeneration is that all characters on the boundary remain bounded; the argument of the above paragraph shows we are not in that case. The other possibility is that there is one and only one primitive class in Δ whose character remains bounded. A deeper result (see [8] or [10]) shows that the trace of this bounded primitive class must converge to $\omega + 1/\omega$ where ω is a root of unity.

To return to our context, X_0 has a finite number of ideal points, so we may pass to a subsequence and assume that the characters of the representations we have constructed are converging to one ideal point. Thus there is an element $\epsilon \in \Delta$ such that $\mathrm{tr}(\phi_j(\epsilon))$ has a limit as $j \to \infty$, and the limiting value has the form $\omega + 1/\omega$ where ω is some root of unity. But the traces in the sequence take their values in a discrete set, so the sequence must eventually be constant. However, if $\epsilon \neq \beta_j$ for a given j, then $\phi_j(\epsilon)$ is a non-zero power of the matrix A and from above this cannot have trace $\omega + 1/\omega$. Hence for large j, $\epsilon = \beta_j$ and this contradicts our assumption that the β_j's were all distinct.

We make some brief comments on the orbifold case. As remarked there is at most a finite number of possibilities for the torsion in the groups $\phi_j(\Gamma)$. Thus by subsequencing, we may assume $\beta_j = \delta_j^r$ where r is fixed, and δ_j is primitive. As above there is a core curve γ_j, dual to δ_j, and using the discussion at the end of §2.1, we deduce the existence of the diagonal matrix A. Exactly as above, we find that the appropriate collection of characters forms a discrete subset of $\mathbf{C}$, in this case 2 is replaced by some $\zeta = \omega + 1/\omega$ where ω is an r-th root of unity. We then finish off exactly as above. □

Remark. It is perhaps worth pointing out that using SnapPea for instance it is not hard to construct examples of manifolds M, and representations ρ with character χ_ρ as in the statement of Theorem 3.2 which do not arise from topological Dehn filling, or orbifold Dehn filling.

We deduce the following strengthening of Siegel's Theorem in the case imaginary quadratic fields.

Corollary 3.5. *Let M be as in Theorem 1.2. Then the total number of O_d points on X_0 taken over the union of all quadratic imaginary number fields is finite.* □

Remark. A key ingredient in the proof of Theorem 3.2 is Lemma 3.4. If we assume $X \subset X(M)$ is any component on which the conclusion of 3.4 holds, then the argument given in the proof of Theorem 3.2 works in this setting. Note that if the conclusion to Lemma 3.4 holds the component X "contributes" to the A-polynomial which is also used. Such algebraic curve components are called **norm curves** in [5]. Thus one has,

Theorem 3.6. *Let M be a 1-cusped finite volume hyperbolic 3-manifold, and $X \subset X(M)$ a norm curve. Then for each d the number of O_d-points on X is finite. For large enough d there are no O_d-points on X other than possibly $\mathbf{Z}$-points.* □

4 Proof of Theorem 1.5

Before commencing with the proof we discuss the character variety of the trefoil knot, and prove some preparatory results, which are standard.

Throughout the paper, T will denote the trefoil knot; this is the $(2, 3)$ torus knot and hence the complement is a Seifert fibered space over the disk with 2 exceptional fibers of orders 2 and 3. The fundamental group is presented as $< a, b \mid a^2 = b^3 >$ (see [6] Chapter 3). In particular such a group surjects onto $\mathbf{Z}_2 * \mathbf{Z}_3$, and so Σ_3. We collect some data about $X(T)$.

Proposition 4.1. *$X(T)$ has a unique component containing an irreducible representation and is given by the vanishing set of $p(z, r) = z^2 + (r - 3)$. In particular this has genus 0. We shall denote this algebraic curve by Y throughout.*

Sketch Proof.. We use the presentation coming from a 2-bridge presentation of the knot, namely $< a, b \mid a^{-1}b^{-1}abab^{-1} = 1 >$, where a and b are both meridians. If ρ is a representation, we can conjugate so that $\rho(a)$ and $\rho(b)$ are

$$\begin{pmatrix} x & 1 \\ 0 & x^{-1} \end{pmatrix} \text{ and } \begin{pmatrix} x & 0 \\ r & x^{-1} \end{pmatrix}$$

respectively.

The relation then implies that either $r = 0$, in which case we get reducible representations, or there is a unique component of irreducible representations defined by the equation, $p(z, r) = 0$, where $p(z, r) = z^2 + (r - 3)$ and the variable z is the trace of a meridian. □

Remark. Note that the variable r used above is related to characters by $r = 2 - \text{tr}(ab^{-1})$, and so there is no loss in using r as a co-ordinate to parametrize characters.

It is easy to see directly that the algebraic curve Y has infinitely many integral points. By Siegel's Theorem 1.1, this implies Y has genus 0 and its projective completion has at most two ideal points.

This discussion leads to a rather more succinct statement of Theorem 1.5.

Theorem 4.2. *Let $K \subset \Sigma$ have hyperbolic complement. Suppose that some component of $X(K)$ contains an irreducible integral point. Then at least one of the following happens:*

- *$\pi_1(\Sigma \setminus K)$ surjects onto the fundamental group of the trefoil knot complement.*
  In this case
  either
  $X(K)$ contains Y as an algebraic curve component.
  or
  $X(K)$ contains a component of dimension at least 2 which contains Y as a subvariety.
- *The integral point corresponds to a Σ_3^* or A_4^* representation*

Finally, we note that Y cannot be the component X_0 of a hyperbolic knot K in Σ (or indeed, for any one cusped hyperbolic 3-manifold of finite volume). A quick way to see this is to observe that the generic character on Y corresponds to an irreducible representation of $\pi_1(T) \to \mathrm{SL}(2, \mathbf{C})$; and in fact, the generic such representation is a faithful representation of $\mathbf{Z}_4 *_{\mathbf{Z}_2} \mathbf{Z}_6$ which therefore contains a free subgroup of finite index. However it is a standard argument that the generic point of X_0 corresponds to the character of a faithful representation of $\pi_1(\Sigma \setminus K)$ and this group cannot have a free subgroup of finite index.

Remark. It is also easy to construct hyperbolic knots whose fundamental group surjects onto the fundamental group of the trefoil. For example, 8_{20} is the Montesinos knot $K(1/3, 2/3, -1/2)$. It follows from [24], that K is hyperbolic and the complement contains no closed embedded essential surface. Hence $X(8_{20})$ contains only algebraic curve components. A homomorphism may be constructed by lifting a 3-colouring of the knot.

Recall that by a knot group we mean $\pi_1(\Sigma \setminus K)$ where Σ is an integral homology 3-sphere. Standard algebraic topology shows that if N is a compact orientable 3-manifold with $\partial N \cong S^1 \times S^1$, then $H_1(N, \mathbf{Z}) \cong \mathbf{Z}$ if and only if N is a knot exterior in a homology 3-sphere.

Also recall that the **signature** of a cocompact Fuchsian group F is a tuple $(g; m_1, \dots, m_r)$ where g is the genus of the underlying Riemann surface of the quotient orbifold $\mathbf{H}^2/F$, and each m_i represents cone points of cone angle $2\pi/m_i$ (or equivalently a conjugacy class of maximal finite subgroup of order m_i).

Lemma 4.3. *Let $K \subset \Sigma$ be a knot and assume $\pi_1(\Sigma \setminus K)$ surjects onto a cocompact Fuchsian group F. Then the signature of F is $(0; m_1, \dots, m_r)$ and the m_i are all coprime.*

Proof.. Any abelian quotient of a knot group is cyclic. Thus, if the genus of the quotient orbifold is greater than 0, then F abelianized has rank at least 2 which is impossible for a knot group. Similarly all the m_i's must be co-prime. □

Lemma 4.4. *Let T denote the trefoil knot and suppose $G_K = \pi_1(\Sigma \setminus K)$ surjects onto $\mathbf{Z}_2 * \mathbf{Z}_3$.*

Then G_K surjects onto $G_T = \pi_1(S^3 \setminus T)$.

Proof.. Let $\rho : G_K \to \mathbf{Z}_2 * \mathbf{Z}_3$ be a surjection and let $p : G_T \to \mathbf{Z}_2 * \mathbf{Z}_3$ be the map which quotients out by the centre.

Consider the subgroup E of $G_K \times G_T$ of elements (g, t) such that $\rho(g) = p(t)$. There is an obvious surjection of E onto G_K which exhibits E as a central extension of G_K. However $H^2(G_K, \mathbf{Z}_2) = 0$, so that E is the product $G_K \times \mathbf{Z}$ and restriction of the obvious projection of E onto G_T gives the required homomorphism. □

Lemma 4.5. *Let Γ be an irreducible subgroup of* $\mathrm{SL}(2, \mathbf{C})$ *such that* $\mathrm{tr}(\gamma) \in \mathbf{Z}$ *for all* $\gamma \in \Gamma$. *Then* Γ *is conjugate in* $\mathrm{SL}(2, \mathbf{C})$ *to a subgroup of* $\rho(\mathcal{O}^1)$ *for some order* $\mathcal{O}$ *in a quaternion algebra* B *over* $\mathbf{Q}$. *In particular:*

If Γ *is infinite* $\mathrm{P}\Gamma$ *is conjugate to a subgroup of an arithmetic Fuchsian group from a quaternion algebra defined over* $\mathbf{Q}$.

If Γ *is finite, then* $\mathrm{P}\Gamma \cong A_4$ *or* Σ_3 *or* V_4*, the Klein 4-group.*

Proof.. The infinite case has a proof identical to that of Theorem 3.1; the finite case follows from Theorem 2.3. Note that the only irreducible subgroups of A_4^* or Σ_3^* are the groups themselves or the extension of V_4 in $\mathrm{SL}(2, \mathbf{C})$. This completes the proof. □

Corollary 4.6. *Let* $\rho : \Gamma \to \mathrm{SL}(2, \mathbf{Q})$ *be an irreducible representation for which* $\chi_\rho(\gamma) \in \mathbf{Z}$ *for all* $\gamma \in \Gamma$.

Then Γ *is conjugate to a subgroup of* $\mathrm{SL}(2, \mathbf{Z})$.

Proof.. Since $\rho(\Gamma)$ is an irreducible subgroup of $\mathrm{SL}(2, \mathbf{Q})$, the quaternion algebra $A\rho(\Gamma)$ coincides with $M(2, \mathbf{Q})$. In particular the quaternion algebra is not ramified at the real place. Theorem 2.3 now implies $\rho(\Gamma)$ must be infinite and Lemma 4.5 then implies that $\rho(\Gamma)$ is conjugate into $\mathcal{O}^1$ where $\mathcal{O}$ is an order of $M(2, \mathbf{Q})$. We may as well assume that $\mathcal{O}$ is maximal, in which case Theorem 2.1 completes the proof. □

We commence with the proof of Theorem 4.2. Let $\Gamma = \pi_1(\Sigma \setminus K)$, X be an irreducible component of $X(K)$ and $\chi_\rho \in X$ be an irreducible integral point. We consider the possibilities for the representation ρ.

If the image is finite, since Σ is a homology 3-sphere, the remarks above show that $\pi_1(\Sigma \setminus K)$ has cyclic abelianization and so cannot surject V_4. The result now follows from 4.5.

Therefore assume that $\rho(\Gamma)$ is infinite. By Lemma 4.5 we can conjugate so that $\rho(\Gamma)$ is a subgroup of the unit group of a maximal order coming from a quaternion algebra defined over $\mathbf{Q}$.

Case 1. $\rho(\Gamma)$ contains a parabolic element.

In this case, the quaternion algebra $A\rho(\Gamma)$ is not a division algebra since a parabolic element α yields the zero divisor $\alpha - I$. Thus by the discussion in §3.3, $A\rho(\Gamma) \cong M(2, \mathbf{Q})$. By the Skolem-Noether Theorem for example, the representation ρ is conjugate to one with image in $\mathrm{SL}(2, \mathbf{Q})$ and in which all traces (invariant under conjugacy) are integers. Corollary 4.6 now shows that the group is conjugate to a subgroup of $\mathrm{SL}(2, \mathbf{Z})$.

At this point it is more convenient to work in $\mathrm{PSL}(2, \mathbf{Z})$, so we consider $\mathrm{P}\rho(\Gamma)$. The group $\mathrm{PSL}(2, \mathbf{Z})$ is a free product of two cyclics $\mathbf{Z}_2 * \mathbf{Z}_3$. Any finitely generated subgroup of such a group is a free product of the form $F * C$

where F is a free group of some rank (possibly zero) and C is a free product of some number (again, possibly zero) of finite cyclic groups of orders 2 and 3. Since Γ is a knot group, homology considerations, taken together with the fact that the image group is irreducible precludes the possibility that $\rho(\Gamma)$ is free, or has a free factor. It follows that $\rho(\Gamma)$ is a free product of finite cyclic groups. However, homological considerations (and the fact that image being irreducible) imply that there can only be two summands, and they must have of co-prime orders, i.e. the image is $\mathbf{Z}_2 * \mathbf{Z}_3$. By Lemma 4.4 we induce a homomorphism onto $\pi_1(S^3 \setminus T)$.

Finally, if C is an algebraic curve defined over $\mathbf{Q}$ the only proper algebraic subvarieties of C are of dimension 0 ([22] chapter 1). Thus if X is an algebraic curve given by the first conclusion of Theorem 1.5 then it must coincide with Y. The other possibility is that there is a higher dimensional component containing the algebraic curve Y.

Case 2. $\rho(\Gamma)$ contains no parabolic elements.

As above it is convenient to consider $\mathrm{P}\rho(\Gamma)$ in PSL(2, $\mathbf{R}$), so that $\mathrm{P}\rho(\Gamma)$ is a subgroup of a cocompact arithmetic Fuchsian group. Standard results about such groups imply that any finitely generated subgroup is either the orbifold group of a closed hyperbolic 2-orbifold, or is a free product $F * C$ of the type stated in the previous case.

Using Lemma 2.2 and arguing as above we again find that in any of the free product cases, the image group must be $\mathbf{Z}_2 * \mathbf{Z}_3$, and so we are in the first case of the theorem.

Otherwise we can assume that $\mathrm{P}\rho(\Gamma)$ is the group of a closed hyperbolic 2-orbifold. By Lemma 4.3 the base is a 2-sphere with cone angles $2\pi/m_i$ for $i = 1, \dots, r$ say. Standard facts about such orbifolds imply that $r \geq 3$ and the above torsion considerations imply that the cone points can only have orders 2 and 3. If there are k cone points of cone angle π and l of cone angle $2\pi/3$, then the abelianization of the orbifold group is $\mathbf{Z}_2^{k-1} \oplus \mathbf{Z}_3^{l-1}$. This is cyclic only when $k = l = 2$. However in this case the orbifold group surjects onto $\mathbf{Z}_2 * \mathbf{Z}_3$. This completes the proof of Theorem 4.2. □

Note that given representations as in the conclusion of Theorem 1.5 there are always integral points. This leads to a converse in the case where all components of $X(K)$ have dimension 1 (for example when $\Sigma \setminus K$ contains no closed embedded essential surface, [8]).

Theorem 4.7. *With K as above, suppose all components of $X(K)$ have dimension 1. Then some component of $X(K)$ contains an irreducible integral point if and only if at least one of the following happens:*

- *$\pi_1(\Sigma \setminus K)$ surjects onto the fundamental group of the trefoil knot complement. In which case $X(K)$ contains the algebraic curve Y as an algebraic curve component.*
- *The integral point corresponds to a Σ_3^* or A_4^* representation.* □

Remark. 1. By analyzing the proof, it follows that Theorem 1.5 can be generalized to knot complements in rational homology 3-spheres, which are both mod 2 and mod 3 homology 3-spheres.
2. We conclude with some comments relating to Siegel's Theorem. Recall that the **rank** of a finitely generated group Γ is the minimal cardinality of a generating set for Γ. With K as above, assume that $\pi_1(\Sigma \setminus K)$ does not surject onto $\pi_1(S^3 \setminus T)$. Then using Theorem 1.5, the number of irreducible integral points on $X(K)$ is a function of the rank of $\pi_1(S^3 \setminus K)$ and the homology of the 2-fold and 3-fold branched covers. In any given example, the algorithms from coset enumeration make calculating the number of **Z**-points very effective.

5 Some computations

In this section we discuss some examples and applications.

5.1 Finite representations of knot groups

We first prove the following lemma about representations of knot groups onto Σ_3 and A_4. Throughout K is a knot in S^3, $\Gamma = \pi_1(S^3 \setminus K)$, and M_n the n-fold cyclic branched cover of K. As remarked in §1, it suffices to consider homomorphisms to Σ_3 and A_4. A standard reference for knot theory is [6].

Lemma 5.1.
1. If $|H_1(M_2; \mathbf{Z})|$ *is finite and not divisible by* 3 *then* Γ *cannot surject onto* Σ_3.
2. If $|H_1(M_3; \mathbf{Z})|$ *is finite and not divisible by* 4 *then* Γ *cannot surject onto* A_4.

Proof.. The group Σ_3 has abelianization $\mathbf{Z}_2$ with a normal subgroup of order 3, and A_4 has abelianization $\mathbf{Z}_3$ with a normal subgroup $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. Thus if Γ surjects onto Σ_3 (resp. A_4) the homomorphism induces a homomorphism from $\pi_1(M_2) \to \mathbf{Z}_3$ (resp. $\pi_1(M_3) \to \mathbf{Z}_2 \oplus \mathbf{Z}_2$). The lemma now follows. □

The homology of cyclic branched covers of knots is readily computed. A standard fact about the homology of the cyclic branched covers of knots is (see [6] pp 116–117), that if this is finite it is given by

$$|H_1(M_n; \mathbf{Z})| = |\prod_{i=1}^{n} \Delta(\zeta_i)|,$$

where $\Delta(t)$ is the Alexander polynomial of K, and ζ_i is an n-th root of unity. Also, $\Delta(1) = 1$ since this is simply the homology of S^3. Summarizing this discussion together with Lemma 5.1 we have,

Corollary 5.2. *Let K be a knot with the property that $\Delta(-1)$ is not divisible by 3, and $\Delta(\omega)\Delta(\overline{\omega})$ is not divisible by 4, where $\omega = \frac{(-1+\sqrt{-3})}{2}$ is a non-trivial cube root of unity. Then Γ admits no homomorphism to Σ_3 or A_4.* □

Recall from the proof of Corollary 1.7 that if Γ does not surject onto Σ_3 or Σ_4, then Γ cannot surject onto $\pi_1(T)$. With this we now establish,

Theorem 5.3. *There exist infinitely many hyperbolic knots such that the component X_0 contains no integral point.*

Proof.. The family of twist knots K_n $(n \in \mathbf{Z})$ are the knots obtained by $1/n$-Dehn surgery on one component of the Whitehead link (see [6] Chapter 15). These knots are hyperbolic knots for all $n \neq 0, 1$ (eg [23]) which correspond to the trivial knot and the trefoil knot respectively. Therefore, as discussed in §4.1, X_0 cannot be the algebraic curve Y.

To prove the theorem, it therefore suffices to exhibit an infinite number of twist knots whose Alexander polynomial satisfies the requirements of Corollary 5.2.

Now the Alexander polynomial of K_n $(n \geq 2)$ is

$$\Delta_n(t) = nt^2 + (1 - 2n)t + n.$$

The proof will be completed by the following claim.

Claim.. If $n = 0 \bmod 6$, then $\Delta_n(-1)$ is not divisble by 3, and $\Delta(\omega)\Delta(\overline{\omega})$ is not divisible by 4.

Proof of Claim.. $\Delta_n(-1) = n+(1-2n)(-1)+n = 4n-1$. Hence if $n = 0 \bmod 6$, $4n - 1$ is not divisible by 3.

For divisibility by 4 consider the algebraic number $n\omega^2 + (1 - 2n)\omega + n$. $\omega = \frac{(-1+\sqrt{-3})}{2}$ and so expanding we get $(3n-1)\frac{(1-\sqrt{-3})}{2}$. The norm of this element (as an element of $\mathbf{Q}(\omega)$) is $(3n - 1)^2$. Hence the product $\Delta(\omega)\Delta(\overline{\omega}) = (3n - 1)^2$, and so if n is even this product can never be divisible by 4. □

5.2 The figure-eight knot

We single out the figure eight knot for special consideration. Using mathematica one can again compute the defining polynomial equation for X_0. In this case, following the notation used in the computation for the trefoil we get;

$$p(z, r) = 5 - 5\,r + r^2 + (-1 + r)\ z^2.$$

The Alexander polynomial for the figure eight knot is $t^2 - 3t + 1$, and so by Corollary 5.2 we deduce that there is no Σ_3 representation, however there is an A_4 representation. This corresponds to the following integral points $z = \pm 1$ and $r = 2$ (it is is easy to see these give a solution to $p(z, r) = 0$).

The algebraic curve is an elliptic curve, being birationally equivalent over $\mathbf{Q}$ to the algebraic curve E (as is easily seen by arguing as above using $x = -r$ and $y = (1 - r)z$):

$$y^2 = x^3 + 6x^2 + 10x + 5.$$

Note that an integral point on X_0 gives an integral point on E.

Using PARI [7], and the tables of Cremona [12], we deduce that the conductor of the algebraic curve E is 40, and its Mordell-Weil group is finite of order 4. Indeed, projectively on E, the rational points in $[x; y; t]$ co-ordinates, are $[0; 1; 0]$ (point at infinity), $[-1; 0; 1]$, $[-2; 1; 1]$ and $[-2; -1; 1]$. Notice that the birational equivalence between E and X_0 described is not defined at the point $[-1; 0; 1]$. From this discussion, we deduce that the only rational points on X_0 are the points above (and infinity). Hence we have,

Corollary 5.4. *If K is the figure eight knot, and $\chi_\rho \in X_0$ is a rational character, then χ_ρ is integral and the image of ρ is finite. In particular there are no rational characters corresponding to representations with infinite image.* □

If we now consider genuine O_d-points on X_0 (i.e. those with at least one co-ordinate not in $\mathbf{Z}$, Theorem 1.2 shows that for large enough d there are no such points, and so for these d the only O_d points coincide with the $\mathbf{Z}$-points described above. However, using the faithful discrete representation there is an O_3-point [25].

It is also clear from this example that Theorem 1.2 does not hold in the context of real quadratics. Rewriting the equation for $p(z, r) = 0$ as a quadratic in r, points on X_0 arise as solutions of:

$$r^2 + (z^2 - 5)r + (5 - z^2) = 0.$$

Choosing $z \in \mathbf{Z}$, with $|z| > 2$, gives an infinitely many quadratic equations all with positive discriminant and hence giving solutions that are integers in real quadratic number fields.

5.3 The knot 5_2

Another simple example is given by the knot 5_2. The Alexander polynomial in this case is $2t^2 - 3t + 2$. It is easy to check that the Alexander polynomial obstruction of Corollary 5.2 applies to show there is no integral point on X_0. In fact one can be explicit about the calculation of X_0. Using the the fact that 5_2 is the twist knot with 2-bridge normal form (7, 5), a presentation for the fundamental group is:

$$< a, b \mid waw^{-1} = b, w = a^{-1}ba^{-1}b^{-1}ab^{-1} > .$$

Now one can compute the the defining polynomial equation for the component X_0 directly using mathematica. One gets,

$$p(z, r) = -7 + 14\,r - 7\,r^2 + r^3 + \left(2 - 3\,r + r^2\right)\, z^2.$$

Thus the algebraic curve $p(z, r) = 0$ has no integral point. This algebraic curve is of genus 2 being birationally equivalent over $\mathbf{Q}$ to the hyperelliptic curve (see [22] Chapter 7 for instance)

$$y^2 = x^5 + 10x^4 + 37x^3 + 63x^2 + 49x + 14.$$

The birational equivalence is seen by first rewriting the equation of the algebraic curve as,

$$-7 + 14\,r - 7\,r^2 + r^3 = \left(-2 + 3\,r - r^2\right)\, z^2.$$

Multiplying both sides by $(-2 + 3\,r - r^2)$ and letting $y = (-2 + 3\,r - r^2)z$ we get the equation given above where $x = -r$.

5.4 Finite Dehn surgeries

Let $K \subset S^3$ be a hyperbolic knot. Fixing the usual meridian-longitude framing (m, ℓ) for K, the question of which surgeries yield 3-manifolds with finite fundamental group is of some interest, see [15] and [4]. Our methods give some obstructions as we now discuss. We use the language of [4], so that by p/q-Dehn surgery on K of type T, O or I we mean that p/q-Dehn surgery on K is manifold whose fundamental group is isomorphic to $A_4^* \times \mathbf{Z}_p$, $S_4^* \times \mathbf{Z}_p$ or $A_5^* \times \mathbf{Z}_p$ respectively, and $\mathbf{Z}_p$ is the cyclic group of order p.

Theorem 5.5. *Suppose that $X(K)$ has no irreducible $\mathbf{Z}$-point (resp. $\mathbf{Z}[\sqrt{2}]$-point, $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$-point, then K admits no Dehn surgery of type T (resp. O, I).*

Proof of Claim.. The $\mathbf{Z}$-point case is clear from the discussion in §5. The remaining cases are exactly the same, since as discussed in §3.8, a surgery of type O or I gives irreducible integral points of $X(K)$ in the appropriate ring of integers. □

It is conjectured that all hyperbolic knots have *Property I*; that is, if K is a hyperbolic knot then no Dehn surgery on K can have fundamental group A_5^* (cf. [4]). An easy corollary of Theorem 5.5 is:

Corollary 5.6. *With K as above. If $X(K)$ has no $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$-point, then K has property I.*

The Poincare homology sphere (which has fundamental group A_5^*) is obtained by surgery on the trefoil. Hence Y has a $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$-point, and so any knot group that surjects onto the group of the trefoil has also a $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$-point in $X(K)$.

Acknowledgements. The second author wishes to thank C. McA. Gordon for some helpful conversations, and C. Popescu, F. Rodriguez-Villegas, J. Tate and J. Vaaler for help with the number theory at various stages of the development of this paper.

References

1. H. Bass, Groups of integral representation type, Pacific J. Math. **86** (1980), 15–51
2. A. Borel, Commensurability classes and volumes of hyperbolic 3-manifolds, Ann. Scuola Norm. Sup. Pisa **8** (1981), 1–33
3. D. W. Boyd, Reciprocal polynomials having small measure, Math. Comp. **35** (1980), 1361–1377
4. S. Boyer, X. Zhang, Finite Dehn surgery on knots, J. Amer. Math. Soc. **9** (1996), 1005–1050
5. S. Boyer, X. Zhang, On Culler-Shalen seminorms and Dehn filling, Ann. Math. **148** (1998), 737–801
6. G. Burde, H. Zieschang, Knots, De Gruyter-Verlag (1985)
7. H. Cohen et al., PARI, Freeware available by anonymous FTP from megrez@math.u-bordeaux.fr, directory pub/pari
8. D. Cooper, M. Culler, H. Gillet, D. D. Long, P. B. Shalen, Plane curves associated to character varieties of 3-manifolds, Invent. Math. **118** (1994), 47–84
9. D. Cooper, D. D. Long, Remarks on the A-polynomial of a knot, J. Knot Theory and its Ramifications **5** (1996), 609–628
10. D. Cooper, D. D. Long, Roots of unity associated to the character variety of a knot complement, J. Australian Math. Soc. **55** (1993), 90–99
11. D. Cooper, D. D. Long, The A-polynomial has ones in the corners, Bull. London Math. Soc. **29** (1997), 231–238
12. J. E. Cremona, Algorithms For Modular Elliptic Curves, Cambridge University Press (1992)
13. M. Culler, P. B. Shalen, Varieties of group representations and splittings of 3-manifolds, Ann. Math. **117** (1983), 109–146
14. M. Culler, P. B. Shalen, Bounded separating incompressible surfaces in knot manifolds, Invent. Math. **75** (1984), 537–545
15. M. Culler, C. McA. Gordon, J. Luecke, P. B. Shalen, Dehn surgery on knots, Ann. Math. **125** (1987), 237–300
16. F. W. Gehring, C. Maclachlan, G. J. Martin, A. W. Reid, Arithmeticity, discreteness and volume, Trans. Amer. Math. Soc. **349** (1997), 3611–3643
17. A. Hatcher, On the boundary curves of incompressible surfaces, Pacific J. Math. **99** (1982), 373–377
18. C. D. Hodgson, Private communication
19. A. Lubotzky, A. Magid, Varieties of group representations of finitely generated groups, Mem. Amer. Math. Soc., **336** (1985)
20. K. Mahler, Lectures on Transcendental Numbers, L. N. M. **546**, Springer-Verlag (1976)
21. J. W. Morgan, P. B. Shalen, Valuations, trees and degenerations of hyperbolic structures, I, Ann. Math. **120** (1984), 401–476
22. D. Mumford, Algebraic Geometry I: Complex Projective Varieties, Grund. der Math. Wissen. 221, Springer-Verlag, (1976)

23. W. D. Neumann, A. W. Reid, Arithmetic of hyperbolic 3-Manifolds, **Topology ’90**, Proc. of Low-dimensional Topology Conference, Ohio State Univ., De Gruyter (1991), 273–310
24. U. Oertel, Closed incompressible surfaces in the complement of star links, Pacific J. Math. **111** (1984), 209–230
25. R. Riley, A quadratic parabolic group, Math. Proc. Camb. Phil. Soc. **77**, (1975), 281–288
26. C. L. Siegel, Einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss. Phy. Math. Kl (1929), 41–69
27. K. Takeuchi, A characterization of arithmetic Fuchsian groups, J. Math. Soc. Japan **27** (1975), 600–612
28. W. P. Thurston, The Geometry and Topology of 3-manifolds, Princeton Univ. mimeographed notes (1979)
29. M.-F. Vignéras, Arithmétique des algèbres de Quaternions, Lect. Notes Math. **800**, Springer-Verlag Berlin 1980