New York Journal of Mathematics

New York J. Math. **27** (2021) 1494–1523.

Arithmetic of the canonical component of the knot 7_4

Nicholas Rouse

ABSTRACT. We prove two arithmetic properties of Dehn surgery points on the canonical component of the $\mathrm{SL}_2\mathbf{C}$-character variety of the knot 7_4. The first is that the residue characteristics of the ramified places of the Dehn surgery points form an infinite set, providing evidence for a conjecture of Chinburg, Reid, and Stover. The second is that the Dehn surgery points have infinite order in the Mordell-Weil group of the elliptic curve obtained by a simple birational transformation of the canonical component into Weierstrass form.

CONTENTS

1. Introduction

Let Γ be a finitely generated group, and let $X(\Gamma)$ denote the $\mathrm{SL}_2\mathbf{C}$-character variety of Γ (see Section 2.1). When Γ is the fundamental group of a compact 3-manifold M, work of Thurston and Culler–Shalen established $X(\Gamma)$ as a powerful tool in the study of the geometry and topology of M. The focus of this paper is arithmetic and algebraic properties of a particular component C (the canonical component, see Section 2.1) of $X(\Gamma)$ when Γ is the fundamental group of a particular hyperbolic knot complement (7_4 of the tables of [17] and $(15, 11)$ in two-bridge notation.). This has already been studied for different reasons ([5]). There are two themes to this: the first is that, following [4], we are particularly

Received April 14, 2021.

2020 *Mathematics Subject Classification.* 57K32, 57K10, 11G05, 11R52.

Key words and phrases. Dehn surgery, hyperbolic knots, Azumaya algebras, character varieties, elliptic curves.

ISSN 1076-9803/2021

interested in a canonically defined quaternion algebra, $A_k(C)$, which is defined over the function field of C, $k(C)$, and specializes at Dehn surgery points of C to quaternion algebras defined over number fields. The second theme is to view C as an elliptic curve and to consider the Mordell-Weil group of naturally occurring number field points on C.

In more detail, for the first part, for knots satisfying an arithmetic condition on their Alexander polynomials (condition ($\star$), see Section 3.2), Chinburg, Reid, and Stover show in [4] that there are only finitely many rational primes lying under any finite prime ramifying the specializations of this quaternion algebra. Let us write S for this set of rational primes. Let us define $S_D \subseteq S$ to be the set of rational primes p such that there is a specialization to the character of a hyperbolic Dehn surgery such that the quaternion algebra is ramified at some prime lying above p. When condition ($\star$) fails, it is shown in [4, Theorem 1.1(3)] (using work of Harari [10]) that S is infinite. They furthermore state as a conjecture [4, Conjecture 6.7] that

Conjecture 1.1. *Let K be a hyperbolic knot in S^3 that fails condition ($\star$), then, in the notation above, $S = S_D$.*

As we note in Section 3.3, 7_4 fails condition ($\star$). Our first main result is:

Theorem 1.2. *Let K be the knot 7_4 and T be the set of rational primes p such that there exists a place $\mathfrak{p}$ lying above p of the trace field of some hyperbolic Dehn surgery $(d, 0)$ at which the canonical quaternion algebra associated to that surgery is ramified. Then T and hence S_D are infinite.*

We now turn our attention to the second result, which concerns the arithmetic of Dehn surgery points in the Mordell-Weil group. Thought of as a variety embedded in $\mathbf{P}^2(\mathbf{C})$, the projective closure of the canonical component C of 7_4 has singular points, but it is birational to a curve of genus one. Together with a choice of basepoint, such a curve is an elliptic curve. Concretely, the canonical component, C, is cut out by $R^3 - R^2Z^2 + 2R^2 - 1 = 0$ and is birational via the coordinate change $R = x, Z = y/x$ to E, the affine variety cut out by $y^2 = x^3 + 2x^2 - 1$. The latter equation is a nonsingular Weierstrass equation and hence determines an elliptic curve by taking the unique point at infinity to be the basepoint. We may then regard a "Dehn surgery point" on the elliptic curve to be any point in the image of the birational map $C \dashrightarrow E$.

A basic fact about elliptic curves is that their points can be made into an abelian group, and (over $\mathbf{C}$, say) the n-torsion points form a subgroup isomorphic to $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$. In general it is a difficult problem to produce infinite order points in a particular number field on a given elliptic curve. One of the few ways uses the theory of Heegner points (see e.g. [7]) which allows one to construct infinite order $\mathbf{Q}$-rational points on certain elliptic curves. However, experimental evidence suggested that hyperbolic Dehn surgery points were never torsion points, and our second main result is that in fact every hyperbolic Dehn surgery point has infinite order.

Theorem 1.3. *Let E be the elliptic curve defined by $y^2 = x^3 + 2x^2 - 1$. With the conventions of the above paragraph, every hyperbolic Dehn surgery point has infinite order in the Mordell-Weil group of E.*

In our setting characters of hyperbolic Dehn surgeries have infinite order, and they are rational points over their trace fields. The proof of 1.3 (see Section 6) combines an algebraic fact (Proposition 6.1) with mostly topological results of Bass, Hatcher, and Thurston. The algebraic fact shows that nonpositive 2-adic valuation of the x-coordinate of a point on E obstructs being a torsion point. The topological results imply that no Dehn surgery point can have such a form.

1.1. Outline. The paper is organized as follows. We introduce some background material on canonical components, trace field, and quaternion algebras in Section 2. Then we discuss their generalization, Azumaya algebras and how they figure into studying ramification in Section 3. We then give a proof of Theorem 1.2 in Section 4. There are many lemmas used in the proof, and we delay their proofs until Section 5 so that the proof of 1.2 may be read more easily. Finally in Section 6 we provide some background material on elliptic curves and prove Theorem 1.3.

1.2. Acknowledgments. The author wishes to thank his advisor, Alan Reid, for suggesting the problems in this paper as well as his support and guidance in both the mathematical and writing phases of this paper's preparation. The author would also like to acknowledge the anonymous referees for their helpful comments and suggestions, with special thanks to the one who pointed out Theorem 5.11, which simplified the original argument.

2. The canonical component, traces fields, and quaternion algebras

In this section we provide some background material about character varieties and quaternion algebras. We then establish the canonical component of 7_4 and a tractable form of the canonical quaternion algebra.

2.1. Character varieties. We begin by recalling that, for a finitely generated group Γ, the $\mathrm{SL}_2\mathbf{C}$-representation variety of Γ is $R(\Gamma) = \mathrm{Hom}(\Gamma, \mathrm{SL}_2\mathbf{C})$. Given a generating set $\{\gamma_i\}$, we identify a representation $\rho : \Gamma \to \mathrm{SL}_2\mathbf{C}$ with

$$(\rho(\gamma_1), \dots, \rho(\gamma_n)) \subset \mathrm{SL}_2\mathbf{C}^n \subset \mathbf{C}^{4n}.$$

Given a different choice of generators, there is a canonical isomorphism between the two subsets of $\mathbf{C}^{4n}$ obtained this way. Fixing an element $\gamma \in \Gamma$, we may define a map I_γ on $R(\Gamma)$ that associates to a representation ρ the trace of ρ. That is, $I_\gamma : R(\Gamma) \to \mathbf{C}$ is defined by $I_\gamma(\rho) = \mathrm{tr}\,\rho(\gamma) = \chi_\rho(\gamma)$. This I_γ is a regular function on the algebraic set $R(\Gamma)$, and the ring T generated by all such I_γ turns out to be finitely generated. This is [6, Proposition 1.4.1]. Fixing a generating set $I_{\gamma_1}, \dots, I_{\gamma_m}$ for T, define a map $t : R(\Gamma) \to \mathbf{C}^m$ by $t(\rho) = (I_{\gamma_1}(\rho), \dots, I_{\gamma_m}(\rho))$. Then define the $\mathrm{SL}_2\mathbf{C}$-character variety of Γ to be $t(R(\Gamma)) \subset \mathbf{C}^m$. This is a closed

algebraic set, and different choices of generators for T give isomorphic algebraic sets. When Γ is the fundamental group of the complement of a hyperbolic knot K in S^3, we define its canonical component to be the irreducible component of $X(\Gamma)$ containing the character of the discrete and faithful representation of $\pi_1(S^3\backslash K)$. We refer the reader to [6] for more detail.

2.2. Computation of the character variety. We start with the fundamental group of the complement of 7_4 in S^3 and some notation for the canonical component.

Notation 2.1. Let K be the knot 7_4 in S^3. Write $\Delta_K(t) = 4t^2 - 7t + 4$ for its Alexander polynomial. We also write Γ for the fundamental group of the complement of K in S^3. We use the following presentation

$$\Gamma = \pi_1(S^3\backslash K) = \langle a, b | aw^2 = w^2 b\rangle,$$

where $w = ab^{-1}ab^{-1}a^{-1}ba^{-1}b$. For a representation $\rho : \Gamma \to \mathrm{SL}_2\mathbf{C}$, we conjugate so that

$$\rho(a) = \begin{pmatrix} x & 1 \\ 0 & 1/x \end{pmatrix}$$

$$\rho(b) = \begin{pmatrix} x & 0 \\ r & 1/x \end{pmatrix}.$$

In defining an algebraic set, one should generally avoid expressions like $1/x$, but here we use it as a shorthand for y where $xy = 1$. Also, note that this presentation for the fundamental group comes from the two-bridge normal form for 7_4, namely $(15, 11)$. These facts and the following are in [5, Section 5].

Proposition 2.2. *If we write*

$$Z = \chi_\rho(a) = \chi_\rho(b) = x + \frac{1}{x},$$

and

$$R = \chi_\rho(ab^{-1}) = \mathrm{tr}\begin{pmatrix} 1-r & x \\ -r/x & 1 \end{pmatrix} = 2 - r,$$

then the $\mathrm{SL}_2\mathbf{C}$ *character variety has canonical component given by the vanishing of* $R^3 - R^2Z^2 + 2R^2 - 1$.

2.3. Quaternion algebras over fields. We now recall some facts about quaternion algebras (see, e.g., [13, Ch.2]). Recall that a **quaternion algebra** A over a field F of characteristic not equal to 2 is a 4-dimensional central simple algebra over F. More concretely, A is a 4-dimensional algebra over F admitting an F-basis $\{1, i, j, ij\}$ with $i^2 = a$, $j^2 = b$, and $ij = -ji$ where $a, b \in F^*$. One may efficiently encode this information with a **Hilbert symbol**, $\left(\frac{a,b}{F}\right)$. Note that any quaternion algebra is described by many Hilbert symbols.

Though we will have occasion to consider quaternion algebra over function fields, our real objective is to study the quaternion algebras that are associated to Dehn surgery points. These are quaternion algebras over number fields. In this

situation, there is a powerful classification theorem that in some sense justifies investigating the ramification set of Theorem 3.5 and Theorem 1.2 in the first place. We begin with a quaternion algebra A over a number field L. Given a place $\mathfrak{p}$ of L, one may form the completion $L_{\mathfrak{p}}$ and extend A to a quaternion algebra $A_{\mathfrak{p}} = A \otimes_L L_{\mathfrak{p}}$. There are exactly two isomorphism classes of quaternion algebras over the local field $L_{\mathfrak{p}}$. If $A_{\mathfrak{p}}$ is isomorphic to $M_2(L_{\mathfrak{p}})$ then A is said to **split** at $\mathfrak{p}$. Otherwise, $A_{\mathfrak{p}}$ is the unique division quaternion algebra over $L_{\mathfrak{p}}$ and A is said to **ramify** at $\mathfrak{p}$. We state the version of the classification theorem for quaternion algebras over number fields as it appears in [13, Theorem 7.3.6].

Theorem 2.3. *Let A be a quaternion algebra over the number field L and let* $\mathrm{Ram}(A)$ *denote the set of places at which A is ramified. Then,*

(1) $\mathrm{Ram}(A)$ *is finite of even cardinality.*
(2) Let A_1 and A_2 be two quaternion algebras over L. Then $A_1 \equiv A_2$ if and only if $\mathrm{Ram}(A_1) = \mathrm{Ram}(A_2)$.
(3) Let S be any finite set of even cardinality of finite and nonreal infinite places, then there exists a quaternion algebra A over L with $\mathrm{Ram}(A) = S$.

There is a relatively easy way to compute the ramification sets. We use the following description of the ramification of a quaternion algebra over a $\mathfrak{p}$-adic field which is sufficient for our purposes.

Theorem 2.4 ([13, Theorem 2.6.6.(b)])**.** *Let L be a non-dyadic $\mathfrak{p}$-adic field, with ring of integers $\mathcal{O}$ and maximal ideal $\mathfrak{p}$. Let $A = \left(\frac{a,b}{L}\right)$, where $a, b \in \mathcal{O}$. If $a \notin \mathfrak{p}$, $b \in \mathfrak{p}\backslash\mathfrak{p}^2$, then A splits if and only if a is a square modulo $\mathfrak{p}$.*

2.4. Number fields and quaternion algebras associated to subgroups of $\mathbf{SL_2C}$. We next turn to some background information about subgroups of $\mathrm{SL}_2\mathbf{C}$. A subgroup Γ of $\mathrm{SL}_2\mathbf{C}$ is **non-elementary** if its image in $\mathrm{PSL}_2\mathbf{C}$ has no finite orbit in its action on $\mathbf{H}^3 \cup \widehat{\mathbf{C}}$. Given an non-elementary subgroup Γ of $\mathrm{SL}_2\mathbf{C}$, we define its **trace field** by $k_\Gamma = \mathbf{Q}(\mathrm{tr}\,\gamma | \gamma \in \Gamma)$ and **quaternion algebra** by the k_Γ-span of elements of Γ. That is,

$$A_\Gamma = \left\{ \sum_{\text{finite}} \alpha_i \gamma_i \middle| \alpha_i \in k_\Gamma, \gamma_i \in \Gamma \right\}.$$

As shown in [13, p.78], we may write a Hilbert symbol for this quaternion algebra as

$$\left(\frac{\chi(g)^2 - 4, \chi(g,h) - 2}{k_\Gamma} \right),$$

where g, h are noncommuting hyperbolic elements of Γ. In fact, this pointwise construction extends to define a quaternion algebra over the function field of the curve.

Proposition 2.5 ([4, Corollary 2.9])**.** *Let Γ be a finitely generated group, and C an irreducible component of the character variety of Γ defined over the number*

field k. Assume that C contains the character of an irreducible representation, and let $g, h \in \Gamma$ be two elements such that there exists a representation ρ with character $\chi_\rho \in C$ for which the restriction of ρ to $\langle g, h\rangle$ is irreducible. Then the canonical quaternion algebra $A_{k(C)}$ is described by the Hilbert symbol

$$\left(\frac{I_g^2 - 4, I_{[g,h]} - 2}{k(C)}\right).$$

For the remainder of the section, let us specialize to the case of $K = 7_4$, $\Gamma = \pi_1(S^3\backslash K)$, and C the canonical component of the $\mathrm{SL}_2\mathbf{C}$-character variety of Γ. Recall that C is cut out by $R^3 - R^2Z^2 + 2R^2 - 1$. We now give an explicit Hilbert symbol for the canonical quaternion algebra associated to Γ.

Lemma 2.6. *The canonical quaternion algebra over $k(C)$ is given by*

$$\left(\frac{Z^2 - 4, R - 2}{k(C)}\right).$$

If we use the coordinate $r = R - 2$, then the Hilbert symbol is given by

$$\left(\frac{-r^3 + 4r^2 - 4r - 1, -r}{k(C)}\right).$$

Proof. If we let a, b be the two generators for the knot group, they satisfy the hypotheses of Proposition 2.5. We then know that our Hilbert symbol is given by

$$\left(\frac{I_a^2 - 4, I_{[a,b]} - 2}{k(C)}\right).$$

For the first term, we have that $I_a^2 - 4 = Z^2 - 4$.

Then from the description of the canonical component, we have $Z^2R^2 = R^3 + 2R^2 - 1$. Since multiplying by a square doesn't affect the Hilbert symbol, we can substitute $Z^2 - 4$ with $Z^2R^2 - 4R^2$. Then,

$$\begin{aligned} Z^2R^2 - 4R^2 &= R^3 + 2R^2 - 1 - 4R^2 \\ &= R^3 - 2R^2 - 1. \end{aligned}$$

From Proposition 2.2, we may substitute the relation $R = 2 - r$ to obtain

$$\begin{aligned} R^3 - 2R^2 - 1 &= (2 - r)^3 - 2(2 - r)^2 - 1 \\ &= -r^3 + 4r^2 - 4r - 1. \end{aligned}$$

For the second term, we use the trace relations ([13, p.121]):

$$\begin{aligned} I_{ab} &= I_aI_b - I_{ab^{-1}} \\ &= Z^2 - R, \end{aligned}$$

so

$$\begin{aligned} I_{[a,b]} &= I_a^2 + I_b^2 + I_{ab}^2 - I_a I_b I_{ab} - 2 \\ &= 2Z^2 + \left(Z^2 - R\right)^2 - Z^2\left(Z^2 - R\right) - 2 \\ &= 2Z^2 - Z^2R + R^2 - 2. \end{aligned}$$

We can multiply $\left(2Z^2 - Z^2R + R^2 - 2\right) - 2 = 2Z^2 - Z^2R + R^2 - 4$ through by R^2 and use the relation from the canonical component to obtain

$$\begin{aligned} 2Z^2R^2 - Z^2R^3 + R^4 - 4R^2 &= 2\left(R^3 + 2R^2 - 1\right) - R\left(R^3 + 2R^2 - 1\right) + R^4 - 4R^2 \\ &= 2R^3 + 4R^2 - 2 - R^4 - 2R^3 + R + R^4 - 4R^2 \\ &= R - 2. \end{aligned}$$

□

Given the description of the canonical quaternion algebra over the function field $k(C)$, one may also pass back to the pointwise-defined quaternion algebras by specializing the entires of the canonical quaternion algebra to points on the curve C. One must pay attention to the field over which these quaternion algebras are defined however. Fortunately, the trace field and the residue field (in the sense of algebraic geometry) coincide.

Lemma 2.7 ([4, Lemma 2.5])**.** *Let C be an irreducible affine or projective curve defined over $\mathbf{Q}$. Let $\tilde{C}$ be the smooth projective completion of the normalization of the reduction of C. For any $z \in \tilde{C}\backslash\mathcal{I}(\tilde{C})$, let $\chi_\rho \in C$ be the associated character, i.e., the image of z on C under the rational map $\tilde{C} \to C$. Then*

$$k(z) = \mathbf{Q}\left(\mathrm{tr}(\rho(\gamma))|\gamma \in \Gamma\right) = k_\rho.$$

is the trace field of some (hence any) representation $\rho \in R(\Gamma)$ with character χ_ρ.

Remark 2.8. Until Section 6, we can ignore the the normalizations, reductions, and smooth projective closures of C because the canonical component is a smooth affine curve. It is not smooth at infinity, but our primary object of interest, Dehn surgery points, lie on C.

3. Extending quaternion algebras over function fields to Azumaya algebras

In this section we describe some of the algebro-geometric considerations for our problem. In particular, we explore the problem of extending a quaternion algebra defined over the function field of a scheme to an element of the Brauer group of that scheme. We begin with general discussion of Brauer groups before specializing to curves, and eventually to the canonical component coming from 7_4.

3.1. Brauer groups of schemes. For any scheme X, one defines the Brauer group by $\operatorname{Br} X = H^2_{\text{ét}}(X, \mathbf{G}_m)$, where $\mathbf{G}_m$ is the multiplicative group scheme. We will have no need for the details of étale cohomology, and the reader may think of X as a variety in this paper. Given this definition, we have an injection $\operatorname{Br} X \hookrightarrow \operatorname{Br} k(X)$ and exact sequence that describes precisely which elements of $\operatorname{Br} k(X)$ are in the image of this injection. We present it as it appears in [16, Theorem 6.8.3], though the result itself is due to Grothendieck and Gabber.

Theorem 3.1. *Let X be a regular integral Noetherian scheme. Let $X^{(1)}$ be the set of codimension 1 points of X. Then the sequence*

$$0 \to \operatorname{Br} X \to \operatorname{Br} k(X) \xrightarrow{res} \bigoplus_{x \in X^{(1)}} H^1(k(x), \mathbf{Q}/\mathbf{Z})$$

is exact with the caveat that one must exclude the p-primary part of all the groups if X is of dimension ≤ 1 and some $k(x)$ is imperfect of characteristic p, or if X is of dimension ≥ 2 and some $k(x)$ is of characteristic p.

In the above theorem, $k(x)$ is the residue field at the point x, and res denotes the residue homomorphism into the Galois cohomology group $H^1(k(x), \mathbf{Q}/\mathbf{Z}) = H^1(\operatorname{Gal}(k(x)^{sep}/k(x)), \mathbf{Q}/\mathbf{Z})$. Note that smooth varieties are regular schemes. We say that $A_{k(X)}$ "extends" over a point $x \in X$ if the residue is trivial at x. This exact sequence says that $A_{k(X)}$ extends to an element of $\operatorname{Br} X$ if and only if it has trivial residue at every codimension 1 point x in X. Elements of $\operatorname{Br} X$ are called **Azumaya algebras**. Quaternion Azumaya algebras are Azumaya algebras that locally look like quaternion algebras. Elements of $\operatorname{Br} k(X)$ that do not belong to $\operatorname{Br} X$ are characterized in terms of their ramification sets as the following result shows.

Theorem 3.2 ([4, Theorem 1.1.(3)])**.** *Let Γ be a finitely generated group with $\mathrm{SL}_2\mathbf{C}$ character variety $X(\Gamma)$. Let C be a geometrically integral 1-dimensional subvariety defined over $\mathbf{Q}$ that contains the character of an irreducible representation and write $\widetilde{C}$ for the smooth projective closure of the normalization of C. Finally suppose that $A_{k(C)}$ is not in the image of the canonical injection $\operatorname{Br} \widetilde{C} \to \operatorname{Br} k(C)$. Then there is no finite set of places S of $\mathbf{Q}$ with the following property: the $k(w)$-quaternion algebra $A_\rho \otimes_{k_\rho} k(w)$ is unramified outside the places of $k(w)$ over S for all but finitely many smooth points $w \in C(\overline{\mathbf{Q}})$ for which $\rho = \rho_w$ is absolutely irreducible.*

Remark 3.3. Both the $\mathrm{SL}_2\mathbf{C}$ character variety and canonical component for 7_4 are defined over $\mathbf{Q}$, and the canonical component is geometrically integral because $R^3 - R^2Z^2 + 2R^2 - 1$ is irreducible even after passing to an algebraic closure. The canonical component is singular at infinity, but—as we will see in the next section—the obstructions to coming from an Azumaya algebra are residues associated to smooth affine points on the canonical component, so we will often slightly abuse notation and write C in place of $\widetilde{C}$.

3.2. Quaternion Azumaya algebras on dimension 1 canonical components. Now let $\Gamma = \pi_1(S^3\backslash K)$ for K a hyperbolic knot. Write C for the normalization of a canonical component of $\mathrm{SL}_2\mathbf{C}$ character variety. Since this scheme has dimension 1 and its residue fields have characteristic zero, we may ignore all the caveats in Theorem 3.1. Moreover, on a curve, the codimension 1 points are just all the points on the curve except for the generic point. The authors of [4] consider the question of whether the canonical quaternion algebra $A_{k(C)}$ extends over all of C. Essentially what they prove is that $A_{k(C)}$ always extends over the points that are characters of irreducible representations and over points at infinity. In the case of canonical components coming from knots in S^3, they further cast the residue condition at the characters of reducible representations in terms of the arithmetic of the Alexander polynomial. In particular

Definition 3.4. Let K be a knot in S^3. If for each root z of its Alexander polynomial in a fixed algebraic closure of $\mathbf{Q}$ and each square root w of z, we have an equality of fields $\mathbf{Q}(w + w^{-1}) = \mathbf{Q}(w)$, then we say that K (or its Alexander polynomial) satisfies condition $(\star)$.

Theorem 3.5 ([4, Theorems 1.2, 1.4])**.** *Let K be a hyperbolic knot with $\Gamma = \pi_1\left(S^3\backslash K\right)$, and suppose that Δ_K satisfies condition $(\star)$. Then,*

(1) $A_{k(C)}$ comes from an Azumaya algebra in $\mathrm{Br}\,\tilde{C}$ where $\tilde{C}$ denotes the normalization of the projective closure of C.

(2) Furthermore, if the canonical component is defined over $\mathbf{Q}$, there exists a finite set S_K of rational primes such that, for any hyperbolic Dehn surgery N on K with trace field k_N, the k_N-quaternion algebra A_N can only ramify at real places of k_N and finite places lying over primes in S_K.

In particular, if condition $(\star)$ holds for the Alexander polynomial of the knot, then $A_{k(C)}$ extends over a smooth, projective model of C and is hence a quaternion Azumaya algebra. In view of the above theorem, we say that K, $\Delta_K(t)$, and $A_{k(C)}$ are **Azumaya positive** if condition $(\star)$ holds and **Azumaya negative** if not.

Let us comment on the connection between the Alexander polynomial and the question of extending $A_{k(C)}$. If z is a root of the Alexander polynomial and w is a square root of z, then condition $(\star)$ says that $\mathbf{Q}(w + w^{-1}) = \mathbf{Q}(w)$. In fact $\mathbf{Q}(w + w^{-1})$ is the residue field for the character of a reducible representation χ_ρ, and $\mathbf{Q}(w)$ is the extension of $\mathbf{Q}(w + w^{-1})$ obtained by adjoining the residue of $A_{k(C)}$ at χ_ρ. So if the fields are equal, the residue is trivial and the result follows. To be precise, in the case of a quaternion algebra like $A_{k(C)}$, its residue at any point x belongs to the Galois cohomology group $H^1(k(x), \mathbf{Z}/2\mathbf{Z})$. This group classifies (at most) quadratic extensions of $k(x)$ and is isomorphic to $k(x)^*/k(x)^{*^2}$ by Kummer theory. What is shown in [4] is that the at most quadratic extension at the character of a reducible representation χ_ρ is precisely $\mathbf{Q}(w)/\mathbf{Q}(w + w^{-1})$, so if there is an equality of these fields, then the residue

must be trivial. We note that their method of proof makes use of the tame symbol, which gives a relatively easy way to compute residue homomorphisms in this context. Given any pair of elements $\alpha, \beta \in k(C)$, the tame symbol of the quaternion algebra $\left(\frac{\alpha,\beta}{k(C)}\right)$ at $x \in C$ is (see [4, Theorem 3.1.(8)])

$$(-1)^{\mathrm{ord}_x(\alpha)\,\mathrm{ord}_x(\beta)}\beta^{\mathrm{ord}_x(\alpha)}/\alpha^{\mathrm{ord}_x(\beta)},$$

where this is understood as an element of $k(x)^*/k(x)^{*^2}$. The point is that when the characteristic of $k(x)$ is not 2, then this agrees with the residue. That is, the residue at x is trivial if and only if this tame symbol represents 1 in $k(x)^*/k(x)^{*^2}$.

In particular, the Brauer class of

$$\left(\frac{I_g^2-4, I_{[g,h]}-2}{k(C)}\right).$$

can only have nontrivial residue when $I_g = \pm 2$ or $I_{[g,h]} = 2$. We note that $I_{[g,h]} = 2$ corresponds to the character of reducible representations, and it turns out to account for all the nontrivial residues. This is proved in [4, Proposition 4.1].

3.3. Calculations for $K = 7_4$. In this subsection our goal is to show how the residues may be calculated either directly or by using the Alexander polynomial, so let us now specialize for the remainder of the section to $K = 7_4$, $\Gamma = \pi_1(S^3\backslash K)$, and C the canonical component of the $\mathrm{SL}_2\mathbf{C}$-character variety of Γ. Let us make some easy observations about $\Delta_K(t) = 4t^2-7t+4$, the Alexander polynomial of 7_4. Its roots are $(7\pm\sqrt{-15})/8$, so the square roots w of its roots are $\pm\frac{\sqrt{15}}{4} \pm \frac{i}{4}$. From this description it is clear that $\mathbf{Q}(w) = \mathbf{Q}(\sqrt{15}, i)$ for each value of w. Also note that $w^{-1} = \overline{w}$, so $\mathbf{Q}(w + w^{-1}) = \mathbf{Q}(\sqrt{15})$ for each value of w. We will shortly see these fields emerge in calculating the tame symbol at characters of reducible representations. For now, note that these calculations show that 7_4 does not satisfy condition ($\star$).

Our curve C is given by the vanishing of $R^3-R^2Z^2+2R^2-1$. As we mentioned at the end of the previous section all nontrivial residues occur at characters of reducible representations, that is, when $R = 2$, and at such characters we compute the residue field as

$$\begin{aligned}\mathbf{Q}[R,Z]/(R^3-R^2Z^2+2R^2-1, R-2) &\cong \mathbf{Q}[Z]/(-4Z^2+15)\\ &\cong \mathbf{Q}[Z]/(Z^2-15) \cong \mathbf{Q}(\sqrt{15}).\end{aligned}$$

Not coincidentally, the residue field here is $\mathbf{Q}(\sqrt{15})$. The tame symbol becomes

$$\frac{1}{\left(\frac{\sqrt{15}}{2}\right)^2-4} = -4 = -1 \in \mathbf{Q}(\sqrt{15})^*/\mathbf{Q}(\sqrt{15})^{*^2}$$

Via Kummer theory, we identify $\mathbf{Q}(\sqrt{15})^*/\mathbf{Q}(\sqrt{15})^{*2}$ with quadratic extensions of $\mathbf{Q}(\sqrt{15})$. So in our case, the class of -1 corresponds to the quadratic extension $\mathbf{Q}(\sqrt{15}, i)/\mathbf{Q}(\sqrt{15})$. In view of the exact sequence in Theorem 3.1, this shows that $A_{k(C)}$ is not in the image of $\mathrm{Br}\, C \to \mathrm{Br}\, k(C)$. In other words $A_{k(C)}$ does not extend to an Azumaya algebra. Then Theorem 3.2 says that the quaternion algebras obtained by specializing $A_{k(C)}$ at points in the character variety ramify at primes lying above infinitely many distinct rational primes. However we do not know that these representations are geometrically interesting just from Harari's work. In fact this setup leaves open the possibility that there exists a finite set S_K for 7_4 as in the statement of Theorem 3.5. Our result shows that even when one restricts to points corresponding to the characters of $(d, 0)$ hyperbolic Dehn surgery, there is still no such finite set S_K.

4. Proof of Theorem 1.2

Our goal is to understand the specializations of the canonical quaternion algebra at Dehn surgery points. We already have a fairly explicit description by combining Lemma 2.7 with Lemma 2.6. Indeed, we have that specifying a point (r, Z) gives a field k_ρ and a quaternion algebra over that field given by the Hilbert symbol

$$\left(\frac{-r^3 + 4r^2 - 4r - 1, -r}{k_\rho}\right). \tag{1}$$

We now give a description of the ramification. It is stated purely algebraically, but in our applications the field k will be the trace field of $(d, 0)$ surgeries, and r will be the corresponding coordinate coming from the character variety.

Proposition 4.2. *Let r be an algebraic integer, k a finite extension of $\mathbf{Q}$ containing r, and $\mathcal{O}$ the ring of integers of k. Let $N_{k/\mathbf{Q}}(r) = \pm p_1^{d_1} \cdots p_m^{d_m}$ be the prime factorization of the field norm of r in $k/\mathbf{Q}$. For each $p_i \equiv 3 \bmod 4$ with d_i odd, there is a prime ideal $\mathfrak{p}_i \subseteq \mathcal{O}$ containing r and lying above p_i such that*

$$\left(\frac{-r^3 + 4r^2 - 4r - 1, -r}{k_{\mathfrak{p}_i}}\right)$$

is a division algebra, where $k_{\mathfrak{p}_i}$ denotes k completed at $\mathfrak{p}_i$.

The above lemma is purely algebraic, but we will apply it when k is the trace field of a $(d, 0)$ surgery. In this setting r will specialize to the algebraic number appearing in the lower left entry of $\rho(b)$ (with the notation of Subsection 2.1) at the character of a Dehn surgery. To apply this proposition, we write r_d for a root of the polynomial obtained by specializing the character variety (with coordinates r and Z) to $Z = 2\cos(2\pi/d)$. Write $q_d(r)$ for this polynomial. Note that $(d, 0)$ hyperbolic Dehn surgery points are obtained by this specialization

so that $\mathbf{Q}(r_d, \zeta_d + \zeta_d^{-1}) = k_d$ is the trace field at the $(d,0)$ surgery. We have

$$q_d(r) = r^3 + \left(6 - \zeta_d^2 - \zeta_d^{-2}\right) r^2 + \left(12 - 4\zeta_d^2 - 4\zeta_d^{-2}\right) r - \left(4\left(\zeta_d^2 + \zeta_d^{-2}\right) - 7\right). \tag{3}$$

In this notation r_d is a root of q_d and is an algebraic integer. Of course, if $q_d(r)$ is not irreducible, then r_d is not well-defined. Even when $q_d(r)$ is irreducible, r_d is only defined up to Galois conjugation; however, the ramified residue characteristics will not depend on the choice of Galois conjugate. For irreducibility we have

Lemma 4.4. *Let ζ_d be a primitive dth root of unity for $d \in \mathbf{Z}_{\geq 1}$ odd. The polynomial $q_d(r) \in \mathbf{Q}\left(\zeta_d + \zeta_d^{-1}\right)[r]$ is irreducible.*

We prove this lemma using a result of [3] on real cyclotomic integers. Irreduciblity also allows us to compute the norm of r_d. In particular, if we let k_d be the field generated by r_d and $\zeta_d + \zeta_d^{-1}$ (so that k_d is the trace field of the $(d,0)$ surgery), then the relative field norm $N_{k_d/\mathbf{Q}(\zeta_d+\zeta_d^{-1})}(r_d)$ is just the negative of the constant term of $q_d(r)$, namely $c_d := 4\left(\zeta_d^2 + \zeta_d^{-2}\right) - 7$. So then the absolute field norm of r_d is equal to $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)$. Then to apply Proposition 4.2, we want to find d such that the factorization of $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d) = N_{k_d/\mathbf{Q}}(r_d)$ contains prime divisors congruent to 3 modulo 4 an odd number of times. Such prime divisors imply the existence of a prime above them at which the canonical quaternion algebra is ramified by Proposition 4.2. We summarize this as

Proposition 4.5. *Let $d \geq 3$ be an odd positive integer. Let k_d and A_d be respectively the trace field and the canonical quaternion algebra associated to the $(d,0)$ surgery. Let p be a positive rational prime such that*

1. *$p \equiv 3 \bmod 4$ and*
2. *p divides $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)$ an odd number of times,*

then there is a finite place $\mathfrak{p}$ of k_d lying above p such that A_d is ramified at p.

To apply this to proving Theorem 1.2, we prove that infinitely many rational primes p satisfy the hypotheses of Proposition 4.5. In particular, we prove

Proposition 4.6. *Let U be the set of positive rational primes with*

1. *If $p \in U$, then $p \equiv 3 \bmod 4$,*
2. *If $p \in U$, then p divides $N_{k_d/\mathbf{Q}}(r_d)$ for some $d \in \mathbf{Z}_{\geq 3}$ an odd number of times.*

Then U is infinite.

Then Theorem 1.2 follows by noting that $U \subseteq S$ where U is as in the statement of Proposition 4.6 and S is as in the statement of Theorem 1.2.

5. Proofs of lemmas and propositions

In this section we record the proofs of the lemmas appearing in the proof of Theorem 1.2

5.1. Irreducibility. First we prove Lemma 4.4. The key ingredient is the following result of [3].

Theorem 5.1 ([3, Theorem 1.0.5])**.** *Let $\alpha \in \mathbf{Q}(\zeta)$ be a real algebraic integer in some cyclotomic extension of the rationals. Let $\lceil\alpha\rceil$ denote the largest absolute value of all conjugates of α. If $\lceil\alpha\rceil \leq 2$, then $\lceil\alpha\rceil = 2\cos(\pi/n)$ for some integer n. If $2 \leq \lceil\alpha\rceil < 76/33$, then $\lceil\alpha\rceil$ is one of the following five numbers:*

$$\begin{aligned}
\frac{\sqrt{7}+\sqrt{3}}{2} &= 2.188901059\ldots,\\
\sqrt{5} &= 2.236067977\ldots,\\
1+2\cos(2\pi/7) &= 2.246979602\ldots,\\
\frac{1+\sqrt{5}}{\sqrt{2}} &= 2\cos(\pi/20)+2\cos(9\pi/20) = 2.288245611\ldots,\\
\frac{1+\sqrt{13}}{2} &= 2.302775637\ldots
\end{aligned}$$

To apply this result, it will be easier to work with $p_d(R) \stackrel{\text{def}}{=} q_d(R-2)$, so that

$$\begin{aligned}
p_d(R) &= R^3 - R^2\left(\zeta_d+\zeta_d^{-1}\right)^2 + 2R^2 - 1\\
&= R^3 - \left(\zeta_d^2+\zeta_d^{-2}\right)R^2 - 1.
\end{aligned} \tag{2}$$

The basic idea is to prove that any root of $p_n(R)$ must lie in an interval where there are only finitely many cyclotomic integers.

Lemma 5.3. *Let $a \in [-2,2]$. Then the absolute value of the largest real root of $R^3 - aR^2 - 1$ is less than 2.21.*

Proof. Figure 1 is a graph of the absolute value of the largest real root of $x^3 - ax^2 - 1$ pictured as a function of a for $a \in [-2,2]$.

The right end point is the real root of $R^3 - 2R^2 - 1$ and is approximately 2.20556943040059. □

Remark 5.4. The discontinuity in Figure 1 comes from the fact that the discriminant is zero for $a \approx -1.88988$. For larger values of a there is exactly one real root, and for smaller values there are three real roots.

Now we may prove Lemma 4.4.

Proof of Lemma 4.4. Since $p_n(R)$ is of degree 3, it suffices to show that $p_n(R)$ has no root in $\mathbf{Q}\left(\zeta_n+\zeta_n^{-1}\right)$. Suppose that $p_n(R)$ has a root α. Then after Galois conjugating $p_n(R)$, we may assume it is the largest among its Galois conjugates. That is, $\alpha = \lceil\alpha\rceil$. Indeed, from Figure 1, it is clear that to obtain a root that is largest in complex absolute value among its Galois conjugates, we must choose the largest Galois conjugate of $\zeta_n^2+\zeta_n^{-2}$. This Galois conjugate is the real number $2\cos(4\pi/n)$. By Lemma 5.3 and [3, Theorem 1.0.5], we then

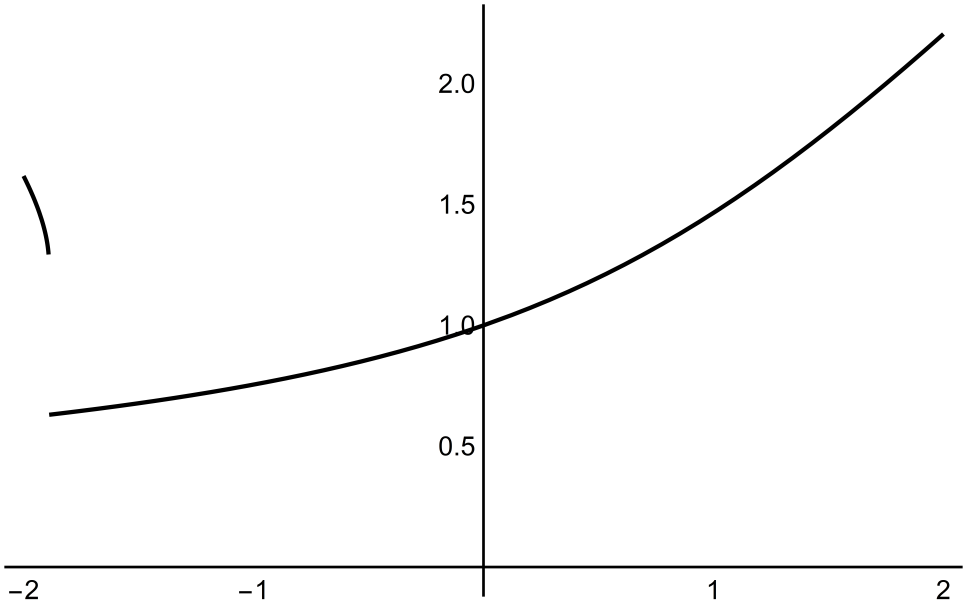

FIGURE 1. The largest real root of $R^3 - aR^2 - 1$ as a function of $a \in [-2, 2]$.

have that $\alpha = \dfrac{\sqrt{7}+\sqrt{3}}{2}$. However, for $n \geq 45$, the largest real root of (the Galois conjugates of) $p_n(R)$ is greater than $\dfrac{\sqrt{7}+\sqrt{3}}{2}$. For $n = 43$, the largest real root is approximately 2.18763964834393, which in particular is smaller than $\dfrac{\sqrt{7}+\sqrt{3}}{2}$.

For $n \leq 41$, we may use a software package to verify that each of those polynomials are irreducible. □

Remark 5.5. We have $p_4(R) = R^3 + 2R^2 - 1 = (R+1)(R^2+R+1)$, and $p_8(R) = R^3 - 1 = (R-1)(R^2+R+1)$, but $p_n(R)$ is in fact irreducible for all other even values of n.

5.2. Ramification. Next we establish the ramification behavior of the canonical quaternion algebra that we will use to produce the infinite set of primes in the statement of Theorem 1.2. We now prove Proposition 4.2.

Proof of Proposition 4.2. To fix notation, let p be a rational prime appearing in the factorization of $N_{k/\mathbf{Q}}(r)$ to an odd power, d. Suppose also that $p \equiv 3 \bmod 4$. Then we know that there are prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_{m'}$ of $\mathcal{O}$ that r belongs to. In fact, for some such prime ideal $\mathfrak{p}_i$, we have that r belongs to $\mathfrak{p}_i^g$ but not $\mathfrak{p}_i^{g+1}$ for some odd integer g. To see this, first write $(r) \subseteq \mathfrak{p}_1^{g_1} \cdots \mathfrak{p}_{m'}^{g_{m'}}$, where each $\mathfrak{p}_i$ lies above p, $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$, and each power g_i is maximal.

Furthermore suppose that every prime ideal lying above p and containing r appears in this factorization. Then we take the ideal norm $\mathfrak{N}\left(\mathfrak{p}_1^{g_1}\cdots\mathfrak{p}_{m'}^{g_{m'}}\right) = p^{g_1 f_1}\cdots p^{g_{m'}f_{m'}} = p^{\sum_{i=1}^{m'} g_i f_i} = p^d$, where f_i is the residue class degree. If each $g_i f_i$ were even, then $\sum_{i=1}^{m'} g_i f_i$ would be an even integer, but d is odd, so there is some i with g_i and f_i both odd. Then, we may assume after scaling r by squares that $r \in \mathfrak{p}\backslash\mathfrak{p}^2$ where $\mathfrak{p}$ has odd residue class degree f.

Now applying Theorem 2.4, we have that

$$\left(\frac{-r^3+4r^2-4r-1,-r}{k_{\mathfrak{p}}}\right)$$

is ramified if and only if $-r^3+4r^2-4r-1$ is not a square modulo $\mathfrak{p}$. Since $r \in \mathfrak{p}$, this is equivalent to asking whether -1 is a square modulo $\mathfrak{p}$. Indeed, -1 is not a square in the finite field $\mathbf{F}_{p^f}$ if and only if $p \equiv 3 \bmod 4$ and f is odd. This can be seen via Jacobi symbols, for example. □

Recall that Lemma 2.6 gives a description of the quaternion algebra over the function field of the canonical component. Specializing r to r_d and taking the ground field to be the trace field of the $(d,0)$ surgery, we obtain

$$\left(\frac{-r_d^3+4r_d^2-4r_d-1,-r_d}{k_d}\right).$$

Moreover, $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)$ is the norm of r_d. So Proposition 4.2 says that the quaternion algebra associated to $(d,0)$ hyperbolic Dehn surgery is ramified at some prime lying above any rational prime divisor of $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d) = N_{k_d/\mathbf{Q}}(r_d)$ that appears to an odd power and is congruent to $3 \bmod 4$. This observation proves Proposition 4.5. Then we are left to prove that we can actually find infinitely many distinct such rational primes as d varies. This is the content of Proposition 4.6, which we now turn to proving.

We wish to understand when $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)$ has a prime divisor p that is congruent to $3 \bmod 4$ and divides $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)$ a strictly odd number of times. In view of Proposition 4.5, this will say that $p \in T$ where T is as in the statement of Theorem 1.2. We will accomplish this by showing that for certain d that $\left|N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)\right| \equiv 3 \bmod 4$. The lemma we now prove basically says that $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)$ is always $1 \bmod 4$.

Lemma 5.6. *Let $d \geq 3$ be an odd positive integer, ζ_d a primitive dth root of unity, and $c_d = 4(\zeta_d^2+\zeta_d^{-2})-7$. Then $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d) \equiv 1 \bmod 4$.*

Proof. Observe that $c_d \equiv 1 \bmod 4$, so the product over the Galois conjugates is also $1 \bmod 4$. □

Then, if we want the *absolute value* of $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)$ to be $3 \bmod 4$, we need the norm itself to be negative. However, determining exactly which d make $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)$ negative turns out to be somewhat difficult.

5.3. The sign of the norm. We start with a lemma that is visibly not about signs, but will later give us some information.

Lemma 5.7. *Let* $\beta = \dfrac{i+\sqrt{15}}{4}$. *Then*

$$\left|\prod_{d|n} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)\right| = \left|2^{n+1}\operatorname{Im}(\beta^n)\right|.$$

Proof. We prove that

$$\left(\prod_{d|n} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)\right)^2 = \left(2^{n+1}\operatorname{Im}(\beta^n)\right)^2.$$

Consider the function $f : \mathbf{Z}_{\geq 1} \to \mathbf{Z}_{\geq 0}$ defined by $f(n)^2 = \operatorname{res}_x(x^n - 1, 4x^4 - 7x^2 + 4)$. It's not completely obvious that $f(n)^2$ is a square integer. For now, however, note that β is a root of $4x^4 - 7x^2 + 4$. The other roots are $-\beta$ and $\pm\overline{\beta}$. By the multiplicative property of the resultant we have

$$\begin{aligned} f(n)^2 &= \operatorname{res}_x(x^n - 1, 4(x-\beta)(x+\beta)(x-\overline{\beta})(x+\overline{\beta})) \\ &= \operatorname{res}_x(x^n - 1, 2(x-\beta)(x+\overline{\beta}) \operatorname{res}_x(x^n - 1, 2(x+\beta)(x-\overline{\beta})). \end{aligned}$$

If we write $g(n) = \operatorname{res}_x\left(x^n - 1, 2(x-\beta)(x+\overline{\beta})\right)$ and $\gamma = 2\beta$, we may compute

$$\begin{aligned} g(n) &= \operatorname{res}_x\left(x^n - 1, 2(x-\beta)(x+\overline{\beta})\right) \\ &= 2^n(\beta^n - 1)(-\overline{\beta}^n - 1) \\ &= 2^n\left(\overline{\beta}^n - \beta^n\right) \\ &= \overline{\gamma}^n - \gamma^n. \end{aligned}$$

Note that since γ is integral over $\mathbf{Z}$ (its minimal polynomial is $x^4 - 7x^2 + 16$), the above calculation shows that $g(n)$ is as well. Moreover, the fixed field of the automorphism $\mathbf{Q}(\beta) \to \mathbf{Q}(\beta)$ determined by $\gamma \mapsto -\overline{\gamma}$ is $\mathbf{Q}(i)$. The easiest way to see this is to note that this automorphism fixes i and takes $\sqrt{15}$ to $-\sqrt{15}$. It follows that $g(n) \in \mathbf{Z}[i]$. We can also calculate that

$$g(n) = 2^n\left(\overline{\beta}^n - \beta^n\right) = -2^{n+1}\operatorname{Im}(\beta^n)i.$$

It then follows that $2^{n+1}\operatorname{Im}(\beta^n) \in \mathbf{Z}$. On the hand, we can compute that the other factor of the original resultant (that is, of $f(n)^2$) is

$$\operatorname{res}_x\left(x^n - 1, 2(x+\beta)(x-\overline{\beta})\right) = 2^n(-\beta^n - 1)(\overline{\beta}^n - 1) = 2^{n+1}\operatorname{Im}(\beta^n)i.$$

It follows that $f(n)^2 = 4^{n+1}\operatorname{Im}(\beta^n)^2 = \left(2^{n+1}\operatorname{Im}(\beta^n)\right)^2$. Since $2^{n+1}\operatorname{Im}(\beta^n) \in \mathbf{Z}$, $f(n)^2$ is in fact a positive square integer, and its positive square root is given by $\pm 2^{n+1}\operatorname{Im}(\beta^n)$.

Writing $\Phi_d(x)$ for the dth cyclotomic polynomial, we have that $x^n - 1 = \prod_{d|n}\Phi_d(x)$, so

$$\begin{aligned}\operatorname{res}_x\left(x^n - 1, 4x^4 - 7x^2 + 4\right) &= \prod_{d|n}\operatorname{res}_x\left(\Phi_d(x), 4x^4 - 7x^2 + 4\right)\\ &= \prod_{d|n} N_{\mathbf{Q}(\zeta_d)/\mathbf{Q}}\left(4\zeta_d^4 - 7\zeta_d^2 + 4\right)\end{aligned}$$

Now consider c_d first as an element of $\mathbf{Q}(\zeta_d)$. However note that $\zeta_d^2 c_d = 4\zeta_d^4 - 7\zeta_d^2 + 4$, and $N_{\mathbf{Q}(\zeta_d)/\mathbf{Q}}(\zeta_d) = 1$, so $N_{\mathbf{Q}(\zeta_d)/\mathbf{Q}}(c_d) = N_{\mathbf{Q}(\zeta_d)/\mathbf{Q}}\left(4\zeta_d^4 - 7\zeta_d^2 + 4\right)$. But $N_{\mathbf{Q}(\zeta_d)/\mathbf{Q}}(c_d) = \left(N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)\right)^2$, since $\mathbf{Q}(\zeta_d)$ is a quadratic extension of $\mathbf{Q}(\zeta_d + \zeta_d^{-1})$. We summarize this as

$$\operatorname{res}_x\left(x^n - 1, 4x^4 - 7x^2 + 4\right) = \left(\prod_{d|n} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)\right)^2,$$

so

$$f(n)^2 = \left(\prod_{d|n} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)\right)^2.$$

□

Next we determine the residue class of $2^{n+1}\operatorname{Im}(\beta^n)$ for odd n.

Lemma 5.8. *For all $n \in \mathbf{Z}_{\geq 1}$ odd, we have*

$$2^{n+1}\operatorname{Im}(\beta^n) \equiv \begin{cases} 1 \bmod 4 & \text{if } n \equiv 1 \bmod 4 \\ 3 \bmod 4 & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

Proof. As in the proof of Lemma 5.7, if we write $\gamma = 2\beta$, then γ is an algebraic integer, and $2^{n+1}\operatorname{Im}(\beta^n)i = \gamma^n - \overline{\gamma}^n$. Then, we have $i\left(\overline{\gamma}^n - \gamma^n\right) = 2^{n+1}\operatorname{Im}(\beta^n)$. We may compute that

$$i\left(\overline{\gamma}^n - \gamma^n\right) \equiv \begin{cases} 1 \bmod 4 & \text{if } n \equiv 1 \bmod 4 \\ 3 \bmod 4 & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

It's worth pointing out that this reduction is $\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/4\mathcal{O}_K$ where $\mathcal{O}_K$ is the ring of integers of the field $K = \mathbf{Q}(\gamma)$. □

Combining Lemmas 5.7, 5.8, and 5.6 gives

Lemma 5.9. *Let $n \geq 5$ be a positive integer such that $n \equiv 1 \bmod 4$ and $\beta = \frac{\sqrt{15}+i}{4}$. Then*

$$\prod_{d|n} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d) = 2^{n+1}\,\mathrm{Im}\,(\beta^n)\,. \tag{10}$$

Proof. By Lemma 5.7, we have an equality of absolute values. So we just have to check that the signs are equal. It suffices to check that they are both congruent to 1 modulo 4. Indeed, each $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d) \equiv 1 \bmod 4$ by Lemma 5.6, and when $n \equiv 1 \bmod 4$, so is $2^{n+1}\,\mathrm{Im}(\beta^n)$ by Lemma 5.8. □

We are left to compute the sign of $\mathrm{Im}(\beta^n)$ for integers n. Since β is on the unit circle in the complex plane, we may write $\beta = e^{2\pi i x}$ so that $\beta^n = e^{2\pi i n x}$. Then $\mathrm{Im}(\beta^n) < 0$ if and only if $\frac{nx}{2\pi}$ is greater than $1/2 \bmod 1$. The following result of Furstenberg allows us to easily prove the existence of such n. Before stating it, we recall that a multiplicative semigroup of the integers is called **lacunary** if it consists of powers of a single integer and **non-lacunary** otherwise.

Theorem 5.11 ([9, Theorem IV.1])**.** *If Σ is a non-lacunary semigroup of integers and α is irrational, then $\Sigma\alpha$ is dense modulo* 1.

We remark that the non-lacunary semigroups we consider are those of the form

$$\{l_1^{r_1} l_2^{r_2} \cdots l_m^{r_m} \,|\, l_i \text{ prime}, l_i \equiv 1 \bmod 4\}$$

with $m \geq 2$.

5.4. Proof of Proposition 4.6. Let us briefly say where we are going. Recall our notation from Section 4 that r_d is the coordinate appearing in the Hilbert symbol for the $(d, 0)$ hyperbolic Dehn surgery. Proposition 4.5 reduced the ramification of the quaternion algebra to finding rational prime divisors on the norm of r_d, and it is technically simpler to work with $c_d = 4(\zeta_d^2 + \zeta_d^{-2}) - 7$, which has the property that $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d) = N_{k_d/\mathbf{Q}}(r_d)$. Using Furstenberg's Theorem 5.11, we wish to construct a sequence (d_i) such that the set of residue characteristics of ramified places of the $(d_i, 0)$ surgeries form an infinite set. In view of Proposition 4.5, this amounts to finding infinitely many distinct rational prime divisors of $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d) = N_{k_d/\mathbf{Q}}(r_d)$ which are equivalent to $3 \bmod 4$ and appear to an odd power in the prime factorization of the norm. Such a sequence will be constructed in Lemma 5.17.

Our first goal is to prove

Lemma 5.12. *Let p be a rational prime. Then, p divides $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d) = N_{k_d/\mathbf{Q}}(r_d)$ for only finitely many values of d coprime to p.*

Let us recall a fact from basic number theory. See, e.g., [14, Proposition 1.10.3].

Proposition 5.13. *Let p be a rational prime and d an integer such that $p \nmid d$. Let $\mathbf{F}_p(\zeta_d)$ be the field obtained by adjoining a primitive dth root of unity to the finite field with p elements, $\mathbf{F}_p$. Then this extension is cyclic of degree equal to the multiplicative order of $p \bmod d$.*

The next lemma follows from well-known facts, but we include a proof for completeness.

Lemma 5.14. *Let $d \in \mathbf{Z}_{\geq 3}$ be odd and ζ_d a primitive dth root of unity. Then the prime divisors of $N_{\mathbf{Q}(\zeta_d)/\mathbf{Q}}(c_d)$ not dividing d have multiplicative order modulo d equal to 1 or 2.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathbf{Q}(\zeta_d)$ lying above the rational prime p such that $c_d = 4\zeta_d^4 - 7\zeta_d^2 + 4$ belongs to $\mathfrak{p}$. Note that since d is odd, c_d is Galois conjugate in $\mathbf{Q}(\zeta_d)/\mathbf{Q}$ to $4\zeta_d^2 - 7\zeta_d + 4$, so it suffices to show the lemma for this latter algebraic integer. Also suppose that $p \nmid d$. Consider the reduction map $\mathbf{Z}[\zeta_d] \to \mathbf{Z}[\zeta_d]/\mathfrak{p} \cong \mathbf{F}_p(\zeta_d)$. Note that this reduction takes dth roots of unity of $\mathbf{Z}[\zeta_d]$ bijectively onto dth roots of unity of $\mathbf{F}_p(\zeta_d)$ hence primitive dth roots of unity remain primitive. By assumption, $4\zeta_d^2 - 7\zeta_d + 4$ is in the kernel of this map. Henceforth we write ζ_d for the image of $\zeta_d \in \mathbf{Z}(\zeta_d)$ under this reduction map. That is, $4\zeta_d^2 - 7\zeta_d + 4 = 0$ in $\mathbf{F}_p(\zeta_d)$. This implies that $\{1, \zeta_d, \zeta_d^2\}$ is linearly dependent over $\mathbf{F}_p$. Since $\{1, \zeta_d, \zeta_d^2, \dots, \zeta_d^{m-1}\}$ is an $\mathbf{F}_p$-basis for $\mathbf{F}_p(\zeta_d)$ where m is the degree of the extension $\mathbf{F}_p(\zeta_d)/\mathbf{F}_p$, we have that $m \leq 2$. Then by Proposition 5.13, the multiplicative order of $p \bmod d$ is either 1 or 2. □

We may now easily prove Lemma 5.12.

Proof of Lemma 5.12. Any prime divisor $p \in \mathbf{Z}_{\geq 2}$ of $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})}(c_d)$ is either divides d itself or has multiplicative order equal to 1 or 2 modulo d. Any prime p has multiplicative order modulo d equal to 1 or 2 for only finitely many values of d (e.g. take $d > p^2$). We conclude that a given prime p divides $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})}(c_d)$ for finitely many values of d. □

Remark 5.15. The sequence of $(d, 0)$ surgeries we construct have d only divisible by primes congruent to $1 \bmod 4$, but the ramified primes we find are all $-1 \bmod 4$, so there is no issue of finding the same prime infinitely often as a divisor of the surgery coefficients.

Lemma 5.16. *Let Σ be a non-lacunary semigroup of integers of the form*

$$\{l_1^{r_1} l_2^{r_2} \cdots l_m^{r_m} \mid l_i \text{ prime}, l_i \equiv 1 \bmod 4\}.$$

Then there exists a sequence $(n_i)_{i=1}^{\infty}$ of positive integers such that

(1) Each n_i is divisible only by the primes $\{l_j\}$ appearing in Σ,
(2) If $j > i$, $n_i \mid n_j$.
(3) If $i \neq j$, then $n_i \neq n_j$,
(4) If i is even, then $2^{n_i+1} \operatorname{Im}(\beta^{n_i}) > 0$, and
(5) If i is odd, then $2^{n_i+1} \operatorname{Im}(\beta^{n_i}) < 0$.

That the sequence is built out of powers of primes from Σ guarantees that each $n_i \equiv 1 \bmod 4$, and in fact each divisor of n_i must also be congruent to $1 \bmod 4$.

Proof. We construct such a sequence by repeatedly applying Theorem 5.11. Let x_1 be defined by $e^{2\pi i x_1} = \beta$. Note that x_1 is irrational (in fact transcendental by Gelfond-Schneider). Let n_1 be any element of Σ such that $n_1 x_1 > 1/2 \bmod 1$. This implies that $2^{n_1+1} \operatorname{Im}(\beta^{n_1}) < 0$. To construct n_2, set $x_2 = n_1 x_1$ so that $e^{2\pi i x_2} = \beta^{n_1}$. Since x_2 is also irrational, Theorem 5.11 applies to Σx_2 to prove an $m_2 \in \Sigma$ such that $m_2 x_2 < 1/2 \bmod 1$. Set $n_2 = m_2 n_1$. Note that $n_1 \mid n_2$. Proceeding in this manner constructs the desired sequence. □

We now extract a sequence $(d_i)_{i=1}^{\infty}$ where $d_i \mid n_i$ and d_i satisfies the hypotheses of Proposition 4.2.

Lemma 5.17. *There exists a sequence $(d_i)_{i=1}^{\infty}$ of positive integers such that*

(1) If $i \neq j$, then $d_i \neq d_j$.

(2) For each i, $\left|N_{\mathbf{Q}\left(\zeta_{d_i}+\zeta_{d_i}^{-1}\right)/\mathbf{Q}}\left(c_{d_i}\right)\right| \equiv 3 \bmod 4$.

Proof. We use the sequence $(n_i)_{i=1}^{\infty}$ constructed in Lemma 5.16. Let us first construct d_1. We have that

$$2^{n_1+1} \operatorname{Im}\left(\beta^{n_1}\right) = \prod_{d \mid n_1} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}\left(c_d\right),$$

by Lemma 5.9 and the fact that the l_i appearing in the definition of Σ in Lemma 5.16 are all $1 \bmod 4$. Since $\prod_{d \mid n_1} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}\left(c_d\right)$ is negative by construction, we must have that some $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}\left(c_d\right)$ is negative. Since $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}\left(c_d\right) \equiv 1 \bmod 4$, by Lemma 5.6, we have that $\left|N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}\left(c_d\right)\right| \equiv 3 \bmod 4$. Set this d equal to d_1. To construct d_2, we first consider n_2. We have that

$$\prod_{d \mid n_1} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}\left(c_d\right) \Bigg| \prod_{d \mid n_2} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}\left(c_d\right),$$

because $n_1 \mid n_2$. However $\prod_{d \mid n_2} N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}\left(c_d\right)$ is positive, so there must be some d_2 such that $d_2 \nmid n_1$ but $d_2 \mid n_2$ with $N_{\mathbf{Q}\left(\zeta_{d_i}+\zeta_{d_i}^{-1}\right)/\mathbf{Q}}\left(c_{d_i}\right)$ negative. Then, as before, $\left|N_{\mathbf{Q}\left(\zeta_{d_2}+\zeta_{d_2}^{-1}\right)/\mathbf{Q}}\left(c_{d_2}\right)\right| \equiv 3 \bmod 4$. Proceeding in this manner we obtain the sequence. □

Now Proposition 4.6 can be proved easily.

Proof of Proposition 4.6. We consider the sequence $(d_i)_{i=1}^{\infty}$ of Lemma 5.17. For each such d_i, we have $\left|N_{\mathbf{Q}(\zeta_{d_i}+\zeta_{d_i}^{-1})/\mathbf{Q}}(c_{d_i})\right| \equiv 3 \bmod 4$, so there is some prime p with $p \equiv 3 \bmod 4$ that divides $\left|N_{\mathbf{Q}(\zeta_{d_i}+\zeta_{d_i}^{-1})/\mathbf{Q}}(c_{d_i})\right|$ an odd number of times.

By Lemma 5.12, any such prime p divides $\left|N_{\mathbf{Q}(\zeta_{d_i}+\zeta_{d_i}^{-1})/\mathbf{Q}}(c_{d_i})\right|$ for only finitely many i. Since $(d_i)_{i=1}^{\infty}$ is an infinite sequence, we conclude that there must be infinitely many distinct rational primes that are congruent to 3 modulo 4 that divide $\left|N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d)\right|$ an odd number of times where d ranges over the odd positive integers. Recalling that $N_{\mathbf{Q}(\zeta_d+\zeta_d^{-1})/\mathbf{Q}}(c_d) = N_{k_d/\mathbf{Q}}(r_d)$ completes the proof. □

6. Torsion points

Recall from the introduction that E is the elliptic curve defined by $y^2 = x^3 + 2x^2 - 1$. We use the traditional variables x and y for an elliptic curve, and one may specify the birational map from the canonical component which is cut out by $R^3 + (2 - Z^2)R^2 - 1 = 0$ either by the map $C \dashrightarrow E$, $(R, Z) \mapsto (R, RZ)$ or by the coordinate change $R = x, Z = \dfrac{y}{x}$. Theorem 1.3 follows from the following proposition.

Proposition 6.1. *Let E be the elliptic curve defined by the Weierstrass equation $y^2 = x^3 + 2x^2 - 1$. Then, excepting the 2-torsion points, every torsion point of E has x-coordinate equal to an algebraic integer with positive 2-adic valuation.*

We now introduce the relevant topological background material to explain how Proposition 6.1 implies Theorem 1.3. We begin by fixing some notation and recalling results of Hatcher and Hatcher-Thurston.

Theorem 6.2 ([12], [11])**.** *Let K be a hyperbolic two-bridge knot. Then*

(1) $E(K)$ has no closed, embedded, essential surface.
(2) All but finitely many Dehn surgeries are non-Haken and hyperbolic.

As noted in the introduction, the knot 7_4 is a two-bridge knot, so Theorem 6.2 implies that the exterior of the knot has no closed, embedded essential surface and all but finitely many of its surgeries are hyperbolic and non-Haken. Bass's theorem (see [1] or [13, Section 5.2]) implies that if $N = \mathbf{H}^3/\Gamma$ is a hyperbolic surgery on 7_4, then the traces of Γ are algebraic integers. In particular at points corresponding the character of Dehn surgeries, the trace of a meridian (with finitely many exceptions) is an algebraic integer. However, when Z is integral, the relation $R^3 + (2 - Z^2)R^2 - 1 = 0$ implies that R is a unit. Then Proposition 6.1 says that $R = x$ is never a unit when R is the first coordinate of a torsion point on X.

Let us briefly treat the finitely many exceptions. There are 3 boundary slopes: $0/1$, $-8/1$, and $-14/1$ (see [8]). The first is not hyperbolic; the second has integral traces as one can check in Snap; the third does have non-integral traces, so we must check it directly. One may compute that R has negative 2-adic valuation at this point and hence Proposition 6.1 also implies that this point cannot be torsion.

Finally, the 2-torsion points are not covered by 6.1. The 1-torsion is just the point at infinity, and is in particular not in the image of the birational map defined above. The nontrivial 2-torsion consists of three points. The y coordinate of each of them is 0 and the three x-coordinates are the roots of x^3+2x^2-1. All of these roots are real, which implies that the trace field associated to the representation is real, but every finite covolume Kleinian group has nonreal trace field, so no 2-torsion can be a hyperbolic Dehn surgery point.

6.1. Division polynomials for elliptic curves. We now recall some basic facts and fix notation about the division polynomials associated to an elliptic curve. These polynomials will be the main tool in the proof of Proposition 6.1. In this section we use the variables x and y to be consistent with the literature on elliptic curves, but one may convert back to traces on the canonical component with the relations $R = x$ and $Z = \dfrac{y}{x}$.

Definition 6.3. For an elliptic curve E defined by the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, we define the following standard quantities

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= c_4^3/\Delta.
\end{aligned}$$

Remark 6.4. For the curve in Proposition 6.1, we have

$$\begin{aligned}
&a_1 = 0, && b_2 = 8, && c_4 = 64, && \Delta = 80,\\
&a_2 = 2, && b_4 = 0, && c_6 = 352, && j = \frac{16384}{5} = \frac{2^{14}}{5},\\
&a_3 = 0, && b_6 = -4 &&&&\\
&a_4 = 0, && b_8 = -8 &&&&\\
&a_5 = -1. &&&&&&
\end{aligned}$$

Definition 6.5. For an elliptic curve E defined by the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, we define two families of polynomials

$\psi_n(x,y)$ and $f_n(x)$ by

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y + a_1x + a_3,\\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8.\\
\psi_4 &= \psi_2(x,y)\cdot\\
&\quad \left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)\,x + (b_4b_8 - b_6^2)\right),
\end{aligned}$$

and then recursively via

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \tag{6}$$

$$\psi_2\psi_{2m} = \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2. \tag{7}$$

We note that $\psi_n(x,y)$ is a polynomial in x when n is odd, and—using the relation $(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$— $(2y + a_1x + a_3)\psi_n(x,y) = \psi_2(x,y)\psi_n(x,y)$ is a polynomial in x when n is even, so we may further define

$$f_n(x) = \begin{cases} \psi_n(x,y) & n \text{ odd},\\ \psi_2(x,y)\psi_n(x,y) & n \text{ even}. \end{cases}$$

These polynomials are known as the **division polynomials**.

Remark 6.8. The notation and terminology surrounding the division polynomials is not entirely standard in the literature. The definition for ψ_n above is consistent with [18, Exercise 3.7]. The definition of f_n agrees with the GP/PARI ([15]) function `elldivpol` so that $f_n(x)$ is the output of `elldivpol(E,n)`.

Remark 6.9. The roots of $f_n(x)$ are precisely the x-coordinates of the nontrivial n-torsion points.

Proposition 6.10. *Let f_n be as above. Then f_n satisfies the following recursive relations.*

(1) If $n = 2m$, then

$$f_2f_{2m} = f_m\left(f_{m-1}^2f_{m+2} - f_{m-2}f_{m+1}^2\right).$$

(2) If $n \equiv 1 \bmod 4$ and we write $n = 2m+1$, then

$$f_2^2f_{2m+1} = f_{m+2}f_m^3 - f_2^2f_{m-1}f_{m+1}^3.$$

(3) If $n \equiv 3 \bmod 4$, and we write $n = 2m+1$, then

$$f_2^2f_{2m+1} = f_2^2f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3.$$

Proof. These all follow from the recursive formulas for ψ_n, but we include a proof since we were unable to find them in the literature.

We have to treat each residue class modulo 4 separately. So first suppose that $n \equiv 0 \bmod 4$. That is, $n = 2m$ for m an even number. Using Equation 7, we have

$$\begin{aligned}
f_n(x) &= \psi_2\psi_{2m}\\
&= \psi_m(f_{m-1}^2\psi_{m+2} - \psi_{m-2}f_{m+1}^2).
\end{aligned}$$

Note that $f_2 = \psi_2^2$, so

$$\begin{aligned} f_2 f_{2m} &= \psi_2\psi_m(f_{m-1}^2\psi_2\psi_{m+2} - \psi_2\psi_{m-2}f_{m+1}^2) \\ &= f_m(f_{m-1}^2 f_{m+2} - f_{m-2}f_{m+1}^2). \end{aligned}$$

Now say that $n \equiv 2 \bmod 4$ so that $n - 2m$ for m an odd number. Using Equation 7 again, we obtain

$$\begin{aligned} f_n = f_{2m} &= \psi_2\psi_{2m} \\ &= f_m(\psi_{m-1}^2 f_{m+2} - f_{m-2}\psi_{m+1}^2). \end{aligned}$$

Then we find

$$\begin{aligned} f_2 f_{2m} &= \psi_2^2 f_{2m} \\ &= f_m\left((\psi_2\psi_{m-1})^2 f_{m+2} - f_{m-2}(\psi_2\psi_{m+1})^2\right) \\ &= f_m\left(f_{m-1}^2 f_{m+2} - f_{m-2}f_{m+1}^2\right). \end{aligned}$$

Next we let $n \equiv 1 \bmod 4$, so $n = 2m + 1$ for m even. Using Equation 6 gives

$$\begin{aligned} f_2^2 f_n &= \psi_2^4 f_{2m+1} \\ &= (\psi_2\psi_{m+2})(\psi_2\psi_m)^3 - f_2^2 f_{m-1}f_{m+1}^3 \\ &= f_{m+2}f_m^3 - f_2^2 f_{m-1}f_{m+1}^3. \end{aligned}$$

Finally, we treat $n \equiv 3 \mod 4$. That is, $n = 2m + 1$ for m odd. Again using Equation 6 yields

$$f_{2m+1} = f_{m+2}f_m^3 - \psi_{m-1}\psi_{m+1}^3,$$

so we have

$$\begin{aligned} f_2^2 f_{2m+1} &= \psi_2^4 f_{2m+1} \\ &= f_2^2 f_{m+2}f_m^3 - (\psi_2\psi_{m-1})(\psi_2\psi_{m+1})^3 \\ &= f_2^2 f_{m+1}f_m^3 - f_{m-1}f_{m+1}^3. \end{aligned}$$

□

6.2. Proof of Proposition 6.1. Let us now specialize to the case where E is the elliptic curve defined by the Weierstrass equation $y^2 = x^3 + 2x^2 - 1$. For reference we list the first four division polynomials for this particular elliptic curve.

$$\begin{aligned} f_1(x) &= 1, \\ f_2(x) &= 4x^3 + 8x^2 - 4, \\ f_3(x) &= 3x^4 + 8x^3 - 12x - 8, \\ f_4(x) &= 8x^9 + 48x^8 + 64x^7 - 168x^6 - 672x^5 - 896x^4 \\ &\quad - 416x^3 + 192x^2 + 256x + 64. \end{aligned}$$

Lemma 6.11. *If $2 \mid n$, then $f_2 \mid f_n$.*

Proof. Note that $f_2(x) = 4(x+1)(x^2+x-1)$ and that $x+1$ and x^2+x-1 have roots equal to the x-coordinates of the nontrivial 2-torsion. Since $E[2] \subseteq E[n]$ whenever $2 \mid n$, we have that $(x+1)(x^2+x-1) \mid f_n$, so it suffices to show that $4 \mid f_n$. Let us write $n = 2m$ and induct on m. The case of $m = 1$ is trivial, and we use the recursive formula

$$f_2 f_{2m} = f_m \left(f_{m-1}^2 f_{m+2} - f_{m-2} f_{m+1}^2 \right)$$

for the inductive step. Since $4 \mid f_2$, but $8 \nmid f_2$, it suffices to show that $16 \mid f_m \left(f_{m-1}^2 f_{m+2} - f_{m-2} f_{m+1}^2 \right)$. First suppose that m is even, so that $m, m+2$, and $m-2$ are all even. Then inductively, $4 \mid f_m, f_{m+2}, f_{m-2}$, which implies the result. Now if m is odd, $m+1$ and $m-1$ are even, so 16 divides both $f_{m=1}^2$ and f_{m+1}^2. □

The main technical proposition is as follows.

Proposition 6.12. *Let f_n be as above.*

(1)

$$\deg(f_n) = \begin{cases} n^2/2 + 1 & n \text{ even}, \\ (n^2-1)/2 & n \text{ odd}. \end{cases}$$

(2) The leading coefficient of $f_n(x)$ is $2n$ when n is even and n when n is odd.

(3) If n is odd, then $f_n(x) \equiv \pm x^{\frac{n^2-1}{2}} \bmod 4$.

(4) Let n be even and k equal to the 2-adic valuation of n. Then $2^{k+1} \mid f_n(x)$ in $\mathbf{Z}[x]$, and $\frac{1}{2^{k+1}} f_n(x) \equiv (x+1)(x^2+x+1)(x^{n^2/2-2}) \bmod 2$.

Before embarking on the proof, let us point out that Proposition 6.12 (3) and 6.12 (4) imply that, excepting the factors coming from the 1 and 2-torsion, the constant term of every irreducible factor of $f_n(x)$ has a factor of 2, even after dividing out by the leading coefficient of $f_n(x)$. This is equivalent to the root of these irreducible factors having positive 2-adic valuation. Proposition 6.1 and hence Theorem 1.3 then follow.

Proof of Proposition 6.12. We prove all parts by induction on n. The base cases are easy to check, so assume each statement is true for all indices less than or equal to $n-1$.

We first prove Proposition 6.12 (1). First suppose that n is even and write $n = 2m$. We then have

$$f_2 f_{2m} = f_m \left(f_{m-1}^2 f_{m+2} - f_{m-2} f_{m+1}^2 \right).$$

Here we have to break into further cases where m is even or odd. Let us treat m even first. Then our inductive hypothesis implies that $\deg(f_m) = m^2/2 + 1$, $\deg(f_{m+2}) = (m+2)^2/2 + 1$, and $\deg(f_{m-2}) = (m-2)^2/2 + 1$. Moreover, $m \pm 1$ is odd, so $\deg(f_{m+1}^2) = m^2 + 2m$ and $\deg(f_{m-1}^2) = m^2 - 2m$. Hence, $\deg(f_{m-1}^2 f_{m+2}) = \deg(f_{m-2} f_{m+1}^2) = \dfrac{3m^2+6}{2}$. Our inductive hypothesis (in particular Proposition 6.12 (2)) implies that the leading coefficient of $f_{m-1}^2 f_{m+2}$

is equal to $2(m+2)(m-1)^2 = 2m^3 - 6m + 4$ whereas the leading coefficient of $f_{m-2}f_{m+1}^2$ is $2(m-2)(m+1)^2 = 2m^3 - 6m - 4$, so coefficient of $x^{\frac{3m^2+6}{2}}$ in $f_{m-1}^2 f_{m+2} - f_{m-2}f_{m+1}^2$ is 8. In particular it's nonzero so that $\deg(f_{m-1}^2 f_{m+2} - f_{m-2}f_{m+1}^2) = \dfrac{3m^2+6}{2}$. It follows that $\deg(f_2 f_{2m}) = m^2/2 + 1 + \dfrac{3m^2+6}{2} = 2m^2 + 4$. Noting that $\deg(f_2) = 3$ gives that $\deg(f_{2m}) = \deg(f_n) = 2m^2 + 1 = n^2/2 + 1$.

Now suppose that m is odd. We still have the same recursive relation because n is even. However since m is odd, we now have $\deg(f_m) = (m^2 - 1)/2$, $\deg(f_{m-1}^2) = m^2 - 2m + 3$, $\deg(f_{m+2}) = (m^2 + 4m + 3)/2$, so then $\deg(f_{m-1}^2 f_{m+2}) = \frac{3}{2}(m^2 + 3)$. Similarly, $\deg(f_{m-2}) = (m^2 - 4m + 3)/2$ and $\deg(f_{m+1}^2) = m^2 + 2m + 3$ together imply $\deg(f_{m-2}f_{m+1}^2) = \frac{3}{2}(m^2 + 3)$ as well. As before, one can compute using Proposition 6.12 (2) of the inductive hypothesis that the coefficient of $x^{\frac{3}{2}(m^2+3)}$ is nonzero (in fact equal to 16), so $\deg(f_{m-1}^2 f_{m+2} - f_{m-2}f_{m+1}^2) = \frac{3}{2}(m^2+3)$. Then we have $\deg(f_2 f_{2m}) = 2m^2+4$, so $\deg(f_{2m}) = \deg(f_n) = 2m^2 + 1 = n^2/2 + 1$.

To handle the case of n odd, we have to separately consider when n is congruent to 1 or 3 modulo 4. If we write $n = 2m+1$, these two cases are equivalent to m even and odd, respectively. Let us treat $n \equiv 1 \bmod 4$ first. The recursive relation is

$$f_2^2 f_{2m+1} = f_{m+2}f_m^3 - f_2^2 f_{m-1}f_{m+1}^3.$$

Here m is even, so $\deg(f_{m+2}) = (m^2 + 4m + 6)/2$, and $\deg(f_m^3) = (3m^2 + 6)/2$. Combining these gives $\deg(f_{m+2}f_m^3) = 2(m^2+m+3)$. Similar calculations give $\deg(f_2^2 f_{m-1}f_{m+1}^3) = 2(m^2+m+3)$. Again the leading coefficients do not cancel, so $f_{m+2}f_m^3 - f_2^2 f_{m-1}f_{m+1}^3$ has degree $2(m^2 + m + 3)$ with leading coefficient $32m + 16$. It follows that $\deg(f_{2m+1}) = 2(m^2 + m)$, so $\deg(f_n) = (n^2 - 1)/2$.

The last case is $n \equiv 3 \bmod 4$. That is, $n = 2m + 1$ for m odd. We have the relation

$$f_2^2 f_{2m+1} = f_2^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3.$$

In this case,

$$\deg(f_2^2) = 6, \quad \deg(f_{m+2}) = \frac{(m+2)^2 - 1}{2}, \quad \deg(f_m^3) = 3\left(\frac{m^2-1}{2}\right).$$

These imply

$$\deg(f_2^2 f_{m+2}f_m^3) = 2(m^2 + m + 3).$$

Similarly, it follows from

$$\deg(f_{m-1}) = \frac{m^2 - 2m + 3}{2} \quad \text{and} \quad \deg(f_{m+1}^3) = \frac{3m^2 + 6m + 9}{2}$$

that $\deg(f_{m-1}f_{m+1}^3) = 2(m^2 + m + 3)$. Similar to earlier cases, we then have that $f_2^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3$ is of degree $2(m^2 + m + 3)$ with leading coefficient

$32m + 16$. Then, as in the $n \equiv 1 \bmod 4$ case, we have $\deg(f_n) = \deg(f_n) = (n^2-1)/2$, which completes the proof of Proposition 6.12 (1).

We now prove Proposition 6.12 (2). For a polynomial g, let us write $\mathrm{LC}(g)$ for its leading coefficient. We have actually done the relevant calculations in the proof of Proposition 6.12 (1). When $n \equiv 0 \bmod 4$, so $n = 2m$ with m even, we have that $\mathrm{LC}\left(f_{m-1}^2 f_{m+2} - f_{m-2} f_{m+1}^2\right) = 8$ so that $\mathrm{LC}(f_2 f_{2m}) = 8\,\mathrm{LC}(f_m) = 16m$. Hence, $\mathrm{LC}(f_{2m}) = \mathrm{LC}(f_n) = 4m = 2n$. Similarly when $n = 2m$ for m odd, we have $\mathrm{LC}\left(f_{m-1}^2 f_{m+2} - f_{m-2} f_{m+1}^2\right) = 16$, so $\mathrm{LC}(f_2 f_{2m}) = 16\,\mathrm{LC}(f_m) = 16m$. For n odd, we have that $\mathrm{LC}(f_2^2 f_{2m+1}) = 16(2m+1)$ so that $\mathrm{LC}(f_{2m+1}) = 2m+1$.

For Proposition 6.12 (3), we first treat the case where $n \equiv 1 \bmod 4$, so we may write $n = 2m+1$ for m even. We note that the relation

$$f_2^2 f_{2m+1} = f_{m+2} f_m^3 - f_2^2 f_{m-1} f_{m+1}^3$$

implies that $f_2^2 \mid f_{m+2} f_m^3$. In fact, Lemma 6.11 implies that f_2 divides both f_{m+2} and f_m so that $f_2^4 \mid f_{m+2} f_m^3$, which in particular implies that $\dfrac{f_{m+2} f_m}{f_2^2} \equiv 0 \bmod 4$ as it has a factor of f_2^2, which is divisible by 4. It follows that $f_{2m+1} \equiv -f_{m-1} f_{m+1}^3 \bmod 4$. By the inductive hypothesis, $f_{m-1} \equiv \pm x^{(m^2-2m)/2} \bmod 4$ and $f_{m+1} \equiv \pm x^{(m^2+2m)/2} \bmod 4$, so $f_{2m+1} \equiv \pm x^{(2m^2+2m)} \bmod 4$. That is, $f_n \equiv \pm x^{(n^2-1)/2} \bmod 4$. The case of $n \equiv 3 \bmod 4$ may be handled similarly, completing the proof of Proposition 6.12 (3).

To begin the proof of Proposition 6.12 (4), let us fix the notation that when n is even, $f_n = f_2 g_n$, and when n is odd $f_n = g_n$. We break into cases based on the 2-adic valuation of n. Let $k = v_2(n)$ be first equal to 1, so we may write $n = 2m$ for m odd. In this case $m \pm 1$ are is even, so we have

$$f_2 f_{2m} = f_m (f_2^2 g_{m-1}^2 f_{m+2} - f_{m-2} f_2^2 g_{m+1}^2),$$

which implies

$$f_{2m} = f_m (f_2 g_{m-1}^2 f_{m+2} - f_{m-2} f_2 g_{m+1}^2).$$

Now since m is odd, exactly one of $m+1$ and $m-1$ is divisible by 4. Say $m-1 \equiv 0 \bmod 4$ (the other case is follows analogously). Then $f_{m-1}/4 = f_2 g_{m-1}/4$ is divisible by 2 by inductive hypothesis. Then we have that

$$\begin{aligned} \frac{f_{2m}}{4} &= f_m \left(\frac{f_2}{4} g_{m-1}^2 f_{m+2} - f_{m-2} \frac{f_2}{4} g_{m+1}^2 \right) \\ &\equiv (x+1)(x^2+x+1) f_m f_{m-2} g_{m+1}^2 \bmod 2. \end{aligned} \tag{13}$$

Now, since $g_{m+1} f_2 = f_{m+1}$, the inductive hypothesis says

$$\frac{f_{m+1}}{4} \equiv (x+1)(x^2+x+1) x^{(m+1)^2/2-2} \bmod 2,$$

so the fact that $f_2/4 \equiv (x+1)(x^2+x+1) \bmod 2$ implies $g_{m+1} \equiv x^{(m+1)^2/2-2} \bmod 2$. So then since f_m and f_{m-2} both have odd indices, we may apply Proposition

6.12 (3) to Equation 13 to obtain

$$\begin{aligned}\frac{f_{2m}}{4} &\equiv (x+1)(x^2+x+1)x^{(m^2-1)/2}x^{((m-2)^2-1)/2}x^{(m+1)^2-4} \bmod 2\\ &\equiv (x+1)(x^2+x+1)x^{2m^2-2}\\ &\equiv (x+1)(x^2+x+1)x^{n^2/2-2},\end{aligned}$$

which handles the case of $k=1$.

Next, suppose that $k=2$. We again write $n=2m$ and here have m even with $v_2(m)=1$. Note that one of $m+2$ and $m-2$ will have 2-adic valuation equal to 2, and the other will have 2-adic valuation at least 3. Both possibilities lead to the same argument, so assume $v_2(m-2)\geq 3$ and hence $v_2(m+2)=2$. Then we write $f_{m+2}=4(x+1)(x^2+x-1)g_{m-2}$. Then our inductive hypothesis implies

$$\frac{f_{m+2}}{8} \equiv (x+1)(x^2+x+1)x^{(m+2)^2/2-2} \bmod 2.$$

So we have $g_{m+2}/2 \equiv x^{(m+2)^2/2-2} \bmod 2$. The inductive hypothesis also implies that $16 \mid f_{m-2}$, and $f_{m-2}=4(x+1)(x^2+x-1)g_{m-2}$, so $4 \mid g_{m-2}$. Hence, $g_{m-2}/2 \equiv 0 \bmod 2$. Note that since $v_2(m)=1$ and $m-1$ is odd we have $f_m/4 \equiv (x+1)(x^2+x+1)x^{m^2/2-2} \bmod 2$ and $f_{m-1}^2 \equiv x^{m^2-2m} \bmod 2$. Combining all this we obtain

$$\begin{aligned}\frac{f_{2m}}{8} &= \frac{f_m}{4}\left(f_{m-1}^2\frac{g_{m+2}}{2}-\frac{g_{m-2}}{2}f_{m+1}^2\right)\\ &\equiv (x+1)(x^2+x+1)x^{2m^2-2}\\ &\equiv (x+1)(x^2+x+1)x^{n^2/2-2}.\end{aligned}$$

The last case to consider is $k\geq 3$. As always, write $n=2m$. Keeping the notation of the previous parts, we write our recursive relation as

$$\frac{f_{2m}}{2^{k+1}} = \frac{f_2 g_m}{2^k}\left(\frac{f_{m-1}^2 g_{m+2}-g_{m-2}f_{m+1}^2}{2}\right).$$

The leading coefficient of $f_{m-1}^2 f_{m+2}-f_{m-2}f_{m+1}^2$ is 8 by Proposition 6.12 (1) and Proposition 6.12 (2). This implies that the leading coefficient of $f_{m-1}^2 g_{m+2}-g_{m-2}f_{m+1}^2=(f_{m-1}^2 f_{m+2}-f_{m+2}f_{m+1}^2)/f_2$ is 2. Then,

$$\frac{f_{m-1}^2 g_{m+2}-g_{m-2}f_{m+1}^2}{2} \tag{14}$$

is monic, and the degree can be checked to be correct using the inductive hypothesis. Then, it suffices to show that every monomial term in Equation 14 other than the leading one is divisible by 2. That is, we want to show that every monomial term besides the leading term in $f_{m-1}^2 g_{m+2}-g_{m-2}f_{m+1}^2$ is divisible by 4. Since $m\pm 1$ is odd, we have that every term other than the leading terms

in $f_{m\pm1}$ are divisible by 4 by Proposition 6.12 (3), so we just need to show it for $g_{m\pm2}$. Note that when m is even,

$$g_{2m} = g_m(f_{m-1}^2 g_{m+2} - g_{m-2} f_{m+1}^2),$$

so one may see that g_{2m} only has its leading term not divisible by 4 inductively. □

Remark 6.15 (Affine Intersection Points). Chu showed in [5, Section 5.1] that there are four affine points on the canonical component, C, for 7_4 which intersect the other component of the character variety containing the character of an irreducible representation. They lie in a number field L of degree 4. These intersection points detect Seifert surfaces and so are also of geometric interest. The image of each of these points under the birational map $C \dashrightarrow E$ has x-coordinate equal to $1 \pm i$; in particular they have positive a 2-adic valuation. However they are still infinite order. One may compute with Magma ([2]) or other software that the torsion subgroup of $E(L)$ is isomorphic to $\mathbf{Z}/6\mathbf{Z}$, but none of these four points has order less that or equal to 6.

References

[1] BASS, HYMAN. Finitely generated subgroups of GL_2. *The Smith conjecture* (New York, 1979), 127–136, Pure Appl. Math., 112. *Academic Press, Orlando, FL,* 1984. MR0758465, Zbl 0599.57003, doi: 10.1016/S0079-8169(08)61638-4. 1514

[2] BOSMA, WIEB; CANNON, JOHN; PLAYOUST, CATHERINE. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.* **24** (1997), no. 3–4, 235–265. MR1484478, Zbl 0898.68039, doi: 10.1006/jsco.1996.0125. 1522

[3] CELEGARI, FRANK; MORRISON, SCOTT; SNYDER, NOAH. Cyclotomic integers, fusion categories, and subfactors. *Comm. Math. Phys.* **303** (2011), no. 3, 845–896. MR2786219, Zbl 1220.18004, arXiv:1004.0665, doi: 10.1007/s00220-010-1136-2. 1505, 1506

[4] CHINBURG, TED; REID, ALAN W.; STOVER, MATTHEW. Azumaya algebras and canonical components. Preprint, 2020. To appear in *Int. Math. Res. Not. IMRN.* arXiv:1706.00952, doi: 10.1093/imrn/rnaa209. 1494, 1495, 1498, 1500, 1501, 1502, 1503

[5] CHU, MICHELLE. Detecting essential surfaces as intersections in the character variety. *Algebr. Geom. Topol.* **17** (2017), no. 5, 2893–2914. MR3704247, Zbl 1376.57005, arXiv:1609.04780, doi: 10.2140/agt.2017.17.2893. 1494, 1497, 1522

[6] CULLER, MARC; SHALEN, PETER B. Varieties of group representations and splittings of 3-manifolds. *Ann. of Math.* (2) **117** (1983), no. 1, 109–146. MR683804, Zbl 0529.57005, doi: 10.2307/2006973. 1496, 1497

[7] DARMON, HENRI; ZHANG, SHOU-WU; DIRS. Heegner points and Rankin L-series. Papers from the Workshop on Special Values of Rankin L-Series held in Berkeley, CA, December 2001. Math. Sci. Res. Publ., 49. *Cambridge University Press, Cambridge*, 2004. xiv+367 pp. ISBN: 0-521-83659-X. MR2083206, Zbl 1051.11004, doi: 10.1017/CBO9780511756375. 1495

[8] DUNFIELD, NATHAN M. A table of boundary slopes of Montesinos knots. *Topology* **40** (2001), no. 2, 309–315. MR1808223, Zbl 0967.57014, arXiv:math/9901120, doi: 10.1016/S0040-9383(99)00064-6. 1514

[9] FURSTENBERG, HARRY. Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation. *Math. Systems Theory* **1** (1967), 1–49. MR213508, Zbl 0146.28502, doi: 10.1007/BF01692494. 1511

[10] HARARI, DAVID. Méthode des fibrations et obstruction de Manin. *Duke Math. J.* **75** (1994), no. 1, 221–260. MR1284820, Zbl 0847.14001, doi: 10.1215/S0012-7094-94-07507-8. 1495

[11] HATCHER, ALLEN E. On the boundary curves of incompressible surfaces. *Pacific J. Math.* **99** (1982), no. 2, 373–377. MR658066, Zbl 0502.57005, doi: 10.2140/pjm.1982.99.373. 1514

[12] HATCHER, ALLEN E.; THURSTON, WILLIAM P. Incompressible surfaces in 2-bridge knot complements. *Invent. Math.* **79** (1985), no. 2, 225–246. MR778125, Zbl 0602.57002, doi: 10.1007/BF01388971. 1514

[13] MACLACHLAN, COLIN; REID, ALAN W. The arithmetic of hyperbolic 3-manifolds. Graduate Texts in Mathematics, 219. *Springer-Verlag, New York*, 2003. xiv+463 pp. ISBN: 0-387-98386-4. MR1937957, Zbl 1025.57001, doi: 10.1007/978-1-4757-6720-9. 1497, 1498, 1499, 1514

[14] NEUKIRCH, JÜRGEN. Algebraic number theory. Grundlehren der Mathematischen Wissenschaften, 322. *Springer-Verlag, Berlin*, 1999. xviii+571 pp. ISBN: 3-540-65399-6. MR1697859, Zbl 0956.11021, doi: 10.1007/978-3-662-03983-0. 1511

[15] The PARI Group. *PARI/GP version* `2.11.2`. Univ. Bordeaux, 2019. `http://pari.math.u-bordeaux.fr/`. 1516

[16] POONEN, BJORN. Rational points on varieties. Graduate Studies in Mathematics, 186. *American Mathematical Society, Providence, RI*, 2017. xv+337 pp. ISBN: 978-1-4704-3773-2. MR3729254, Zbl 1387.14004, doi: 10.1090/gsm/186. 1501

[17] ROLFSEN, DALE. Knots and links. Mathematics Lecture Series, 7. *Publish or Perish, Inc., Berkeley, Calif.*, 1976. ix+439 pp. MR0515288, Zbl 0339.55004. 1494

[18] SILVERMAN, JOSEPH H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. *Springer, Dordrecht*, 2009. xx+513 pp. ISBN: 978-0-387-09493-9. MR2514094, Zbl 1194.11005, doi: 10.1007/978-0-387-09494-6. 1516

(Nicholas Rouse) DEPARTMENT OF MATHEMATICS, RICE UNIVERSITY, HOUSTON, TX 77005, USA

`nicholas.rouse@rice.edu`

This paper is available via `http://nyjm.albany.edu/j/2021/27-58.html`.