American Mathematical Society

CURRENT EVENTS BULLETIN

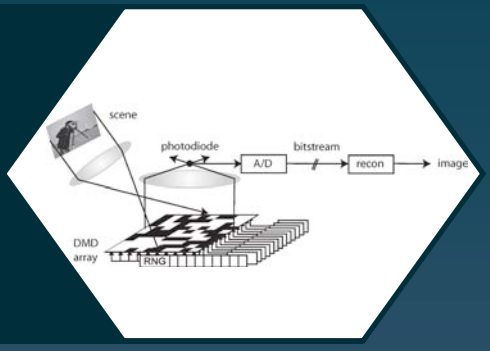
Wednesday, January 7, 2009, 1:00 PM to 5:00 PM
Joint Mathematics Meetings, Washington DC

Organized by David Eisenbud, University of California, Berkeley

1:00 PM

Matthew James Emerton

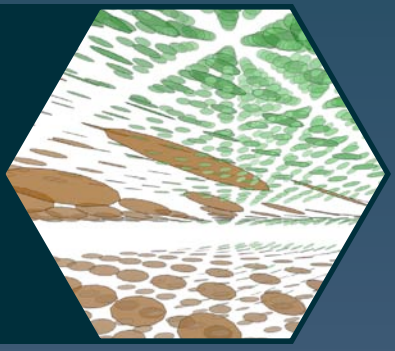
Topology, representation theory and arithmetic: Three-manifolds and the Langlands program



2:00 PM

Olga Holtz

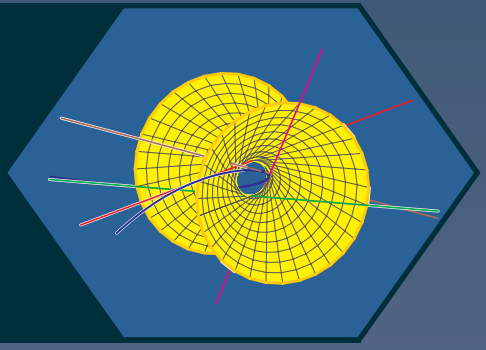
Compressive sensing: A paradigm shift in signal processing



3:00 PM

Michael Hutchings

From Seiberg-Witten theory to closed orbits of vector fields: Taubes's proof of the Weinstein conjecture



4:00 PM

Frank Sottile

Frontiers of reality in Schubert calculus

Introduction to the Current Events Bulletin

Will the Riemann Hypothesis be proved this week? What is the Geometric Langlands Conjecture about? How could you best exploit a stream of data flowing by too fast to capture? I love the idea of having an expert explain such things to me in a brief, accessible way. I think we mathematicians are provoked to ask such questions by our sense that underneath the vastness of mathematics is a fundamental unity allowing us to look into many different corners -- though we couldn't possibly work in all of them. And I, like most of us, love common-room gossip.

The Current Events Bulletin Session at the Joint Mathematics Meetings, begun in 2003, is an event where the speakers do not report on their own work, but survey some of the most interesting current developments in mathematics, pure and applied. The wonderful tradition of the Bourbaki Seminar is an inspiration, but we aim for more accessible treatments and a wider range of subjects. I've been the organizer of these sessions since they started, but a broadly constituted advisory committee helps select the topics and speakers. Excellence in exposition is a prime consideration.

A written exposition greatly increases the number of people who can enjoy the product of the sessions, so speakers are asked to do the hard work of producing such articles. These are made into a booklet distributed at the meeting. Speakers are then invited to submit papers based on them to the *Bulletin of the AMS*, and this has led to many fine publications.

I hope you'll enjoy the papers produced from these sessions, but there's nothing like being at the talks -- don't miss them!

David Eisenbud, Organizer
University of California, Berkeley
de@msri.org

For PDF files of talks given in prior years, see
http://www.ams.org/ams/current-events-bulletin.html.
The list of speakers/titles from prior years may be found at the end of this booklet.

TOPOLOGY, REPRESENTATION THEORY, AND ARITHMETIC: THREE-MANIFOLDS AND THE LANGLANDS PROGRAM

MATTHEW EMERTON

Abstract. Using ideas from the Langlands program, F. Calegari and N. Dunfield have constructed a tower of finite covers whose members are closed hyperbolic rational homology 3-spheres, and whose injectivity radii grow without bound. The goal of this note is to sketch some of the ideas of the Langlands program, and to explain how they can be brought to bear on the study of hyperbolic 3-manifolds, and in particular, how they are applied in the construction of Calegari and Dunfield.

1. Introduction

Thurston has raised the following question regarding the topology of closed hyperbolic 3-manifolds (recall that *closed* means compact without boundary):

1.1. **Question.** If M is a closed connected hyperbolic 3-manifold, does M admit a finite cover whose first Betti number is positive?

To give this question some context, we recall some facts about the fundamental groups of closed hyperbolic 3-manifolds, as well as some terminology.

First, the facts: If M is a closed connected hyperbolic 3-manifold, then its fundamental group $\pi_1(M)$ is *infinite*, but *residually finite* (i.e. for any element $\gamma \in \pi_1(M) \setminus 1$, there exists a homomorphism $\pi_1(M) \to G$ with finite image such that the image of γ is non-trivial). Thus $\pi_1(M)$ admits many finite quotients, and correspondingly M admits many finite covers. Indeed, one can say something more precise: M admits finite covers of arbitrarily large *injectivity radius*.[1]

Next, the terminology: A closed connected orientable 3-manifold M is called a *rational homology sphere* if its first Betti number equals 0. By Poincaré duality, this implies that its second Betti number also equals 0, and thus that M has the same Betti numbers as the 3-sphere S^3. (Equivalently, the homology of M, computed with *rational* coefficients, coincides with that of S^3, whence the name.)

Returning now to Thurston's question we see that we can reformulate it in the following (negative) fashion:

1.2. **Question.** Can one find a closed hyperbolic 3-manifold that is a rational homology sphere, and all of whose finite covers are again rational homology spheres?

Received by the editors November 17, 2008.

2000 *Mathematics Subject Classification.* Primary .

The author was supported in part by NSF grant DMS-0701315.

[1]The injectivity radius of a closed Riemannian manifold N is one-half of the length of the shortest closed geodesic in N; thus it can be regarded as (one-half of) a minimal diameter of N.

In fact Thurston conjectured that the answer to his question in this form is *no*, or equivalently, that the answer to Question 1.1 is *yes*. This is the so-called *Virtual Positive Betti Number Conjecture* (the term virtual refers to the consideration of finite covers), which remains unproved at the moment. (We refer to [9] for a discussion of some of the literature and results related to this conjecture.)

Cooper raised the following question, related to Question 1.2 (see Problem 3.58 of [8]):

1.3. **Question.** Can one find a closed hyperbolic 3-manifold that is a rational homology sphere, and which admits finite covers of arbitrarily large injectivity radius that are again rational homology spheres?

Note that a negative answer to this question would yield a negative answer to Question 1.2 (since, as was recalled above, any closed hyperbolic manifold does admit covers of arbitrarily large injectivity radius), and hence a positive answer to Question 1.1, proving the Virtual Positive Betti Number Conjecture.

Unfortunately, the answer to Question 1.3 is in fact *yes*, and the goal of this note is to discuss a theorem of Frank Calegari and Nathan Dunfield to this effect [5, Thm. 1.4]:

1.4. **Theorem.** *There exists an infinite tower of finite covers*

$$\cdots \to M_n \to \cdots \to M_2 \to M_1 \to M_0,$$

each member of which is a closed hyperbolic rational homology sphere, and such that injectivity radius of M_n grows without bound as $n \to \infty$.

In one sense, this result was not a surprise: unlike Question 1.2, Cooper's Question 1.3 was actually expected to have a positive answer. What was surprising was the method of proof that Calegari and Dunfield gave of their Theorem 1.4: their proof relies on ideas from the Langlands program and the theory of Galois representations, topics that at first glance seem quite far removed from the topology of 3-manifolds.

We should note that Calegari and Dunfield's proof of Theorem 1.4 is contingent on certain other conjectures, not related to topology, but rather of an arithmetic nature. Namely, their proof relies on the Generalized Riemann Hypothesis, as well as on a particular case of Conjecture 1.7 below. Subsequently, Boston and Ellenberg [3] found an unconditional proof of Theorem 1.4. However, it is the original argument of Calegari and Dunfield that will be the focus of these notes, since it is this argument that exhibits a surprising link between the topology of 3-manifolds and questions of arithmetic.

In the remainder of this introduction, we give the briefest sketch of some of the ideas in the Langlands program, including a very rough statement of Langlands' reciprocity conjecture (Conjecture 1.7 below), which plays a key role in Calegari and Dunfield's proof of Theorem 1.4, before closing with an outline of the contents of the main body of this note.

1.5. **Langlands' reciprocity conjecture.** The Langlands program is an elaborate web of theorems and conjectures relating the representation theory of and harmonic analysis on certain Lie groups with arithmetic, and in particular, with representations of certain Galois groups. I will not try to make a precise statement of any of its tenets or conjectures here, but will content myself with briefest possible sketch of the ideas.

Recall that a complex number α is called an algebraic number if it is algebraic over $\mathbb{Q}$, i.e. if $f(\alpha) = 0$ for some polynomial $f(X) \in \mathbb{Q}[X]$. The set of all algebraic numbers forms a subfield $\overline{\mathbb{Q}} \subset \mathbb{C}$. Alternatively, one may define $\overline{\mathbb{Q}}$ to be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, or to the the union of all the finite subextensions F of $\mathbb{Q}$ in $\mathbb{C}$. Finite extensions F of $\mathbb{Q}$ are usually referred to as *number fields*. If F is any number field in $\mathbb{C}$, then $\overline{\mathbb{Q}}$ is also the algebraic closure of F in $\mathbb{C}$, and we may consider the so-called absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ of F; this is the group of all automorphisms of $\overline{\mathbb{Q}}$ that restrict to the identity on F. (It is in fact naturally a profinite group, rather than just a group, but we suppress this detail here.) The group $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ is one of the characters in the Langlands story.

The other main characters in the story are automorphic eigenforms on reductive groups, the definition of which we now very briefly sketch. Suppose that $F \subset \overline{\mathbb{Q}}$ is a number field (i.e. of finite degree over $\mathbb{Q}$). Let G be a semi-simple or reductive linear algebraic group over F. (One can think of $\mathrm{GL}(n, F)$, although, as we will see below, there are other important examples too.) Let $G_{\mathbb{R}}$ denote the set of real points of G. (If $G = \mathrm{GL}(n, F)$ where $F = \mathbb{Q}(\alpha)$ is the number field obtained by adjoining the algebraic number α to $\mathbb{Q}$, and if the minimal polynomial of α has r_1 real roots and $2r_2$ complex roots, then $G_{\mathbb{R}} := \mathrm{GL}(n, \mathbb{R})^{r_1} \times \mathrm{GL}(n, \mathbb{C})^{r_2}$.) Let Γ be a *congruence subgroup* of the integer points of G. (See Subsections 4.2, 4.4, and 4.7 below for the definition of this notion in certain special cases; note in particular that Γ is then a discrete subgroup of $G_{\mathbb{R}}$.)

Consider the space $\mathcal{C}^\infty(\Gamma\backslash G_{\mathbb{R}})$ of smooth complex valued functions on the quotient $\Gamma\backslash G_{\mathbb{R}}$. This space is equipped with many commuting operators, namely the Casimir and higher Casimir operators (these are differential operators, analogous to a Laplacian, induced by the action of centre of the enveloping algebra of the Lie algebra of $G_{\mathbb{R}}$ on $\mathcal{C}^\infty(\Gamma\backslash G_{\mathbb{R}})$), and also the Hecke operators, which are indexed by (all but a finite number of) the prime ideals of the ring of integers of F.

1.6. **Definition.** An automorphic eigenform is a function $f \in \mathcal{C}^\infty(\Gamma\backslash G_{\mathbb{R}})$ which is a simultaneous eigenvector of all of the commuting operators discussed above, i.e. of all the Casimirs and Hecke operators, and which is slowly increasing at infinity.

We don't recall the precise definitions of the various operators alluded to above, or of the term "slowly increasing" as it is used in the above definition, referring the reader instead to the discussion of [2]. We will outline the definition of the Hecke operators in certain special cases in Subsection 4.9 below.

If f is an automorphic eigenform, then f determines a collection of eigenvalues, one eigenvalue for each of the Casimirs and each Hecke operator, which we will refer to as the *system of eigenvalues* attached to f.

Of importance for us is the following conjecture, which is a vaguely stated form of Langlands' Reciprocity Conjecture:

1.7. **Conjecture.** (a) *If $f \in \mathcal{C}^\infty(\Gamma\backslash G_{\mathbb{R}})$ is an automorphic eigenform, whose (appropriately normalized) eigenvalues under all the Casimir operators are integral, then the system of eigenvalues attached to f determines, and is in turn determined by, a certain representation of the Galois group* $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

(b) *Any representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ *satisfying appropriate hypotheses is determined by an automorphic eigenform in the sense of part* (a).

This statement is overly simplified, and there are a myriad of details that we have omitted. Just to indicate some: (i) f should determine not just one representation,

but in fact a whole family representations; we refer to subsection 5.1 below for some examples of such families. (ii) One can be precise about the group of matrices in which the values of the Galois representations associated to f should lie. In general, this requires a discussion of dual groups and L-groups (see e.g. [1]). In the case when $G = \mathrm{GL}(n, F)$, one can say that the associated Galois representations should be n-dimensional. (iii) There is an explicit description of the manner in which the system of eigenvalues attached to f, and the corresponding Galois representations, should determine each other. This description relies on, among other things, the Satake isomorphism (as explained e.g. in [6]). (iv) We have given no indication of what the "appropriate hypotheses" on a Galois representation in part (b) of the conjecture might be. For some examples of Galois representations satisfying these unspecified hypothesis, we again refer to Subsection 5.1.

To elaborate on all these points, and on the many others that we are omitting, would turn this brief note into a technical treatise, which is certainly not our goal. (In the case when $G = \mathrm{GL}(n, F)$ for a number field F, we refer to the article [12] of Taylor for a rather complete discussion.) Rather, we hope to give some indication as to how one can use Conjecture 1.7 to deduce concrete statements in mathematics, such as Theorem 1.4.

Let us close the present discussion by observing that (even in the vague form in which we have presented it), Conjecture 1.7 relates two kinds of objects, namely automorphic eigenforms and the Galois groups $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, which *seem to have absolutely nothing to do with one another!* The first have to do with spectral theory on Lie groups, and the second to do with algebraic symmetries of algebraic numbers. It is the connection it provides between two totally different parts of mathematics that gives Conjecture 1.7 its force; it is also what makes the proof of even special cases of the conjecture so difficult. (See Subsection 5.4 below for a discussion of some of those special cases.)

1.8. **An outline of the paper.** In Section 2, we recall the basic facts about hyperbolic manifolds and hyperbolic spaces. In particular, we recall the connection between n-dimensional hyperbolic space and the Lie group $SO(n, 1)$. In the cases when $n = 2$ and 3, we recast this connection in terms of the more familiar groups $\mathrm{PSL}(2, \mathbb{R})$ and $\mathrm{PSL}(2, \mathbb{C})$.

In Section 3, we recall the basic facts concerning homology and cohomology of manifolds. After first considering the case of arbitrary dimension we then specialize the discussion to the cases of dimensions 2 and 3.

In Section 4, we introduce the notion of congruence quotients of $\mathbb{H}^2$ and $\mathbb{H}^3$. In particular, we define a particular tower of congruence quotients of $\mathbb{H}^3$ which satisfies the requirements of Theorem 1.4. (See Theorem 4.8.) Finally, we give a brief indication of how cohomology classes on congruence quotients give rise to automorphic forms, and outline the definition of the Hecke operators (in the context of cohomology).

In Section 5, we discuss the Langlands reciprocity conjecture for 2-dimensional Galois representations in more detail. We begin by giving some examples of 2-dimensional Galois representations, namely, those that arise from elliptic curves. We then describe the reciprocity conjecture for automorphic eigenforms and 2-dimensional Galois representations associated to $\mathbb{Q}$ and to quadratic imaginary number fields. Next, we very briefly sketch how a special case of the reciprocity conjecture was used by Andrew Wiles to prove Fermat's Last Theorem. We then

explain how the reciprocity conjecture can be used to deduce Theorem 1.4. Finally, we explain how the reciprocity conjecture implies a positive answer to the virtual positive Betti number conjecture for arithmetic closed hyperbolic 3-manifolds.

These examples illustrate the different ways in which the reciprocity conjecture can be applied: in the proof of Fermat's Last Theorem, one uses the non-existence of certain kinds of automorphic forms to establish the non-existence of certain kinds of Galois representations, from which one in turn deduces Fermat's Last Theorem. By contrast, in the proof of Theorem 1.4, as we will see, one uses the non-existence of certain Galois representations to deduce the non-existence of certain automorphic forms, from which one in turn deduces that certain hyperbolic 3-manifolds are rational homology spheres. Finally, in the proof of the virtual positive Betti number conjecture in the arithmetic case, one uses the existence of certain Galois representations to force the existence of certain automorphic forms.

2. Hyperbolic Manifolds

In this section we discuss some of the basics of the theory of hyperbolic manifolds. We begin with a discussion in the general setting of n-dimensional hyperbolic manifolds, before specializing to the case of surfaces and 3-manifolds. We focus on explaining the connection with the Lie groups $\mathrm{SO}(n,1)$ (see in particular Subsection 2.4 below), since this gives the first indication that ideas from the Langlands program could be applied to the study of hyperbolic manifolds.

2.1. **Hyperbolic manifolds as quotients of hyperbolic space.** Let M be a connected complete n-dimensional smooth Riemannian manifold (with $n \geq 2$). We say that M is *hyperbolic* if M all the sectional curvatures of M are constant and negative. Rescaling the metric of M if necessary, we may and do assume that the sectional curvatures of M are then in fact all equal to -1.

The Riemannian metric on M pulls back to a Riemannian metric on the universal cover $\tilde{M}$ of M, which thus becomes a complete n-dimensional simply connected hyperbolic manifold. Such a manifold is unique, up to isometry, and we denote it by $\mathbb{H}^n$. It is referred to as *hyperbolic n-space*.

The original manifold M may be obtained as the quotient $\Gamma\backslash\mathbb{H}^n$ for a certain group of deck-transformations Γ acting on $\mathbb{H}^n$. Since the metric on $\mathbb{H}^n$ is simply pulled back from M, the group Γ is a group of isometries of $\mathbb{H}^n$, and it thus a discrete subgroup of the group $\mathrm{Isom}(\mathbb{H}^n)$ of all isometries of $\mathbb{H}^n$. If M is furthermore orientable, then Γ lies in the index 2 subgroup $\mathrm{Isom}^0(\mathbb{H}^n)$ of $\mathrm{Isom}(\mathbb{H}^n)$ consisting of orientation-preserving isometries.

2.2. **A quadric model of $\mathbb{H}^n$.** Hyperbolic n-space admits many models; in this subsection we describe one of them.

Let Q denote the quadratic form $x_1^2 + \cdots x_n^2 - x_{n+1}^2$ on $\mathbb{R}^{n+1}$. This quadratic forms induces a corresponding pseudo-Riemannian metric

$$g := dx_1^2 + \cdots dx_n^2 - dx_{n+1}^2$$

on $\mathbb{R}^{n+1}$. Let X denote the quadric

$$X := \{x \in \mathbb{R}^{n+1} \,|\, Q(x) = -1\} \subset \mathbb{R}^{n+1},$$

and let $X^+ := \{x \in X \,|\, x_{n+1} > 0\} \subset X$. (The quadric X is the union of two connected components, of which X^+ is one; the other is the subset X^- of X consisting of points for which $x_{n+1} < 0$.) If $g_{|X^+}$ denotes the restriction of g to

X^+, then $g_{|X^+}$ is a true Riemannian metric on X^+ (i.e. it is positive definite). Furthermore, the sectional are curvatures of X^+ are constant and negative. Since X^+ is simply connected (indeed, it is homeomorphic to $\mathbb{R}^n$), we find that X^+ provides a model for $\mathbb{H}^n$.

2.3. **A Lie theoretic description of $\mathbb{H}^n$.** Let $\mathrm{O}(n,1)$ denote the subgroup of $\mathrm{GL}(n+1,\mathbb{R})$ which preserves the quadratic form Q. The group $\mathrm{O}(n,1)$ then clearly preserves the quadric X, and one easily sees that it acts transitively on X.

If x is a point of X, and $\mathrm{O}(n,1)_x$ denotes the stabilizer of x in $\mathrm{O}(n,1)$, then $\mathrm{O}(n,1)_x$ acts faithfully by orthogonal transformations on the tangent hyperplane to X at x (orthogonal with respect to the positive definite quadratic form given by the metric $g_{|X}$), and in this manner one obtains an isomorphism $\mathrm{O}(n,1)_x \xrightarrow{\sim} \mathrm{O}(n)$, where $\mathrm{O}(n)$ denotes the usual orthogonal group of $n \times n$ matrices that preserve a positive definite n-dimensional quadratic form. Thus there is an identification

$$\mathrm{O}(n,1)/\mathrm{O}(n) \xrightarrow{\sim} X.$$

If we let $\mathrm{O}(n,1)^+$ denote the index 2 subgroup of $\mathrm{O}(n,1)$ consisting of transformations which take X^+ to itself, then we obtain a corresponding identification

$$\mathrm{O}(n,1)^+/\mathrm{O}(n) \xrightarrow{\sim} X^+ = \mathbb{H}^n, \tag{2.1}$$

and we also obtain an identification

$$\mathrm{O}(n,1)^+ \xrightarrow{\sim} \mathrm{Isom}(X^+) = \mathrm{Isom}(\mathbb{H}^n).$$

Any matrix in $\mathrm{O}(n,1)$ has determinant equal to ± 1. If we let $\mathrm{SO}(n,1)^+$ denote the subgroup of $\mathrm{O}(n,1)^+$ consisting of matrices of determinant 1, then $\mathrm{SO}(n,1)^+$ is identified with the index 2 subgroup $\mathrm{Isom}^0(\mathbb{H}^n)$ of orientation preserving isometries in $\mathrm{Isom}(\mathbb{H}^n)$. The identification (2.1) induces an identification

$$\mathrm{SO}(n,1)^+/\mathrm{SO}(n) \xrightarrow{\sim} X^+ = \mathbb{H}^n.$$

The group $\mathrm{SO}(n,1)^+$ is a connected semi-simple Lie group, and $\mathrm{SO}(n)$ is a maximal compact subgroup of $\mathrm{SO}(n,1)^+$. In general, the quotient of a connected semi-simple Lie group G by its maximal compact subgroup is referred to as the symmetric space associated to G. Thus $\mathbb{H}^n$ is the symmetric space associated to $\mathrm{SO}(n,1)^+$.

We can thus summarize the discussion of this section as follows: the group $\mathrm{Isom}^0(\mathbb{H}^n)$ of orientation-preserving isometries of $\mathbb{H}^n$ is isomorphic to the connected semi-simple Lie group $\mathrm{SO}(n,1)^+$, and $\mathbb{H}^n$ may be identified with the symmetric space associated to $\mathrm{SO}(n,1)^+$.

2.4. **Hyperbolic manifolds and discrete subgroups of $\mathrm{SO}(n,1)^+$.** If we combine the discussion of subsections 2.1 and 2.3, we find that any orientable complete hyperbolic n-manifold M may be written as a quotient

$$M \xrightarrow{\sim} \Gamma\backslash \mathrm{SO}(n,1)/SO(n),$$

where Γ is a discrete torsion-free subgroup of $\mathrm{SO}(n,1)$. (The torsion-free condition ensures that Γ acts properly discontinuously on $\mathrm{SO}(n,1)/SO(n) = \mathbb{H}^n$.)

2.5. **The upper half-space model for $\mathbb{H}^n$.** Another model for $\mathbb{H}^n$ is the n-dimensional upper half-space

$$\mathcal{H}^n := \{(x_1, \ldots, x_n) \in \mathbb{R}^n \,|\, x_n > 0\},$$

equipped with the metric $ds^2 := \dfrac{dx_1^2 + \ldots dx_n^2}{x_n^2}$. One computes that this is a metric of constant negative curvature, and so does indeed realize $\mathcal{H}^n$ as a model of $\mathbb{H}^n$. We will discuss this model in more detail in the two cases $n = 2$ and 3.

2.6. **The upper half-plane model of $\mathbb{H}^2$.** The group $\mathrm{SO}(2,1)^+$ is more familiar than it might seem. Indeed, there is an isomorphism[2]

$$\mathrm{PSL}(2,\mathbb{R}) := \mathrm{SL}(2,\mathbb{R})/\{\pm 1\} \xrightarrow{\sim} \mathrm{SO}(2,1)^+.$$

Thus there is also an isomorphism

$$\mathrm{PSL}(2,\mathbb{R}) \xrightarrow{\sim} \mathrm{Isom}^0(\mathbb{H}^2). \tag{2.2}$$

As we now explain, the upper half-plane model of $\mathbb{H}^2$ makes this isomorphism apparent.

Let us rewrite the upper half-plane $\mathcal{H}^2$ in the form

$$\mathcal{H}^2 := \{z = x + iy \in \mathbb{C} \,|\, y > 0\}$$

(i.e. we think of it as being the *complex upper half-plane*); the metric on $\mathcal{H}^2$ then becomes

$$ds^2 := \frac{dx^2 + dy^2}{y^2}.$$

The group $\mathrm{PSL}(2,\mathbb{R})$ is now seen to act on $\mathcal{H}^2$ as follows: an element $\gamma \in \mathrm{PSL}(2,\mathbb{R})$, represented by a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$, acts on $\mathcal{H}^2$ via the formula

$$\gamma \cdot z := \frac{az + b}{cz + d}. \tag{2.3}$$

One easily computes that this action preserves the metric ds^2, and thus we obtain a concrete description of the isomorphism (2.2).

2.7. **The upper half-space model of $\mathbb{H}^3$.** The group $\mathrm{SO}(3,1)^+$ is also more familiar than it might seem. Indeed, there is an isomorphism[3]

$$\mathrm{PSL}(2,\mathbb{C}) := \mathrm{SL}(2,\mathbb{C})/\{\pm 1\} \xrightarrow{\sim} \mathrm{SO}(3,1)^+.$$

---

[2]This isomorphism can be understood conceptually as follows: $\mathrm{SL}(2,\mathbb{R})$ acts on its Lie algebra $\mathfrak{sl}_2$ (the space of 2×2-matrices of trace zero) via conjugation (the so-called adjoint action). This action factors through $\mathrm{PSL}(2,\mathbb{R})$, and preserves the quadratic form $\langle X, Y\rangle := \mathrm{Trace}(XY)$, which has signature $(2,1)$.

[3]Here is a theoretical description of this isomorphism: let V denote the two-dimensional complex vector space $\mathbb{C}^2$ equipped with the standard representation of $\mathrm{SL}(2,\mathbb{C})$, and let $\overline{V}$ denote $\mathbb{C}^2$ equipped with the complex conjugate action of $\mathrm{SL}(2,\mathbb{C})$. The tensor product $W := V \otimes_{\mathbb{C}} \overline{V}$ is then a 4-dimensional representation of $\mathrm{SL}(2,\mathbb{C})$. The subgroup $\{\pm 1\}$ acts trivially on W, and so W is in fact a representation of $\mathrm{PSL}(2,\mathbb{C})$. Furthermore, the character of W is real valued, and in fact W descends to a representation $W_{\mathbb{R}}$ of $\mathrm{PSL}(2,\mathbb{C})$ on a 4-dimensional real vector space. One computes that in the space of quadratic forms on $W_{\mathbb{R}}$, there is a unique line that is invariant under $\mathrm{PSL}(2,\mathbb{C})$, and that the non-zero quadratic forms in this line have signature $(3,1)$ and $(1,3)$. Thus $\mathrm{PSL}(2,\mathbb{C})$ preserves a quadratic form of signature $(3,1)$ on $W_{\mathbb{R}}$; this yields the stated isomorphism.

This isomorphism then induces an isomorphism

$$\mathrm{PSL}(2,\mathbb{R}) \xrightarrow{\sim} \mathrm{Isom}^0(\mathbb{H}^2). \tag{2.4}$$

As we now explain, the upper half-space model of $\mathbb{H}^3$ makes this isomorphism apparent.

Let us rewrite 3-dimensional upper half-space in the form

$$\mathcal{H}^3 := \{(z,t) \in \mathbb{C} \times \mathbb{R} \,|\, t > 0\}.$$

We can then identify the Riemann sphere $\mathbb{C}P^1 := \mathbb{C} \cup \{\infty\}$ with the "sphere at infinity" of $\mathcal{H}^3$, and the action of $\mathrm{Isom}^0(\mathbb{H}^3) = \mathrm{Isom}^0(\mathcal{H}^3)$ on $\mathcal{H}^3$ induces a corresponding action by conformal transformations on $\mathbb{C}P^1$. On the the other hand, from complex analysis we know that the group of conformal transformations of $\mathbb{C}P^1$ is identified with $\mathrm{PSL}(2,\mathbb{C})$, acting by linear fractional transformations (via the formula (2.3)). Thus we obtain a homomorphism $\mathrm{Isom}^0(\mathbb{H}^3) \to \mathrm{PSL}_2(\mathbb{C})$, which is in fact the inverse of the isomorphism (2.4).

3. The homology and cohomology of closed manifolds

As its title indicates, in this section, we describe some of the basic facts about the algebraic topology of closed manifolds.

3.1. **Homology.** If M is a closed connected n-manifold, then we can compute its homology groups $H_i(M,A)$ with coefficients in any abelian group A via singular chains. We will primarily be interested in the cases when A is one of the fields $\mathbb{Q}$ or $\mathbb{C}$. In this case the homology groups are actually $\mathbb{Q}$- or $\mathbb{C}$-vector spaces, and the universal coefficients theorem provides an isomorphism

$$\mathbb{C} \otimes_{\mathbb{Q}} H_i(M,\mathbb{Q}) \xrightarrow{\sim} H_i(M,\mathbb{C});$$

in particular, the dimension of H_i is independent of whether we use $\mathbb{Q}$ and $\mathbb{C}$; it is referred to as the ith Betti number of M, and denoted b_i. It is always finite.

If M is orientable, then Poincaré duality shows that $H_i(M,\mathbb{Q})$ and $H_{n-i}(M,\mathbb{Q})$ are naturally dual vector spaces (and similarly with $\mathbb{Q}$ replaced by $\mathbb{C}$). In particular $b_i = b_{n-i}$. Since there is no homology in negative degrees, we see that $b_i = 0$ if $i < 0$, and thus also $b_i = 0$ if $i > n$. Since M is connected, $b_0 = 1$. Thus $b_n = 1$ also.

3.2. **Definition.** The Euler characteristic of M is defined to be

$$\chi(M) := \sum_{i \geq 0} (-1)^i b_i.$$

Since b_i vanishes if $i > n$, this sum is well-defined.

3.3. *Remark.* If n is odd and M is orientable, then it follows from Poincaré duality (or more precisely, the formula $b_i = b_{n-i}$ for all i) that $\chi(M) = 0$.

If M is triangulable, i.e. is homeomorphic to a simplicial complex, then we may also compute homology simplicially, in terms of some given triangulation. The Euler-Poincaré formula then shows that we may also compute $\chi(M)$ as the alternating sum, for $i \geq 0$, of the number of simplices of dimension i appearing in some given triangulation of M.

We recall that closed surfaces and closed 3-manifolds are always triangulable.

The following lemma describes the behaviour of Euler characteristics under finite covering maps.

3.4. **Lemma.** *If $N \to M$ is a finite covering map of connected closed manifolds, of degree d say, then $\chi(N) = d\,\chi(M)$.*

Sketch of proof. We sketch a proof in the case when M is triangulable. (Since closed surfaces and closed 3-manifolds are always triangulable, this argument establishes the lemma in dimensions $n = 2$ or 3.) Fix a triangulation of M and use this triangulation to compute $\chi(M)$. Then, pull back this triangulation to N via the covering map and use this pulled-back triangulation to compute $\chi(N)$. Since the covering map has degree d, every simplex in the triangulation of M pulls back to d simplices in N. The formula follows. □

While the preceding lemma gives excellent control over the behaviour of the Euler characteristic in finite covers, it is significantly more difficult in general to control the behaviour of individual Betti numbers, as we will see.

3.5. **Cohomology.** If M is a closed connected n-manifold, then we can compute its cohomology group $H^i(M, A)$ with coefficients in any abelian group A via singular cochains. We will primarily be interested in the cases when A is one of the fields $\mathbb{Q}$ or $\mathbb{C}$. In this case the ith cohomology group is actually a $\mathbb{Q}$- or $\mathbb{C}$-vector space, and is naturally dual to the ith homology group. In particular, it has the same dimension, namely the ith Betti number b_i.

De Rham theory shows that we may also compute the complex cohomology spaces $H^i(M, \mathbb{C})$ using differential forms. If we fix a Riemannian metric g on M, then we may furthermore use Hodge theory to identify $H^i(M, \mathbb{C})$ with the space of harmonic i-forms on M. (The connection with analysis provided by de Rham theory and Hodge theory is one reason for considering cohomology as well as homology, even though from the point of view of the singular theory, they carry essentially the same information.)

If $N \to M$ is a finite cover, then pulling back cohomology classes induces a map $H^i(M, \mathbb{Q}) \to H^i(N, \mathbb{Q})$, which is in fact injective. (Indeed, if the cover is regular, with covering group G, then we can be more precise: by functoriality of cohomology, the group G acts on $H^i(N, \mathbb{Q})$, and $H^i(M, \mathbb{Q})$ is identified with the space of G-invariant elements in $H^i(N, \mathbb{Q})$.) This yields the following lemma:

3.6. **Lemma.** *If $N \to M$ is a finite covering map of closed manifolds, then the ith Betti number of N is greater than or equal to the ith Betti number of M.*

Note that this statement is much weaker than the very precise statement regarding Euler characteristics provided by Lemma 3.4. In the following subsections, we will discuss the extent to which we can improve it in the cases of surfaces and 3-manifolds.

3.7. **The topology of closed hyperbolic surfaces.** If M is a closed connected orientable surface, then $b_0 = b_2 = 1$, while $b_1 = 2g$, where g is the genus of M. Thus the Euler characteristic $\chi(M) = 2 - 2g$.

If M is equipped with a Riemannian metric with curvature K (a real-valued function on M, since M is a surface), then the *Gauss-Bonnet theorem* states that

$$\int_M K = 2\pi\,\chi(M).$$

In particular, if M is a hyperbolic manifold, so that $K \equiv -1$, then we find that

$$\chi(M) = -\frac{\mathrm{vol}(M)}{2\pi},$$

and so is negative; equivalently, the genus $g > 1$. (Conversely, if $\chi(M)$ is negative, then M admits a hyperbolic metric — indeed, a $(6g-6)$-dimensional moduli space of them.)

If N is a finite covering space of M, of degree d say, then Lemma 3.4 shows that $\chi(N) = d\,\chi(M)$. Consequently, if M has genus g, then N has genus $d(g-1)+1$. In particular, if M is hyperbolic, so that $g > 1$, then the genus of a degree d cover of M grows linearly with d (since $g > 1$), and hence so does the first Betti number. (Of course, b_0 and b_2 are both equal to 1 for any connected cover of M.)

3.8. **The topology of closed hyperbolic 3-manifolds.** If M is a closed connected orientable 3-manifold, then $b_0 = b_3 = 1$, while Poincaré duality shows that $b_1 = b_2$. In particular, as was noted in Remark 3.3, the Euler characteristic $\chi(M) = 0$. If N is any finite cover of M, then similarly $\chi(N) = 0$. Thus the formula of Lemma 3.4, while it is just as valid for for 3-manifolds as for surfaces, yields no information about the individual Betti numbers of N. Also, Lemma 3.6, while it shows that Betti numbers of N can't be less than those of M, does not imply that they must be greater than those of M.

Thus, unlike in the case of surfaces, it is not obvious that if one considers a tower of finite covers of M, then the first Betti number must increase as one moves up the tower. In fact, not only is is not obvious, it is not true! Indeed, Theorem 1.4 establishes the existence of an infinite tower of finite covers every member of which has $b_1 = 0$ (i.e. is a rational homology sphere).[4]

To prove Theorem 1.4, we need a tool that allows us to compute individual Betti numbers, at least for certain hyperbolic 3-manifolds. This tool will be provided by the Langlands reciprocity conjecture, applied in the context of arithmetic hyperbolic 3-manifolds.

4. Congruence quotients of $\mathbb{H}^2$ and $\mathbb{H}^3$

In this section we introduce the notion a congruence quotient of $\mathbb{H}^2$ or $\mathbb{H}^3$. The notion of a congruence quotient of $\mathbb{H}^n$ in fact make sense for any n, but we will focus on the cases $n = 2$ and 3, since then we can work with the more familiar groups $\mathrm{PSL}(2,\mathbb{R})$ and $\mathrm{PSL}(2,\mathbb{C})$, rather than the groups $\mathrm{SO}(n,1)$ (which are the groups we would have to deal with to study general values of n).

4.1. **First examples of discrete subgroups.** If we combine the discussions of Subsections 2.4, 2.6, and 2.7, we see that in order to find examples of hyperbolic surfaces or three folds, we have to find examples of discrete torsion-free subgroups of $\mathrm{PSL}(2,\mathbb{R})$ or $\mathrm{PSL}(3,\mathbb{C})$.

Some basic models for discrete objects inside continuous ones are provided by the inclusions $\mathbb{Z} \subset \mathbb{R}$ and $\mathbb{Z}[i] \subset \mathbb{C}$. (Here $\mathbb{Z}[i]$ denotes the ring of *Gaussian integers*, consisting of complex numbers whose real and imaginary parts are both

[4]We should point out that the existence of infinite towers of finite covers all of which are rational homology spheres was known prior to the work of Calegari and Dunfield in [5]; the new contribution of their work is to show that the tower can furthermore be chosen so that the injectivity radius grows without bound.

integers.) These immediately suggest examples of discrete subgroups in $\mathrm{PSL}(2,\mathbb{R})$ and $\mathrm{PSL}(2,\mathbb{C})$, namely $\mathrm{PSL}(2,\mathbb{Z})$ and $\mathrm{PSL}(2,\mathbb{Z}[i])$ respectively.

Unfortunately neither of these groups is torsion free, and so each of the quotients $\mathrm{PSL}(2,\mathbb{Z})\backslash\mathbb{H}^2$ and $\mathrm{PSL}(2,\mathbb{Z}[i])\backslash\mathbb{H}^3$ is an orbifold rather than a manifold. Also, neither of these quotients is compact.

4.2. **Congruence quotients of $\mathbb{H}^2$.** Although neither of the two groups $\mathrm{PSL}(2,\mathbb{Z})$ or $\mathrm{PSL}(2,\mathbb{Z}[i])$ is torsion-free, it is easy to construct closely related discrete subgroups which *are* torsion-free, the so-called *congruence subgroups*.

We begin by focusing on the $\mathrm{PSL}(2,\mathbb{Z})$ case. In fact it will be simpler to work with $\mathrm{SL}(2,\mathbb{Z})$, and we will do this from now on. Since $\mathrm{PSL}(2,\mathbb{Z})$ is a quotient of $\mathrm{SL}(2,\mathbb{Z})$, each of the subgroups we construct will have an associated image in $\mathrm{PSL}(2,\mathbb{Z})$, which will then be a discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$.

If n is any integer, then reduction modulo n induces a ring homomorphism $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$, and hence a homomorphism of groups

$$\mathrm{SL}(2,\mathbb{Z})\to\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z}). \tag{4.1}$$

The kernel of this map is denoted $\Gamma(n)$. It is referred to as the principal congruence subgroup of level n. It has finite index in $\mathrm{SL}(2,\mathbb{Z})$ (since $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ is finite), and is torsion-free if $n\geq 3$ (as its image in $\mathrm{PSL}(2,\mathbb{R})$). Thus we have produced an infinite family of discrete torsion-free subgroups of $\mathrm{PSL}(2,\mathbb{R})$, giving rise to an infinite family of hyperbolic surfaces. Note that if m divides n, then $\Gamma(m)\subset\Gamma(n)$ (with finite index), and so $\Gamma(m)\backslash\mathbb{H}^2$ is a finite cover of $\Gamma(n)\backslash\mathbb{H}^2$. Thus we also have lots of finite covering maps.

In fact, we will need to consider a slightly different family of congruence subgroups, usually denote $\Gamma_1(n)$, and defined as follows:

4.3. **Definition.** The group $\Gamma_1(n)\subset\mathrm{SL}(2,\mathbb{Z})$ is defined to be the preimage under (4.1) of the subgroup of upper triangular unipotent matrices in $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$; i.e.

$$\Gamma_1(n):=\{\gamma\in\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})\,|\,\gamma\equiv\begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix}\bmod N\}.$$

The groups $\Gamma_1(n)$ are torsion-free provided $n\geq 4$. Also, if m divides n, then $\Gamma_1(m)$ is a finite index subgroup of $\Gamma_1(n)$ Thus the quotients $\Gamma_1(n)\backslash\mathbb{H}^2$ give an infinite family of hyperbolic surfaces, with many finite covering maps between them.

In the number-theoretic literature, the group $\mathrm{SL}(2,\mathbb{Z})$ is referred to as the *modular group*, and the quotients $\Gamma(n)\backslash\mathbb{H}^2$ and $\Gamma_1(n)\backslash\mathbb{H}^2$ are called *modular curves*. In this note we will refer to them as *congruence quotients* (for the obvious reason: that they are quotients of $\mathbb{H}^2$ by congruence subgroups of $\mathrm{SL}(2,\mathbb{Z})$).

4.4. **Congruence quotients of $\mathbb{H}^3$.** One can define congruence subgroups of $\mathrm{PSL}(2,\mathbb{C})$ in an analogous manner to the case of $\mathrm{PSL}(2,\mathbb{R})$. Before doing so, we make some preliminary remarks.

The first remark is that the inclusion $\mathrm{SL}(2,\mathbb{C})\hookrightarrow\mathrm{GL}(2,\mathbb{C})$ induces an isomorphism

$$\mathrm{PSL}(2,\mathbb{C}):=\mathrm{SL}(2,\mathbb{C})/\{\pm 1\}\xrightarrow{\sim}\mathrm{GL}(2,\mathbb{C})/\mathbb{C}^\times=:\mathrm{PGL}(2,\mathbb{C}).$$

(Here $\mathbb{C}^\times$, the multiplicative group of non-zero complex numbers, embeds into $\mathrm{GL}(2,\mathbb{C})$ as the subgroup of non-zero scalar matrices.) Thus, in order to construct discrete subgroups of $\mathrm{PSL}(2,\mathbb{C})$, it suffices to construct such subgroups of $\mathrm{GL}(2,\mathbb{C})$; we can then pass to their images in $\mathrm{PGL}(2,\mathbb{C})=\mathrm{PSL}(2,\mathbb{C})$. The reason for working

with $\mathrm{GL}(2,\mathbb{C})$ rather than $\mathrm{SL}(2,\mathbb{C})$ at this point is dictated by the requirements of the paper [5] — it will allow us to apply the Langlands reciprocity conjecture in such a way as to construct a tower of rational homology spheres satisfying the requirements of Theorem 1.4.

The second remark is that $\mathbb{Z}[i]$ is not the only "discrete model" for the complex numbers that we have available for forming discrete subgroups of $\mathrm{GL}(2,\mathbb{C})$. If d is any positive square-free integer, then $F := \mathbb{Q}(\sqrt{-d})$ is a subfield of $\mathbb{C}$ with the property that $\mathbb{R} \otimes_{\mathbb{Q}} F \xrightarrow{\sim} \mathbb{C}$ (so F is to $\mathbb{C}$ as $\mathbb{Q}$ is to $\mathbb{R}$), and the ring of integers[5] $\mathcal{O}_F$ of F is a discrete subring of $\mathbb{C}$. (Such number fields F are called *quadratic imaginary*.)

For any choice of F, the group $\mathrm{GL}(2,\mathcal{O}_F)$ is a discrete subgroup of $\mathrm{GL}(2,\mathbb{C})$. If $\mathfrak{n}$ is a non-zero ideal in $\mathcal{O}_F$, then $\mathcal{O}_F/\mathfrak{n}$ is a finite ring, and we have the reduction map

$$\mathrm{GL}(2,\mathcal{O}_F) \to \mathrm{GL}(2,\mathcal{O}_F/\mathfrak{n}). \tag{4.2}$$

4.5. **Definition.** We define $\Gamma_1(\mathfrak{n})$ to be the subgroup of $\mathrm{GL}(2,\mathcal{O}_F)$ obtained as the preimage under (4.2) of the subgroup of upper triangular unipotent matrices in $\mathrm{GL}(2,\mathcal{O}_F/\mathfrak{n})$; i.e.

$$\Gamma_1(n) := \{\gamma \in \mathrm{GL}(2,\mathcal{O}_F/\mathfrak{n}) \,|\, \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod \mathfrak{n}\}.$$

Just as in the two-dimensional case, for a fixed choice of F, for all but finitely many ideal $\mathfrak{n}$, the group $\Gamma_1(\mathfrak{n})$ will have torsion-free image in $\mathrm{PSL}(2,\mathbb{C})$, and of course, if $\mathfrak{m} \subset \mathfrak{n}$ is an inclusion of non-zero ideals, then $\Gamma_1(\mathfrak{m}) \subset \Gamma_1(\mathfrak{n})$. Thus we obtain an infinite collection of hyperbolic 3-manifolds, of the form $\Gamma_1(\mathfrak{n})\backslash\mathbb{H}^3$, with many finite covering maps between them. Just as in the surface case, we refer to these hyperbolic 3-manifolds as *congruence quotients* of $\mathbb{H}^3$.

4.6. **Noncompactness and unipotent elements.** The congruence quotients we have constructed so far, namely $\Gamma_1(n)\backslash\mathbb{H}^2$ and $\Gamma_1(\mathfrak{n})\backslash\mathbb{H}^3$, are important examples of hyperbolic manifolds, but they have the disadvantage, from the point of view of proving Theorem 1.4, that they are *not* compact (although they are of finite volume).

In the surface case, these quotients have ends that look like cylinders on a circle (i.e. are homeomorphic to $S^1 \times \mathbb{R}$), while in the 3-manifold case they have ends that look like cylinders on a torus (i.e. are homeomorphic $S^1 \times S^1 \times R$).

The reason that the quotients $\Gamma_1(n)\backslash\mathbb{H}^2$ are not compact is that the groups $\Gamma_1(n)$ contain non-identity unipotent elements, such as the element $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The presence of such elements forces the fundamental domains for these groups in $\mathbb{H}^2$ to contain vertical "strips" going off to infinity, which contribute cylindrical ends to the corresponding quotient surface. A similar phenomenon occurs with the groups $\Gamma_1(\mathfrak{n})$, which also contain unipotent elements.

4.7. **Compact congruence quotients of $\mathbb{H}^2$ and $\mathbb{H}^3$.** In this subsection we explain how to construct other kinds of congruence quotient of $\mathbb{H}^2$ and $\mathbb{H}^3$ which *are*

[5]The ring of integers $\mathcal{O}_F$ is equal to $\mathbb{Z}[\sqrt{-d}]$ if $d \equiv 1$ or $2 \bmod 4$, and $\mathbb{Z}[(1+\sqrt{-d})/2]$ if $d \equiv 3 \bmod 4$.

closed manifolds. To do this, we need to find discrete subgroups Γ which do *not* contain unipotent elements. We now explain how we can do this.

A matrix T in $\mathrm{SL}(2,\mathbb{R})$ or $\mathrm{SL}(2,\mathbb{C})$ is unipotent if and only if $T-1$ is a nilpotent element of the ring of matrices $\mathrm{M}(2,\mathbb{R})$ or $\mathrm{M}(2,\mathbb{C})$. Thus, in order to be able to define a notion of congruence subgroup that does not contain non-identity unipotent elements, we need to find an "integral model" for $\mathrm{M}(2,\mathbb{R})$ (say) which does not contain non-zero nilpotent elements. That is, we need to find a $\mathbb{Z}$-algebra A that contains no non-zero nilpotents, such that upon extending scalars to $\mathbb{R}$, we obtain an isomorphism $\mathbb{R}\otimes_{\mathbb{Z}} A \xrightarrow{\sim} \mathrm{M}(2,\mathbb{R})$. How can we do this?

The answer to this question is: via the theory of quaternion algebras! To see why, begin by recalling that Hamilton's ring of quaternions is the (associative, but non-commutative) 4-dimensional $\mathbb{R}$-algebra $\mathbb{H}$ (this is the traditional notation, but do not confuse it with a hyperbolic space!) generated by elements i and j with the commutation relations

$$i^2 = j^2 = -1, \quad ij = -ji.$$

(The elements $1, i, j$, and $k := ij$ form a basis for $\mathbb{H}$ as an $\mathbb{R}$-vector space.) The algebra $\mathbb{H}$ is a division algebra, and so in particular, contains no non-zero nilpotent elements, but there is an isomorphism $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{H} \xrightarrow{\sim} \mathrm{M}(2,\mathbb{C})$.

Now, the theory of quaternion algebras over number fields allows us to greatly generalize Hamilton's construction. For example, the associative $\mathbb{Q}$-algebra D generated by elements i and j with the commutation relations

$$i^2 = 2, \quad j^2 = 3, \quad ij = -ji$$

is a 4-dimensional division algebra over $\mathbb{Q}$, and so in particular contains no non-zero nilpotents, but there is an isomorphism

$$\mathbb{R}\otimes_{\mathbb{Q}} D \xrightarrow{\sim} \mathrm{M}(2,\mathbb{R}), \tag{4.3}$$

given by

$$i \mapsto \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{-2} \end{pmatrix}, \qquad j \mapsto \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}.$$

Let B denote a maximal order in D; i.e. B is a maximal $\mathbb{Z}$-subalgebra of D that is finitely generated as a $\mathbb{Z}$-module. (So B is like a "ring of integers" of D, although, unlike in the case of rings of integers in number fields, B is not unique, but is only unique up to conjugation by a non-zero element of D.) We can use the isomorphism (4.3) to regard B as a subring of $\mathrm{M}(2,\mathbb{R})$, and then define a discrete subgroup Γ of $\mathrm{SL}(2,\mathbb{R})$ via $\Gamma := B\bigcap \mathrm{SL}(2,\mathbb{R})$. Since D, and hence B, contains no non-zero nilpotents, the group Γ contains no non-identity unipotent elements. Thus $\Gamma\backslash\mathbb{H}^2$ is *compact*.

Now Γ is not torsion-free, and so the quotient $\Gamma\backslash\mathbb{H}^2$ is an orbifold rather than a manifold. However, by considering the reduction modulo n maps

$$B \to B/nB$$

for natural numbers n, we may define congruence subgroups of Γ analogous to $\Gamma(n)$ or $\Gamma_1(n)$, and so obtain many torsion-free finite index subgroups of Γ. In this way, we can construct infinitely many closed hyperbolic surfaces, with many finite covering maps between them. (And this is just for one particular choice of D!) We refer to these surfaces, obtained by choosing an appropriate $\mathbb{Q}$-algebra D as above, and then constructing the associated group Γ and its congruence subgroups, as *compact congruence quotients* of $\mathbb{H}^2$.

We can similarly construct compact congruence quotients of $\mathbb{H}^3$. We first choose a quadratic imaginary number field F. We then construct a 4-dimensional division algebra D over F. Since $\mathbb{C}$ is algebraically closed, there will automatically be an isomorphism

$$\mathbb{C} \otimes_F D \xrightarrow{\sim} \mathrm{M}(2, \mathbb{C}). \tag{4.4}$$

We then choose a maximal $\mathcal{O}_F$-order B in D, and using (4.4) to regard B as a subring of $\mathrm{M}(2, \mathbb{C})$, we then set $\Gamma := B \bigcap \mathrm{GL}(2, \mathbb{C})$. For any non-zero ideal $\mathfrak{n} \subset \mathcal{O}_F$, we can use the reduction map $B \to B/\mathfrak{n}B$ to define congruence subgroups of Γ analogous to $\Gamma_1(\mathfrak{n})$. All but finitely many of these congruence subgroups will be torsion-free, and the corresponding quotients of $\mathbb{H}^3$ will then be *compact*. We refer to the closed hyperbolic 3-manifolds constructed in this manner as *compact congruence quotients* of $\mathbb{H}^3$.

We now give a concrete example, which is directly relevant to the proof of Theorem 1.4. Begin by taking $F = \mathbb{Q}(\sqrt{-2})$. Let $\pi := 1 - \sqrt{-2}$, $\overline{\pi} := 1 + \sqrt{-2}$. Note that π and $\overline{\pi}$ are prime elements of $\mathcal{O}_F := \mathbb{Z}[\sqrt{-2}]$, and that $\pi\overline{\pi} = 3$. Let D be the associate F-algebra generated by elements i and j satisfying commutation relations

$$i^2 = -1, j^2 = -3, ij = -ji.$$

Then D is a division algebra. We take B to be a maximal order in D, and define Γ as above. Finally, for any $n \geq 0$ we define a congruence subgroup Γ_n of Γ analogous to $\Gamma_1(\pi^n)$. (We refer to [5, §2] for the precise definition.) Following [5], we write

$$X[\overline{\pi}\pi^n] := \Gamma_n \backslash \mathbb{H}^3.$$

(The notation reflects the choice of congruence subgroup, together with the fact that the construction of D involves the number $3 = \overline{\pi}\pi$.) If n is sufficiently large than Γ_n is torsion-free, and thus $X[\overline{\pi}\pi^n]$ is a closed hyperbolic 3-manifold.

Calegari and Dunfield prove the following result [5, §2], which has Theorem 1.4 as an immediate consequence.

4.8. **Theorem.** (1) *The injectivity radius of $X[\overline{\pi}\pi^n]$ grows without bound as $n \to \infty$.* (2) *Each $X[\overline{\pi}\pi^n]$ is a rational homology sphere.*

We will give the barest of sketches of the proof of this theorem in Subsection 5.7 below, which, as we have already emphasized, relies on the Langlands reciprocity conjecture.

4.9. **Automorphic forms, cohomology, and Hecke operators.** The reason that the reciprocity conjecture can be applied to the problem of computing the Betti numbers of congruence quotients is because there is a relationship between cohomology of congruence quotients and automorphic forms, which we now sketch.

Suppose that Γ is one of the (many) congruence subgroups of $\mathrm{SL}(2, \mathbb{R})$ (resp. $\mathrm{GL}(2, \mathbb{C})$) that we have defined. If the quotient $\Gamma\backslash\mathbb{H}^2$ (resp. $\Gamma\backslash\mathbb{H}^3$) is a closed manifold, then, as was remarked in Subsection 3.5, we may identify its ith cohomology group (with $\mathbb{C}$-coefficients) with the space of harmonic differential i-forms on $\Gamma\backslash\mathbb{H}^2$ (resp. $\Gamma\backslash\mathbb{H}^3$). (In fact, suitably interpreted, such a result holds true even when $\Gamma\backslash\mathbb{H}^2$ (resp. $\Gamma\backslash\mathbb{H}^3$) is not compact.) Now since $\Gamma\backslash\mathbb{H}^2 := \Gamma\backslash \mathrm{PSL}(2, \mathbb{R})/\mathrm{SO}(2)$ (resp. $\Gamma\backslash\mathbb{H}^3 := \Gamma\backslash \mathrm{PSL}(2, \mathbb{C})/\mathrm{SO}(3)$), we may pull-back a harmonic differential i-form on $\Gamma\backslash\mathbb{H}^2$ (resp. $\Gamma\backslash\mathbb{H}^3$) to obtain a certain kind of differential i-form on $\Gamma\backslash \mathrm{PSL}(2, \mathbb{R})$ (resp. $\Gamma\backslash \mathrm{PSL}(2, \mathbb{C})$), which may then be described explicitly in terms of a certain automorphic form on $\Gamma\backslash \mathrm{PSL}(2, \mathbb{R})$ (resp. $\Gamma\backslash \mathrm{PSL}(2, \mathbb{C})$). Since this automorphic

forms arises from a harmonic i-form, it will automatically be an eigenvector for the Casimir and higher Casimir operators (that were discussed in the introduction).

It will not necessarily be an eigenvector for the Hecke operators. However, we can define an action of the Hecke operators directly on the cohomology of $\Gamma\backslash\mathbb{H}^2$ (resp. $\Gamma\backslash\mathbb{H}^3$). If we then begin with a cohomology class that *is* an eigenvector for the Hecke operators on cohomology, then the corresponding automorphic form will be an eigenvector for the Hecke operators as well, and so will be an automorphic eigenform, in the sense of the introduction.

The Hecke operators on cohomology are defined by certain Hecke correspondences.[6] We won't give the general description of these correspondence, but will content ourselves with describing them in the very simplest case, namely for the quotient $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}^2$.

First, we need to define yet another species of congruence subgroup.

4.10. **Definition.** For any integer $n \geq 1$, the group $\Gamma_0(n) \subset \mathrm{SL}(2,\mathbb{Z})$ is defined to be the preimage under (4.1) of the subgroup of upper triangular matrices in $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$; i.e.

$$\Gamma_0(n) := \{\gamma \in \mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z}) \,|\, \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N\}.$$

Since $\Gamma_0(n) \subset \mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$, there is a natural projection $\mathrm{pr} : \Gamma_0(n)\backslash\mathbb{H}^2 \to \mathrm{SL}(2,\mathbb{Z})\backslash H^2$.

An easy calculation shows that the matrix $\begin{pmatrix} 0 & 1 \\ n & 0 \end{pmatrix}$ normalizes $\Gamma_0(n)$. Thus the automorphism of $\mathbb{H}^2$ induced by this matrix induces a corresponding automorphism of $\Gamma_0(n)\backslash\mathbb{H}^2$, which we denote by w_n.

Now, for any prime p, the pth Hecke correspondence T_p is defined by the following diagram:

$$\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}^2 \xleftarrow{\mathrm{pr}} \Gamma_0(p)\backslash\mathbb{H}^2 \xrightarrow{w_p} \Gamma_0(p)\backslash\mathbb{H}^2 \xrightarrow{\mathrm{pr}} \mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}^2,$$

or, in symbols, $T_p := \mathrm{pr} \circ w_p \circ \mathrm{pr}^{-1}$. (We obtain a correspondence, since pr is not one-one, and so pr^{-1} is multi-valued.) The operator induced by T_p on cohomology is called the pth Hecke operator. The T_p commute among themselves (essentially, because of the Chinese remainder theorem).

If we replace $\mathrm{SL}(2,\mathbb{Z})$ by $\Gamma_1(n)$ (for some $n \geq 1$), then we may form an analogous diagram for any p that does not divide n. Similarly, if $\Gamma\backslash\mathbb{H}^2$ is a compact congruence quotient, then we may construct an analogous diagram for all but finitely many p. In this way, we obtain a commuting family of operators on the cohomology of any such quotient, indexed by all but finitely many primes. One can make similar constructions after replacing $\mathbb{H}^2$ by $\mathbb{H}^3$.

As already noted, eigenvectors for the Hecke operators on cohomology of $\Gamma\backslash\mathbb{H}^2$ of $\Gamma\backslash\mathbb{H}^3$ give rise to automorphic eigenforms on $\Gamma\backslash\,\mathrm{PSL}(2,\mathbb{R})$ or $\Gamma\backslash\,\mathrm{PSL}(2,\mathbb{C})$.

[6] A correspondence is a multi-valued continuous map. Cohomology is not only contravariantly functorial under continuous maps, but under correspondences: heuristically, one pulls back a cohomology class under each choice of single valued "branch" of the correspondence, and then sums the results.

5. Two-dimensional Galois representations and the Langlands' reciprocity conjecture for GL_2

In this section we begin by explaining how an elliptic curve defined over a number field gives rise to a family of Galois representations, which encode Diophantine information related to the curve. These are the basic examples of families of Galois representations of the type that appear in Conjecture 1.7. We then state a slightly more precise form of this conjecture in the context of congruence subgroups of $\mathrm{PSL}(2,\mathbb{R})$ or $\mathrm{PSL}(2,\mathbb{C})$. Finally, we explain various implications of the conjecture, including Fermat's Last Theorem (which is now a theorem of Wiles, since, together with Taylor, he was able to prove the relevant case of the reciprocity conjecture in this context), Theorem 1.4 (proved conditionally on the reciprocity conjecture by Calegari and Dunfield [5], but then unconditionally by Boston and Ellenberg [3]), and the virtual positive Betti number conjecture in the case of congruence quotients.

5.1. **Elliptic curves.** Let F be a number field. An *elliptic curve* E over F is an equation of the form $y^2 = x^3 + ax^2 + bx + c$, with $a, b, c \in F$, for which the cubic $x^3 + ax^2 + bx + c$ is separable (i.e. has distinct roots). Our goal in this subsection is to explain how E gives rise to representations of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

We begin by considering the set of complex solutions to E in $\mathbb{C}^2$. This set is a manifold[7] that is homeomorphic to a torus with 1 point removed. We can naturally adjoin this missing point as a "point at infinity" to the set of solutions of E (equivalently, consider the set of solutions not just in $\mathbb{C}^2$, but in the complex projective plane $\mathbb{C}P^2$). We denote this completed set of solutions by $E(\mathbb{C})$; it is topologically a torus.

Now a torus is homeomorphic to the quotient $\mathbb{R}^2/\mathbb{Z}^2$, and so admits not just the structure of a topological space, but the structure of an abelian topological group (thinking of it as a quotient of the additive topological group $\mathbb{R}^2$). We can then transport this group structure back to $E(\mathbb{C})$, and ask whether is has any intrinsic meaning.

The answer is *yes*: the set $E(\mathbb{C})$ does have an intrinsic abelian group structure. More precisely, the point at infinity is the identity for this group structure, while three points $P, Q, R \in E(\mathbb{C})$ sum to zero in this group structure precisely if they are collinear. One can check[8] that these two rules do indeed define an abelian group structure on $E(\mathbb{C})$. As we have more-or-less already stated, there is then an isomorphism of topological groups $E(\mathbb{C}) \xrightarrow{\sim} \mathbb{R}^2/\mathbb{Z}^2$.

If $n \geq 1$ is a positive integer, then the n-torsion subgroup of $\mathbb{R}^2/\mathbb{Z}^2$ (i.e. the kernel of multiplication by n) is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$. Thus, if we write $E[n]$ to denote the n-torsion subgroup of $E(\mathbb{C})$, there is an isomorphism $E[n] \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^2$.

Now, the points of $E[n]$ are obtained by solving an (increasingly elaborate, as n gets large) series of equations involving intersecting various lines with the elliptic curve E. Since the coefficients of the equation giving rise to E lie in F, we see

[7] It is here that the assumption that $x^3 + ax^2 + bx + c$ has distinct roots is used.

[8] This check is non-trivial. One relies very much on the fact that since the points in $E(\mathbb{C})$ are solutions to a *cubic* equation in x and y, any line meets $E(\mathbb{C})$ in exactly three points (counted with the correct multiplicities), by Bézout's Theorem. With this observation in hand one can check that the two stated rules give a well-defined commutative binary operation, with inverses. The verification of associativity remains a non-trivial application of Bézout's Theorem, together with some related projective geometry.

that this series of equations again has coefficients lying in F. Thus the coordinates of the points of $E[n]$ are algebraic over $\overline{\mathbb{Q}}$, i.e. $E[n] \subset E(\overline{\mathbb{Q}})$ (the subset of $E(\mathbb{C})$ consisting of points having algebraic number coordinates), and $E[n]$ is preserved under the natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

Now comes the punchline: the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ on $E[n]$ induces a homomorphism

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{Aut}(E[n]) \xrightarrow{\sim} \mathrm{Aut}\big((\mathbb{Z}/n\mathbb{Z})^2\big) = \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}).$$

In short, the elliptic curve E gives rise to a family of two-dimensional representations $\rho_{E,n}$ of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, with coefficients in the various rings $\mathbb{Z}/n\mathbb{Z}$.

5.2. **The Diophantine significance of $\rho_{E,n}$.** As in the preceding section, let E denote an elliptic curve over the number field F, given by the equation $y^2 = x^3 + ax^2 + bx + c$. Let $\mathcal{O}_F$ denote the ring of integers of F. Suppose that $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_F$ satisfying the following two properties: (a) $\mathfrak{p}$ does not contain the denominators of any of a, b, or c; (b) $\mathfrak{p}$ does not divide the discriminant of $x^3 + ax^2 + bx + c$. Then, by virtue of (a), we may reduce a, b, and c modulo $\mathfrak{p}$, to obtain elements $\overline{a}$, $\overline{b}$, and $\overline{c}$ in the field $\mathbb{F} := \mathcal{O}_F/\mathfrak{p}$. By virtue of (b), the cubic $x^3 + \overline{a}x^2 + \overline{b}x + \overline{c}$ has distinct roots in $\mathbb{F}[x]$, and so $y^2 = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c}$ defines an elliptic curve $\overline{E}$ over $\mathbb{F}$. Let $\overline{E}(\mathbb{F})$ denote the set of solutions in $\mathbb{F}$ to the equation defining $\overline{E}$ (including the one point at infinity), and write[9]

$$a_{\mathfrak{p}} := 1 + |\mathbb{F}| - |\overline{E}(\mathbb{F})|.$$

(Here we have written $|X|$ to denote the order of the finite set X.)

The quantities $a_{\mathfrak{p}}$ are of interest from a Diophantine point of view; they describe the number of the solutions to the various congruences $\overline{E}$ induced by the equation E. The following proposition shows that they may be recovered from the family of Galois representations $\rho_{E,n}$ attached to E. We first recall that algebraic number theory associates to each non-zero prime ideal a canonical element[10] $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

5.3. **Proposition.** *For each prime $\mathfrak{p}$, the trace of $\rho_{E,n}(\mathrm{Frob}_{\mathfrak{p}})$ is congruence to $a_{\mathfrak{p}}$ mod n.*

The Cebotarev density theorem shows that the elements $\mathrm{Frob}_{\mathfrak{p}}$ are dense in the group $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$. Thus, knowing all the quantities $a_{\mathfrak{p}}$ is equivalent to knowing the characters of all the representations $\rho_{E,n}$. This in turn is essentially[11] equivalent

[9]The number of points on a projective line over $\mathbb{F}$ is equal to $|\mathbb{F}| + 1$ (there are the elements of $\mathbb{F}$ together with the point at infinity). The quantity $a_{\mathfrak{p}}$ may thus be regarded as measuring the extent to which number of points on the elliptic curve $\overline{E}$ over $\mathbb{F}$ deviates from the number of points on the projective line.

[10]In fact, $\mathrm{Frob}_{\mathfrak{p}}$ is not an element, but a conjugacy class of cosets. Precisely, if $D_{\mathfrak{p}} \subset \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ is choice of decomposition group at $\mathfrak{p}$ — and such a choice is well-defined up to conjugation — then $\mathrm{Frob}_{\mathfrak{p}}$ is a canonically determined element of the quotient $D_{\mathfrak{p}}/I_{\mathfrak{p}}$, where $I_{\mathfrak{p}}$ denotes the inertia subgroup of $D_{\mathfrak{p}}$. In what follows, it will not cause any harm to speak as if $\mathrm{Frob}_{\mathfrak{p}}$ is in fact a well-determined element of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

[11]Since $\rho_{E,n}$ is defined over the ring $\mathbb{Z}/n\mathbb{Z}$, which is not a field in general, it is not the case in general that $\rho_{E,n}$ is determined by its character. But this is a technical detail, which can safely be ignored for the sake of the present discussion.

to knowing all the Galois representations $\rho_{E,n}$. Thus the family of Galois representations $\rho_{E,n}$ is an algebraic package that encodes the collection of interesting Diophantine data $a_{\mathfrak{p}}$.

5.4. **Reciprocity.** We are now in a position to state a slightly more precise form of Conjecture 1.7. We let F denote either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d})$ for some square-free $d > 0$. In the first case, let Γ either be a congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$, or else a congruence subgroup associated to a 4-dimensional division algebra over $\mathbb{Q}$ as in Subsection 4.7. In the second case, let Γ either be a congruence subgroup of $\mathrm{GL}(2,\mathcal{O}_F)$, or else a congruence subgroup associated to a 4-dimensional division algebra over F as in Subsection 4.7.

In the first case, we consider automorphic eigenforms on $\Gamma\backslash \mathrm{PSL}(2,\mathbb{R})$. In the second case, we consider automorphic eigenforms on $\Gamma\backslash \mathrm{PSL}(2,\mathbb{C})$. In either case, there is a Hecke operator associated to all but finitely many non-zero prime ideals[12] $\mathfrak{p}$ in $\mathcal{O}_F$, and so if f is an automorphic Hecke eigenform, it has an associated Hecke eigenvalue $a_{\mathfrak{p}}$ for all but finitely many $\mathfrak{p}$.

5.5. **Conjecture.** (a) *If f is an automorphic Hecke eigenform, whose (suitably normalized) eigenvalue under the Casimir is integral, then the eigenvalues $a_{\mathfrak{p}}$ are algebraic integers, lying in the ring of integers $\mathcal{O}_L$ of some number field L, and for every non-zero ideal $\mathfrak{n} \subset \mathcal{O}_L$, there is a representation $\rho_{f,\mathfrak{n}} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}(2,\mathcal{O}_L/\mathfrak{n})$ with the property that $a_{\mathfrak{p}}$ is congruent mod $\mathfrak{n}$ to the trace of $\rho_{f,\mathfrak{n}}(\mathrm{Frob}_{\mathfrak{p}})$ for all but finitely many non-zero prime ideals $\mathfrak{p} \subset \mathcal{O}_F$.*

(b) *Suppose given a number field L, and a family of Galois representations $\rho_{\mathfrak{n}} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}(2,\mathcal{O}_L/\mathfrak{n})$, such that the traces of $\rho_{f,\mathfrak{n}}(\mathrm{Frob}_{\mathfrak{p}})$ are compatible (in an obvious sense) as $\mathfrak{n}$ varies, for all but finitely many non-zero prime ideals $\mathfrak{p} \subset \mathcal{O}_F$, and satisfying some other technical conditions which we suppress. Then there exists an automorphic Hecke eigenform f as in* (a) *such that $\rho_{\mathfrak{n}} = \rho_{f,\mathfrak{n}}$ for all $\mathfrak{n}$.*

If E is an elliptic curve over F, then we can take $L = \mathbb{Q}$, and the family of representations $\rho_{E,n}$ is one to which part (b) of the conjecture should apply. Thus every elliptic curve is conjectured to be associated to an automorphic eigenform, in the sense of the conjecture. Taking into account Proposition 5.3, we see that the Hecke eigenvalues of the eigenform encode the number of points on E modulo the various prime ideal $\mathfrak{p}$.

5.6. **Fermat's Last Theorem.** In the papers [13, 14], Taylor and Wiles proved part (b) of the reciprocity conjecture for the Galois representations arising from (most[13]) elliptic curves over the field $\mathbb{Q}$ of rational numbers. The conjecture in this case (which predates Langlands' more general conjecture, and was known as the Shimura-Taniyama, or Shimura-Taniyama-Weil, conjecture) famously implies Fermat's Last Theorem. Let us very briefly sketch the reason why (following the strategy due to Frey and Serre).

Fermat's Last Theorem for the exponent 3 was proved by Euler, and for the exponent 4 by Fermat himself. Suppose then that $u^p + v^p = w^p$ for some prime

[12] In fact, this is correct only if $\mathcal{O}_F$ has class number 1; otherwise, the situation is slightly more complicated. We suppress this technical detail.

[13] More precisely, they proved the conjecture for those Galois representations arising from so-called *semi-stable* elliptic curves over $\mathbb{Q}$. The conjecture for Galois representations arising from arbitrary elliptic curves was completely established in [4].

$p \geq 5$ and some integers u, v, and w. We can form the elliptic curve E with equation

$$y^2 = x(x - u^p)(x + v^p).$$

This elliptic curve gives rise to its Galois representations $\rho_{E,n}$, and hence, via the reciprocity conjecture, to an automorphic eigenform f. This automorphic eigenform will in turn contribute to the H^1 of some compact congruence quotient of $\mathbb{H}^2$. Moreover, a careful investigation of the properties of the Galois representations $\rho_{E,n}$, and in particular of the representation $\rho_{E,p}$, due to Ribet [10], allows one to compute this congruence quotient precisely.[14] A direct computation then shows that this particular congruence quotient has genus 0, and hence that $H^1 = 0$. Consequently, the eigenform can't exist, and thus neither can the solution to Fermat's Last Theorem.

5.7. **Rational homology spheres.** To prove Theorem 4.8, Calegari and Dunfield show that the reciprocity conjecture implies that each of the manifolds $X[\overline{\pi}\pi^n]$ has trivial first Betti number. The proof is by contradiction: Suppose that some $X[\overline{\pi}\pi^n]$ has positive first Betti number. Then there is a non-zero eigenvector for the Hecke operators in $H^1(X[\overline{\pi}\pi^n], \mathbb{C})$, whose harmonic representative will be an automorphic eigenform. Part (a) of the reciprocity conjecture implies that this eigenform gives rise to a family of Galois representations. Analyzing the properties of the resulting Galois representations, one finds that in fact they cannot exist![15] Thus b_1 must vanish after all.

We won't attempt to explain here the Galois-theoretic argument that rules out the existence of these representations. We mention only that it relies on the fact that $F := \mathbb{Q}(\sqrt{-2})$ has fairly small discriminant (-8), and that $\pi\overline{\pi} = 3$, which is a small prime.

Although great progress has been made on part (a) of the reciprocity conjecture in the case when F is quadratic imaginary (by Taylor, et. al. [7, 11]), it is not known in sufficient generality to make the argument of [5] unconditional. (Another, unconditional, proof of Theorem 1.4 has been found by Boston and Ellenberg.) Never the less, the reciprocity conjecture is certainly believed to be true, and the argument of Calegari and Dunfield gives a good indication of the range of its influence in diverse areas of mathematics.

5.8. **The virtual positive Betti number conjecture for congruence quotients of $\mathbb{H}^3$.** We close this note by observing that the reciprocity conjecture implies the virtual positive Betti number conjecture for compact congruence quotients

[14] One can reasonably ask where the property that (u, v, w) solves the Fermat equation is actually used. The answer is as follows: the discriminant of the cubic $x(x - u^p)(x + v^p)$ is equal to $-u^p v^p (u^p + w^p) = (-uvw)^p$, and in particular is a perfect pth power. Because of this, the representation $\rho_{E,p}$ is endowed with rather remarkable properties — too remarkable, as it turns out, for it to even exist.

This is not the place to explain carefully how the nature of the discriminant influences the properties of the representation $\rho_{E,p}$. But it may help to mention a simpler, but related, Galois-theoretic phenomenon: if $f(x) \in \mathbb{Q}[x]$ is an irreducible degree n polynomial, then the Galois group of the splitting field of $f(x)$ is a subgroup of the symmetric group S_n, and is typically equal to this group. However, if the discriminant of $f(x)$ is a square, then the Galois group in fact lies inside the alternating group A_n.

[15] In the non-existence proof as it is written in [5], the Generalized Riemann Hypothesis is also required. However, Calegari has informed me that in fact the argument can be made to work without it.

of $\mathbb{H}^3$. Fix $F = \mathbb{Q}(\sqrt{-d})$, and a 4-dimensional division algebra D over F, as in Subsection 4.7. If Γ_1 and Γ_2 are two congruence subgroups of $\mathrm{GL}(2,\mathbb{C})$ arising from these choices, then $\Gamma_1 \bigcap \Gamma_2$ has finite index in each of Γ_1 and Γ_2, and so $(\Gamma_1 \bigcap \Gamma_2)\backslash\mathbb{H}^3$ is a common finite cover of each of $\Gamma_1\backslash\mathbb{H}^3$ and $\Gamma_2\backslash\mathbb{H}^3$. Taking into account Lemma 3.6, it thus suffices to exhibit one Γ (arising from the particular choice of F and D) for which $\Gamma\backslash\mathbb{H}^3$ has positive first Betti number. For this, it suffices to exhibit a certain kind of non-zero automorphic eigenform. If one grants the reciprocity conjecture (in particular, part (b) of the conjecture), then to do this, it suffices in turn to write down certain kinds of Galois representations. Now one can write down lots of elliptic curves over the quadratic imaginary field F, so many in fact that one can find plenty of the required kinds of Galois representations. This proves the result.

References

1. Borel A., *Automorphic L-functions*, in Automorphic Forms, Representations, and L-functions (A. Borel, W. Casselman ed.), Proc. Symp. Pure Math. **33**, part 2, Amer. Math. Soc., Providence, RI (1979), 27–61.
2. Borel A., Jacquet H., *Automorphic forms and automorphic representations*, in Automorphic Forms, Representations, and L-functions (A. Borel, W. Casselman ed.), Proc. Symp. Pure Math. **33**, part 1, Amer. Math. Soc., Providence, RI (1979), 189–202.
3. Boston N., Ellenberg J. S., *Pro-p groups and towers of rational homology spheres*, Geom. Topol. **10** (2006), 331–334.
4. Breuil C., Conrad B., Diamond F., Taylor R., *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.
5. Calegari F., Dunfield N., *Automorphic forms and rational homology 3-spheres*, Geom. Topol. **10** (2006), 295–329.
6. Gross B. H., *On the Satake isomorphism*, in Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser. **254**, Cambridge Univ. Press, Cambridge (1998), 223–237.
7. Harris M., Soudry D., Taylor R., *l-adic representations associated to modular forms over imaginary quadratic fields. II.*, Invent. Math. **114** (1993), 289–310.
8. Kirby R. C., *Problems in low-dimensional topology*, in Geometric topology (Athens, GA, 1993), AMS/IP Stud. Adv. Math. 2.2, Amer. Math. Soc., Providence, RI (1997), 35–473.
9. Reid A., *The geometry and topology of arithmetic hyperbolic 3-manifolds*, to appear in Proc. Symposium Topology, Complex Analysis and Arithmetic of Hyperbolic Spaces, Kyoto 2006, RIMS Kokyuroku Series.
10. Ribet K.A., *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
11. Taylor R. L., *l-adic representations associated to modular forms over imaginary quadratic fields. II.*, Invent. Math. **116** (1994), 619–643.
12. Taylor R. L., *Galois representations*, Ann. Fac. Sci. Toulouse Math. (6) **13** (2004), 73–119.
13. Taylor R., Wiles A.J., *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), 553–572.
14. Wiles A.J., *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), 443–551.

E-mail address: emerton@math.northwestern.edu

Mathematics Department, Northwestern University, 2033 Sheridan Rd., Evanston, IL 60208

E-mail address: emerton@math.northwestern.edu