BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 37, Number 2, Pages 119–140
S 0273-0979(99)00856-3
Article electronically published on December 21, 1999

FROM DYNAMICS ON SURFACES TO RATIONAL POINTS ON CURVES

CURTIS T. MCMULLEN

M. Jourdain: *You mean when I say, 'Nicole, bring me my slippers...', I'm speaking in prose?*

—Molière, 1670

1. Introduction

Fermat's last theorem states that for $n \geq 3$ the equation

$$X^n + Y^n = Z^n \tag{1}$$

has no integer solutions with $X, Y, Z \geq 1$. Inspiring generations of work in number theory, its proof was finally achieved by Wiles. A qualitative result, Finite Fermat, was obtained earlier by Faltings; it says the Fermat equation has only a *finite* number of solutions (for each given n, up to rescaling).

This paper is an appreciation of some of the topological intuitions behind number theory. It aims to trace a logical path from the classification of surface diffeomorphisms to the proof of Finite Fermat. The route we take is the following:

§2. The isotopy classes of surface diffeomorphisms $f : S \to S$ form the *mapping class group* $\mathrm{Mod}(S)$. Thurston showed the elements of $\mathrm{Mod}(S)$ can be classified into 3 types, depending on their dynamics: finite order, reducible and pseudo-Anosov. We begin by explaining a complex-analytic approach to this classification, using the geometry of the moduli space $\mathcal{M}_g$ of Riemann surfaces of genus g.

§3. An analytic family of Riemann surfaces C/B determines a classifying map $B \to \mathcal{M}_g$ and a monodromy map $\pi_1(B) \to \pi_1(\mathcal{M}_g) = \mathrm{Mod}(S)$. Continuing the study of moduli space, we sketch the Imayoshi-Shiga proof that there are only finitely many families (truly varying and of fixed genus) over a fixed 1-dimensional base B. A key step is to show that a family is determined by its monodromy.

§4. Next we present Parshin's trick, using branched coverings, to deduce the finiteness of sections $s : B \to C$ from the finiteness of families C/B.

§5. To begin the transition to algebra, we connect Galois theory to the fundamental group, homology and monodromy.

§6. Finally we sketch Falting's proof of Finite Fermat. Let C be the Riemann surface defined by the Fermat equation (1). Arithmetically, we think of this curve as a family spread out over a base $B = \operatorname{Spec} \mathbb{Z} - S$ consisting of (most

Received by the editors February 1999, and in revised form September 22, 1999.
2000 *Mathematics Subject Classification.* Primary 11G30; Secondary 32G15, 57Mxx.
Research partially supported by the NSF.

of) the prime numbers. An integral solution can be reduced mod p, so it determines a section of C/B. The role of the monodromy is played by the action of the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$ on the homology of C. By controlling the dynamics of the Galois group, we find there are just finitely many families C/B, hence finitely many sections of C/B, hence finitely many solutions to the Fermat equation (1).

In retrospect it seems Fermat, like his contemporary M. Jourdain, was unwittingly speaking of not just number theory but topology.

This paper is based on a lecture given at MSRI in 1997 in recognition of Thurston's term as director, 1992-97, and was inspired in part by an essay of Littlewood [Lit]. For historical accounts and detailed proofs of the developments we outline here, see the references and notes collected at the end. I would like to thank B. Mazur, R. Taylor and the referees for their help.

2. Complex analysis and dynamics on surfaces

Let S be a smooth oriented surface of genus $g \geq 0$. By a *simple loop* $\alpha \subset S$ we mean an unoriented embedded circle that cannot be shrunk to a point. Let $\mathcal{S}$ be the set of isotopy classes of simple loops on S. The *intersection pairing*

$$i : \mathcal{S} \times \mathcal{S} \to \{0, 1, 2, 3, \ldots\}$$

is defined so $i(\alpha, \beta)$ is the minimum possible number of transverse intersections between representatives of α and β.

The *mapping class group* $\mathrm{Mod}(S)$ is the group of isotopy classes of orientation-preserving diffeomorphism $f : S \to S$; the group law is composition. There is a natural action of $\mathrm{Mod}(S)$ on $(\mathcal{S}, i)$.

In this section we discuss a *dynamical* classification of elements of $\mathrm{Mod}(S)$ that sheds light on the behavior of their iterates $f^n : S \to S$.

Example: the torus. For $g = 1$, we have $\mathrm{Mod}(S) \cong SL_2(\mathbb{Z})$ because the mapping class group acts faithfully on the homology $H_1(S, \mathbb{Z}) \cong \mathbb{Z}^2$. Moreover, a simple loop can be recorded by its slope in homology, giving an isomorphism between $\mathcal{S}$ and the rational points on a circle:

$$\mathcal{S} = \mathbb{P}H_1(S, \mathbb{Q}) \cong \mathbb{P}(\mathbb{Q}^2) \subset \mathbb{RP}^1 = \mathbb{R} \cup \{\infty\}.$$

Then $\mathrm{Mod}(S)$ acts on $\mathcal{S}$ by Möbius transformations, preserving the form

$$i\left(\frac{p}{q}, \frac{r}{s}\right) = \left|\det \begin{pmatrix} p & r \\ q & s \end{pmatrix}\right|.$$

The automorphisms of a torus can be classified into 3 types, depending on their dynamical behavior.

1. *Finite order.* The mapping $f_* : H_1(S, \mathbb{R}) \to H_1(S, \mathbb{R})$ has complex eigenvalues, and $f^n = \mathrm{id}$ for some $n > 0$.
2. *Reducible.* The map f_* has a multiple eigenvalue of ± 1. Then f preserves a rational slope $p/q \in \mathbb{P}H_1(S, \mathbb{R})$, and so it *stabilizes* a simple loop $\alpha \in \mathcal{S}$. Thus f or f^2 is a Dehn twist about α.
3. *Anosov.* The mapping f_* has real eigenvalues $K^{\pm 1}$, preserving a pair of irrational slopes $\lambda_\pm \in \mathbb{P}H_1(S, \mathbb{R})$.

   Using the identification $S \cong \mathbb{R}^2/\mathbb{Z}^2$, the linear action of $f_* \in SL_2(\mathbb{Z})$ gives a linear, area-preserving map $F : S \to S$ isotopic to f. In the Anosov case, F preserves the pair of foliations $\mathcal{F}_\pm$ of S by lines of slope $\lambda_\pm$. The leaves of $\mathcal{F}_+$

are stretched by a factor of K, and those of $\mathcal{F}_-$ are shrunk by $1/K$. For any $\alpha, \beta \in \mathcal{S}$, the loop $F^n(\alpha)$ is nearly parallel to $\mathcal{F}_+$, with length comparable to K^n; thus the intersection number satisfies

$$i(F^n(\alpha), \beta) \asymp K^n \to \infty \tag{2}$$

as $n \to \infty$.

Higher genus. Now suppose S has genus $g \geq 2$. To generalize the classification above, let us say $f \in \mathrm{Mod}(S)$ is:

2′. *Reducible* if there exists a finite set $\alpha_1, \ldots, \alpha_n \in \mathcal{S}$, permuted by f, with $i(\alpha_i, \alpha_j) = 0$; and
3′. *Pseudo-Anosov* if there is an expansion factor $K > 1$ such that the intersection number $i(f^n(\alpha), \beta)$ grows like K^n for all $\alpha, \beta \in \mathcal{S}$.

Our main goal in this section is to sketch the proof of Thurston's result:

Theorem 2.1 (Classification of Surface Diffeomorphisms)**.** *Any mapping class* $f \in \mathrm{Mod}(S)$ *is either reducible, pseudo-Anosov or of finite order.*

In the pseudo-Anosov case, the proof also furnishes foliations of S with isolated singularities whose leaves are stretched by $K^{\pm 1}$ under a suitable representative of f.

Remark on surface bundles. An S-bundle $C \to B$ determines a *monodromy representation*

$$\pi_1(B) \to \mathrm{Mod}(S)$$

recording the twisting of the fibers under transport around loops in the base. The simplest case is that of a 3-manifold fibering over the circle, $M^3 \to S^1$; then the image of $\pi_1(S^1)$ is a cyclic group $\langle f \rangle \subset \mathrm{Mod}(S)$. Thurston has shown M^3 admits a metric of constant negative curvature iff f is pseudo-Anosov.

Riemann surfaces. The proof of the classification we present is motivated by:

Theorem 2.2. *Let X be a compact Riemann surface of genus $g \geq 2$. Then the conformal automorphism group* $\mathrm{Aut}(X)$ *is finite, and any isotopy class* $f \in \mathrm{Mod}(X)$ *is represented by at most one conformal map.*

To see this finiteness, first recall a Riemann surface of genus 2 or more is *hyperbolic*; that is, the universal cover $\widetilde{X}$ of X is isomorphic to the unit disk $\Delta \subset \mathbb{C}$. Thus X is the quotient of Δ by a conformal action of $\pi_1(X) \subset \mathrm{Aut}(\Delta)$ (Figure 1). Since $\mathrm{Aut}(\Delta)$ preserves the metric

$$\rho = \frac{2\,|dz|}{1 - |z|^2} \tag{3}$$

of constant curvature -1 on Δ, we obtain a *hyperbolic metric* on X canonically determined by its conformal structure.

The classical *Schwarz Lemma* states that a holomorphic map $f : X \to Y$ between hyperbolic Riemann surfaces can only shrink the hyperbolic metric; that is,

$$d(f(x), f(x')) \leq d(x, x')$$

for all $x, x' \in X$. In particular, $\mathrm{Aut}(X)$ acts by isometries.

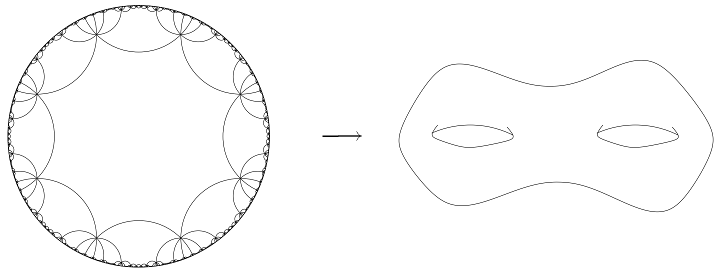

FIGURE 1. A surface of genus 2 covered by the hyperbolic disk

Proof of Theorem 2.2. Let $f, g : X \to X$ be a pair of isotopic conformal maps. Since X is compact, in the course of the isotopy points move only a bounded distance D. Lifting to the universal cover, we obtain a pair of analytic maps $\widetilde{f}, \widetilde{g} : \Delta \to \Delta$ with $d(f(x), g(x)) \leq D$ in the hyperbolic metric (3). Since the ratio of Euclidean to hyperbolic distance tends to zero at the boundary of the disk, we have $\widetilde{f} = \widetilde{g}$ on S^1. But an analytic map is determined by its boundary values, so $\widetilde{f} = \widetilde{g}$ and thus $f = g$.

Thus the natural map $\mathrm{Aut}(X) \to \mathrm{Mod}(X)$ is injective; in particular, $\mathrm{Aut}(X)$ is discrete. On the other hand, $\mathrm{Aut}(X)$ is also compact, because it preserves the hyperbolic metric on X; thus the automorphism group of X is finite. $\square$

Teichmüller space. To relate $\mathrm{Mod}(S)$ to $\mathrm{Aut}(X)$, we now introduce the *Teichmüller space* $\mathrm{Teich}(S)$ of all complex structures on S.

A point in $\mathrm{Teich}(S)$ is specified by a Riemann surface X together with a diffeomorphism $h : S \to X$. The map h provides a *marking* of X by S; for example, it gives an identification between $\pi_1(S)$ and $\pi_1(X)$. Two marked surfaces $(h : S \to X)$ and $(g : S \to Y)$ define the same point in $\mathrm{Teich}(S)$ if $g \circ h^{-1} : X \to Y$ is isotopic to a conformal map.

The mapping-class group $\mathrm{Mod}(S)$ acts on $\mathrm{Teich}(S)$ by changing the marking; that is, $f \in \mathrm{Mod}(S)$ acts by

$$f \cdot (h : S \to X) = (h \circ f^{-1} : S \to X).$$

The *moduli space* of Riemann surfaces of genus $g = g(S)$ is the quotient space:

$$\mathcal{M}(S) = \mathrm{Teich}(S)/\,\mathrm{Mod}(S).$$

From the definitions it is immediate that $f \cdot X = X$ in $\mathrm{Teich}(S)$ if and only if f is represented by a conformal automorphism of X. But $\mathrm{Aut}(X)$ is finite, so we can then conclude that f has finite order. Thus to classify elements $f \in \mathrm{Mod}(S)$, one is led to consider the dynamics of f on Teichmüller space.

Length functions. Next we introduce the *geodesic length* functions

$$\ell : \mathcal{S} \times \mathrm{Teich}(S) \to \mathbb{R}_+,$$

assigning to each simple loop $\alpha \subset S$ the length $\ell_\alpha(X)$ of the geodesic representative of $h(\alpha)$ in the hyperbolic metric on X. These ℓ_α provide coordinates making $\mathrm{Teich}(S)$ into a smooth manifold, diffeomorphic to a ball of dimension $6g - 6$.

By Gauss-Bonnet, the hyperbolic area of X is a constant, $\pi(4g - 4)$. Thus the only way the shape of X can degenerate is by a thin neck pinching off. More precisely, letting

$$L(X) = \inf\{\ell_\alpha(X)\}$$

denote the length of the shortest geodesic loop on X, we have:

Theorem 2.3 (Mumford). *For any $r > 0$, $\{X \,:\, L(X) \geq r\}$ is a compact subset of the moduli space $\mathcal{M}(S)$.*

A short geodesic is the core of a long, thin tube, and we have:

Proposition 2.4. *There is an $\epsilon_0 > 0$ such that if:*

$$\{\alpha_1, \ldots, \alpha_n\} = \{\alpha \,:\, \ell_\alpha(X) < \epsilon_0\},$$

then $i(\alpha_i, \alpha_j) = 0$ and $n \leq 3g - 3$.

The count $3g - 3$ is purely topological: it is the maximum number of disjoint simple loops on S with no pair isotopic.

Distance between Riemann surfaces. As a final ingredient to the study of surface diffeomorphisms, we introduce a metric on $\operatorname{Teich}(S)$ such that $\operatorname{Mod}(S)$ acts by isometries.

The *Teichmüller metric* is defined by

$$d(X, Y) = \frac{1}{2} \log \inf \left\{ K \geq 1 \;:\; \begin{array}{c} \text{there exists a } K\text{-quasiconformal map} \\ f : X \to Y \text{ respecting markings} \end{array} \right\}.$$

Here a diffeomorphism $f : X \to Y$ is *K-quasiconformal* if $f' : \mathrm{T}X \to \mathrm{T}Y$ sends infinitesimal circles to ellipses with major and minor axes in ratio $1 \leq M/m \leq K$. Just as conformal maps are hyperbolic isometries, quasiconformal maps distort lengths of closed geodesics by a bounded factor; we have:

$$\frac{1}{K}\ell_\alpha(X) \leq \ell_\alpha(Y) \leq K\ell_\alpha(X) \tag{4}$$

when there is a K-quasiconformal map $f : X \to Y$.

Proof of Theorem 2.1 (Classification of Surface Diffeomorphisms). Since $\operatorname{Teich}(S)$ is simply-connected, we can identify $\operatorname{Mod}(S)$ with $\pi_1(\mathcal{M}(S))$, the orbifold fundamental group of moduli space. A mapping-class f then determines a free homotopy class of loop $\gamma : S^1 \to \mathcal{M}(S)$. The strategy of the proof is to seek the shortest representative of γ.

To this end, define the *translation length* of f by

$$\tau(f) = \inf_{X \in \operatorname{Teich}(S)} d(X, f \cdot X). \tag{5}$$

We distinguish 3 cases.

I. $\tau(f) = 0$, **achieved.** If f has a fixed-point $X \in \operatorname{Teich}(S)$, then by definition the marking $h : S \to X$ transfers f to the isotopy class of a conformal automorphism $F : X \to X$. Since $\operatorname{Aut}(X)$ is finite, F has finite order, so f has finite order as well.

II. $\tau(f) > 0$, **achieved.** Next suppose we can find a Riemann surface such that $d(X, f \cdot X) = \tau(f) > 0$. Then the isotopy class of f can be represented by a K^2-quasiconformal map $F : X \to X$, where $K = \exp(\tau(f)) > 1$. By a theorem of Teichmüller, outside a finite set of singularities there exist complex charts in the domain and range such that this optimal map F is an affine stretch:

$$F(x + iy) = \frac{x}{K} + iKy.$$

Because $d(X, f \cdot X)$ is minimized, the lines of stretch are preserved by F, defining a pair of invariant singular foliations $\mathcal{F}_\pm$ whose leaves are stretched by $K^{\pm 1}$. Thus for $\alpha, \beta \in \mathcal{S}$, the loop $F^n(\alpha)$ is stretched along $\mathcal{F}_+$ as $n \to \infty$, so the intersection number satisfies

$$i(F^n(\alpha), \beta) \asymp K^n$$

and f is pseudo-Anosov.

III. $\tau(f)$ is not achieved. Finally, suppose the infimum in (5) is not achieved. Consider a sequence $X_n \in \mathrm{Teich}(S)$ with $d(X_n, f \cdot X_n) \to \tau(f)$. The corresponding loops $\gamma_n : S^1 \to \mathcal{M}(S)$ must exit every compact subset of moduli space, else we could extract a convergent subsequence. Thus by Mumford's theorem the length of the shortest hyperbolic geodesic on X_n must shrink to zero. We will show the short geodesics on X_n reveal the reducibility of the mapping-class f.

Since $d(X_n, f \cdot X_n)$ is bounded, there is a uniform K such that f is represented by a K-quasiconformal map

$$F_n : X_n \to X_n.$$

Let $\epsilon = \epsilon_0 / K^{3g-3}$, and choose n large enough such that the shortest loop $\gamma \in \mathcal{S}$ on X_n has length $\ell_\gamma(X_n) < \epsilon$.

Let

$$A = \{\alpha \ : \ \ell_\alpha(X_n) < \epsilon_0\} \subset \mathcal{S}$$

be the set of all isotopy classes of short loops on X_n; then $|A| \leq 3g-3$ by Proposition 2.4. On the other hand, the bound (4) on the length distortion of K-quasiconformal maps implies the loops

$$\langle \gamma, F_n(\gamma), F_n^2(\gamma) \ldots, F_n^{3g-3}(\gamma) \rangle$$

have lengths less than

$$\langle \epsilon, K\epsilon, K^2\epsilon, \ldots, K^{3g-3}\epsilon = \epsilon_0 \rangle,$$

so they all belong to A. Thus $\gamma = F_n^i(\gamma)$ for some $1 \leq i \leq 3g-3$, and hence f is reducible. $\square$

The torus, *reprise*. For genus $g = 1$, $\mathrm{Teich}(S)$ is isomorphic to the upper half-plane $\mathbb{H}$ with $\mathrm{Mod}(S) \cong SL_2(\mathbb{Z})$ acting by Möbius transformations. The moduli space $\mathcal{M}_1 = \mathbb{H}/SL_2(\mathbb{Z})$ is the $(2,3,\infty)$ orbifold, a sphere with one cusp and two cone-points (Figure 2). Every nontrivial loop on $\mathcal{M}_1$ is either

- represented by a geodesic,
- homotopic to a cone point, or
- homotopic to a short loop around the cusp.

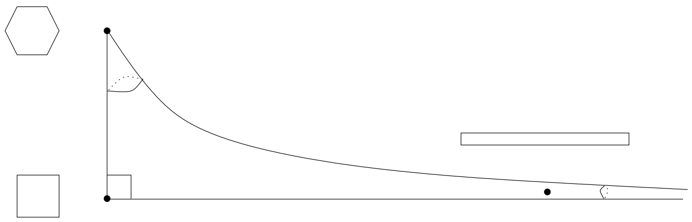

FIGURE 2. The moduli space of a torus, $\mathcal{M}_1 = \mathbb{H}/SL_2(\mathbb{Z})$

These possibilities correspond to the Anosov, finite order, and reducible mapping-classes respectively.

3. Families of Riemann surfaces

In this section we will show that an argument similar to the classification of surface diffeomorphisms leads to a proof of:

Theorem 3.1 (Geometric Shafarevich Conjecture). *For a given base B and genus $g \geq 2$, there are only finitely many truly varying families C/B with fibers of genus g.*

Definitions. By a *family* C/B we mean the data of:

- a 1-dimensional complex manifold B, connected, forming the *base* of the family; and
- a 2-dimensional complex manifold C, the *total space*, equipped with a holomorphic fibration $\pi : C \to B$ such that
- the *fibers* $C_t = \pi^{-1}(t)$ are compact Riemann surfaces of genus g; and
- B is isomorphic to $\overline{B} - P$, the complement of a finite set P (possibly empty) in a compact Riemann surface $\overline{B}$.

A family is *locally constant* if $C_t \cong C_u$ for all $t, u \in B$; otherwise it is *truly varying.* We regard two families C, C' over B as the same if there is an isomorphism $C \cong C'$ respecting the projections to B.

The proof of finiteness we will sketch, due to Imayoshi and Shiga, is based on a Schwarz Lemma for moduli space.

Complex geometry of $\mathcal{M}_g$. Let $\mathcal{M}_g$ denote the moduli space of Riemann surface of genus $g \geq 2$; $\mathcal{T}_g$ its universal covering, Teichmüller space; and $\mathrm{Mod}_g = \pi_1(\mathcal{M}_g)$ the mapping-class group.

There is a natural complex structure on $\mathcal{M}_g$ such that any family C/B determines a holomorphic *classifying map*

$$F : B \to \mathcal{M}_g,$$

defined by $F(t) = [C_t]$, and a *monodromy representation*

$$F_* : \pi_1(B, t) \to \mathrm{Mod}(C_t) \cong \pi_1(\mathcal{M}_g),$$

recording the twisting of the fiber under transport around closed paths in the base.

With the complex structure lifted from $\mathcal{M}_g$, $\mathcal{T}_g$ is isomorphic to an open, bounded domain in $\mathbb{C}^{3g-3}$. Lifting F to the universal cover $\widetilde{B}$ of B, we obtain a bounded analytic map

$$\widetilde{F} : \widetilde{B} \to \mathcal{T}_g \subset \mathbb{C}^{3g-3}.$$

Thus *if $\widetilde{B}$ is isomorphic to $\widehat{\mathbb{C}}$ or $\mathbb{C}$,* then $\widetilde{F}$ must be constant and therefore *all families C/B are trivial.*

Now consider the case where B is hyperbolic, i.e. $\widetilde{B} \cong \Delta$. Even in this case, the boundedness of $\mathcal{T}_g$ controls the geometry of maps $\widetilde{F} : \Delta \to \mathcal{T}_g$. This control is made precise by Royden's theorem:

Theorem 3.2 (Modular Schwarz Lemma). *Any holomorphic map $F : B \to \mathcal{M}_g$ is distance-decreasing from the hyperbolic metric on B to the Teichmüller metric on $\mathcal{M}_g$. In fact $d(F(s), F(t)) \leq d(s, t)/2$.*

We regard this theorem as a Schwarz Lemma for maps with target $\mathcal{M}_g$.

Example: Monodromy over Δ^*. Let C/Δ^* be a family of Riemann surfaces of genus g over the punctured disk $\Delta^* = \{t \ : \ 0 < |t| < 1\}$. In the hyperbolic metric, Δ^* has a *cusp* at $t = 0$; as r tends to zero, the hyperbolic length of the circle $S^1(r)$ also tends to zero. The classifying map $F : \Delta^* \to \mathcal{M}_g$ shrinks distances, so the generator of the monodromy group

$$F_*(\pi_1(\Delta^*)) = \langle f \rangle \subset \mathrm{Mod}_g$$

has translation length $\tau(f) = 0$. By the classification of surface diffeomorphisms, f is reducible or of finite order. Thus a finite iterate f^n is simply a product of Dehn twists (a classical observation of Lefschetz).

Proof of Theorem 3.1 (Geometric Shafarevich Conjecture). Mimicking the proof of finiteness of $\mathrm{Aut}(X)$, we will show there are only finitely many truly varying families C/B by showing the space $\mathcal{F}$ of all classifying maps $F : B \to \mathcal{M}_g$ is compact and discrete.

I. Irreducibility. Fix a basepoint $t \in B$. As for a mapping-class, we say C/B is *reducible* if the monodromy group

$$H = F_*(\pi_1(B, t)) \subset \mathrm{Mod}(C_t)$$

preserves a collection of disjoint simple loops $\{\alpha_1, \ldots, \alpha_m\}$ on C_t.

Suppose C/B is reducible, and let α be a simple loop on C_t with finite monodromy. After passing to a finite covering of B, we can assume α is invariant under $\pi_1(B)$. By a theorem of Wolpert, the geodesic length $L(u) = \ell_\alpha(C_u)$ (now globally well-defined) is subharmonic; that is $\Delta u \geq 0$. By the maximum principle, $L(u)$ is constant on B.

Consider the smallest convex subsurface $D \subset C_t$ carrying all loops such as α with finite monodromy. Using the rigidity of D and an argument with quasifuchsian groups, one can show that $\partial D = \emptyset$. Thus $D = C_t$, and the family C/B is trivial.

Summing up, a truly varying family C/B is irreducible.

II. Compactness. To show $\mathcal{F}$ is compact, we begin by showing the basepoint $F(t)$ must lie in a compact subset of moduli space. By Mumford's theorem, it suffices to find $\epsilon > 0$ such that the length of the shortest geodesic on $[C_t] = F(t)$ satisfies $L(C_t) \geq \epsilon$.

Choose a finite set of closed paths $\gamma_1, \ldots, \gamma_n$ on B generating $\pi_1(B, t)$. By Royden's theorem, there is a uniform bound $K \geq 1$ (depending only on $\max \ell(\gamma_i)$) such that the monodromy of C/B around γ_i is represented by a K-quasiconformal map $f_i : C_t \to C_t$.

Let $\epsilon = \epsilon_0/K^{3g-3}$. Suppose the shortest loop α_1 on C_t has length less than ϵ, and let $\{\alpha_1, \ldots, \alpha_m\}$ enumerate all loops on C_t shorter than ϵ_0, in order of increasing length. Since $m \leq 3g - 3$ there is an index p such that

$$K \ell_{\alpha_p}(C_t) < \ell_{\alpha_{p+1}}(C_t).$$

Now f_i changes the lengths of loops by at most a factor of K (by (4), so f_i must permute the loops $\{\alpha_1, \ldots, \alpha_p\}$. Since $\langle f_i \rangle$ generates the full monodromy group $F_*(\pi_1(B))$, the system of curves $\{\alpha_1, \ldots, \alpha_p\}$ is invariant over the entire base B, and thus C/B is reducible. Hence C/B is trivial, contrary to our assumption that C/B is a truly varying family.

Thus $F(t)$ lies in the compact set $\{X \in \mathcal{M}_g \ : \ L(X) \geq \epsilon\}$ for all $F \in \mathcal{F}$. Since $F : B \to \mathcal{M}_g$ is distance decreasing, the family $\mathcal{F}$ is bounded and equicontinuous on each compact subset of B. Thus any sequence has a convergent subsequence, and hence $\mathcal{F}$ is compact.

III. Discreteness. Finally, we show $\mathcal{F}$ is discrete. If $F, G \in \mathcal{F}$ are close enough, then they are homotopic. We will show this implies $F = G$.

Since F and G are homotopic, there are lifts

$$\widetilde{F}, \widetilde{G} \,:\, \Delta \to \mathcal{T}_g \,\subset\, \mathbb{C}^{3g-3}$$

with

$$\sup_{t \in \Delta} d(\widetilde{F}(t), \widetilde{G}(t)) \,\leq\, D \tag{6}$$

in the Teichmüller metric on $\mathcal{T}_g$.

By a theorem of Fatou, a bounded analytic function such as $\widetilde{F}$ has well-defined boundary values $\widetilde{F}(t)$ for almost every $t \in S^1$. In a truly varying family, the boundary values lie in ∂T_g, since the image $\widetilde{F}(\Delta)$ is properly embedded in Teichmüller space.

Now ∂T_g contains a countable union of complex hypersurfaces A, parameterizing curves with nodes that arise as limits of curves of genus g. Along a given component of A, the nodes are marked by a set of simple closed curves on S. But the monodromy $F_*(\pi_1(B))$ is irreducible, so there are no distinguished simple closed curves on S, and thus (almost all) the boundary values of $\widetilde{F}$ lie in $\partial T_g - A$.

On the other hand, one knows that the ratio of the Euclidean metric on $\mathbb{C}^n$ to the Teichmüller metric on $\mathcal{T}_g$ tends to infinity at points in $\partial T_g - A$, so by (6) we have $\widetilde{F}(t) = \widetilde{G}(t)$ for almost every $t \in S^1$. Since a holomorphic function is determined by its boundary values, we have $F = G$.

IV. Finiteness. Having shown $\mathcal{F}$ is compact and discrete, we conclude that the set of potential classifying maps for C/B is finite. The classifying map $F : B \to \mathcal{M}_g$ determines the family C/B up to finitely many choices (limited by $|\operatorname{Hom}(\pi_1(B), \operatorname{Aut}(C_t))|$), and hence there are only finitely many truly varying families C/B of genus g. ☐

From the proof we also record:

Corollary 3.3 (Rigidity). *A truly varying family C/B is determined up to finitely many choices by its monodromy $F_* : \pi_1(B) \to \operatorname{Mod}_g$.*

4. Branched covers

In this section we present Parshin's argument bounding the number of holomorphic *sections* of a family C/B in terms of the number of *families* D/B of higher genus. (The same construction was used by Kodaira to construct truly varying families over a compact base.)

Theorem 4.1. *Given a genus $g \geq 1$ and a base B, there exists a genus $h \geq 2$ and a finite-to-one map*

$$\left\{ \begin{array}{c} \textit{Families } C/B \textit{ with fibers of genus } g, \\ \textit{equipped with sections } s : B \to C \end{array} \right\} \to \left\{ \begin{array}{c} \textit{Families } D/B \\ \textit{with fibers of genus } h \end{array} \right\}.$$

For each $t \in B$, the surface D_t is a covering of C_t branched over the single point $s(t) \in C(t)$.

Here we regard (C, s) and (C', s') as the same if there is an isomorphism $C \cong C'$ over B sending s to s'.

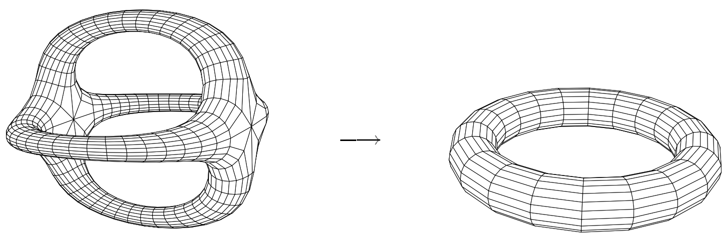

FIGURE 3. A surface of genus 3 is a double cover of a torus branched along 4 points

Proof. Given a pointed topological surface (S, p) of genus g, we can form the covering space

$$\pi : T \to (S, p)$$

corresponding to the kernel of the map

$$\pi_1(S, p) \to H_1(S, \mathbb{Z}/2) \cong (\mathbb{Z}/2)^{2g}.$$

Letting $P = \pi^{-1}(p)$, we can similarly form the branched covering $U \to T$ corresponding to the map

$$\pi_1(T - P) \to H^1(T - P, \mathbb{Z}/2).$$

Since $|P| > 1$, any small loop around a point of P is nonzero in $H^1(T - P, \mathbb{Z}/2)$, and hence $U \to T$ is branched over every point in P.

The composite branched covering $U \to (S, p)$ is *canonical*, so the corresponding family of branched coverings $D_t \to (C_t, s(t))$ fits together to form a family D/B. The original family C/B is a quotient of D/B by a subgroup of $\mathrm{Aut}(D/B)$, and the graph of the section $s(B) \subset C$ corresponds to the fixed-point set of an element of $\mathrm{Aut}(D/B)$. Since $\mathrm{Aut}(D/B)$ is finite, the family D/B determines C/B and $s : B \to C$ up to finitely many choices. □

Example. Let $(S, p) = (\mathbb{R}^2/\mathbb{Z}^2, 0)$ be a flat torus. Then $(T, P) \to (S, p)$ covers S by degree 4, with P the points of order 2 on T. The covering $U \to T$, branched over P, has genus 33 and deck group $(\mathbb{Z}/2)^5$; it is the compositum of 5 double coverings, each of the form shown in Figure 3.

Corollary 4.2 (Geometric Mordell Conjecture). *A truly varying family C/B of genus $g \geq 2$ has only a finite number of sections $s : B \to C$.*

Proof. For each section $s : B \to C$, we can form the family D/B of genus $h \geq 2$ branched over $s(B)$. The number of truly varying families D/B is finite, so the number of pairs (C, s) is finite up to automorphism over B. But $\mathrm{Aut}(C/B)$ is finite, so the number of sections $s : B \to C$ is finite as well. □

5. MONODROMY OVER A FIELD

To begin the passage from geometry to arithmetic, in this section we discuss relatives of the fundamental group, homology and monodromy that can be constructed via algebraic geometry.

Valuations. Let $\overline{B}$ be a *compact* Riemann surface. Algebraically, $\overline{B}$ is specified by its field of meromorphic functions $K = K(\overline{B})$.

A (discrete) *valuation* on K is a surjective homomorphism

$$v : K^* \to \mathbb{Z},$$

defined on the multiplicative group of K and satisfying $v(f+g) \geq \min(v(f), v(g))$. All valuations are of the form

$$v_p(f) = \mathrm{ord}_p(f),$$

where $\mathrm{ord}_p(f) = n$ (or $-n$) if f has a zero (or pole) of order n at p. Thus the points of $\overline{B}$ can be recovered as the valuations of K.

Algebraic π_1. Let $\overline{K}$ denote the algebraic closure of K. The Galois group $\mathrm{Gal}(\overline{K}/K)$ is a first approximation to an algebraic version of $\pi_1(\overline{B})$.

To describe this Galois group topologically, recall that the *profinite completion* of a group G is the inverse limit

$$\widehat{G} = \varprojlim G/N$$

over all normal subgroups N of finite index. For any space E, let $\widehat{\pi}_1(E)$ denote the profinite completion of $\pi_1(E)$.

Every algebraic extension of K is of the form $K' = K(\overline{B}')$, where $\overline{B}' \to \overline{B}$ is a finite covering branched over a finite set $P \subset \overline{B}$. Since $\overline{B}'$ is determined by a subgroup of finite index in $\pi_1(\overline{B} - P)$, we can take the limit over all possible P and obtain:

$$\mathrm{Gal}(\overline{K}/K) \;=\; \varprojlim_{P} \;\widehat{\pi}_1(\overline{B} - P).$$

Thus the algebraic closure $\overline{K}$ detects the fundamental group of $\overline{B}$ 'punctured everywhere'.

Ramification. To construct a Galois group closer to $\pi_1(\overline{B})$, let us say a field extension K'/K of degree d is *ramified* over a valuation v_p if there are fewer than d extensions of v_p to a valuation v' on K'. The ramified valuations v_p correspond exactly to the branch points p of $\overline{B}' \to \overline{B}$.

Let $\overline{K}_P \subset \overline{K}$ denote the field generated by all finite extensions of K ramified only over v_p, $p \in P \subset B$. Then for any finite set $P \subset B$ we have

$$\mathrm{Gal}(\overline{K}_P/K) \;\cong\; \widehat{\pi}_1(\overline{B} - P). \tag{7}$$

In particular we can recover $\widehat{\pi}_1(\overline{B})$ as a Galois group by taking $P = \emptyset$.

Monodromy. Let C/B be a family over a base $B = \overline{B} - P$. With the Galois-theory version (7) of $\pi_1(B)$ in hand, we now turn to the construction of an algebraic relative of the monodromy map

$$F_* : \pi_1(B, t) \to \mathrm{Mod}(C_t).$$

The first step is to retreat from the mapping-class group by replacing $\pi_1(C_t)$ with the family of groups $H_1(C_t, \mathbb{Z}) \cong \mathbb{Z}^{2g}$. We then obtain a *linear representation*

$$\rho : \pi_1(B, t) \to \mathrm{Aut}(H_1(C_t, \mathbb{Z})) = GL_{2g}(\mathbb{Z}), \tag{8}$$

recording the twisting of homology around loops on the base.

Next fix a prime ℓ, and let $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n$ denote the ℓ-adic integers. Note that any prime $p \neq \ell$ becomes invertible in ℓ; the local ring $\mathbb{Z}_\ell$ is the *completion* of $\mathbb{Z}$ at ℓ. By reducing mod ℓ^n we obtain a system of *finite* representations

$$\rho_{\ell^n} : \pi_1(B) \to GL_{2g}(\mathbb{Z}/\ell^n)$$

that fit together to determine a map

$$\widehat{\rho}_\ell : \mathrm{Gal}(\overline{K}_P/K) \cong \widehat{\pi}_1(B) \;\to\; GL_{2g}(\mathbb{Z}_\ell).$$

This *ℓ-adic Galois representation* is nothing more than the completion at ℓ of the monodromy on integral homology (8). Our goal is to reconstruct $\widehat{\rho}_\ell$ using the methods of algebraic geometry.

The Jacobian. The first step is to use the *Jacobian* to build an algebraic version of the homology of C.

Let X be a compact Riemann surface of genus $g \geq 1$. A *divisor* $D = \sum a_p \cdot p \in \mathbb{Z}[X]$ is a finite formal sum of points of X; its *degree* is $\sum a_p$. A *principal divisor* is one of the form

$$D = (f) = \sum_p v_p(f) \cdot p,$$

where $f \in K^*(X)$ is a meromorphic function and $v_p(f)$ is the valuation of f at p. The *Jacobian* of X is the quotient

$$\mathrm{Jac}(X) = \mathrm{Div}_0(X)/\{(f) \ : \ f \in K^*(X)\}$$

of divisors of degree zero by principal divisors.

By a theorem of Abel, the Jacobian is a complex projective torus, or *Abelian variety*, alternatively described as:

$$\mathrm{Jac}(X) = \Omega(X)^*/H_1(X,\mathbb{Z}) \cong \mathbb{C}^g/\Lambda.$$

Here $\Omega(X)$ is the vector space of holomorphic 1-forms θ on X; these pair linearly with cycles $\gamma \in H_1(X,\mathbb{Z})$ by

$$\langle \gamma, \theta \rangle = \int_\gamma \theta \quad \in \mathbb{C}.$$

Fixing $q \in X$, there is a natural embedding

$$X \to \mathrm{Jac}(X)$$

sending p to the divisor $p - q$ and inducing an isomorphism on homology:

$$H_1(X,\mathbb{Z}) \cong H_1(\mathrm{Jac}(X),\mathbb{Z}). \tag{9}$$

Moreover the map $X^g \to \mathrm{Jac}(X)$ given by $(p_i) \mapsto \sum (p_i - q)$ is surjective. Using this surjectivity one can derive algebraic equations for $\mathrm{Jac}(X)$ as a projective variety in terms of equations for X.

For any Abelian variety A of dimension g, let $A[n] \cong (\mathbb{Z}/n)^{2g}$ denote its points of order n. Then from (9) we have

$$H_1(X,\mathbb{Z}/\ell^n) \cong \mathrm{Jac}(X)[\ell^n].$$

Since the group law on $\mathrm{Jac}(X)$ is algebraic, the finite set $\mathrm{Jac}(X)[\ell^n]$ is defined by a system of algebraic equations and can be constructed without reference to the topology of X. This is the desired algebraic version of homology.

Families of Abelian varieties. We can now associate to each family C/B a family of Abelian varieties A/B with $A_t = \mathrm{Jac}(C_t)$. For any $n \geq 0$, the family of groups $A_t[\ell^n] \cong (\mathbb{Z}/\ell^n)^{2g}$ becomes trivial after passing to a finite covering of the base, and thus the deck transformations determine a representation

$$\rho_{\ell^n} : \pi_1(B) \to \operatorname{Aut} A[\ell^n] = GL_{2g}(\mathbb{Z}/\ell^n).$$

Since the target is finite, we obtain a system of representations of $\widehat{\pi}_1(B) \cong \operatorname{Gal}(\overline{K}_P/K)$, $K = K(\overline{B})$, compatible under the map

$$A[\ell^{n+1}] \to A[\ell^n]$$

given by multiplication by ℓ. Passing to the limit as $n \to \infty$, we obtain a purely algebraic construction of the ℓ-adic representation

$$\widehat{\rho}_\ell : \operatorname{Gal}(\overline{K}_P/K) \to GL_{2g}(\mathbb{Z}_\ell). \tag{10}$$

This is the desired algebraic version of monodromy.

Moduli of Abelian varieties. For one final perspective on (10), we recall that the moduli space of (principally polarized) Abelian varieties is given by the quotient $\mathcal{A}_g = \mathcal{H}_g/Sp_{2g}(\mathbb{Z})$, where $\mathcal{H}_g$ is the *Siegel upper halfspace* of $g \times g$ symmetric complex matrices Z with $\operatorname{Im}(Z)$ positive definite.

From a family C/B we obtain maps

$$B \xrightarrow{F} \mathcal{M}_g \xrightarrow{\mathrm{Jac}} \mathcal{A}_g$$

whose composition $\mathrm{Jac} \circ F$ classifies the family $A = \operatorname{Jac}(C)/B$. Passing to profinite fundamental groups, we obtain a sequence of successively coarser monodromy representations:

$$\operatorname{Gal}(\overline{K}_P/K) \cong \widehat{\pi}_1(B) \;\to\; \widehat{\pi}_1(\mathcal{M}_g) \;\to\; \widehat{\pi}_1(\mathcal{A}_g) \;\to\; \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

The first map records the action of the Galois group of the base on all *finite covers* of the fibers; the last, on the ℓ-adic homology of the fibers. This last representation is the ℓ-adic monodromy $\widehat{\rho}_\ell$.

6. Finite Fermat

In this section we finally sketch the proof of:

Theorem 6.1 (Finite Fermat). *For $n \geq 4$, the equation*

$$X^n + Y^n = Z^n \tag{11}$$

has only a finite number of integral solutions with $\gcd(X, Y, Z) = 1$.

In brief, the idea of the proof is to think of the Riemann surface $C \subset \mathbb{P}^2(\mathbb{C})$ defined by (11) as a *family* C/B spread out over the prime numbers $p \in \mathbb{Z}$. The fiber C_p is the reduction of $C \bmod p$. An integral solution to the Fermat equation gives a coherent family of points on each fiber C_p, and hence a *section* of C/B. The condition $n \geq 4$ implies the genus bound $g(C) \geq 2$; thus Finite Fermat follows from an arithmetic version of the *finiteness of sections* for families C/B.

To understand the sense in which the Fermat equation determines a family C/B, we begin with a study of the base.

$\operatorname{Spec} \mathbb{Z}$. The *spectrum* of the ring of integers $\mathbb{Z}$ is the space

$$\operatorname{Spec} \mathbb{Z} = \{0, 2, 3, 5, 7, 11, \ldots\}$$

consisting of the *prime numbers* $p \in \mathbb{Z}$, plus the 'generic point' 0. This space comes equipped with a topology and a sheaf $\mathcal{O}$ that plays the role of the sheaf of holomorphic functions on a Riemann surface. The global sections of $\mathcal{O}$ are $\mathbb{Z}$ itself, and the field of meromorphic functions becomes $K(B) = \mathbb{Q}$.

One can also see the prime numbers as points by considering valuations on $K(B) = \mathbb{Q}$. Indeed, every valuation $v : \mathbb{Q}^* \to \mathbb{Z}$ is of the form

$$v_p(r/s) = \mathrm{ord}_p(r) - \mathrm{ord}_p(s)$$

for some prime number $p \in \mathbb{Z}$, where $\mathrm{ord}_p(r)$ is the largest n such that p^n divides r.

The shape of a prime. A valuation v on a field K determines:

- a local ring $\mathcal{O}_v = \{f \,:\, v(f) \geq 0\} \subset K$,
- the maximal ideal $m_v = \{f \,:\, v(f) > 0\}$ in $\mathcal{O}_v$,
- a residue field $k = \mathcal{O}_v/m_v$, and
- a local fundamental group $G = \mathrm{Gal}(\overline{k}/k)$.

For example, if B is a compact Riemann surface, $K = K(B)$ and $v = v_p$ for $p \in B$, then $\mathcal{O}_v$ is the ring of meromorphic functions analytic at p, and the map

$$\mathcal{O}_v \mapsto \mathcal{O}_v/m_v = k \cong \mathbb{C}$$

is simply the point evaluation $f \mapsto f(p)$. Since $\mathbb{C}$ is algebraically closed, the local fundamental group G at p is trivial, reflecting the contractibility of p.

In contrast, a prime $p \in \mathbb{Z}$ behaves more like a circle than a point. For the corresponding valuation $v = v_p$ on $K = \mathbb{Q}$ we have

$$\begin{aligned} \mathcal{O}_v &= \mathbb{Z}_{(p)} = \{r/s \,:\, (s,p) = 1\} \\ m_v &= p\mathbb{Z}_{(p)} \\ k &= \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \\ G &= \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \widehat{\mathbb{Z}}. \end{aligned}$$

The local fundamental group $G = \widehat{\mathbb{Z}}$ (the profinite completion of $\mathbb{Z}$) is (topologically) generated by the *Frobenius automorphism* σ_p of $\overline{\mathbb{F}}_p$ sending x to x^p. Since $\widehat{\pi}_1(S^1) = \widehat{\mathbb{Z}}$ as well, we are led to picture a prime as a topological circle.

The fibers of C. Let C/B be a family over a Riemann surface B. Then the fiber C_p over $p \in B$ can be described as the *reduction* of C to a curve over the residue field $\mathbb{C} = \mathcal{O}_p/m_p$.

Similarly, if $C \subset \mathbb{P}^2$ is a plane curve defined by a homogeneous equation $F(X,Y,Z) \in \mathbb{Z}[X,Y,Z]$, then for each prime $p \in \mathrm{Spec}\,\mathbb{Z}$ we can reduce F mod p to obtain a curve C_p in the projective plane over $\mathbb{F}_p$. We say C has *good reduction at p* if C_p is smooth.

Loops in the base. When C is smooth to begin with, it has good reduction outside a finite set of primes S; removing these points from the base, we obtain a family with smooth fibers C_p, $p \notin S$. Thus the natural base for C is

$$B = (\mathrm{Spec}\,\mathbb{Z}) - S = \mathrm{Spec}\, S^{-1}\mathbb{Z}.$$

By analogy with (7), the fundamental group of the base is

$$\widehat{\pi}_1(B) = \mathrm{Gal}(\overline{\mathbb{Q}}_S/\mathbb{Q}),$$

where $\overline{\mathbb{Q}}_S$ is the maximal algebraic extension of $\mathbb{Q}$ unramified outside S.

For example, the Fermat curve is given in the affine chart $Z \neq 0$ by the equation $f(x,y) = x^n + y^n = 1$, with differential

$$df(x,y) = nx^{n-1}dx + ny^{n-1}dy.$$

So long as p does not divide n, the equation $f = df = 0$ has no solutions in $\overline{\mathbb{F}}_p^2$ and C_p is smooth. On the other hand, df vanishes identically when p divides n, so the prime divisors of n give exactly the points of bad reduction S.

For each prime $p \notin S$, the Frobenius $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ lifts to an element of $\mathrm{Gal}(\overline{\mathbb{Q}}_S/\mathbb{Q})$, well-defined up to conjugacy, that we also denote by σ_p. By a theorem of Čebotarev, the Frobenius elements are *dense* in $\mathrm{Gal}(\overline{\mathbb{Q}}_S/\mathbb{Q})$. One can picture a prime p as a loop in the base $B = (\mathrm{Spec}\,\mathbb{Z}) - S$, and σ_p as the corresponding element in $\widehat{\pi}_1(B)$. Monodromy around these 'prime loops' plays a crucial role in the study of families defined over $\mathbb{Q}$.

Homology and monodromy. Let C be a curve of genus g defined over $\mathbb{Q}$, with smooth fibers over $B = \mathrm{Spec}\,\mathbb{Z} - S$. Fix a prime ℓ, and replace S with $S \cup \{\ell\}$. Then the Jacobian $A = \mathrm{Jac}(C)$ and the map $x \mapsto \ell x$ on A have natural definitions over $\mathbb{Q}$ with good reduction outside S.

From the geometric theory of the Jacobian, discussed earlier, there is a natural isomorphism

$$A[\ell^n] = H_1(C, \mathbb{Z}/\ell^n).$$

At the same time $A[\ell^n]$ has coordinates lying in a finite extension of $\mathbb{Q}$, so we get an action of the Galois group on the homology of C. Taking the limit as $n \to \infty$, we obtain the *ℓ-adic Galois representation*

$$\widehat{\rho}_\ell : \widehat{\pi}_1(B) = \mathrm{Gal}(\overline{\mathbb{Q}}_S/\mathbb{Q}) \;\to\; \mathrm{Aut}\, H_1(C, \mathbb{Z}_\ell) \cong GL_{2g}(\mathbb{Z}_\ell).$$

This linear action of $\widehat{\pi}_1(B)$ on the homology of C is the arithmetic version of the monodromy.

Solutions to Fermat's equation and branched covers. Now suppose we have relatively prime integers (X, Y, Z) (such as $(1, 0, 1)$) solving Fermat's equation $X^n + Y^n = Z^n$. Then $P = [X : Y : Z] \in \mathbb{P}^2(\mathbb{Q})$ gives a *rational point* on C. Using Parshin's trick, we obtain a Riemann surface D with a covering $D \to C$ branched over P. The genus of D is controlled by that of C, and D is defined over $\mathbb{Q}$ with good reduction outside S. Finally, D determines the rational point $P \in C$ up to finite ambiguity.

Thus to prove Theorem 6.1 (Finite Fermat), it suffices to establish:

Theorem 6.2 (Arithmetic Shafarevich Conjecture)**.** *Fix a number field K, a finite set of primes S of K and a genus $g \geq 2$. Then there are only finitely many curves C of genus g defined over K with good reduction outside S.*

Sketch of the proof. For concreteness we treat the case $K = \mathbb{Q}$. Let $A = \mathrm{Jac}(C)$, adjoin ℓ to S and let

$$\widehat{\rho}_\ell : \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) \to GL_{2g}(\mathbb{Q}_\ell)$$

be the monodromy representation. Let $\sigma_p \in \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ be a lift of the Frobenius for each prime $p \notin S$. Since the conjugacy class of σ_p is determined by p, the trace

$$\mathrm{Tr}(\sigma_p) = \mathrm{Tr}(\widehat{\rho}_\ell(\sigma_p))$$

is well-defined.

The strategy of the proof is to show that there are only finitely many possibilities for $\widehat{\rho}_\ell$ and that each determines A and hence C up to finite ambiguity. We will sketch the main steps, and indicate their resonance with ideas in the geometric proof of §3.

1. Semisimplicity. *The representation $\widehat{\rho}_\ell$ is semisimple. In particular, $\widehat{\rho}_\ell$ is determined (up to conjugacy) by its trace*

$$\mathrm{Tr} \circ \widehat{\rho}_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}_S/\mathbb{Q}) \to \mathbb{Z}_\ell.$$

This semisimplicity is like the irreducibility of the monodromy

$$F_* : \pi_1(B) \to \mathrm{Mod}(S)$$

demonstrated in §3. For example, if $F_*(\pi_1(B))$ were reducible, generated by Dehn twists about disjoint, homologically nontrivial loops, then $\widehat{\rho}_\ell$ would be unipotent rather than semisimple, with the same trace as the trivial representation.

2. Finite generation. *There is a finite set of primes T disjoint from S such that the traces $\langle \mathrm{Tr}(\sigma_p) \ : \ p \in T\rangle$ determine $\widehat{\rho}_\ell$.*

This statement is similar to the finite generation of $\pi_1(B)$. One first shows that different representations can be distinguished over an extension $K/\mathbb{Q}$ of degree $d \leq d(\ell, g)$. According to Hermite, there are only finitely many such extensions unramified outside S, and by Čebotarev there is a finite set of primes T such that for each K, $\langle \sigma_p : p \in T\rangle$ represents every conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$. The traces of these σ_p then determine $\widehat{\rho}_\ell$.

3. The Weil bounds. *For any prime $p \notin S$, the trace of the Frobenius lies in $\mathbb{Z}$ and obeys a bound $|\mathrm{Tr}(\sigma_p)| \leq N(p, g)$ independent of C.*

Weil showed the number of points on a curve over a finite field can be computed by applying the Lefschetz fixed-point formula to the Frobenius; more precisely,

$$\begin{aligned} |C(\mathbb{F}_p)| &= \textstyle\sum_{i=0}^2 (-1)^i \,\mathrm{Tr}(\sigma_p | H^i(C, \mathbb{Q}_\ell)) \\ &= 1 - \mathrm{Tr}(\sigma_p | H^1(C, \mathbb{Q}_\ell)) + p. \end{aligned} \tag{12}$$

Each trace above actually lies on $\mathbb{Z}$. Since

$$H^1(C, \mathbb{Q}_\ell)^* \ = \ H_1(C, \mathbb{Z}_\ell) \otimes \mathbb{Q}_\ell,$$

we see the trace of the monodromy, $\mathrm{Tr}(\sigma_p)$, is the same as the middle term in the Lefschetz formula, namely the trace of the Frobenius on H^1. On the other hand, $|C(\mathbb{F}_p)|$ is bounded above by Riemann-Roch; there is a rational map $C(\mathbb{F}_p) \to \mathbb{P}^1(\mathbb{F}_p)$ of degree $1 < d = O(g)$, so we have

$$|C(\mathbb{F}_p)| \leq d(g)|\mathbb{P}^1(\mathbb{F}_p)| \ = \ O(gp).$$

By (12), we have $|\mathrm{Tr}(\sigma_p)| = O(gp)$ as well. (The Riemann hypothesis for curves over finite fields, also proved by Weil, gives the sharper bound $|\mathrm{Tr}(\sigma_p)| \leq 2g\sqrt{p}$.)

Combining (1–3), we deduce:

Only finitely many representations $\widehat{\rho}_\ell$ occur for fixed (S, g).

Remark: Lengths of primes. The Weil bound is reminiscent of the Modular Schwarz Lemma (Theorem 3.2), i.e. the contracting property for holomorphic maps $F : B \to \mathcal{M}_g$. For example, when $g = 1$ each $\alpha \in SL_2(\mathbb{Z})$ determines a closed loop on $\mathcal{M}_g$ whose Teichmüller length satisfies

$$2\cosh(\ell_\alpha(\mathcal{M}_g)) = |\mathrm{Tr}(\alpha)|.$$

Since F shrinks the hyperbolic metric on B by at least a factor of two, for $\alpha \in \pi_1(B)$ we obtain the *a priori* bound:

$$|\mathrm{Tr}(F_*\alpha)| \leq 2\cosh(\ell_\alpha(B)/2).$$

Is the Weil bound perhaps a measurement of the 'hyperbolic length' of the loop represented by a prime?

4. Isogeny. *The representation $\widehat{\rho}_\ell$ determines A up to isogeny over $\mathbb{Q}$.*

A homomorphism $\phi : A \to B$ between Abelian varieties of the same dimension is an *isogeny* if its kernel is finite. If $|\operatorname{Ker}(\phi)|$ is relatively prime to ℓ, then ϕ induces an isomorphism

$$A[\ell^n] \to B[\ell^n]$$

for every n and hence an isomorphism between the ℓ-adic representations $\widehat{\rho}_\ell$ for A and B. Hence the best one can hope for is that $\widehat{\rho}_\ell$ determines A up to isogeny, and indeed this is the case.

This result is an arithmetic version of the *rigidity* of families C/B, i.e. the fact that a truly varying family is determined by its monodromy (Corollary 3.3).

5. Heights. *Given A, there is an upper bound $h(B) \le h_0$ on the height of any Abelian variety B isogenous to A over $\mathbb{Q}$.*

Let $\Omega(A)$ be the 1-dimensional vector space of holomorphic sections of the canonical bundle of $A = \mathbb{C}^g/\Lambda$. Any $\theta \in \Omega(A)$ lifts to a constant form

$$\theta \;=\; C\, dz_1 \cdots dz_g$$

on $\mathbb{C}^g$. The arithmetic structure of A determines an additive subgroup of *integral* g-forms,

$$\Omega(A)_{\mathbb{Z}} \;=\; \mathbb{Z}\theta_0 \subset \Omega(A).$$

The *intrinsic height* $h(A)$ measures the volume of the complex manifold $A(\mathbb{C})$ with respect to the minimal integral form:

$$h(A) \;=\; -\frac{1}{2}\log\left(\frac{1}{2^g}\int_{A(\mathbb{C})} |\theta_0|^2\right).$$

The pulled-back volume increases under an isogeny $\pi : A \to B$:

$$\int_A |\pi^*(\theta_0)|^2 \;=\; \deg(A/B)\int_B |\theta_0|^2;$$

however, in compensation one *usually* finds a shift in the minimal integral form,

$$[\Omega(A)_{\mathbb{Z}} : \pi^*\Omega(B)_{\mathbb{Z}}] \;=\; \deg(A/B),$$

and thus $h(A) = h(B)$. Taking into account the less usual isogenies, one still obtains a bound $h(B) \le h_0$ depending only on A.

In the case of Riemann surfaces, a natural height on the moduli space $\mathcal{M}_g$ is given by $h(X) = -\log L(X)$, where $L(X)$ is the length of the shortest geodesic. To replace Mumford's theorem that

$$\mathcal{M}_g(\epsilon) = \{X \;:\; L(X) \ge \epsilon > 0\}$$

is compact, we have:

6. Finiteness. *The set of Abelian varieties $A/\mathbb{Q}$ with height $h(A) \le h_0$ is finite.*

Let us define the *naive height* of $A/\mathbb{Q}$ by

$$H(A) = \log\max\{|p_1|, |q_1|, \ldots, |p_n|, |q_n|\},$$

where $(p_i/q_i)_{i=1}^n$ are the rational numbers appearing in suitable equations defining A. It suffices to show $H(A)$ is controlled by $h(A)$.

To convey the idea of the result, suppose A is the elliptic curve with equation

$$y^2 \;=\; x(x-1)(x-p/q),$$

$0 < p/q < 1/2$. Then $H(A) = \log q$. Clearing denominators, we obtain the minimal integral form

$$\theta_0 = \frac{dy}{x(x-1)(qx-p)}$$

on A, with volume

$$\int_A |\theta_0|^2 \;=\; 2\int_{\mathbb{C}} \frac{|dx|^2}{|x(x-1)(qx-p)|} \;\asymp\; \frac{\log(q/p)}{q^2} \;\leq\; \frac{\log q}{q^2}.$$

The intrinsic height is essentially $\log(1/\operatorname{vol}(A))$, so we find $h(A) \asymp \log q \asymp H(A)$. Thus a bound on $h(A)$ pins A down to a finite set.

The general case entails the delicate construction of an arithmetic moduli for higher-dimensional Abelian varieties.

Combining (4–6), we deduce:

> *Only finitely many Abelian varieties $A/\mathbb{Q}$ correspond to a given Galois representation $\widehat{\rho}_\ell$.*

7. Polarizations. The last step in the proof is to show: *The curve C is determined by the Abelian variety $A = \operatorname{Jac}(C)$ up to finitely many choices.*

The intersection pairing of topological 1-cycles on C gives a symplectic form

$$\omega \;:\; \wedge^2 H_1(A,\mathbb{Z}) \;=\; \wedge^2 H_1(C,\mathbb{Z}) \;\to\; \mathbb{Z}.$$

The form ω is called a *principal polarization* of A; it determines a flat metric making A into a Kähler manifold of total volume 1.

The classical Torelli Theorem states that C is uniquely determined by the pair (A,ω). To show A alone determines C up to finite ambiguity, it suffices to show the set of principal polarizations falls into finitely many orbits under the action of $\operatorname{Aut} A$.

To give an idea of the proof, we sketch instead a related result for a real torus $T = \mathbb{R}^n/\mathbb{Z}^n$. Instead of principal polarizations, we consider positive definite quadratic forms $q : H^1(T,\mathbb{Z}) \to \mathbb{Z}$ determining flat metrics on T of total volume 1. We will show such q fall into finitely many orbits under the action of $\operatorname{Aut} T$.

The set of all pairs (T,q) determines a discrete set $Q \subset \mathcal{M}$, where

$$\mathcal{M} \;=\; SO_n(\mathbb{R})\backslash SL_n(\mathbb{R})/SL_n(\mathbb{Z})$$

is the moduli space of flat tori of volume 1. On the other hand, because q is an integral form, the q-length of the shortest geodesic loop satisfies $L(T,q) \geq 1$. By a result of Mahler (a precursor to Mumford's theorem),

$$\{(T,g) \in \mathcal{M} \;:\; L(T,g) \geq 1\}$$

is compact, so Q is finite. Thus there are only finitely many possibilities for q up to the action of $\operatorname{Aut} T$.

Conclusion. Combining (1–7), we deduce that only a finite number of curves $C/\mathbb{Q}$ of genus g have good reduction outside S.

The methods can be generalized to an arbitrary number field K. $\square$

With the Shafarevich conjecture in hand, Parshin's covering trick yields:

Corollary 6.3 (Arithmetic Mordell's Conjecture)**.** *A smooth curve C of genus $g \geq 2$ defined over a number field K has only a finite number of K-rational points.*

In particular, the Fermat equation with $n \geq 4$ has only a finite number of solutions.

More on arithmetic topology. The parallel approaches to the Shafarevich conjectures, detailed above, are but one instance of the interplay between topology, complex geometry and number theory. We conclude by mentioning a few more examples and references.

1. The action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the homology of a curve C can be refined to a representation into the arithmetic mapping-class group $\widehat{\mathrm{Mod}(C)}$. This mixture of Galois theory and topology, especially in the case $C = \mathbb{P}^1 - \{0, 1, \infty\}$, forms the basis for Grothendieck's theory of *'dessins d'enfants'* and has been the subject of much recent activity [Sch].
2. The intrinsic height of an Abelian variety, formulated above, is an example of *Arakelov geometry*, which aims to treat the finite and infinite places of a field on an equal footing [Lg2], [So].
3. The analogy between number fields and functions fields of Riemann surfaces goes back at least to Weil [Wl2].
4. A dictionary between complex-analytic Nevanlinna theory and Diophantine approximation has been developed by Vojta, leading to another proof of Mordell's conjecture [Voj1], [Voj2].
5. Mochizuki has developed the methods of Teichmüller theory in the p-adic setting [Mo].
6. Finally, we mention that Mazur and others have suggested that one should picture the primes $p \in \mathrm{Spec}\,\mathbb{Z}$ not just as loops, but as *knots in a 3-sphere.* Class field theory then parallels the investigation of the homology of branched covers of S^3, and Iwasawa theory provides the analogue of the Alexander polynomial for a prime.

   In support of the correspondence
   $$\mathrm{Spec}\,\mathbb{Z} \quad \longleftrightarrow \quad S^3,$$
   note that $\mathrm{Spec}\,\mathbb{Z}$ is 'simply-connected' (there are no unramified extensions of $\mathbb{Q}$) and a 'homology 3-sphere' ($H^p(\mathrm{Spec}\,\mathbb{Z}, \mathbb{G}_m) = 0$ except in dimensions $p = 0$ and $p = 3$ [Maz1, p. 538]).

   Ideas from number theory can also inform research on 3-manifolds; for examples, see Reznikov's papers on 'arithmetic topology' [Rez1], [Rez2, §14].

7. Notes

§1. The proof of Fermat's last theorem appears in [Wi], [TW]; for surveys, see [RS], [Ri] and [DDT].

§2. Thurston's classification of surface diffeomorphisms is outlined in [Th1] and developed in detail in [FLP]; here we present Bers' complex-analytic approach [Bers]. Mumford's compactness theorem appears in [Mum]; for a related result due to Weil, see [Wl1]. For more about the hyperbolic geometry of surfaces, see Buser's text [Bus].

The theme of short geodesics, appearing here in the proofs of the classification of surface diffeomorphisms and of the geometric Shafarevich conjecture, is also seen in Thurston's work on rational maps and hyperbolic 3-manifolds via iteration on Teichmüller space [Mc1]. The theory of hyperbolic 3-manifolds fibering over the circle is presented in [Th2] and [Ot]; see also [Mc2, §3], [Br].

We remark that by Mostow rigidity and the Hyperbolization Conjecture, the mapping-class group $\mathrm{Mod}(M^3)$ is expected to be *finite* for most closed 3-manifolds.

§3. The geometric Shafarevich conjecture was proved by Arakelov, generalizing Parshin's treatment of the case of a compact base B [Ar], [Par]. The proof sketched here is a slight variant of that by Imayoshi and Shiga [IS]; we use Wolpert's result that $\ell_\alpha(X)$ is subharmonic [Wol].

A systematic introduction to the complex geometry of Teichmüller space is provided by the texts [Gd], [IT], [Le], and [Nag]. These books present Bers' model for Teichmüller space as a bounded domain and cover Royden's theorem that the Teichmüller and Kobayashi metrics coincide.

The finiteness of families C/B also holds for genus $g = 1$ if we require that C admits a section $s : B \to C$. Without a section, there may be infinitely many families of elliptic curves C/B for a given classifying map $F : C \to \mathcal{M}_1$. Similarly one can construct infinitely many curves $C/\mathbb{Q}$ of genus 1 with a fixed locus of bad reduction (and $C(\mathbb{Q}) = \emptyset$); see [Maz2, p. 241].

§4. The geometric Mordell conjecture was formulated by Lang and proved by Manin [Lg1, p. 29], [Man]; see also [Gr]. Parshin's trick appears in [Par]. The same construction was used by Kodaira to exhibit truly varying families C/B over a compact base [Ko].

For an alternate proof of the geometric Mordell conjecture, one can repeat the argument of §3 using the fact that a section of C/B determines a classifying map $F : C/B \to \mathcal{M}_{g,1}$ to the moduli space of *pointed* Riemann surfaces of genus g.

Deligne proved quite generally that for any smooth complex projective family of varieties V/B, the number of possible linear monodromy representations of dimension n for a fixed B is finite [De2]. More precisely, if $t \in B$ is a basepoint and $\dim H^i(V_t, \mathbb{Q}) = n$, then there are at most $N(B, n)$ possibilities for the map

$$\rho : \pi_1(B, t) \to GL(H^i(V_t, \mathbb{Q})) \cong GL_n(\mathbb{Q})$$

up to conjugacy.

§5. A detailed treatment of the Jacobian of a Riemann surface can be found in Griffiths and Harris [GH].

§6. The arithmetic conjectures of Mordell and Shafarevich were proved by Faltings [Fal]. Our sketch follows Deligne's presentation [De1]; see also [Sz], [CS]. More about arithmetic on curves, leading up to Falting's theorem, can be found in Mazur's survey [Maz2].

Work on the Weil conjectures is surveyed in [Ka]. The finiteness of the number of principal polarizations of a given Abelian variety is proved in [NN]; see also Milne's article [CS, Ch. V, §18].

References

[Ar] S. Arakelov. Families of algebraic curves with fixed degeneracies. *Math. USSR Izv.* **35**(1971), 1269–1293. MR **48**:298

[Bers] L. Bers. An extremal problem for quasiconformal maps and a theorem by Thurston. *Acta Math.* **141**(1978), 73–98. MR **57**:16704

[Br] J. Brock. Iteration of mapping classes on a Bers slice: examples of algebraic and geometric limits of hyperbolic 3-manifolds. In *Lipa's Legacy (New York, 1995)*, volume 211 of *Contemp. Math.*, pages 81–106. Amer. Math. Soc., 1997. MR **98k**:30057

[Bus] P. Buser. *Geometry and Spectra of Compact Riemann Surfaces.* Birkhauser Boston, 1992. MR **93g**:58149

[CS] G. Cornell and J. H. Silverman, editors. *Arithmetic Geometry*. Springer-Verlag, 1986. MR **89b:**14029

[DDT] H. Darmon, F. Diamond, and R. Taylor. Fermat's last theorem. In *Current Developments in Mathematics, 1995 (Cambridge, MA)*, pages 1–154. Internat. Press, 1994. MR **99d:**11067a

[De1] P. Deligne. Preuve des conjectures de Tate et Shafarevitch [d'après G. Faltings]. In *Séminaire Bourbaki, 1983/84*, pages 25–41. Astérisque, volume 121–122, 1985. MR **87c:**11026

[De2] P. Deligne. Un théorème de finitude pour la monodromie. In *Discrete Groups in Geometry and Analysis (New Haven, Conn., 1984)*, pages 1–19. Birkhäuser, 1987. MR **88h:**14013

[Fal] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73**(1983), 349–366. MR **85g:**11026a

[FLP] A. Fathi, F. Laudenbach, and V. Poénaru. *Travaux de Thurston sur les surfaces*. Astérisque, volume 66–67, 1979. MR **82m:**57003

[Gd] F. Gardiner. *Teichmüller Theory and Quadratic Differentials*. Wiley Interscience, 1987. MR **88m:**32044

[Gr] H. Grauert. Mordells Vermutung über rationale Punkte auf algebraischen Kurven und Funktionenkörper. *IHES Publ. Math.* **25**(1965), 131–149. MR **36:**5139

[GH] P. Griffiths and J. Harris. *Principles of Algebraic Geometry*. Wiley Interscience, 1978. MR **80b:**14001

[IS] Y. Imayoshi and H. Shiga. A finiteness theorem for holomorphic families of Riemann surfaces. In *Holomorphic Functions and Moduli II*, pages 207–219. Springer-Verlag: MSRI publications volume 11, 1988. MR **89i:**32046

[IT] Y. Imayoshi and M. Taniguchi. *An Introduction to Teichmüller Spaces*. Springer-Verlag, 1992. MR **94b:**32031

[Ka] N. Katz. An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields. In *Mathematical developments arising from Hilbert problems*, volume 28 of *Proc. Symp. Pure Math.*, pages 275–305. Amer. Math. Soc., 1976. MR **54:**12780

[Ko] K. Kodaira. A certain type of irregular algebraic surface. *J. d'Analyse Math.* **19**(1967), 207–215. MR **35:**7354

[Lg1] S. Lang. Integral points on curves. *IHES Publ. Math.* **6**(1960), 27–43. MR **24A:**86

[Lg2] S. Lang. *Introduction to Arakelov theory*. Springer-Verlag, 1988. MR **89m:**11059

[Le] O. Lehto. *Univalent functions and Teichmüller spaces*. Springer-Verlag, 1987. MR **88f:**30073

[Lit] J. E. Littlewood. From Fermat's Last Theorem to the Abolition of Capital Punishment. In B. Bollabas, editor, *Littlewood's Miscellany*. Cambridge University Press, 1986. MR **88d:**01036

[Man] Y. Manin. A proof of the analog of the Mordell conjecture for algebraic curves over function fields. *Soviet Math. Dokl.* **152**(1963), 1061–1063. MR **27:**4812

[Maz1] B. Mazur. Notes on étale cohomology of number fields. *Ann. Sci. Éc. Norm. Sup.* **6**(1973), 521 – 556. MR **49:**8993

[Maz2] B. Mazur. Arithmetic on curves. *Bull. Amer. Math. Soc.* **14**(1986), 207–259. MR **88e:**11050

[Mc1] C. McMullen. Rational maps and Kleinian groups. In *Proceedings of the International Congress of Mathematicians Kyoto 1990*, pages 889–900. Springer-Verlag, 1991. MR **93h:**57024

[Mc2] C. McMullen. *Renormalization and 3-Manifolds which Fiber over the Circle*, volume 142 of *Annals of Math. Studies*. Princeton University Press, 1996. MR **97f:**57022

[Mo] S. Mochizuki. The intrinsic Hodge theory of p-adic hyperbolic curves. In *Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998)*, volume Extra Vol. II, pages 187–196, 1998. MR **99j:**14023

[Mum] D. Mumford. A remark on Mahler's compactness theorem. *Proc. Amer. Math. Soc.* **28**(1971), 289–294. MR **43:**2157

[Nag] S. Nag. *The Complex Analytic Theory of Teichmüller Space*. Wiley, 1988. MR **89f:**32040

[NN] M. S. Narasimhan and M. V. Nori. Polarisations on an abelian variety. *Proc. Indian Acad. Sci. Math. Sci.* **90**(1981), 125–128. MR **83f:**14033

[Ot] J.-P. Otal. *Le théorème d'hyperbolisation pour les variétés fibrées de dimension trois*. Astérisque, volume 235, 1996. MR **97e:**57013

[Par] A. N. Parshin. Algebraic curves over function fields. *Soviet Math. Dokl.* **183**(1968), 524–526. MR **38:**4478

[Rez1] A. Reznikov. Three-manifolds class field theory. *Selecta Math.* **3**(1997), 361–399. MR **96b:**57041

[Rez2] A. Reznikov. Hakenness and b_1. *Preprint, 1998.*

[Ri] K. Ribet. Galois representations and modular forms. *Bull. Amer. Math. Soc.* **32**(1995), 375–402. MR **96b:**11073

[RS] K. Rubin and A. Silverberg. A report on Wiles' Cambridge lectures. *Bull. Amer. Math. Soc.* **31**(1994), 15–38. MR **94k:**11062

[Sch] L. Schneps, editor. *The Grothendieck theory of dessins d'enfants (Luminy, 1993)*, volume 200 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, 1994. MR **95f:**11001

[So] C. Soulé. *Lectures on Arakelov geometry*. Cambridge University Press, 1992. MR **94e:**14031

[Sz] L. Szpiro. La conjecture de Mordell [d'après G. Faltings]. In *Séminaire Bourbaki, 1983/84*, pages 83–104. Astérisque, volume 121–122, 1985. MR **87c:**11033

[TW] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)* **141**(1995), 553–572. MR **96d:**11072

[Th1] W. P. Thurston. On the geometry and dynamics of diffeomorphisms of surfaces. *Bull. Amer. Math. Soc.* **19**(1988), 417–432. MR **89k:**57023

[Th2] W. P. Thurston. Hyperbolic structures on 3-manifolds II: Surface groups and 3-manifolds which fiber over the circle. *Preprint, 1986.*

[Voj1] P. Vojta. *Diophantine Approximations and Value Distribution Theory*, volume 1239 of *Lecture Notes in Mathematics*. Springer-Verlag, 1987. MR **91k:**11049

[Voj2] P. Vojta. Siegel's theorem in the compact case. *Ann. of Math.* **133**(1991), 509–548. MR **93d:**11065

[Wl1] A. Weil. On discrete subgroups of Lie groups. *Annals of Math.* **72**(1960), 369–384. MR **25:**1241

[Wl2] A. Weil. Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques [1939a]. In *Oeuvres Scient.*, volume I, pages 236–240. Springer-Verlag, 1980.

[Wi] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* **141**(1995), 443–551. MR **96d:**11071

[Wol] S. Wolpert. Geodesic length functions and the Nielsen problem. *J. Diff. Geom.* **25**(1987), 275–296. MR **88e:**32032

Mathematics Department, Harvard University, 1 Oxford Street, Cambridge, MA 02138-2901