Riemann Surfaces in

Dynamics, Topology and Arithmetic

III. From dynamics on surfaces to rational points on curves

Curtis T. McMullen

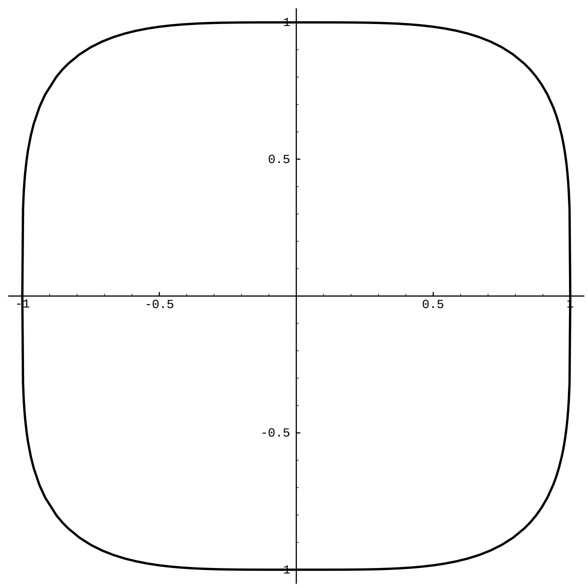
Harvard University, Cambridge, MA

Finite Fermat

Fermat's equation: $X^n + Y^n = Z^n$.

Theorem *For $n \geq 4$, Fermat's equation has only finitely many solutions with $X, Y, Z \in \mathbb{Z}$ and $(X, Y, Z) = 1$.*

—Faltings, 1983 (Mordell's Conjecture)



The curve $X^4 + Y^4 = 1$ meets $\mathbb{Q} \times \mathbb{Q}$ in a finite set.

Our goal:

Trace a path from the classification of surface diffeomorphisms to the proof of Finite Fermat.

Roadmap

Geometry

- Consider families of Riemann surfaces C/B,
  $\dim B = 1$, fiber genus $g \geq 2$.
- **There are only finitely many truly varying families over a given base B.**
- **Each family has only finitely many sections $\sigma : B \to C$.**

Arithmetic

- Consider $X^n + Y^n = Z^n$ as a curve C over

$$\mathrm{B} = (\text{prime numbers } p \in \mathbb{Z}) \ .$$

- Sections $\rightsquigarrow$ Integral solutions.
  Monodromy $\rightsquigarrow$ Action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $H_*(C)$.

- Control of Galois dynamics $\implies$
  Finiteness of families C/B $\implies$
  Finiteness of sections $\implies$
  Finiteness of integral solutions = **Finite Fermat**.

Finiteness of Families

Theorem *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.*

—Parshin 1968; Arakelov 1971; Imayoshi and Shiga, 1988.

Family C/B means:

- **Base:** $B = \overline{B} - S$, the complement of a finite set S in a compact Riemann surface $\overline{B}$.
- **Total space:** C, $\dim_{\mathbb{C}} C = 2$, equipped with a holomorphic fibration $\pi : C \to B$;
- **Fibers:** $C_t = \pi^{-1}(t) =$ compact Riemann surfaces of genus g.

A family is either

- **locally constant:** $C_t \cong C_u$ for all $t, u \in B$; or
- **truly varying**.

Classifying map and monodromy

Family $C/B \implies$

Classifying map:

$$\begin{aligned} F &: B \to \mathcal{M}_g \\ F(t) &= [C_t] \end{aligned}$$

Monodromy representation:

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

Lift:

$$\widetilde{F} : \widetilde{B} \to \mathcal{T}_g \overset{\beta}{\hookrightarrow} \mathbb{C}^{3g-3},$$

with image a bounded domain.

Theorem *If B is a compact Riemann surface of genus 0 or 1, then all families C/B are trivial.*

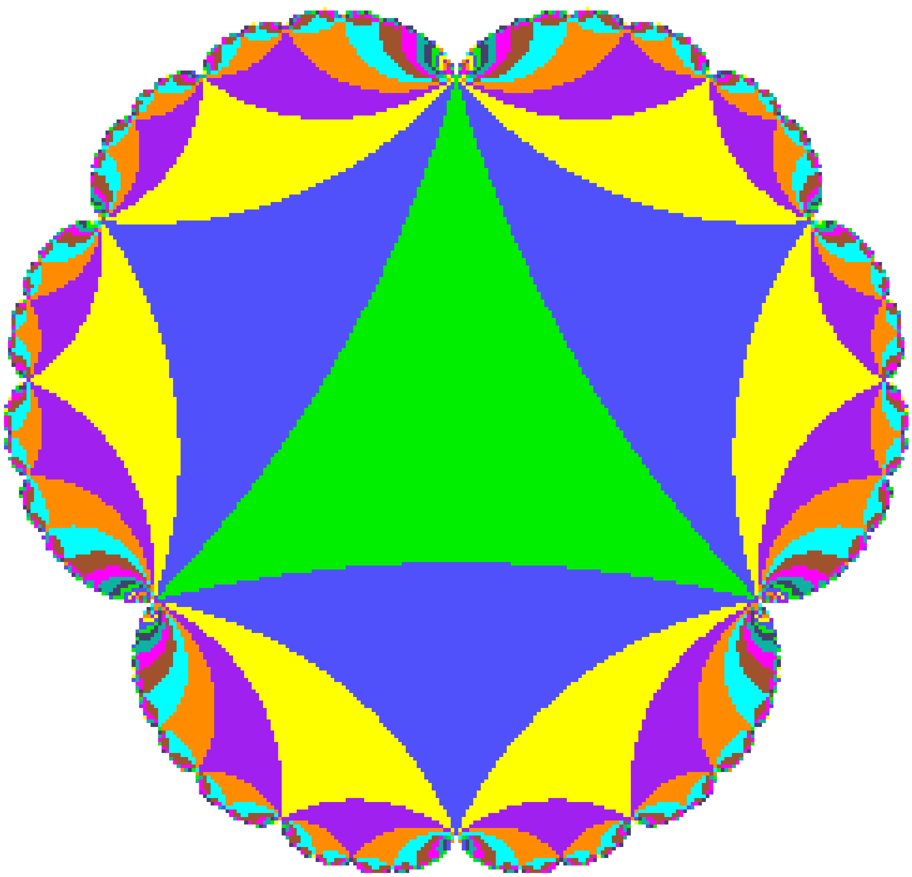
Proof. A bounded holomorphic function on $\widehat{\mathbb{C}}$ or $\mathbb{C}$ is constant. ∎

Bers' embedding of Teichmüller space

For any basepoint $X \in \text{Teich}(S)$, Bers gives a complex analytic embedding:

$$\beta_X : \text{Teich}(S) \to Q(X) \cong \mathbb{C}^{3g-3}.$$

The image is a **bounded domain**.



Embedding of $\text{Teich}(S)$ for S a punctured torus

Modular Schwarz Lemma

Now assume the base B is a hyperbolic Riemann surface.

Theorem *The classifying map $F : B \to \mathcal{M}_g$ is distance-decreasing from the*

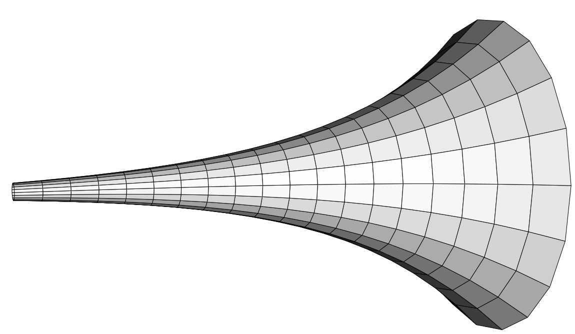
(hyperbolic metric on B) to the
(Teichmüller metric on $\mathcal{M}_g$).

Corollary (Lefschetz) *For any family C/Δ^*, a finite iterate of the monodromy is a product of Dehn twists.*

Proof.

$\pi_1(\Delta^*)$ has short generator $\implies$ $\tau(\text{monodromy}) = 0$ $\implies$ monodromy is virtually a Dehn twist,

by the classification of surfaces diffeomorphisms. ∎



The hyperbolic geometry of Δ^*

Proof of Finiteness of Families

I. Reducible $\implies$ trivial.

Reducible means the monodromy group

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

preserves simple loops $\{\alpha_1, \ldots, \alpha_m\}$ on C_t.

Reducible $\implies$ Each hyperbolic length

$$L_i(t) = \ell_{\alpha_i}(C_t)$$

is subharmonic on B, hence constant.

$\implies$ Boundary values of $\widetilde{F} : \widetilde{B} \to \mathcal{T}_g$
lie in (convex) locus where $\{\alpha_1, \ldots, \alpha_m\}$ are pinched

$\implies$ $\widetilde{F}(\widetilde{B}) \subset \partial\mathcal{T}_g$
$\implies$ $\widetilde{F}$ is constant $\implies$ C/B is trivial.

Avoiding the end of $\mathcal{M}_g$

II. Compactness. The space

$$\mathcal{F} = (\text{classifying maps } F : B \to \mathcal{M}_g),$$

for truly varying families, is compact.

Modular Schwarz Lemma $\implies$
F Lipschitz with constant 1 for all $F \in \mathcal{F}$.

Fix a basepoint $t \in B$.

$F_n(t) = C_n \to \infty$ in $\mathcal{M}_g \implies$
C_n has short loops $\{\alpha_1, \ldots, \alpha_m\}$ for $n \gg 0$ (Mumford)
$\implies$ monodromy reducible $\implies$ F is constant.

Thus $F(t) \in K$ compact $\subset \mathcal{M}_g$ for all $F \in \mathcal{F}$

$\implies$ $\mathcal{F}$ is compact (Arzela-Ascoli).

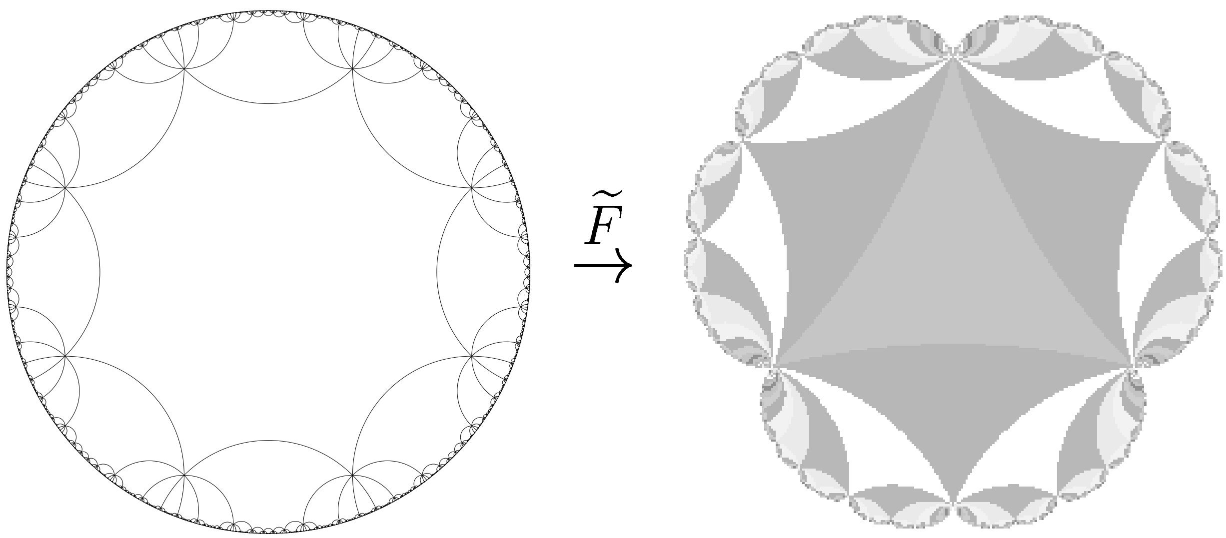
The role of monodromy

III. Discreteness. A classifying map is determined by its monodromy.

$\widetilde{F}(gx) = F_*(g) \cdot \widetilde{F}(x) \implies$ Monodromy determines

$$\partial\widetilde{F} : \partial\widetilde{B} \to \partial\mathcal{T}_g,$$

which determines F.



$\widetilde{B}$ $\qquad\qquad$ $\mathcal{T}_g$

IV. Finiteness. Compact + discrete $\implies$ $\mathcal{F}$ is finite.

The classifying map F determines C/B up to finitely many choices $\implies$ the set of truly varying families is finite. ∎

- Compare the finiteness of $\mathrm{Aut}(X)$.

From sections to families

Theorem (Parshin trick)
Given a genus $g \geq 1$ and a base B, there exists a genus $h \geq 2$ and a finite-to-one map

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

Construction of D from (C, s):

Take covering space $(D', s') \to (C, s)$ coming from

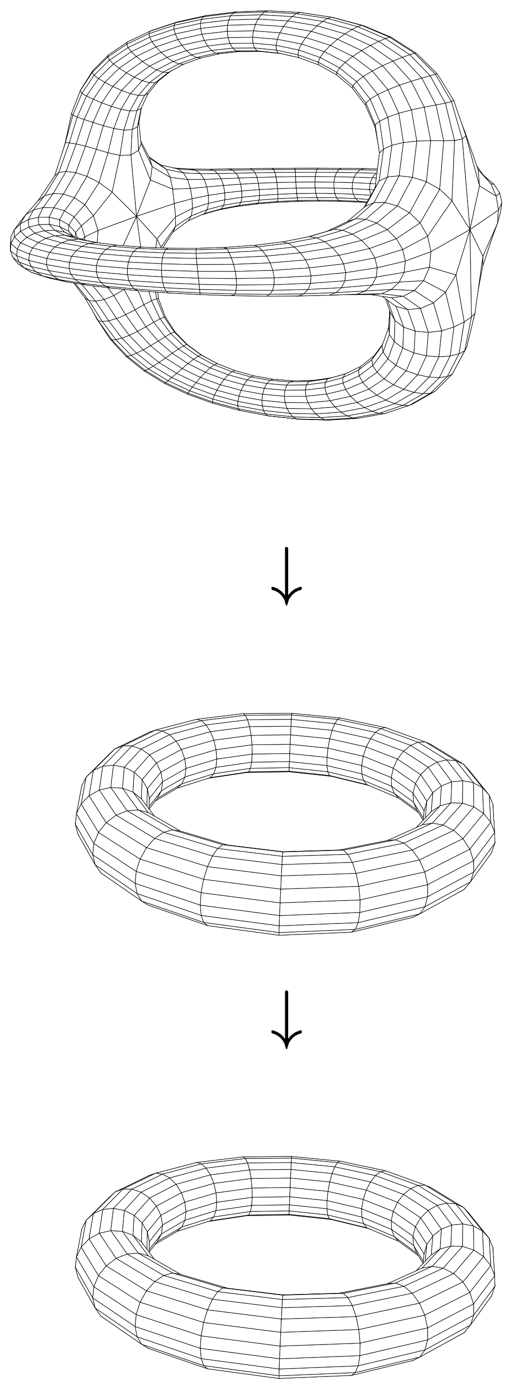
$$\pi_1(C) \to H_1(C, \mathbb{Z}/2);$$

Take branched covering $D \to D'$ coming from

$$\pi_1(D' - s') \to H_1(D' - s', \mathbb{Z}/2).$$

Composite is a **natural solvable cover** $D \to C$ branched over s.

Branched covers



Geometric Mordell Conjecture

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

From geometry to algebra

Geometry	**Algebra**
$\overline{B}$ = compact Riemann surface	K = field of meromorphic functions on $\overline{B}$
Point $p \in \overline{B}$	Valuation $v_p : K^* \to \mathbb{Z}$ $v_p(f)$ = order of zero of f at p.
Finite branched covers $\overline{B}' \to \overline{B}$	Finite field extensions K'/K
Covering spaces of $B = \overline{B} - S$	K'/K unramified outside S
Profinite completion $\widehat{\pi}_1(B)$ $= \varprojlim \pi_1(B)/N$, $\pi_1(B)/N$ finite	Galois group $\mathrm{Gal}(\overline{K}_S/K)$, $\overline{K}_S = \varinjlim K'$, K'/K finite, unramified outside S

The Jacobian

For X a Riemann surface of genus g:
The Jacobian of X is the Abelian group–variety:

$$\begin{aligned} \mathrm{Jac}(X) &= (\text{holomorphic 1-forms on } X)^*/H_1(X,\mathbb{Z}) \\ &\cong \mathbb{C}^g/\Lambda. \end{aligned}$$

Family $C/B \mapsto$ Family of Abelian varieties A/B:

$$A_t = \mathrm{Jac}(C_t).$$

Geometry	**Algebra**
Bundle of homology groups $H_1(C_s, \mathbb{Z}/\ell^n)$	Points of finite order $A[\ell^n] \cong (\mathbb{Z}/\ell^n)$
Action of $\pi_1(B,t)$ on $H_1(C_t, \mathbb{Z}/\ell^n)$	Action of $\mathrm{Gal}(\overline{K}_S/K)$ on points $A[\ell^n]$ of variety A/K

Algebraic monodromy

Algebraic monodromy:

$$\rho_\ell : \mathrm{Gal}(\overline{K}_S/K) \to GL_{2g}(\mathbb{Z}_\ell),$$

obtained in limit as $n \to \infty$:

$$\begin{aligned} \mathbb{Z}_\ell &= \varprojlim \mathbb{Z}/\ell^n \\ &= \text{(the } \ell\text{-adic integers).} \end{aligned}$$

Retreat to action of π_1 on $H_1(C_t)$:

$$\begin{array}{ccccc} \pi_1(B,t) & \xrightarrow{F_*} & \mathrm{Mod}(C_t) & & \textbf{(Geometry)} \\ \downarrow & & \downarrow & & \\ \widehat{\pi}_1(B) & & \mathrm{Aut}\, H_1(C_t, \mathbb{Z}_\ell) & & \\ \downarrow & & \downarrow & & \\ \mathrm{Gal}(\overline{K}_S/K) & \xrightarrow{\rho_\ell} & GL_{2g}(\mathbb{Z}_\ell) & & \textbf{(Algebra)} \end{array}$$

$\mathbb{Z}$ as a space

Geometry	**Algebra**
Base $\overline{B}$ = compact Riemann surface	Base $\operatorname{Spec}\mathbb{Z} = \{0, 2, 3, 5, 7, 11, 13, \ldots\}$
$K =$ (meromorphic functions on $\overline{B}$.)	$K = \mathbb{Q}$
Points $p \in \overline{B}$	Primes $p \in \mathbb{Z}$
$v_p(f) =$ (order of zero of f at p)	$v_p(ap^n) = n$

Shape of a prime

<table>
<tr><th>Geometry</th><th>Algebra</th></tr>
<tr><td colspan="2">Valuation $v_p \rightsquigarrow$
Local field $k =$
$\{f \in K^* \ : \ v_p(f) \geq 0\}/\{v_p(f) > 0\}$
Local $\widehat{\pi}_1 = \mathrm{Gal}(\overline{k}/k)$</td></tr>
<tr><td>$k = \mathbb{C}$</td><td>$k = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$</td></tr>
<tr><td>$\widehat{\pi}_1 = \{1\} = \widehat{\pi}_1(p)$</td><td>$\widehat{\pi}_1 = \widehat{\mathbb{Z}} = \widehat{\pi}_1(S^1)$</td></tr>
<tr><td>Points look like points</td><td>Points look like circles</td></tr>
</table>

Finite Fermat and Families

Theorem *The degree $n \geq 4$ Fermat curve $C \subset \mathbb{P}^2$, defined by*

$$X^n + Y^n = Z^n,$$

has only finitely many rational points.

Strategy: Regard C as a family of curves over the primes of $\mathbb{Z}$.

Geometry	**Algebra**
Family C/B	Curve $C/\mathbb{Z}$
Fibers $C_p/k = \mathbb{C}$ smooth for $p \in B = \overline{B} - S$	Fibers $C_p/k = \mathbb{F}_p$, smooth for $p \in \operatorname{Spec} \mathbb{Z} - S$
Section $s : B \to C$, $s(p) \in C_p$	Rational point s on C, $s \bmod p \in C_p$

Shafarevich Conjecture

Theorem *For any genus $g \geq 2$ and finite set of primes $S \subset \mathbb{Z}$, there are only finitely many curves $C/\mathbb{Z}$ of genus g smooth outside S.*

Similarly for number fields $K/\mathbb{Q}$.

$\Longrightarrow$ Finite Fermat, by the **Parshin trick**:

Geometry	**Algebra**
Section determines a new family D/B	Point $s \in C(\mathbb{Q})$ determines arithmetic curve $D \to C$ branched over s

Monodromy dictionary

Geometry	Algebra
$\pi_1(B) = \pi_1(\overline{B} - S)$	$\mathrm{Gal}(\overline{\mathbb{Q}}_S/\mathbb{Q})$
Mapping-class group $\mathrm{Mod}(C_t)$	$\mathrm{Aut}\, H_1(C, \mathbb{Z}_\ell) \cong GL_{2g}(\mathbb{Z}_\ell)$
Monodromy representation $F_* : \pi_1(B, t) \to \mathrm{Mod}(C_t)$	ℓ-adic Galois representation $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}_S/\mathbb{Q}) \to GL_{2g}(\mathbb{Z}_\ell)$
Points look like points	Primes look like loops
??	Frobenius loops $[\sigma_p] \in \mathrm{Gal}(\overline{\mathbb{Q}}_S/\mathbb{Q})$ for each prime $p \notin S$

Proof of the Shafarevich Conjecture

---

1. Semisimplicity.

The monodromy $\widehat{\rho}_\ell$ is semisimple.
$\Longrightarrow$ *$\widehat{\rho}_\ell$ is determined by its trace*

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

Example: $\rho_\ell(g) = \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ is ruled out.
$\rightsquigarrow$ Irreducibility of F_*.

---

2. Finite generation.

There is a finite set of primes T such that

$$\langle \mathrm{Tr}(\sigma_p) \ : \ p \in T \rangle$$

determines $\widehat{\rho}_\ell$.

$\rightsquigarrow$ Finite generation of $\pi_1(B)$.

Finiteness of monodromy

---

3. The Weil bounds.

Traces are integers, and we have the bound

$$|\operatorname{Tr} \circ \rho_\ell(\sigma_p)| \leq M$$

independent of C.

Proof: Lefschetz fixed-point formula for Frobenius gives

$$\begin{aligned} |C(\mathbb{F}_p)| &= |\{x : \sigma_p(x) = x\}| = O(gp) \\ &= \sum (-1)^i \operatorname{Tr}(\sigma_p | H^i(C, \mathbb{Q}_\ell)) \\ &= 1 - \operatorname{Tr}(\sigma_p | H^1(C, \mathbb{Q}_\ell)) + p. \end{aligned}$$

$\rightsquigarrow$ Modular Schwarz Lemma $\Longrightarrow$

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

Q. Does the Weil bound control the 'hyperbolic length' of a prime?

(1–3): *Only finitely many monodromy representations $\widehat{\rho}_\ell$ occur for fixed genus $g(C)$.*

Final steps: Rigidity and finiteness

---

4. Rigidity.

Monodromy $\widehat{\rho}_\ell$ *determines* $A = \mathrm{Jac}(C)$ *up to isogeny over* $\mathbb{Q}$.

Isogeny $A \sim A'$ = finite-to-one surjective map.

---

5. Finiteness.

There are only finitely many $A' \sim A$ *over* $\mathbb{Q}$.

Idea: control the height

$$h(A) \;=\; -\log\left(\int_{A(\mathbb{C})} |\theta|^2\right),$$

$\theta \in \Omega_{\mathbb{Z}}(A)$; and show

$$|\{A \;:\; h(A) \leq H\}| < \infty.$$

$\rightsquigarrow$ Mumford's Theorem: $\{C \in \mathcal{M}_g \;:\; \ell(C) \geq r > 0\}$ is compact.

---

6. Torelli theorem.

$A = \mathrm{Jac}(C)$ *determines* C.

∎

Primes as knots

One should picture the primes $p \in \operatorname{Spec}\mathbb{Z}$ not just as loops, but as knots in S^3.

—Mazur, Manin, ...

Evidence:

- $\operatorname{Spec}\mathbb{Z}$ is simply-connected
  (there are no unramified extension of $\mathbb{Q}$)
- $\operatorname{Spec}\mathbb{Z}$ is a homology 3-sphere
  ($H^p(\operatorname{Spec}\mathbb{Z}, \mathbb{G}_m) = 0$ except for $p = 0$ and $p = 3$)
- Class field theory $\longleftrightarrow$ homology of branched covers of S^3
- Iwasawa theory provides the Alexander polynomial of a prime.