ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 39, Number 2, 2009

LIFTING PROPERTIES OF PRIME GEODESICS

DARIN BROWN

ABSTRACT. We continue the study begun by Sarnak and Stopple of prime geodesics on $\Gamma\backslash\mathcal{H}$, Γ the modular group. We now allow Γ to be a Fuchsian group whose matrix entries lie in the ring of integers $\mathcal{O}_K$ of a number field K. There is a one-to-one correspondence between the prime geodesics $\mathcal{P}$ on $\Gamma\backslash\mathcal{H}$ and the primitive hyperbolic conjugacy classes $\{\gamma\}$ in Γ. An eigenvalue ε of an element of $\{\gamma\}$ determines a quadratic extension field $K(\varepsilon)$ of K. On the other hand, a prime ideal Q of $\mathcal{O}_K$ determines covering surfaces of $\Gamma\backslash\mathcal{H}$. A Frobenius map relates the lifting of $\mathcal{P}$ to the splitting of Q in $K(\varepsilon)$.

1. Introduction. One of the most important objects of study in number theory and geometry is the *modular group*

$$\Gamma := SL\,(2, \mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{Z} \text{ and } ad - bc = 1 \right\},$$

which acts on the upper half-plane $\mathcal{H} := \{z \in \mathbf{C} : \mathrm{Im}\,(z) > 0\}$ via linear fractional transformation $z \mapsto (az+b)/(cz+d)$. The orbits of $\mathcal{H}$ under this action form a quotient surface which has *fundamental domain*

$$\Gamma\backslash\mathcal{H} := \{z \in \mathbf{C} : |z| > 1 \text{ and } |\mathrm{Re}\,(z)| < 1/2\}.$$

Gauss was the first to study the modular group when he explored the equivalence and reduction of binary quadratic forms. Gauss must have been aware of the interplay here between number theory and geometry: definite forms may be interpreted as points in $\mathcal{H}$, and indefinite forms may be interpreted as geodesic semicircles on $\mathcal{H}$. Reduction of forms is obtained by letting the modular group carry points or geodesics to the fundamental domain. This gives a geometric explanation for why the study of indefinite forms is more difficult than the study of definite forms.

If $\gamma \in \Gamma$ and $|\mathrm{tr}\,(\gamma)| > 2$, then γ is *hyperbolic* and determines two distinct real fixed points. The geodesic semi-circle on $\mathcal{H}$ joining

Received by the editors on June 2, 2005, and in revised form on August 4, 2006.
DOI:10.1216/RMJ-2009-39-2-437

these points projects to a periodic geodesic on $\Gamma\backslash\mathcal{H}$. The segment of this geodesic semi-circle joining a point P to γP projects to a *closed geodesic* on $\Gamma\backslash\mathcal{H}$, i.e., a closed curve. In this way, there is a one-to-one correspondence between the closed geodesics on $\Gamma\backslash\mathcal{H}$ and the hyperbolic conjugacy classes in Γ. A *prime geodesic* on $\Gamma\backslash\mathcal{H}$ is a closed geodesic that traces out its image exactly once. Prime geodesics satisfy an asymptotic distribution law similar to the prime number theorem [**7**, page 40].

The *Selberg trace formula* is a nonabelian generalization of Poisson summation which relates the length spectrum of $\Gamma\backslash\mathcal{H}$ to the spectral decomposition of the hyperbolic Laplace-Beltrami operator

$$\Delta := y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right)$$

on $L^2(\Gamma\backslash\mathcal{H})$. ("You see the lengths, and you hear the eigenvalues." [**13**, page 295].) Finding the lengths of prime geodesics on $\Gamma\backslash\mathcal{H}$ is then important, because this tells us about the Selberg trace formula.

Now, suppose Γ is a *Fuchsian group* (a discontinuous subgroup of $SL(2,\mathbf{R})$) whose matrix entries lie in the ring of integers $\mathcal{O}_K$ of a number field K. For a prime geodesic $\mathcal{P}$ on $\Gamma\backslash\mathcal{H}$ and a prime ideal Q of $\mathcal{O}_K$, the *Frobenius conjugacy class* $\mathrm{Frob}\,(\mathcal{P})$ is the conjugacy class obtained by reducing the associated hyperbolic conjugacy class $\{\gamma\}$ modulo Q. This *Frobenius map* $\mathcal{P} \mapsto \mathrm{Frob}\,(\mathcal{P})$ is analogous to the map taking a prime ideal to its Frobenius conjugacy class in the Galois group of an extension of number fields. On the other hand, an eigenvalue ε of an element of $\{\gamma\}$ determines a quadratic extension field $K(\varepsilon)$ of K. Our first two results relate $\mathrm{Frob}\,(\mathcal{P})$ to the splitting of Q in $K(\varepsilon)$ and to the characteristic polynomial $f(x)$ of γ, respectively. The first of these shows the strong connection between number theory and geometry.

Using these results, we are able to determine how the geodesic $\mathcal{P}$ lifts to $\Gamma(Q)\backslash\mathcal{H}$, where $\Gamma(Q)$ is the congruence subgroup of all matrices in Γ that are equivalent to $\pm I$ mod Q. Using a Selberg zeta function, we are able to derive a *reciprocity law* which relates the lifting of $\mathcal{P}$ to $\Gamma_0(Q)\backslash\mathcal{H}$ to the splitting of Q in $K(\varepsilon)$, where $\Gamma_0(Q)$ is the congruence subgroup of all matrices in Γ which are upper-triangular mod$Q$.

Stopple [**12**] investigated these results in the particular case $\Gamma = SL(2,\mathbf{Z})$. The splitting behavior of prime ideals in quadratic extensions is, of course, well understood. The general idea here is to use this understanding to gain information about prime geodesics.

2. Prime geodesics. Let $\overline{\mathcal{H}} := \mathcal{H} \cup \mathbf{R} \cup \{\infty\}$. For any two distinct points P and P' in $\overline{\mathcal{H}}$, let $G(P, P')$ denote the geodesic segment joining P and P'. If Γ is a Fuchsian group, then the identification map makes $\mathcal{H}$ a covering surface of $\Gamma\backslash\mathcal{H}$, and $G(P, P')$ projects to a geodesic segment $\mathcal{P}(P, P')$ on $\Gamma\backslash\mathcal{H}$. In particular, if $\gamma \in \Gamma$ is hyperbolic, then we define $G(\gamma) := G(z, w)$, where z and w are the fixed points of γ. The geodesic $G(\gamma)$ on $\mathcal{H}$ then projects to a *periodic geodesic* $\mathcal{P}(z, w)$ on $\Gamma\backslash\mathcal{H}$. This periodic geodesic traces out its image infinitely often and has infinite length. If we fix $P \in G(\gamma)$, we obtain the *closed geodesic* $\mathcal{P}(P, \gamma P)$. This closed geodesic traces out its image an integral number of times and has finite length. We choose not to distinguish between closed geodesics which differ only by a change of basepoint P on $G(\gamma)$. In this way, we obtain a mapping $\gamma \mapsto \mathcal{P}(\gamma) := \mathcal{P}(P, \gamma P)$ which maps hyperbolic elements of Γ to closed geodesics on $\Gamma\backslash\mathcal{H}$. We make the standing assumption that all closed geodesics are nonconstant. Under this assumption, the given map is surjective, and it can be shown that $\mathcal{P}(\gamma) = \mathcal{P}(\gamma')$ if and only if γ and γ' are conjugate in Γ. This establishes a one-to-one correspondence between the hyperbolic conjugacy classes $\{\gamma\}$ in Γ and the closed geodesics on $\Gamma\backslash\mathcal{H}$.

Proposition 1. *Let K be a number field with a ring of integers $\mathcal{O}_K$, and let Γ be a Fuchsian group with $\Gamma \subseteq \mathrm{SL}(2, \mathcal{O}_K)$. Let $\mathcal{P}$ be a closed geodesic on $\Gamma\backslash\mathcal{H}$ with associated hyperbolic conjugacy class $\{\gamma\}$. Let $f(x) = x^2 - tx + 1$ be the characteristic polynomial of γ, where $t > 2$ is the trace of γ. Suppose that $f(x)$ is irreducible over K. Then there exists a unique $\varepsilon > 1$ such that*

- *$K(\varepsilon)$ is a real quadratic extension of K.*
- *ε is a unit in $K(\varepsilon)$.*
- *The minimum polynomial of ε over K is $f(x)$.*
- *The eigenvalues of γ are ε, ε^{-1}, and so the Jordan form of γ is $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$ and $t = \varepsilon + \varepsilon^{-1}$.*

• *The length* $l = l(\mathcal{P})$ *of the closed geodesic* $\mathcal{P}$ *is* $l = 2\log(\varepsilon) := \log(N(\mathcal{P}))$, *where* $N(\mathcal{P})$ *is called the norm of* $\mathcal{P}$, *and so* $\varepsilon = \exp(l/2) = N(\mathcal{P})^{1/2}$ *and* $t = 2\cosh(l/2)$.

It follows that, for any integer $n \neq 0$, the closed geodesic $\mathcal{P}^n$ has associated hyperbolic conjugacy class $\{\gamma\}^n$.

Proof. If γ and γ' are conjugate, then they have the same trace t and the same characteristic polynomial $f(x)$. We calculate the eigenvalue $\varepsilon = (t + \sqrt{t^2 - 4})/2$. If $f(x)$ is irreducible over K, then $f(x)$ is clearly the minimum polynomial of ε over K. Using the Jordan form of γ, the length of $\mathcal{P}$ is the length of the geodesic segment $G(i, \gamma i) = G(i, \varepsilon^2 i)$, which is found to be $2\log(\varepsilon)$. For the last result, note that $\mathcal{P}(\gamma)^{-1} = \mathcal{P}(P, \gamma P)^{-1} = \mathcal{P}(\gamma P, P) = \mathcal{P}((\gamma P), \gamma^{-1}(\gamma P)) = \mathcal{P}(\gamma^{-1})$, while for $n > 0$, $\varepsilon(\mathcal{P}^n) = \exp(l(\mathcal{P}^n)/2) = \exp(nl(\mathcal{P})/2) = \varepsilon(\mathcal{P})^n$, and the result follows by passing to Jordan forms. □

Of particular interest to us are the *prime geodesics* on $\Gamma\backslash\mathcal{H}$; these are the closed geodesics that trace out their image exactly once. There is a one-to-one correspondence between the *primitive* hyperbolic conjugacy classes $\{\gamma\}$ in Γ and the prime geodesics $\mathcal{P}$ on $\Gamma\backslash\mathcal{H}$; here, γ is primitive if it generates its stabilizer $\Gamma_\gamma = \{\delta \in \Gamma : \delta^{-1}\gamma\delta = \gamma\}$ in Γ, or equivalently, if whenever $\alpha \in \Gamma$ and $\alpha^n = \gamma$ for some $n \geq 1$, then $\alpha = \gamma$. In general, Γ_γ is infinitely cyclic and generated by some primitive $\alpha \in \Gamma$. Thus, $\gamma = \alpha^{\pm n}$ for some $n \geq 1$, and so $\{\gamma\} = \{\alpha^{\pm 1}\}^n$. In other words, *each hyperbolic conjugacy class is an integral multiple of a unique primitive hyperbolic conjugacy class* and, geometrically, *each closed geodesic is an integral multiple of a unique prime geodesic.*

3. The lifting of prime geodesics. The set of all formal products $\Pi\mathcal{P}_i^{n_i}$ of prime geodesics is the geometric analogue of the set of all fractional ideals in the ring of integers of a number field. The closed geodesics themselves are then analogous to prime powers. We can fix a positive orientation on the closed geodesics and obtain the analogue of integral ideals; the prime geodesics are then analogous to prime ideals. We wish to obtain the geometric analogues of the notions related to an extension of number fields, namely, the Galois group, the splitting of prime ideals, the decomposition subgroup, and the

Frobenius element/conjugacy class. This requires a brief discussion of deck transformations.

For any subgroup Δ of Γ, $\Delta\backslash\mathcal{H}$ is a covering surface of $\Gamma\backslash\mathcal{H}$, with projection map $p : \Delta\backslash\mathcal{H} \to \Gamma\backslash\mathcal{H}$ given by $p(\Delta z) = \Gamma z$. Note that $1\backslash\mathcal{H} = \mathcal{H}$ is the universal covering surface of $\Gamma\backslash\mathcal{H}$. A *deck transformation* of this covering map p is a homeomorphism $f : \Delta\backslash\mathcal{H} \to \Delta\backslash\mathcal{H}$ such that $p \circ f = p$. The set of all deck transformations of $\Delta\backslash\mathcal{H}$ forms a group, the *deck transformation group* $\mathrm{Aut}\,(p)$ of the covering map p. This group is the geometric analogue of the field automorphism group of an extension of number fields.

If $\Delta \neq 1$, then each prime geodesic $\overline{\mathcal{P}}$ on $\Delta\backslash\mathcal{H}$ projects to a closed geodesic $p \circ \overline{\mathcal{P}}$ on $\Gamma\backslash\mathcal{H}$. Now, $p \circ \overline{\mathcal{P}}$ is an integral multiple of a unique prime geodesic $\mathcal{P}$ on $\Gamma\backslash\mathcal{H}$, say $p \circ \overline{\mathcal{P}} = \mathcal{P}^n$. We have $l(\overline{\mathcal{P}}) = n \cdot l(\mathcal{P})$, and we say that $\overline{\mathcal{P}}$ is an nth *degree prime geodesic lying over* $\mathcal{P}$. Geometrically, this means that, as the image of $\overline{\mathcal{P}}$ is traced out once, the image of $\mathcal{P}$ is traced out n times. This projection of prime geodesics is the geometric analogue of a prime ideal of inertial degree n lying over another prime ideal. We may turn this observation around and ask the following question: for each prime geodesic $\mathcal{P}$ on $\Gamma\backslash\mathcal{H}$, how does $\mathcal{P}$ behave as it is *lifted* to $\Delta\backslash\mathcal{H}$? More precisely, we ask the following two questions.

1. *Which prime geodesics in* $\Delta\backslash\mathcal{H}$ *lie over* $\mathcal{P}$? (*Or at least, how many prime geodesics lie over* $\mathcal{P}$?)

2. *What are the lengths* (*degrees over* $\mathcal{P}$) *of these geodesics?*

This lifting of prime geodesics is the geometric analogue of the splitting of prime ideals. In general, these are very difficult questions to answer, much more difficult than the analogous questions for prime ideals.

4. The Frobenius map. Assume we have a regular (normal) covering map $p : \Delta\backslash\mathcal{H} \to \Gamma\backslash\mathcal{H}$ and an nth degree prime $\overline{\mathcal{P}}$ lying over $\mathcal{P}$. Fix a basepoint x on the image of the geodesic $\mathcal{P}$, and choose an element $\bar{x} \in p^{-1}(x)$ of the fibre on the image of $\overline{\mathcal{P}}$. Then p induces a monomorphism $p_{\#} : \pi_1(\Delta\backslash\mathcal{H}, \bar{x}) \to \pi_1(\Gamma\backslash\mathcal{H}, x)$ of fundamental groups and a monodromy action of $\pi_1(\Gamma\backslash\mathcal{H}, x)$ on the fibre above x, given by the terminal point of a lifting of an element of $\pi_1(\Gamma\backslash\mathcal{H}, x)$. The deck transformation group $\mathrm{Aut}\,(p)$ is then a Galois group $\mathrm{Gal}\,(p)$ isomorphic to the quotient group $\pi_1(\Gamma\backslash\mathcal{H}, x)/p_\#(\pi_1(\Delta\backslash\mathcal{H}, \bar{x}))$ via the monodromy action, and by a coGalois correspondence, $\mathrm{Gal}\,(p)$ is also isomorphic to the quotient group Γ/Δ. Moreover, $\mathrm{Gal}\,(p)$ acts transitively on the set of all primes above $\overline{\mathcal{P}}$ via a change of basepoint. Details and proofs of these facts may be found in [**9**, Chapter 14] and [**7**, pages 45–49].

The prime geodesic $\mathcal{P}$ is itself an element of $\pi_1(\Gamma\backslash\mathcal{H}, x)$, and so we define the *Frobenius element* of $\overline{\mathcal{P}}$ over $\mathcal{P}$ to be the element of $\mathrm{Gal}\,(p)$ associated with $\mathcal{P}$ under this isomorphism. This Frobenius element generates a cyclic *decomposition subgroup* $D(\overline{\mathcal{P}}|\mathcal{P})$ of $\mathrm{Gal}\,(p)$ of order n. This decomposition subgroup is the stabilizer subgroup of $\overline{\mathcal{P}}$ under the action of $\mathrm{Gal}\,(p)$ on the primes above $\mathcal{P}$. Since $\mathrm{Gal}\,(p)$ is isomorphic to Γ/Δ, we see that the Frobenius element is actually an element of Γ/Δ, and the decomposition subgroup is the cyclic subgroup of Γ/Δ generated by this element. As in the case with the Frobenius element of a prime ideal, if $\overline{\mathcal{P}}_1$ and $\overline{\mathcal{P}}_2$ lie over the same prime $\mathcal{P}$, then they are conjugate in Γ/Δ. (Geometrically, the conjugation map is a change of basepoint.) In other words, *each prime geodesic* $\mathcal{P}$ *on* $\Gamma\backslash\mathcal{H}$ *determines a unique Frobenius conjugacy class* $\mathrm{Frob}\,(\mathcal{P})$ *in the Galois group* $\mathrm{Gal}\,(p) \approx \Gamma/\Delta$.

Let us examine these ideas in a particular case. Let K be a number field with a ring of integers $\mathcal{O}_K$, and let Γ be a Fuchsian group with $\Gamma \subseteq SL(2, \mathcal{O}_K)$. Let Q be an ideal of $\mathcal{O}_K$ (not necessarily prime); then

$$\Delta = \Gamma(Q) := \{\gamma \in \Gamma : \gamma \equiv \pm I \bmod Q\}$$

is a subgroup of Γ, the *principal congruence subgroup of level* Q. Here, $A \equiv B \bmod Q$ means that each pair of corresponding entries of A and B is congruent mod Q. Now, assume that Q is a prime ideal of $\mathcal{O}_K$ lying over an odd rational prime p. Then $\mathcal{O}_K/Q \cong \mathbf{F}_q$ is a finite field, where $q = p^n$ for some integer n. We reduce $\gamma \bmod Q$ by reducing each entry of $\gamma \bmod Q$. This defines a reduction mapping $\Gamma \hookrightarrow \mathrm{SL}\,(2, \mathcal{O}_K) \to \mathrm{SL}\,(2, \mathcal{O}_K/Q) \cong \mathrm{SL}\,(2, q)$ where $\gamma \mapsto \widetilde{\gamma}$. Note that $\Gamma(Q)$ is the kernel of this reduction mapping $\gamma \mapsto \widetilde{\gamma}/\pm I$; we conclude that the Galois group $\Gamma/\Delta = \Gamma/\Gamma(Q)$ is isomorphic to the image of this mapping. In general, the reduction mapping might not be surjective, and so $\Gamma/\Gamma(Q)$ might only be isomorphic to a proper subgroup of $\mathrm{PSL}\,(2, q)$.

The dual nature of $f(x)$ (as a characteristic polynomial of γ, and as a minimum polynomial of ε) is the key that will allow us to connect number theory to geometry in the results that follow. Note that $\tilde{f}(x) := f(x) \bmod Q$ is a polynomial over $\mathbf{F}_q$, and the roots of $\tilde{f}(x)$ are

$$x = \frac{t \pm \sqrt{\Delta}}{2} \bmod Q$$

where $t = \mathrm{tr}\,(\gamma)$, $\Delta = t^2 - 4$. Then $\tilde{f}(x)$ is simply the characteristic polynomial of $\widetilde{\gamma}$ considered as a linear operator on the vector space $\mathbf{F}_q \times \mathbf{F}_q$. We can then classify $\widetilde{\gamma}$ according to its Jordan form. However, some care must be taken. Because $\mathbf{F}_q$ is not algebraically closed, it might not be possible to find a matrix in $\mathrm{SL}\,(2,q)$ that conjugates $\widetilde{\gamma}$ to its Jordan form. If this occurs, the conjugacy classes in $\mathrm{SL}\,(2,q)$ associated with that Jordan form will be proper subsets of the Jordan form class. This leads to the following

Definition 2. Let K, $\mathcal{O}_K$, Γ, Q, p, $\mathcal{P}$, $\{\gamma\}$ and $\widetilde{\gamma}$ be as above. The *Frobenius conjugacy class* of γ (the *Frobenius conjugacy class* of $\mathcal{P}$) is the conjugacy class of $\widetilde{\gamma}/\pm I$ in $\mathrm{PSL}\,(2,q)$ and is denoted $\mathrm{Frob}\,(\gamma) = \mathrm{Frob}\,(\mathcal{P})$. (Note that the definition of $\mathrm{Frob}\,(\mathcal{P})$ does not depend on the choice of γ, because $\mathrm{Frob}\,(\mathcal{P})$ is only determined up to conjugacy.)

Fix a nonsquare D in $\mathbf{F}_q$. The *Q-type* of $\mathrm{Frob}\,(\mathcal{P})$ is defined as follows.

• $\mathrm{Frob}\,(\mathcal{P})$ is *Q-central* if $\widetilde{\gamma}$ is conjugate to $\pm I$.

• $\mathrm{Frob}\,(\mathcal{P})$ is *Q-parabolic* if $\widetilde{\gamma}$ is conjugate to one of the following forms:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & D \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -D \\ 0 & -1 \end{pmatrix}.$$

• $\mathrm{Frob}\,(\mathcal{P})$ is *Q-hyperbolic* if $\widetilde{\gamma}$ is conjugate to

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad a \neq \pm 1.$$

• $\mathrm{Frob}\,(\mathcal{P})$ is *Q-elliptic* if $\widetilde{\gamma}$ is conjugate to

$$\begin{pmatrix} a & b \\ Db & a \end{pmatrix}, \quad a \neq \pm 1,$$

Although $\text{Frob}\,(\mathcal{P})$ is a conjugacy class in $\text{PSL}\,(2,q)$, we work in $\text{SL}\,(2,q)$ and implicitly identify matrices and conjugacy classes that are congruent $\bmod \pm I$. Also, it is possible to give explicit formulae for matrices which conjugate $\widetilde{\gamma}$ to its Frobenius conjugacy class representative in $\text{SL}\,(2,q)$ above, thereby showing that each matrix in $\text{SL}\,(2,q)$ is in fact conjugate to precisely one matrix of the above form [**2**, Appendix]. In terms of the characteristic polynomial $\tilde{f}$,

$$\text{Frob}\,(\mathcal{P}) \text{ is } \left\{ \begin{array}{l} Q\text{-central} \\ Q\text{-parabolic} \\ Q\text{-hyperbolic} \\ Q\text{-elliptic} \end{array} \right\} \iff$$

$$\left\{ \begin{array}{l} \tilde{f} \text{ has a double root } = \pm 1 \text{ and } \widetilde{\gamma} \text{ is diagonal} \\ \tilde{f} \text{ has a double root } = \pm 1 \text{ and} \\ \qquad \qquad \text{the Jordan form of } \widetilde{\gamma} \text{ has a single } 2 \times 2 \text{ block} \\ \tilde{f} \text{ has two distinct roots in } \mathbf{F}_q \\ \tilde{f} \text{ has two distinct roots in the quadratic extension } \mathbf{F}_q(\sqrt{D}) \text{ of } \mathbf{F}_q \end{array} \right\}.$$

The presence of D in a matrix indicates that it cannot be conjugated in $\text{SL}\,(2,q)$ to its Jordan form. The elliptic case gives a Pellian equation $a^2 - Db^2 = 1$.

A *congruence subgroup of level* Q is any subgroup Δ of Γ that contains $\Gamma(Q)$, such that whenever Δ contains $\Gamma(Q')$, then Q divides Q'. In addition to $\Gamma(Q)$ itself, an important example of a congruence subgroup of level Q is

$$\Delta = \Gamma_0(Q) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod Q \right\}.$$

For $\Delta = \Gamma(Q)$, we will obtain complete answers to each of the two questions above regarding the lifting of prime geodesics. For $\Delta = \Gamma_0(Q)$, however, we only give a partial answer–disregarding exceptional cases, we will determine the number of *first-degree geodesics* lying over $\mathcal{P}$, i.e., the number of geodesics $\overline{\mathcal{P}}$ such that $p \circ \overline{\mathcal{P}} = \mathcal{P}$. In both of these cases, we will show that the lifting behavior in question is almost always completely determined by the length of $\mathcal{P}$.

Algebra	**Geometry**
Number field K	Hyperbolic surface $\Gamma\backslash\mathcal{H}$
Field extension L/K	Covering projection $p{:}\Delta\backslash\mathcal{H}\to\Gamma\backslash\mathcal{H}$
Galois field extension L/K	Regular covering projection p: $\Delta\backslash\mathcal{H}\to\Gamma\backslash\mathcal{H}$
Algebraic closure $\overline{\mathbf{Q}}/K$	Universal covering projection $\mathcal{H}\to\Gamma\backslash\mathcal{H}$
Field automorphism group $\mathrm{Aut}\,(p)$	Deck transformation group $\mathrm{Aut}\,(L/K)$
Galois group $\mathrm{Gal}\,(L/K)$ of a Galois extension L/K	Galois group $\mathrm{Gal}\,(p)\approx\Gamma/\Delta$ of a regular covering projection p
Absolute Galois group $\mathrm{Gal}\,(\overline{\mathbf{Q}}/K)$	Fundamental group $\pi_1(\Gamma\backslash\mathcal{H},x)\approx\Gamma$
Prime ideal Q of $\mathcal{O}_K$	Prime geodesic $\mathcal{P}$ on $\Gamma\backslash\mathcal{H}$
Power Q^n of a prime ideal Q	Closed geodesic $\mathcal{P}^n$
Fractional ideal I of $\mathcal{O}_K$	Formal product $\Pi\mathcal{P}_i^{n_i}$ of prime geodesics
Integral ideal I of $\mathcal{O}_K$ where $n_i\geq 0$ for all i	Formal product $\Pi\mathcal{P}_i^{n_i}$ of positively-oriented prime geodesics,
Norm of the ideal I	Norm of the closed geodesic $\mathcal{P}$
Prime ideal $\mathfrak{P}$ of inertial degree n lying over Q	Prime geodesic $\overline{\mathcal{P}}$ of degree n lying over $\mathcal{P}$
Splitting of prime ideal Q in L	Lifting of prime geodesic $\mathcal{P}$ to $\Delta\backslash\mathcal{H}$
Minimum polynomial $f(x)$ of ε	Characteristic polynomial $f(x)$ of γ
Decomposition subgroup $D(\mathfrak{P}\mid Q)$	Decomposition subgroup $D(\overline{\mathcal{P}}\mid\mathcal{P})$
Frobenius element/conjugacy class of Q	Frobenius element/ conjugacy class $\mathrm{Frob}\,(\mathcal{P})$
Artin L-function	Selberg zeta function
Landau prime ideal theorem	Prime geodesic theorem [**7**, page 40]
Chebotarev density theorem	Prime geodesic theorem with constraints [**7**, page 49]

5. Algebra and geometry. We present a table which lists various corresponding objects from each of the algebraic and geometric areas. This is not (yet!) an exact mathematical correspondence but should be thought of as a conceptual mental map. The polynomial $f(x)$ is the only object which is strictly identical in both areas.

6. First results. The following proposition reinterprets the definition of the Q-type of $\mathrm{Frob}\,(\mathcal{P})$ into the language of the splitting of prime ideals, by using the fact that the characteristic polynomial $f(x)$ of γ is also the minimum polynomial of the quadratic unit ε.

Proposition 3. *Let K be a number field with a ring of integers $\mathcal{O}_K$, and let Γ be a Fuchsian group with $\Gamma \subseteq \mathrm{SL}(2, \mathcal{O}_K)$. Let Q be a prime ideal of $\mathcal{O}_K$ lying over an odd rational prime p. Let $\mathcal{P}$ be a prime geodesic on $\Gamma\backslash\mathcal{H}$ with associated hyperbolic conjugacy class $\{\gamma\}$. Suppose the characteristic polynomial $f(x) = x^2 - tx + 1$ of γ is irreducible over K, and let $\varepsilon > 1$ be a root of $f(x)$. Let* $\mathrm{ind}(\varepsilon)$ *be the conductor of order $\mathcal{O}_K[\varepsilon]$ in $\mathcal{O}_{K(\varepsilon)}$. If* $\mathrm{Frob}(\mathcal{P})$ *is not Q-central, and if $p \nmid \mathrm{ind}(\varepsilon)$, then*

$$\mathrm{Frob}\ (\mathcal{P})\ \textit{is} \left\{\begin{array}{l} Q\textit{-parabolic} \\ Q\textit{-hyperbolic} \\ Q\textit{-elliptic} \end{array}\right\} \iff Q \left\{\begin{array}{l} \textit{ramifies} \\ \textit{splits} \\ \textit{is inert} \end{array}\right\}\ \textit{in}\ K(\varepsilon).$$

Proof. We combine the definition of the Q-type of $\mathrm{Frob}(\mathcal{P})$ with a standard result on the decomposition of prime ideals in quadratic extensions [**4**, page 79].

$$\begin{aligned} \mathrm{Frob}\ (\mathcal{P})\ \text{is} & \left\{\begin{array}{l} Q\text{-parabolic} \\ Q\text{-hyperbolic} \\ Q\text{-elliptic} \end{array}\right\} \\ & \iff \tilde{f}(x) \left\{\begin{array}{l} \text{has a double root} \\ \text{has two distinct roots} \\ \text{has no roots} \end{array}\right\}\ \text{in}\ \mathbf{F}_q \\ & \iff Q \left\{\begin{array}{l} \text{ramifies} \\ \text{splits} \\ \text{is inert} \end{array}\right\}\ \text{in}\ K(\varepsilon). \qquad \square \end{aligned}$$

The following proposition states that determining the Q-type of the Frobenius conjugacy class $\mathrm{Frob}(\mathcal{P})$ is essentially as difficult as determining squares in $\mathbf{F}_q$.

Proposition 4. *Let K, $\mathcal{O}_K$, Γ, Q, p, $\mathcal{P}$ and $\{\gamma\}$ be as above, let $f(x) = x^2 - tx + 1$ be the characteristic polynomial of γ, and let $\Delta = t^2 - 4$. Then*

$$\text{Frob}\,(\mathcal{P}) \;\; is \;\; \left\{ \begin{array}{l} Q\textit{-central} \\ Q\textit{-parabolic} \\ Q\textit{-hyperbolic} \\ Q\textit{-elliptic} \end{array} \right\}$$

$$\iff \left\{ \begin{array}{l} t \equiv \pm 2 \bmod Q \;\; \textit{and} \;\; \gamma \;\; \textit{is diagonal} \bmod Q \\ t \equiv \pm 2 \bmod Q \;\; \textit{and} \;\; \gamma \;\; \textit{is not diagonal} \bmod Q \\ t \not\equiv \pm 2 \bmod Q \;\; \textit{and} \;\; \Delta \;\; \textit{is a square} \bmod Q \\ \Delta \;\; \textit{is not a square} \bmod Q \end{array} \right\}.$$

In particular, if Frob $(\mathcal{P})$ *is not Q-central, then the Q-type of* Frob $(\mathcal{P})$ *is completely determined by the length of $\mathcal{P}$.*

Proof. We show that each condition on the right implies its corresponding condition on Frob $(\mathcal{P})$; since these conditions are mutually exclusive and exhaustive, this will complete the proof. We begin by making the usual identification $\mathcal{O}_K/Q \cong \mathbf{F}_q$. Let

$$\widetilde{\gamma} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

• Suppose $t \equiv \pm 2 \bmod Q$ and γ is diagonal mod$Q$. Then $b = c = 0$ in $\mathbf{F}_q$, and we have

$$\begin{aligned} & ad - bc = 1 \\ & \Longrightarrow ad = 1 \Longrightarrow 2^2 = (a+d)^2 = \left(a + a^{-1}\right)^2 = a^2 + 2 + a^{-2} \\ & \Longrightarrow a^2 + a^{-2} = 2 \\ & \Longrightarrow \left(a - a^{-1}\right)^2 = 0 \Rightarrow a = a^{-1} = d \Longrightarrow a^2 = 1 \Longrightarrow a = d = \pm 1 \\ & \Longrightarrow \widetilde{\gamma} = \pm I. \end{aligned}$$

Thus, Frob $(\mathcal{P})$ is Q-central.

• Suppose $t \equiv \pm 2 \bmod Q$ and γ is not diagonal mod Q. Then $\Delta = t^2 - 4 \in Q$, i.e., $\Delta = 0$ in $\mathbf{F}_q$. By the quadratic formula, $\tilde{f}(x)$ has a double root in $\mathbf{F}_q$, and since $\widetilde{\gamma} \neq \pm I$, Frob $(\mathcal{P})$ is Q-parabolic.

• Suppose $t \not\equiv \pm 2 \bmod Q$ and Δ is a square in $\mathbf{F}_q$. Since $\Delta = t^2 - 4 = (t+2)(t-2) \not\equiv 0 \bmod Q$, Δ is a nonzero square in $\mathbf{F}_q$, so $\tilde{f}(x)$ has two distinct roots in $\mathbf{F}_q$, and Frob $(\mathcal{P})$ is Q-hyperbolic.

• Finally, suppose Δ is not a square in $\mathbf{F}_q$. Then $\tilde{f}(x)$ must have two distinct roots in a quadratic extension of $\mathbf{F}_q$, and $\mathrm{Frob}\,(\mathcal{P})$ is Q-elliptic.

The last statement follows because $t = 2\cosh(l/2)$, $\Delta = t^2 - 4$ and $f(x) = x^2 - tx + 1$. □

Note that, in practice, distinguishing between Q-central and Q-parabolic matrices is trivial; we simply check if each off-diagonal entry is an element of Q.

We now explore the behavior of a prime geodesic as it is lifted to $\Gamma(Q)\backslash\mathcal{H}$.

Theorem 5. *Let K be a number field with a ring of integers $\mathcal{O}_K$, and let Γ be a Fuchsian group with $\Gamma \subseteq \mathrm{SL}\,(2, \mathcal{O}_K)$. Let Q be a prime ideal of $\mathcal{O}_K$ lying over an odd rational prime p. Let $|\mathcal{O}_K/Q| = q = p^n$, and let $|\Gamma/\Gamma(Q)| = r$. Let $\mathcal{P}$ be a prime geodesic on $\Gamma\backslash\mathcal{H}$ with associated hyperbolic conjugacy class $\{\gamma\}$, let $\widetilde{\gamma} = \gamma \bmod Q$, and let $\varepsilon > 1$ be a root of the irreducible quadratic $f(x)$, as usual. Then all the prime geodesics on $\Gamma(Q)\backslash\mathcal{H}$ lying over $\mathcal{P}$ have the same degree, and*

• *If* $\mathrm{Frob}\,(\mathcal{P})$ *is Q-central, then $\mathcal{P}$ splits completely, i.e., $\mathcal{P}$ lies under exactly r first-degree prime geodesics on $\Gamma(Q)\backslash\mathcal{H}$.*

• *If* $\mathrm{Frob}\,(\mathcal{P})$ *is Q-parabolic, then $\mathcal{P}$ lies under exactly r/p prime geodesics of degree p on $\Gamma(Q)\backslash\mathcal{H}$.*

• *If* $\mathrm{Frob}\,(\mathcal{P})$ *is Q-hyperbolic or Q-elliptic, then $\mathcal{P}$ lies under exactly r/m prime geodesics of degree m on $\Gamma(Q)\backslash\mathcal{H}$, where m is the order of an eigenvalue of $\widetilde{\gamma}$ (up to sign) in the multiplicative group of units of the quadratic extension field $\mathbf{F}_{q^2}$.*

In particular, if $\mathrm{Frob}\,(\mathcal{P})$ *is not Q-central, then the number and degree of the prime geodesics on $\Gamma(Q)\backslash\mathcal{H}$ lying over $\mathcal{P}$ is completely determined by the length of $\mathcal{P}$.*

Proof. Since $\Gamma(Q)$ is the kernel of the reduction mapping $\gamma \mapsto \widetilde{\gamma}/\pm I$, it is a normal subgroup of Γ, and the factor group $\Gamma/\Gamma(Q)$ acts transitively on the set of prime geodesics on $\Gamma(Q)\backslash\mathcal{H}$ lying over $\mathcal{P}$. Thus, all the prime geodesics have the same degree, which is equal to the order m of $\widetilde{\gamma}/\pm I$ in $\Gamma/\Gamma(Q) \subseteq \mathrm{PSL}\,(2, q)$, and there are r/m geodesics lying over $\mathcal{P}$ [**7**, page 47]. Note that m is equal to the order of $\widetilde{\gamma}$ (up to sign) in SL $(2, q)$. Since the order of an element is invariant under conjugation, we may suppose that $\widetilde{\gamma}$ is a Frobenius conjugacy class representative.

- If Frob $(\mathcal{P})$ is Q-central, clearly $m = 1$ and $r/m = r$.
- If Frob $(\mathcal{P})$ is Q-parabolic, then a calculation shows that the order of $\widetilde{\gamma}$, up to sign, is the characteristic p of $\mathbf{F}_q$. Thus, $m = p$ and $r/m = r/p$.
- If Frob $(\mathcal{P})$ is Q-hyperbolic or Q-elliptic, then the order of $\widetilde{\gamma}$, up to sign, is equal to the order of its Jordan form, up to sign, over $\mathbf{F}_{q^2}$. Since this Jordan form is diagonal, and since the eigenvalues are inverses, this is equal to the order of an eigenvalue of $\widetilde{\gamma}$ (up to sign) in the multiplicative group of units of $\mathbf{F}_{q^2}$.

If Frob $(\mathcal{P})$ is not Q-central, then by the previous result, the Q-type of Frob $(\mathcal{P})$ is completely determined by the length of $\mathcal{P}$. If Frob $(\mathcal{P})$ is Q-parabolic, then $\mathcal{P}$ lies under exactly r/p prime geodesics of degree p on $\Gamma(Q)\backslash\mathcal{H}$. If Frob $(\mathcal{P})$ is Q-hyperbolic or Q-elliptic, then an eigenvalue of $\widetilde{\gamma}$ can be found by reducing the eigenvalue ε of γ mod Q, and since $\varepsilon = \exp(l/2)$, the order of this eigenvalue in $\mathbf{F}_{q^2}$ depends only on the length of $\mathcal{P}$. In each case, the number and degree of prime geodesics on $\Gamma(Q)\backslash\mathcal{H}$ lying over $\mathcal{P}$ is completely determined by the length of $\mathcal{P}$. □

7. Interlude–the Selberg zeta function. Before stating and proving the reciprocity law, we present some facts concerning the Selberg zeta function attached to a representation of a Fuchsian group. Let Γ_1 be a subgroup of a Fuchsian group Γ, and let σ be a unitary finite-dimensional representation of Γ_1. Suppose also that $\Gamma_2 = \text{kernel}\,(\sigma)$ contains $\Gamma(Q)$. We define

$$Z\left(s, \Gamma_1/\Gamma_2, \sigma\right) = \prod_{\mathcal{P}} \prod_{k=0}^{\infty} \det \left(I - \sigma\left(\text{Frob }(\mathcal{P})\right) N\left(\mathcal{P}\right)^{-s-k}\right).$$

Here, $\mathcal{P}$ varies over all prime geodesics on $\Gamma_1\backslash\mathcal{H}$, and Frob $(\mathcal{P})$ is a conjugacy class in the finite group Γ_1/Γ_2. (The definition of Frob $(\mathcal{P})$ originally given corresponds to $\Gamma_1 = \Gamma$ and $\Gamma_2 = \Gamma(Q)$.) Taking $\Gamma_1 = \Gamma_2$ and $\sigma = 1$, the trivial representation gives a Selberg zeta function which is more commonly denoted $Z(s, \Gamma_1)$.

The Selberg zeta function has several useful properties similar to those of the Artin L-function [**5**, page 517]. For example, if Γ_2 and Γ_3

are both normal subgroups of Γ_1 with $\Gamma_3 < \Gamma_2$, then any representation σ of Γ_1/Γ_2 defines a unique representation (also denoted σ) of Γ_1/Γ_3. This is called pullback. We have

$$Z\left(s, \Gamma_1/\Gamma_2, \sigma\right) = Z\left(s, \Gamma_1/\Gamma_3, \sigma\right).$$

The Selberg zeta function is also well-behaved with respect to direct sums.

$$Z\left(s, \Gamma_1/\Gamma_2, \sigma_1 \oplus \sigma_2\right) = Z\left(s, \Gamma_1/\Gamma_2, \sigma_1\right) Z\left(s, \Gamma_1/\Gamma_2, \sigma_2\right).$$

Finally, suppose Γ_1 is a subgroup of Γ_0 and σ is a representation of Γ_1 as before. Then Γ_1/Γ_2 is a subgroup of Γ_0/Γ_2, and we can form the induced representation $\operatorname{ind}(\sigma)$ (not to be confused with the index $\operatorname{ind}(\varepsilon)$) [**8**, page 38]. One can show that

$$Z\left(s, \Gamma_1/\Gamma_2, \sigma\right) = Z\left(s, \Gamma_0/\Gamma_2, \operatorname{ind}\left(\sigma\right)\right).$$

All of these properties hold for all *local factors* of the zeta function; in fact, the above properties are proved by piecing together the properties for all local factors.

8. Reciprocity law.

Theorem 6. *Let K be a number field with a ring of integers $\mathcal{O}_K$, and let Γ be a Fuchsian group with $\Gamma \subseteq \mathrm{SL}\left(2, \mathcal{O}_K\right)$. Let Q be a prime ideal of $\mathcal{O}_K$ lying over an odd rational prime p, and let $|\mathcal{O}_K/Q| = q = p^n$. Let $\mathcal{P}$ be a prime geodesic on $\Gamma\backslash\mathcal{H}$ with associated hyperbolic conjugacy class $\{\gamma\}$, and let $\varepsilon > 1$ be a root of the irreducible quadratic $f(x)$, as usual. Then*

$$\mathcal{P} \text{ lies under exactly } \left[\Gamma : \Gamma_0\left(Q\right)\right] \text{ first-degree prime geodesics on } \Gamma_0\left(Q\right)\backslash\mathcal{H} \iff \mathrm{Frob}\left(\mathcal{P}\right) \text{ is } Q\text{-central}.$$

If $\mathrm{Frob}\,(\mathcal{P})$ *is not* Q*-central, and if* $p \nmid \mathrm{ind}\,(\varepsilon)$*, then*

$$\mathcal{P} \text{ lies under exactly } \begin{Bmatrix} 1 \\ 2 \\ 0 \end{Bmatrix} \text{ first-degree prime geodesics on } \Gamma_0(Q)\backslash\mathcal{H} \iff Q \begin{Bmatrix} \text{ramifies} \\ \text{splits} \\ \text{is inert} \end{Bmatrix} \text{ in } K(\varepsilon).$$

In particular, if $\mathrm{Frob}\,(\mathcal{P})$ *is not* Q*-central, and if* $p \nmid \mathrm{ind}\,(\varepsilon)$*, then the number of first-degree prime geodesics on* $\Gamma_0(Q)\backslash\mathcal{H}$ *lying over* $\mathcal{P}$ *is completely determined by the length of* $\mathcal{P}$*.*

Proof. Suppose $\overline{\mathcal{P}}_1, \dots, \overline{\mathcal{P}}_g$ are the prime geodesics lying over $\mathcal{P}$. Then $N(\overline{\mathcal{P}}_i) = N(\mathcal{P})^{f_i}$, i.e., the length of $\overline{\mathcal{P}}_i$ is f_i times the length of $\mathcal{P}$, and $f_1 + \cdots + f_g = [\Gamma : \Gamma_0(Q)]$. Since $\Gamma_0(Q)$ is not a normal subgroup of Γ, the f_i need not all be equal. By using the above properties of the Selberg zeta function and comparing the local factors associated to the prime $\mathcal{P}$, we expand as a polynomial in $N(\mathcal{P})^{-s}$ and see that

$$\begin{aligned} &1 - F \cdot N(\mathcal{P})^{-s} + \cdots + \text{higher terms} \\ &\quad = 1 - [\text{trace }(\text{ind }(1)\,(\text{Frob }(\mathcal{P})))]\, N(\mathcal{P})^{-s} + \cdots + \text{higher terms}, \end{aligned}$$

where F is the number of first-degree prime geodesics on $\Gamma_0(Q)\backslash\mathcal{H}$ lying over $\mathcal{P}$, 1 is the trivial representation of $\Gamma_0(Q)/\Gamma(Q)$, and $\mathrm{ind}\,(1) = 1$ induced up to $\Gamma/\Gamma(Q)$. But, by a result in the character theory of finite groups [**8**, page 30], $\mathrm{trace}\,(\mathrm{ind}\,(1)(\mathrm{Frob}\,(\mathcal{P})))$ is the number of elements $\widetilde{\delta}/\pm I$ of $\Gamma/\Gamma(Q)$ that conjugate an element $\widetilde{\gamma}/\pm I$ of $\mathrm{Frob}\,(\mathcal{P})$ to $\Gamma_0(Q)/\Gamma(Q)$, i.e., to upper-triangular, and such that they are not congruent $\mathrm{mod}\,\Gamma_0(Q)/\Gamma(Q)$. This number is independent of the choice of the element $\widetilde{\gamma}/\pm I$ of $\mathrm{Frob}\,(\mathcal{P})$.

For the remainder of the proof, we work with matrices $\widetilde{\gamma}$, which are only determined up to sign. This does not affect any of the arguments.

• If $\mathrm{Frob}\,(\mathcal{P})$ is Q-central, then $\widetilde{\gamma} = \pm I$, so any matrix $\widetilde{\delta}$ in $\Gamma/\Gamma(Q)$ will conjugate $\widetilde{\gamma}$ to upper-triangular; hence, $F = [\Gamma : \Gamma_0(Q)]$.

If $\mathrm{Frob}\,(\mathcal{P})$ is not Q-central, and if $p \nmid \mathrm{ind}\,(\varepsilon)$, then the proposition relating the Q-type of $\mathrm{Frob}\,(\mathcal{P})$ to the splitting of Q applies.

• If Q ramifies in $K(\varepsilon)$, then $\mathrm{Frob}\,(\mathcal{P})$ is Q-parabolic, and we may assume

$$\widetilde{\gamma} = \pm \begin{pmatrix} 1 & \widetilde{D} \\ 0 & 1 \end{pmatrix}, \quad \widetilde{D} \neq 0.$$

Since $\widetilde{\gamma}$ is already upper-triangular, clearly $I^{-1}\widetilde{\gamma}I = \widetilde{\gamma}$ is upper-triangular. Also, if $\widetilde{\delta} = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is any other element of $\Gamma/\Gamma(Q)$ such that $\widetilde{\delta}^{-1}\widetilde{\gamma}\widetilde{\delta}$ is upper-triangular, then the lower-left entry of $\widetilde{\delta}^{-1}\widetilde{\gamma}\widetilde{\delta}$ is $-\widetilde{D}C^2 = 0$, which implies $C = 0$, so that $\widetilde{\delta}$ is upper-triangular. Hence, $F = 1$.

• If Q splits in $K(\varepsilon)$, then $\mathrm{Frob}\,(\mathcal{P})$ is Q-hyperbolic, and we may assume

$$\widetilde{\gamma} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad a \neq \pm 1.$$

Since $\widetilde{\gamma}$ is already upper-triangular, again $I^{-1}\widetilde{\gamma}I = \widetilde{\gamma}$ is upper-triangular. However, the matrix $\widetilde{\beta} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is clearly not upper-triangular, and $\widetilde{\beta}$ acts by conjugation to switch the eigenvalues on the diagonal of $\widetilde{\gamma}$. If $\tilde{\delta} = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is any other element of $\Gamma/\Gamma(Q)$ such that $\tilde{\delta}^{-1}\widetilde{\gamma}\tilde{\delta}$ is upper-triangular, then the lower-left entry of $\tilde{\delta}^{-1}\widetilde{\gamma}\tilde{\delta}$ is $AC(a^{-1} - a) = 0$. As $a \neq a^{-1}$, we have $C = 0$ or $A = 0$. In the former case, $\tilde{\delta}$ is upper-triangular, and in the latter case $\widetilde{\beta}^{-1}\tilde{\delta}$ is upper-triangular. Hence, $F = 2$.

• If Q is inert in $K(\varepsilon)$, then $\mathrm{Frob}\,(\mathcal{P})$ is Q-elliptic, and an element $\widetilde{\gamma}$ of the Frobenius class cannot possibly be conjugate in $\Gamma/\Gamma(Q)$ to any upper-triangular matrix, since this matrix would necessarily be in Jordan form and hence not be Q-elliptic. Hence, $F = 0$.

The last statement follows by considering the proposition relating the Q-type of $\mathrm{Frob}\,(\mathcal{P})$ to the splitting type of Q in $K(\varepsilon)$, and the proposition which says that the Q-type of $\mathrm{Frob}\,(\mathcal{P})$ is completely determined by the length of $\mathcal{P}$. □

9. Future directions. There are many possible directions for further research based upon these ideas.

• The examples given so far [**2**, Chapter 6] involve the three simplest *Hecke groups*. Examples using other Hecke groups or Fuchsian groups would be welcome.

• Can these ideas be used to say anything about the lifting behavior of prime geodesics on surfaces determined by Fuchsian groups that are not of the type given in the results?

• Can these ideas be used to say anything about the number of *nonfirst-degree* geodesics lying over a given prime geodesic when $\Delta = \Gamma_0(Q)$?

• Can these ideas be used to say anything about the lifting behavior of prime geodesics to $\Delta\backslash\mathcal{H}$ for congruence subgroups $\Delta \neq \Gamma(Q)$ or $\Gamma_0(Q)$?

• The above table of analogies (including Galois groups, splitting/lifting of primes, Frobenius maps, zeta functions, and asymptotic distribution of primes) appears in many other areas of mathematics, e.g., in graph theory [**9, 10**] and in the theory of dynamical systems [**5**]. Is there a general theory which encompasses many of these cases? The beginnings of such a theory can be found in the categorical Galois theory of Grothendieck, Borceux, and Janelidze [**1**] and in the theory of abstract analytic number theory developed by Knopfmacher [**3**]. The former provides a context for algebraic aspects, while the latter focuses on analytic techniques and provides abstract asymptotic distribution results. Each theory has its own notion of "zeta function." Can the two approaches be combined?

REFERENCES

1. Francis Borceux and George Janelidze, *Galois theories*, Cambridge University Press, Cambridge, 2001

2. Darin Brown, *Lifting properties of prime geodesics on hyperbolic surfaces*, Ph.D. dissertation, University of California at Santa Barbara, 2004.

3. John Knopfmacher, *Abstract analytic number theory*, Dover, New York, 1975.

4. Daniel A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.

5. Jurgen Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin, 1999.

6. David Ruelle, *Dynamical zeta functions and transfer operators*, Notices Amer. Math. Soc. **49** (2002), 887–895.

7. Peter Sarnak, *Prime geodesic theorems*, Ph.D. dissertation, Stanford University, 1980.

8. Jean-Pierre Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977.

9. Allan Sieradski, *An introduction to topology and homotopy*, PWS-Kent, Boston, 1992.

10. Harold Stark, and Audrey Terras, *Zeta functions of finite graphs and coverings*, Adv. Math. **121** (1996), 124–165.

11. ———, *Zeta functions of finite graphs and coverings*, Part II, Adv. Math. **154** (2000), 132–195.

12. Jeffrey Stopple, *A reciprocity law for prime geodesics*, J. Number Theory **29** (1988), 224–230.

13. Audrey Terras, *Harmonic analysis on symmetric spaces and applications* I, Springer-Verlag, New York, 1985.

P.O. Box 4302, Manteca, CA 95337-6114
Email address: darincbrown@yahoo.com