A bound for the number of automorphisms of an arithmetic Riemann surfaces

Exposition of a paper by Mikhail Belolipetsky and Gareth Jones

Linda Gruendken[1], Guillermo Mantilla[2], Dermot McCarthy[3], David Roe[4], Kate Stange[5], Ying Zong[1], Maryna Viazovska[6]

[1]University of Pennsylvania, [2]University of Wisconsin, [3]University College Dublin

[4]Harvard University, [5]Brown University, [6]Max Planck Institute

Arizona Winter School, 2008

Outline

Outline

Outline

Consider a Riemann surface as a quotient of $\mathcal{H}$ by its surface group.

$$\mathcal{S} = \Gamma_S \backslash \mathcal{H}$$

Consider a Riemann surface as a quotient of $\mathcal{H}$ by its surface group.

$$\mathcal{S} = \Gamma_S \backslash \mathcal{H}$$

Then its automorphisms can be obtained from the automorphisms of $\mathcal{H}$:

$$\begin{aligned}\mathrm{Aut}(\mathcal{S}) &= \{\alpha \in \mathrm{PSL}(2, \mathbb{R}) : \alpha \Gamma_S \alpha^{-1} = \Gamma_S\}/\Gamma_S \\ &= N(\Gamma_S)/\Gamma_S\end{aligned}$$

(Think: Given $\gamma \in \Gamma_S$, we need $\alpha(\gamma(x)) = \gamma'(\alpha(x))$ for some $\gamma' \in \Gamma_S$.)

Given arithmetic Γ, we will build an arithmetic Riemann surface $\mathcal{S}$ with surface group Γ_S, such that $\Gamma \leq N(\Gamma_S)$.

Given arithmetic Γ, we will build an arithmetic Riemann surface $\mathcal{S}$ with surface group Γ_S, such that $\Gamma \leq N(\Gamma_S)$.

Find a torsion-free normal subgroup K finite index in Γ:

$$1 \longrightarrow K \longrightarrow \Gamma \xrightarrow{p} G \longrightarrow 1$$

Given arithmetic Γ, we will build an arithmetic Riemann surface $\mathcal{S}$ with surface group Γ_S, such that $\Gamma \leq N(\Gamma_S)$.

Find a torsion-free normal subgroup K finite index in Γ:

$$\begin{tikzcd} 1 \arrow[r] & K \arrow[r] & \Gamma \arrow[r, "p"] & G \arrow[r] & 1 \end{tikzcd}$$

Then, if we determine $\mathcal{S}$ by $\Gamma_S = K$, we have

$$\begin{tikzcd} 1 \arrow[r] & \Gamma_S \arrow[r] & N(\Gamma_S) \arrow[r] & \mathrm{Aut}(\mathcal{S}) \arrow[r] & 1 \\ 1 \arrow[r] & \Gamma_S \arrow[r] & \Gamma \arrow[r] \arrow[u, hook] & G \arrow[r] \arrow[u, hook] & 1 \end{tikzcd}$$

Given arithmetic Γ, we will build an arithmetic Riemann surface $\mathcal{S}$ with surface group Γ_S, such that $\Gamma \leq N(\Gamma_S)$.

Find a torsion-free normal subgroup K finite index in Γ:

$$1 \longrightarrow K \longrightarrow \Gamma \xrightarrow{p} G \longrightarrow 1$$

Then, if we determine $\mathcal{S}$ by $\Gamma_S = K$, we have

$$\begin{tikzcd}
1 \arrow[r] & \Gamma_S \arrow[r] & N(\Gamma_S) \arrow[r] & \mathrm{Aut}(\mathcal{S}) \arrow[r] & 1 \\
1 \arrow[r] & \Gamma_S \arrow[r] & \Gamma \arrow[r] \arrow[u, hook] & G \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

We call this a *surface-kernel epimorphism* or SKE.

To verify that the kernel is torsion free, we must check that every element of Γ of finite order has its order preserved by $p : \Gamma \to G$.

To verify that the kernel is torsion free, we must check that every element of Γ of finite order has its order preserved by $p : \Gamma \to G$.

For Fuchsian groups, it suffices to check this for the elements $\gamma_1, \ldots, \gamma_k$ in the canonical presentation.

To verify that the kernel is torsion free, we must check that every element of Γ of finite order has its order preserved by $p : \Gamma \to G$.

For Fuchsian groups, it suffices to check this for the elements $\gamma_1, \ldots, \gamma_k$ in the canonical presentation.

Given Γ, to build an SKE, need:

To verify that the kernel is torsion free, we must check that every element of Γ of finite order has its order preserved by $p : \Gamma \to G$.

For Fuchsian groups, it suffices to check this for the elements $\gamma_1, \ldots, \gamma_k$ in the canonical presentation.

Given Γ, to build an SKE, need:

- epimorphism $p : \Gamma \to G$ to finite group

To verify that the kernel is torsion free, we must check that every element of Γ of finite order has its order preserved by $p : \Gamma \to G$.

For Fuchsian groups, it suffices to check this for the elements $\gamma_1, \ldots, \gamma_k$ in the canonical presentation.

Given Γ, to build an SKE, need:

- epimorphism $p : \Gamma \to G$ to finite group
- p preserves orders of γ_i

To verify that the kernel is torsion free, we must check that every element of Γ of finite order has its order preserved by $p : \Gamma \to G$.

For Fuchsian groups, it suffices to check this for the elements $\gamma_1, \ldots, \gamma_k$ in the canonical presentation.

Given Γ, to build an SKE, need:

- epimorphism $p : \Gamma \to G$ to finite group
- p preserves orders of γ_i

Then we know that G is a subgroup of $\mathrm{Aut}(\mathcal{S})$.

Recall that all triangle groups with a given signature are conjugate, hence triangle groups with a given signature are either all arithmetic, or none are arithmetic.

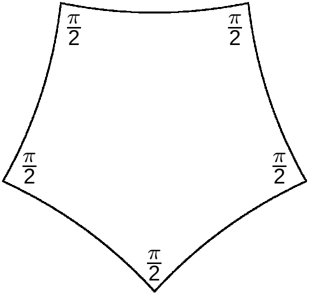
Recall that all triangle groups with a given signature are conjugate, hence triangle groups with a given signature are either all arithmetic, or none are arithmetic.

Arithmetic:

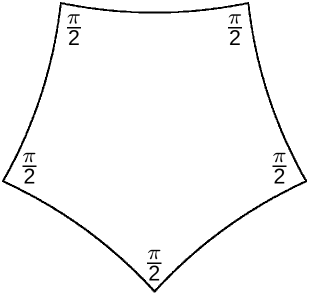
$$\begin{aligned} &(2,3,n), \quad n = 7,8,9,10,11,12,14,16,18,24,30 \\ &(2,4,n), \quad n = 5,6,7,8,9,10,12,18 \\ &(2,5,n), \quad n = 5,6,8,10,20,30 \\ &\qquad\qquad etc. \end{aligned}$$

K. Takeuchi. Arithmetic triangle groups. *J. Math. Soc. Japan* **29** (1977), 91-106.

Consider the right-angled hyperbolic pentagon:

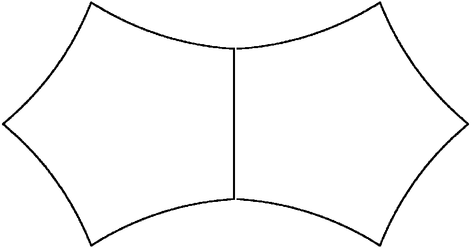


Consider the right-angled hyperbolic pentagon:

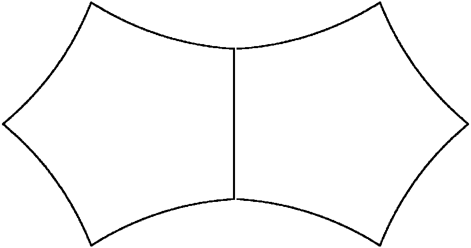


Let Γ be the orientation-preserving subgroup of the group of reflections in its sides.

The fundamental domain for Γ is two copies of the pentagon:

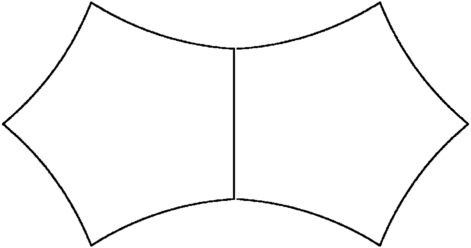


The fundamental domain for Γ is two copies of the pentagon:



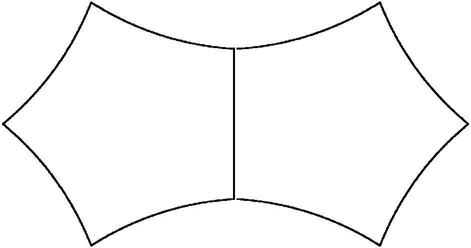
- Only sequences of an even number of reflections are orientation preserving automorphisms.

The fundamental domain for Γ is two copies of the pentagon:



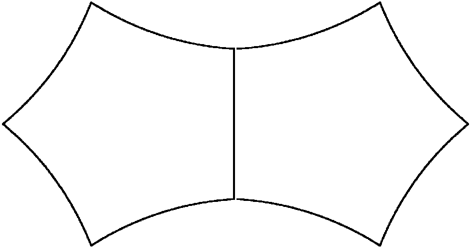
- Only sequences of an even number of reflections are orientation preserving automorphisms.
- Two reflections give rotation around an angle of π. This is order 2. There are five such elements of Γ.

The fundamental domain for Γ is two copies of the pentagon:



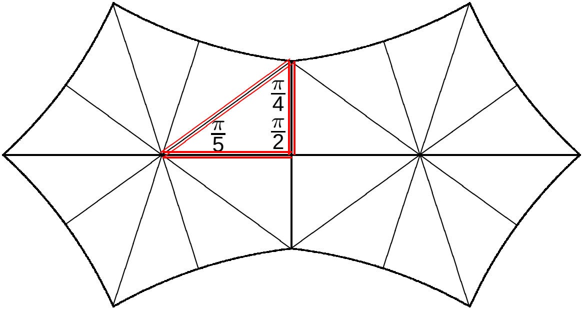
- Only sequences of an even number of reflections are orientation preserving automorphisms.
- Two reflections give rotation around an angle of π. This is order 2. There are five such elements of Γ.
- The signature of the group Γ is $(2, 2, 2, 2, 2)$.

The fundamental domain for Γ is two copies of the pentagon:



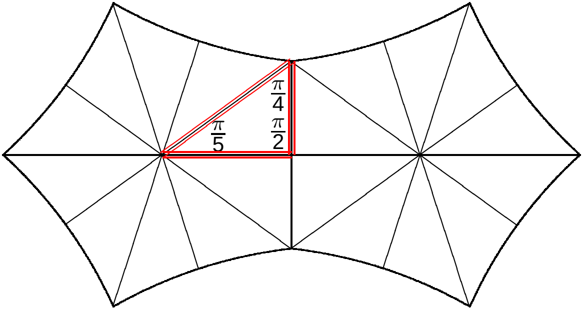
- Only sequences of an even number of reflections are orientation preserving automorphisms.
- Two reflections give rotation around an angle of π. This is order 2. There are five such elements of Γ.
- The signature of the group Γ is $(2, 2, 2, 2, 2)$.
- The Riemann surface $\mathcal{S} = \Gamma\backslash\mathcal{H}$ is of genus zero.

Subdivide the pentagon into 10 congruent triangles:



To show Γ is arithmetic:

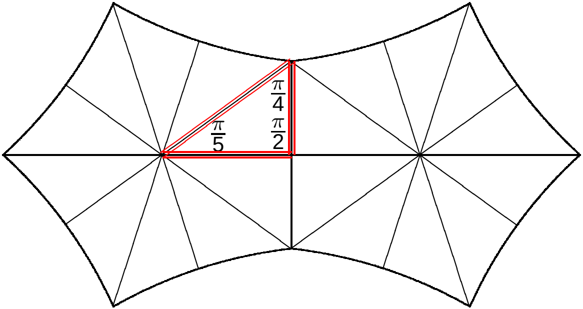
Subdivide the pentagon into 10 congruent triangles:



To show Γ is arithmetic:

- Consider the Fuchsian group Γ' for a triangle.

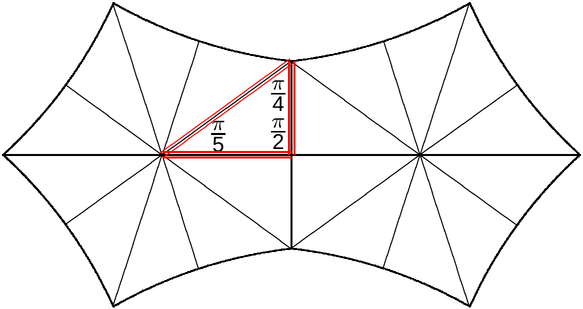
Subdivide the pentagon into 10 congruent triangles:



To show Γ is arithmetic:

- Consider the Fuchsian group Γ' for a triangle.
- The triangle has angles $\pi/2$, $\pi/4$ and $\pi/5$. So Γ' is the $(2, 4, 5)$ triangle group, which is arithmetic.

Subdivide the pentagon into 10 congruent triangles:



To show Γ is arithmetic:

- Consider the Fuchsian group Γ' for a triangle.
- The triangle has angles $\pi/2$, $\pi/4$ and $\pi/5$. So Γ' is the $(2, 4, 5)$ triangle group, which is arithmetic.
- But Γ is a subgroup of Γ' of index 10. Hence the two groups are commensurable, and so Γ is arithmetic.

Outline

Lemma

Let $\{\mathcal{S}_g\}_{g\in\mathcal{G}}$ be an infinite sequence of arithmetic surfaces of different genera g, such that for each $g \in \mathcal{G}$, the group of automorphisms of $\mathcal{S}_g$ has order $a(g+b)$ for some fixed a and b. Then $b = -1$.

Lemma

Let $\{\mathcal{S}_g\}_{g \in \mathcal{G}}$ be an infinite sequence of arithmetic surfaces of different genera g, such that for each $g \in \mathcal{G}$, the group of automorphisms of $\mathcal{S}_g$ has order $a(g+b)$ for some fixed a and b. Then $b = -1$.

Proof. Let $\mathcal{S}$ be a surface from the given sequence.

Then $\mathrm{Aut}(\mathcal{S}) \cong N(\Gamma_{\mathcal{S}})/\Gamma_{\mathcal{S}}$, where $\Gamma_{\mathcal{S}}$ is the surface group corresponding to $\mathcal{S}$.

Lemma

Let $\{\mathcal{S}_g\}_{g\in\mathcal{G}}$ be an infinite sequence of arithmetic surfaces of different genera g, such that for each $g \in \mathcal{G}$, the group of automorphisms of $\mathcal{S}_g$ has order $a(g+b)$ for some fixed a and b. Then $b = -1$.

Proof. Let $\mathcal{S}$ be a surface from the given sequence.

Then $\mathrm{Aut}(\mathcal{S}) \cong N(\Gamma_\mathcal{S})/\Gamma_\mathcal{S}$, where $\Gamma_\mathcal{S}$ is the surface group corresponding to $\mathcal{S}$.

The Riemann-Hurwitz formula yields

$$\mu(N(\Gamma_\mathcal{S})) = \frac{\mu(\Gamma_\mathcal{S})}{|\mathrm{Aut}(\mathcal{S})|} = \frac{2\pi(2g-2)}{a(g+b)} ,$$

so $\mu(N(\Gamma_\mathcal{S})) \to 4\pi/a$ as $g \to \infty$.

$\Gamma_{\mathcal{S}}$ arithmetic $\Rightarrow N(\Gamma_{\mathcal{S}})$ arithmetic.

$\Gamma_{\mathcal{S}}$ arithmetic $\Rightarrow N(\Gamma_{\mathcal{S}})$ arithmetic.

The measures of arithmetic groups form a discrete subset of $\mathbb{R}$ (Borel).

$\Gamma_{\mathcal{S}}$ arithmetic $\Rightarrow N(\Gamma_{\mathcal{S}})$ arithmetic.

The measures of arithmetic groups form a discrete subset of $\mathbb{R}$ (Borel).

So for all but finitely many $g \in \mathcal{G}$,

$$\frac{2\pi(2g-2)}{a(g+b)} = \mu(N(\Gamma_{\mathcal{S}})) = \frac{4\pi}{a} \, .$$

Therefore $b = -1$.

It follows from Lemma 1 that the Accola-Maclachlan lower bound for $N(g)$, $8(g+1)$, cannot be attained by infinitely many arithmetic surfaces.

It follows from Lemma 1 that the Accola-Maclachlan lower bound for $N(g)$, $8(g+1)$, cannot be attained by infinitely many arithmetic surfaces.

In fact it is never attained by arithmetic surfaces, since the extremal surfaces for this bound are uniformized by surface subgroups of (2, 4, 2(g+1))-groups with $g \geq 24$ (Maclachlan), and these are not arithmetic (Takeuchi).

Lemma

$N_{ar}(g) \geq 4(g-1)$ *for all* $g \geq 2$.

Lemma

$N_{ar}(g) \geq 4(g-1)$ *for all* $g \geq 2$.

Proof. Let $\Gamma = \langle \gamma_1, \ldots, \gamma_5 \mid \gamma_j^2 = \gamma_1 \ldots \gamma_5 = 1 \rangle$ be an arithmetic group with signature (2, 2, 2, 2, 2).

Lemma

$N_{ar}(g) \geq 4(g-1)$ *for all* $g \geq 2$.

Proof. Let $\Gamma = \langle \gamma_1, \ldots, \gamma_5 \mid \gamma_j^2 = \gamma_1 \ldots \gamma_5 = 1 \rangle$ be an arithmetic group with signature (2, 2, 2, 2, 2).

Let $G = D_{2(g-1)} = \langle a, b \mid a^{2(g-1)} = b^2 = (ab)^2 = 1 \rangle$.

Lemma

$N_{ar}(g) \geq 4(g-1)$ *for all* $g \geq 2$.

Proof. Let $\Gamma = \langle \gamma_1, \ldots, \gamma_5 \mid \gamma_j^2 = \gamma_1 \ldots \gamma_5 = 1 \rangle$ be an arithmetic group with signature (2, 2, 2, 2, 2).

Let $G = D_{2(g-1)} = \langle a, b \mid a^{2(g-1)} = b^2 = (ab)^2 = 1 \rangle$.

Define $\theta : \Gamma \to G$ by $\gamma_j \mapsto ab, b, a^{g-2}b, b, a^{g-1}$.

Lemma

$N_{ar}(g) \geq 4(g-1)$ for all $g \geq 2$.

Proof. Let $\Gamma = \langle \gamma_1, \ldots, \gamma_5 \mid \gamma_j^2 = \gamma_1 \ldots \gamma_5 = 1 \rangle$ be an arithmetic group with signature (2, 2, 2, 2, 2).

Let $G = D_{2(g-1)} = \langle a, b \mid a^{2(g-1)} = b^2 = (ab)^2 = 1 \rangle$.

Define $\theta : \Gamma \to G$ by $\gamma_j \mapsto ab, b, a^{g-2}b, b, a^{g-1}$.

θ is a SKE and thus $K = \ker(\theta)$ is a surface group.

The surface $\mathcal{S} = \mathcal{H}/K$ is arithmetic and $\mathrm{Aut}(\mathcal{S}) \geq \Gamma/K \cong G$.

The surface $\mathcal{S} = \mathcal{H}/K$ is arithmetic and $\mathrm{Aut}(\mathcal{S}) \geq \Gamma/K \cong G$.

$\mu(\Gamma) = \pi$ and $|G| = 4(g-1)$, so by Riemann-Hurwitz

$$\mu(K) = \mu(\Gamma)|G| = 2\pi(2g-2).$$

The surface $\mathcal{S} = \mathcal{H}/K$ is arithmetic and $\mathrm{Aut}(\mathcal{S}) \geq \Gamma/K \cong G$.

$\mu(\Gamma) = \pi$ and $|G| = 4(g-1)$, so by Riemann-Hurwitz

$$\mu(K) = \mu(\Gamma)|G| = 2\pi(2g-2).$$

So $\mathcal{S}$ has genus g as K is a surface group.

The surface $\mathcal{S} = \mathcal{H}/K$ is arithmetic and $\mathrm{Aut}(\mathcal{S}) \geq \Gamma/K \cong G$.

$\mu(\Gamma) = \pi$ and $|G| = 4(g-1)$, so by Riemann-Hurwitz

$$\mu(K) = \mu(\Gamma)|G| = 2\pi(2g-2).$$

So $\mathcal{S}$ has genus g as K is a surface group.

Then $N_{ar}(g) \geq |\mathrm{Aut}(\mathcal{S})| \geq |G| = 4(g-1)$ as required.

Outline

Theorem

$N_{ar}(g) \geq 4(g-1)$ for all $g \geq 2$, and this bound is attained for infinitely many values of g.

Theorem

$N_{ar}(g) \geq 4(g-1)$ for all $g \geq 2$, and this bound is attained for infinitely many values of g.

- $G := Aut(\mathcal{S})$ has order $|G| > 4(g-1)$ for some compact arithmetic surface $\mathcal{S}$ of genus $g \geq 2$.

Theorem

$N_{ar}(g) \geq 4(g-1)$ for all $g \geq 2$, and this bound is attained for infinitely many values of g.

- $G := Aut(\mathcal{S})$ has order $|G| > 4(g-1)$ for some compact arithmetic surface $\mathcal{S}$ of genus $g \geq 2$.
- Imposing specific conditions on g we a get a contradiction.

Theorem

$N_{ar}(g) \geq 4(g-1)$ for all $g \geq 2$, and this bound is attained for infinitely many values of g.

- $G := Aut(\mathcal{S})$ has order $|G| > 4(g-1)$ for some compact arithmetic surface $\mathcal{S}$ of genus $g \geq 2$.
- Imposing specific conditions on g we a get a contradiction.
- Show that infinitely many values of g satisfy these conditions. For these $N_{\text{ar}}(g) = 4(g-1)$.

By our hypothesis, $G \cong \Gamma/K$ for some co-compact arithmetic group Γ and normal surface subgroup $K = \Gamma_{\mathcal{S}}$ of Γ, with

$$4\pi(g-1) = \mu(K) = |G|\mu(\Gamma) > 4(g-1)\mu(\Gamma), \qquad (1)$$

By our hypothesis, $G \cong \Gamma/K$ for some co-compact arithmetic group Γ and normal surface subgroup $K = \Gamma_S$ of Γ, with

$$4\pi(g-1) = \mu(K) = |G|\mu(\Gamma) > 4(g-1)\mu(\Gamma), \tag{1}$$

Borel's discreteness theorem implies that there are only finitely many measures of co-compact arithmetic groups $\mu(\Gamma) < \pi$.

By our hypothesis, $G \cong \Gamma/K$ for some co-compact arithmetic group Γ and normal surface subgroup $K = \Gamma_{\mathcal{S}}$ of Γ, with

$$4\pi(g-1) = \mu(K) = |G|\mu(\Gamma) > 4(g-1)\mu(\Gamma), \tag{1}$$

Borel's discreteness theorem implies that there are only finitely many measures of co-compact arithmetic groups $\mu(\Gamma) < \pi$.

Hurwitz's formula and (1) show that these correspond to a finite set Σ of signatures.

By our hypothesis, $G \cong \Gamma/K$ for some co-compact arithmetic group Γ and normal surface subgroup $K = \Gamma_{\mathcal{S}}$ of Γ, with

$$4\pi(g-1) = \mu(K) = |G|\mu(\Gamma) > 4(g-1)\mu(\Gamma), \qquad (1)$$

Borel's discreteness theorem implies that there are only finitely many measures of co-compact arithmetic groups $\mu(\Gamma) < \pi$.

Hurwitz's formula and (1) show that these correspond to a finite set Σ of signatures.

For each $\sigma \in \Sigma$, the number $q = \frac{\mu(\Gamma)}{4\pi}$ is rational and depends only on the signature σ of Σ, so writing $q = r/s = r_\sigma/s_\sigma$ in reduced form, we have $|G| = (g-1)/q = (g-1)s/r$.

Restrictions on g

Let $R = \text{lcm}\{r_\sigma | \sigma \in \Sigma\}$, and $S = max\{s_\sigma | \sigma \in \Sigma, r_\sigma = 1\}$.

Restrictions on g

Let $R = \text{lcm}\{r_\sigma | \sigma \in \Sigma\}$, and $S = max\{s_\sigma | \sigma \in \Sigma, r_\sigma = 1\}$.

Let Π denote the finite set of primes which divide an elliptic period m_j of some signature $\sigma \in \Sigma$ with $r_\sigma = 1$.

Restrictions on g

Let $R = \text{lcm}\{r_\sigma | \sigma \in \Sigma\}$, and $S = max\{s_\sigma | \sigma \in \Sigma, r_\sigma = 1\}$.

Let Π denote the finite set of primes which divide an elliptic period m_j of some signature $\sigma \in \Sigma$ with $r_\sigma = 1$.

Let p be a prime such that $p \notin \Pi$, $(p, R) = 1$ and $p > S$. Suppose $g = p + 1$.

Restrictions on g

Let $R = \mathrm{lcm}\{r_\sigma | \sigma \in \Sigma\}$, and $S = max\{s_\sigma | \sigma \in \Sigma, r_\sigma = 1\}$.

Let Π denote the finite set of primes which divide an elliptic period m_j of some signature $\sigma \in \Sigma$ with $r_\sigma = 1$.

Let p be a prime such that $p \notin \Pi$, $(p, R) = 1$ and $p > S$. Suppose $g = p + 1$.

Then $|G| = ps$ with $(s, p) = 1$ and $s < p + 1$. By Sylow's Theorems there is a $P \cong \mathbb{Z}/p\mathbb{Z}$ with $P \trianglelefteq G$.

Restrictions on g

Let $R = \mathrm{lcm}\{r_\sigma | \sigma \in \Sigma\}$, and $S = max\{s_\sigma | \sigma \in \Sigma, r_\sigma = 1\}$.

Let Π denote the finite set of primes which divide an elliptic period m_j of some signature $\sigma \in \Sigma$ with $r_\sigma = 1$.

Let p be a prime such that $p \notin \Pi$, $(p, R) = 1$ and $p > S$. Suppose $g = p + 1$.

Then $|G| = ps$ with $(s, p) = 1$ and $s < p + 1$. By Sylow's Theorems there is a $P \cong \mathbb{Z}/p\mathbb{Z}$ with $P \trianglelefteq G$.

Let Δ denote the inverse image of P in Γ, a normal subgroup of Γ with $\Gamma/\Delta \cong Q := G/P$.

Restrictions on g

Let $R = \text{lcm}\{r_\sigma | \sigma \in \Sigma\}$, and $S = max\{s_\sigma | \sigma \in \Sigma, r_\sigma = 1\}$.

Let Π denote the finite set of primes which divide an elliptic period m_j of some signature $\sigma \in \Sigma$ with $r_\sigma = 1$.

Let p be a prime such that $p \notin \Pi$, $(p, R) = 1$ and $p > S$. Suppose $g = p + 1$.

Then $|G| = ps$ with $(s, p) = 1$ and $s < p + 1$. By Sylow's Theorems there is a $P \cong \mathbb{Z}/p\mathbb{Z}$ with $P \trianglelefteq G$.

Let Δ denote the inverse image of P in Γ, a normal subgroup of Γ with $\Gamma/\Delta \cong Q := G/P$.

Since $|Q|$ is coprime to p, the natural epimorphism $G \to Q$ preserves the orders of the images of all elliptic generators of Γ.

The inclusions $K \trianglelefteq \Delta \trianglelefteq \Gamma$ induce an étale $\mathbb{Z}/p\mathbb{Z}$-covering of Riemann surfaces

$$\begin{tikzcd}
\mathcal{S} \cong K \setminus \mathcal{H} \arrow[d, "P \cong \mathbb{Z}/p\mathbb{Z}"'] \arrow[dd, bend left=60, dash, "G"] \\
\mathcal{T} \cong \Delta \setminus \mathcal{H} \arrow[d, "Q"'] \\
\Gamma \setminus \mathcal{H}
\end{tikzcd}$$

The inclusions $K \trianglelefteq \Delta \trianglelefteq \Gamma$ induce an étale $\mathbb{Z}/p\mathbb{Z}$-covering of Riemann surfaces

$$\begin{tikzcd}
\mathcal{S} \cong K \backslash \mathcal{H} \arrow[d, "P \cong \mathbb{Z}/p\mathbb{Z}"'] \arrow[dd, bend left, "G"] \\
\mathcal{T} \cong \Delta \backslash \mathcal{H} \arrow[d, "Q"'] \\
\Gamma \backslash \mathcal{H}
\end{tikzcd}$$

In particular we have that $Q \leq Aut(\mathcal{T})$, and $\mathcal{T}$ has genus $1 + (g-1)/p = 2$.

The inclusions $K \trianglelefteq \Delta \trianglelefteq \Gamma$ induce an étale $\mathbb{Z}/p\mathbb{Z}$-covering of Riemann surfaces

$$\begin{tikzcd}
\mathcal{S} \cong K \setminus \mathcal{H} \arrow[d, "P \cong \mathbb{Z}/p\mathbb{Z}"'] \arrow[dd, bend left, "G"] \\
\mathcal{T} \cong \Delta \setminus \mathcal{H} \arrow[d, "Q"'] \\
\Gamma \setminus \mathcal{H}
\end{tikzcd}$$

In particular we have that $Q \leq Aut(\mathcal{T})$, and $\mathcal{T}$ has genus $1 + (g-1)/p = 2$.

Then Q is a group of automorphisms of a Riemann surface $\mathcal{T}$ of genus 2.

Notice that $|Aut(\mathcal{T})| \leq 84$, thus there are just finitely many possibilities for $Aut(\mathcal{T})$ and hence for Q.

Notice that $|Aut(\mathcal{T})| \leq 84$, thus there are just finitely many possibilities for $Aut(\mathcal{T})$ and hence for Q.

Let E be the least common multiple of the exponents of all the groups of automorphisms of Riemann surfaces of genus 2.

Notice that $|Aut(\mathcal{T})| \leq 84$, thus there are just finitely many possibilities for $Aut(\mathcal{T})$ and hence for Q.

Let E be the least common multiple of the exponents of all the groups of automorphisms of Riemann surfaces of genus 2.

Riemann surfaces of genus 2 are hyperelliptic, therefore their automorphism groups always contain an element of order 2.

Notice that $|Aut(\mathcal{T})| \leq 84$, thus there are just finitely many possibilities for $Aut(\mathcal{T})$ and hence for Q.

Let E be the least common multiple of the exponents of all the groups of automorphisms of Riemann surfaces of genus 2.

Riemann surfaces of genus 2 are hyperelliptic, therefore their automorphism groups always contain an element of order 2.

In particular $E \equiv 0 \pmod 2$.

Outline

Outline of remainder of proof

- Consider $H_1(\mathcal{T}, \mathbb{F}_p)$.

Outline of remainder of proof

- Consider $H_1(\mathcal{T}, \mathbb{F}_p)$.
- We give an action of Q on this $\mathbb{F}_p$-vector space.

Outline of remainder of proof

- Consider $H_1(\mathcal{T}, \mathbb{F}_p)$.
- We give an action of Q on this $\mathbb{F}_p$-vector space.
- It decomposes into 1-dimensional submodules.

Outline of remainder of proof

- Consider $H_1(\mathcal{T}, \mathbb{F}_p)$.
- We give an action of Q on this $\mathbb{F}_p$-vector space.
- It decomposes into 1-dimensional submodules.
- Q acts faithfully.

Outline of remainder of proof

- Consider $H_1(\mathcal{T}, \mathbb{F}_p)$.
- We give an action of Q on this $\mathbb{F}_p$-vector space.
- It decomposes into 1-dimensional submodules.
- Q acts faithfully.
- We find $Q \subset \mathrm{GL}_1(\mathbb{F}_p)^4$, which constrains the exponent ϵ of Q.

Outline of remainder of proof

- Consider $H_1(\mathcal{T}, \mathbb{F}_p)$.
- We give an action of Q on this $\mathbb{F}_p$-vector space.
- It decomposes into 1-dimensional submodules.
- Q acts faithfully.
- We find $Q \subset \mathrm{GL}_1(\mathbb{F}_p)^4$, which constrains the exponent ϵ of Q.
- Thus ϵ divides $\gcd(E, p-1)$, which we can force to be 2.

Outline of remainder of proof

- Consider $H_1(\mathcal{T}, \mathbb{F}_p)$.
- We give an action of Q on this $\mathbb{F}_p$-vector space.
- It decomposes into 1-dimensional submodules.
- Q acts faithfully.
- We find $Q \subset \mathrm{GL}_1(\mathbb{F}_p)^4$, which constrains the exponent ϵ of Q.
- Thus ϵ divides $\gcd(E, p-1)$, which we can force to be 2.
- This gives a contradiction using the area formula.

Outline of remainder of proof

- Consider $H_1(\mathcal{T}, \mathbb{F}_p)$.
- We give an action of Q on this $\mathbb{F}_p$-vector space.
- It decomposes into 1-dimensional submodules.
- Q acts faithfully.
- We find $Q \subset \mathrm{GL}_1(\mathbb{F}_p)^4$, which constrains the exponent ϵ of Q.
- Thus ϵ divides $\gcd(E, p-1)$, which we can force to be 2.
- This gives a contradiction using the area formula.
- We have infinitely many p satisfying our conditions.

We consider first the module structure of $H_1(\mathcal{T})$.

$\mathcal{T}$ has genus 2, so $H_1(\mathcal{T}, \mathbb{Z}) \cong \mathbb{Z}^4$.

We consider first the module structure of $H_1(\mathcal{T})$.

$\mathcal{T}$ has genus 2, so $H_1(\mathcal{T}, \mathbb{Z}) \cong \mathbb{Z}^4$.

$H_0(\mathcal{T}, \mathbb{Z}) \cong \mathbb{Z}$, so $\mathrm{Tor}(H_0(\mathcal{T}, \mathbb{Z}), G) = 0$ for all G.

We consider first the module structure of $H_1(\mathcal{T})$.

$\mathcal{T}$ has genus 2, so $H_1(\mathcal{T}, \mathbb{Z}) \cong \mathbb{Z}^4$.

$H_0(\mathcal{T}, \mathbb{Z}) \cong \mathbb{Z}$, so $\mathrm{Tor}(H_0(\mathcal{T}, \mathbb{Z}), G) = 0$ for all G.

By the Universal Coefficient Theorem,

$$H_1(\mathcal{T}, \mathbb{F}_p) \cong H_1(\mathcal{T}, \mathbb{Z}) \otimes \mathbb{F}_p \cong \mathbb{F}_p^4.$$

We consider first the module structure of $H_1(\mathcal{T})$.

$\mathcal{T}$ has genus 2, so $H_1(\mathcal{T}, \mathbb{Z}) \cong \mathbb{Z}^4$.

$H_0(\mathcal{T}, \mathbb{Z}) \cong \mathbb{Z}$, so $\mathrm{Tor}(H_0(\mathcal{T}, \mathbb{Z}), G) = 0$ for all G.

By the Universal Coefficient Theorem,

$$H_1(\mathcal{T}, \mathbb{F}_p) \cong H_1(\mathcal{T}, \mathbb{Z}) \otimes \mathbb{F}_p \cong \mathbb{F}_p^4.$$

We also have

$$H_1(\mathcal{T}, \mathbb{C}) \cong H_1(\mathcal{T}, \mathbb{Z}) \otimes \mathbb{C} \cong \mathbb{C}^4.$$

Q acts on $\mathcal{T}$, and thus on $H_1(\mathcal{T}, \mathbb{F}_p)$.

Q acts on $\mathcal{T}$, and thus on $H_1(\mathcal{T}, \mathbb{F}_p)$.

The sequence

$$1 \to \Delta \to \Gamma \to Q \to 1$$

gives an action of Q on Δ.

Q acts on $\mathcal{T}$, and thus on $H_1(\mathcal{T}, \mathbb{F}_p)$.

The sequence

$$1 \to \Delta \to \Gamma \to Q \to 1$$

gives an action of Q on Δ.

Δ is the group of deck transformations for $\mathcal{T}$, so $\Delta \cong \pi_1(\mathcal{T})$.

Q acts on $\mathcal{T}$, and thus on $H_1(\mathcal{T}, \mathbb{F}_p)$.

The sequence

$$1 \to \Delta \to \Gamma \to Q \to 1$$

gives an action of Q on Δ.

Δ is the group of deck transformations for $\mathcal{T}$, so $\Delta \cong \pi_1(\mathcal{T})$.

Thus $\Delta/\Delta' \cong H_1(\mathcal{T}, \mathbb{Z})$ and $\Delta/\Delta'\Delta^p \cong H_1(\mathcal{T}, \mathbb{F}_p)$.

Q acts on $\mathcal{T}$, and thus on $H_1(\mathcal{T}, \mathbb{F}_p)$.

The sequence

$$1 \to \Delta \to \Gamma \to Q \to 1$$

gives an action of Q on Δ.

Δ is the group of deck transformations for $\mathcal{T}$, so $\Delta \cong \pi_1(\mathcal{T})$.

Thus $\Delta/\Delta' \cong H_1(\mathcal{T}, \mathbb{Z})$ and $\Delta/\Delta'\Delta^p \cong H_1(\mathcal{T}, \mathbb{F}_p)$.

In fact, these isomorphisms are Q-equivariant.

$$H^1(\mathcal{T}, \mathbb{C}) \cong H^{1,0}(\mathcal{T}, \mathbb{C}) \oplus H^{0,1}(\mathcal{T}, \mathbb{C}).$$

$$H^1(\mathcal{T}, \mathbb{C}) \cong H^{1,0}(\mathcal{T}, \mathbb{C}) \oplus H^{0,1}(\mathcal{T}, \mathbb{C}).$$

These spaces give complex conjugate representations of Q.

$$H^1(\mathcal{T}, \mathbb{C}) \cong H^{1,0}(\mathcal{T}, \mathbb{C}) \oplus H^{0,1}(\mathcal{T}, \mathbb{C}).$$

These spaces give complex conjugate representations of Q.

After Poincaré duality, $H_1(\mathcal{T}, \mathbb{C})$ decomposes into a pair of two dimensional Q-invariant subspaces.

$H^1(\mathcal{T}, \mathbb{C}) \cong H^{1,0}(\mathcal{T}, \mathbb{C}) \oplus H^{0,1}(\mathcal{T}, \mathbb{C})$.

These spaces give complex conjugate representations of Q.

After Poincaré duality, $H_1(\mathcal{T}, \mathbb{C})$ decomposes into a pair of two dimensional Q-invariant subspaces.

Those subspaces must both decompose or both be irreducible.

$$H^1(\mathcal{T}, \mathbb{C}) \cong H^{1,0}(\mathcal{T}, \mathbb{C}) \oplus H^{0,1}(\mathcal{T}, \mathbb{C}).$$

These spaces give complex conjugate representations of Q.

After Poincaré duality, $H_1(\mathcal{T}, \mathbb{C})$ decomposes into a pair of two dimensional Q-invariant subspaces.

Those subspaces must both decompose or both be irreducible.

Since $p \nmid |Q|$, Maschke's Theorem gives $H_1(\mathcal{T}, \mathbb{F}_p) \cong \bigoplus V_i$.

$$H^1(\mathcal{T}, \mathbb{C}) \cong H^{1,0}(\mathcal{T}, \mathbb{C}) \oplus H^{0,1}(\mathcal{T}, \mathbb{C}).$$

These spaces give complex conjugate representations of Q.

After Poincaré duality, $H_1(\mathcal{T}, \mathbb{C})$ decomposes into a pair of two dimensional Q-invariant subspaces.

Those subspaces must both decompose or both be irreducible.

Since $p \nmid |Q|$, Maschke's Theorem gives $H_1(\mathcal{T}, \mathbb{F}_p) \cong \bigoplus V_i$.

So $H_1(\mathcal{T}, \mathbb{F}_p)$ decomposes into a pair of two dimensional subspaces, both irreducible or both reducible.

We now construct a 1-dimensional quotient of $H_1(\mathcal{T}, \mathbb{F}_p)$.

We now construct a 1-dimensional quotient of $H_1(\mathcal{T}, \mathbb{F}_p)$.

$\Delta/K \cong P \cong C_p$, so K contains $\Delta'\Delta^p$.

We now construct a 1-dimensional quotient of $H_1(\mathcal{T}, \mathbb{F}_p)$.

$\Delta/K \cong P \cong C_p$, so K contains $\Delta'\Delta^p$.

P is a 1-dimensional $\mathbb{F}_p$-vector space with Q-action.

We now construct a 1-dimensional quotient of $H_1(\mathcal{T}, \mathbb{F}_p)$.

$\Delta/K \cong P \cong C_p$, so K contains $\Delta'\Delta^p$.

P is a 1-dimensional $\mathbb{F}_p$-vector space with Q-action.

So $H_1(\mathcal{T}, \mathbb{F}_p) \cong \Delta/\Delta'\Delta^p \twoheadrightarrow \Delta/K \cong P$.

We now construct a 1-dimensional quotient of $H_1(\mathcal{T}, \mathbb{F}_p)$.

$\Delta/K \cong P \cong C_p$, so K contains $\Delta'\Delta^p$.

P is a 1-dimensional $\mathbb{F}_p$-vector space with Q-action.

So $H_1(\mathcal{T}, \mathbb{F}_p) \cong \Delta/\Delta'\Delta^p \twoheadrightarrow \Delta/K \cong P$.

Thus

$$V = H_1(\mathcal{T}, \mathbb{F}_p) \cong \bigoplus_{i=1}^{4} V_i,$$

with each V_i a 1-dimensional Q-invariant subspace of V.

We now construct a 1-dimensional quotient of $H_1(\mathcal{T}, \mathbb{F}_p)$.

$\Delta/K \cong P \cong C_p$, so K contains $\Delta'\Delta^p$.

P is a 1-dimensional $\mathbb{F}_p$-vector space with Q-action.

So $H_1(\mathcal{T}, \mathbb{F}_p) \cong \Delta/\Delta'\Delta^p \twoheadrightarrow \Delta/K \cong P$.

Thus

$$V = H_1(\mathcal{T}, \mathbb{F}_p) \cong \bigoplus_{i=1}^{4} V_i,$$

with each V_i a 1-dimensional Q-invariant subspace of V.

Therefore we have a map $Q \to \mathrm{GL}_1(\mathbb{F}_p)^4$.

Lemma

Lemma (Farkas & Kra, V.3.4) If $A \in \mathrm{SL}_k(\mathbb{Z})$ *has finite order* $m > 1$ *and* $A \equiv I \pmod{n}$ *then* $m = n = 2$.

Lemma

Lemma (Farkas & Kra, V.3.4) If $A \in \mathrm{SL}_k(\mathbb{Z})$ has finite order $m > 1$ and $A \equiv I \pmod{n}$ then $m = n = 2$.

So in fact, $Q \hookrightarrow \mathrm{GL}_1(\mathbb{F}_p)^4 \cong (C_{p-1})^4$.

Lemma

Lemma (Farkas & Kra, V.3.4) If $A \in \mathrm{SL}_k(\mathbb{Z})$ has finite order $m > 1$ and $A \equiv I \pmod{n}$ then $m = n = 2$.

So in fact, $Q \hookrightarrow \mathrm{GL}_1(\mathbb{F}_p)^4 \cong (C_{p-1})^4$.

Therefore Q has exponent ϵ dividing $p - 1$.

Lemma

Lemma (Farkas & Kra, V.3.4) If $A \in \mathrm{SL}_k(\mathbb{Z})$ has finite order $m > 1$ and $A \equiv I \pmod{n}$ then $m = n = 2$.

So in fact, $Q \hookrightarrow \mathrm{GL}_1(\mathbb{F}_p)^4 \cong (C_{p-1})^4$.

Therefore Q has exponent ϵ dividing $p - 1$.

ϵ thus divides $\gcd(E, p - 1)$.

Choose p with $\gcd(E, p-1) = 2$.

Choose p with $\gcd(E, p-1) = 2$.

Δ is a surface group, so each elliptic period equals 2.

Choose p with $\gcd(E, p-1) = 2$.

Δ is a surface group, so each elliptic period equals 2.

This contradicts $0 < \mu(\Gamma) < \pi$.

In summary, we have required that $g - 1 = p$ is prime, $p > S$, $p \notin \Pi$, p is coprime to R and $\gcd(p - 1, E) = 2$.

In summary, we have required that $g-1=p$ is prime, $p>S$, $p\notin\Pi$, p is coprime to R and $\gcd(p-1,E)=2$.

By Dirichlet's theorem, there are infinitely primes

$$p\equiv -1 \pmod{E}.$$

In summary, we have required that $g - 1 = p$ is prime, $p > S$, $p \notin \Pi$, p is coprime to R and $\gcd(p - 1, E) = 2$.

By Dirichlet's theorem, there are infinitely primes

$$p \equiv -1 \pmod{E}.$$

All but finitely many satisfy the other required properties.

In summary, we have required that $g - 1 = p$ is prime, $p > S$, $p \notin \Pi$, p is coprime to R and $\gcd(p - 1, E) = 2$.

By Dirichlet's theorem, there are infinitely primes

$$p \equiv -1 \pmod{E}.$$

All but finitely many satisfy the other required properties.

Therefore we have an infintely many g that lead to a contradiction.

Outline

Main Theorem

- **Main Theorem:** Let Σ be the set of all signatures of cocompact arithmetic Fuchsian groups with volume strictly less than π.

Main Theorem

- **Main Theorem:** Let Σ be the set of all signatures of cocompact arithmetic Fuchsian groups with volume strictly less than π.
  Writing $\frac{\mu(\Gamma_\sigma)}{4\pi}$ as a fraction r_σ/s_σ in lowest terms for every $\sigma \in \Sigma$, let $R = \text{lcm}\{r_\sigma\}$, let Π be the list of primes that divide the period of an elliptic element of one of the Γ_σ, and $S = \max\{s_\sigma\}$.

Main Theorem

- **Main Theorem:** Let Σ be the set of all signatures of cocompact arithmetic Fuchsian groups with volume strictly less than π.
  Writing $\frac{\mu(\Gamma_\sigma)}{4\pi}$ as a fraction r_σ/s_σ in lowest terms for every $\sigma \in \Sigma$, let $R = \mathrm{lcm}\{r_\sigma\}$, let Π be the list of primes that divide the period of an elliptic element of one of the Γ_σ, and $S = \max\{s_\sigma\}$.
  Assume that $g - 1 =: p$ is a prime such that $\gcd(p, R) = 1$, $p \notin S$, $p > S$ and such that $\gcd(p - 1, E) = 2$, where E is the least common multiple of the exponents of all automorphism groups of Riemann surfaces of genus 2.

Main Theorem

- **Main Theorem:** Let Σ be the set of all signatures of cocompact arithmetic Fuchsian groups with volume strictly less than π.
  Writing $\frac{\mu(\Gamma_\sigma)}{4\pi}$ as a fraction r_σ/s_σ in lowest terms for every $\sigma \in \Sigma$, let $R = \mathrm{lcm}\{r_\sigma\}$, let Π be the list of primes that divide the period of an elliptic element of one of the Γ_σ, and $S = \max\{s_\sigma\}$.
  Assume that $g - 1 =: p$ is a prime such that $\gcd(p, R) = 1$, $p \notin S$, $p > S$ and such that $\gcd(p - 1, E) = 2$, where E is the least common multiple of the exponents of all automorphism groups of Riemann surfaces of genus 2.
  Then the size of the automorphism group of any surface of genus g cannot be greater than $4(g - 1)$, so we have to have equality.

Explicit Sequence Theorem

Goal

Construct a specific sequence of genera g such that N_{ar} attains the lower bound.

Explicit Sequence Theorem

Goal

Construct a specific sequence of genera g such that N_{ar} attains the lower bound.

Theorem (Main Theorem)

For all primes $p \equiv 23, 47, 59 \pmod{60}$, we have $N_{ar}(g) = 4(g-1)$. The least genus g for which the the lower bound $N_{ar}(g) = 4(g-1)$ is attained is $g = 24$.

Explicit Sequence Theorem

Goal

Construct a specific sequence of genera g such that N_{ar} attains the lower bound.

Theorem (Main Theorem)

For all primes $p \equiv 23, 47, 59 \pmod{60}$, we have $N_{ar}(g) = 4(g-1)$. The least genus g for which the the lower bound $N_{ar}(g) = 4(g-1)$ is attained is $g = 24$.

Idea

Construct primes p satisfying the hypotheses of the Main Theorem. Then $g = p + 1$ will be such that:

$$N_{ar}(g) = 4(g-1).$$

Strategy

1. Listing all Arithmetic Fuchsian Signatures
2. The Conditions on Sufficiently Large Primes p
3. Smaller Primes

List of Possible Signatures

- Want to find the set Σ of all signatures of cocompact arithmetic Fuchsian groups with volume strictly less than π.

List of Possible Signatures

- Want to find the set Σ of all signatures of cocompact arithmetic Fuchsian groups with volume strictly less than π.
- Writing $\mu(\Gamma_\sigma)$ as a fraction r_σ/s_σ in lowest terms for every $\sigma \in \Sigma$, we need to determine $R = \text{lcm}\{r_\sigma\}$, the list Π of primes that divide an elliptic period m_k, and $S = \max\{s_\sigma\}$.

List of Possible Signatures

- Want to find the set Σ of all signatures of cocompact arithmetic Fuchsian groups with volume strictly less than π.
- Writing $\mu(\Gamma_\sigma)$ as a fraction r_σ/s_σ in lowest terms for every $\sigma \in \Sigma$, we need to determine $R = \text{lcm}\{r_\sigma\}$, the list Π of primes that divide an elliptic period m_k, and $S = \max\{s_\sigma\}$.
- Then by the proof of the Main Theorem, for any prime p not dividing R, not contained in Π and greater than S, we cannot have

$$|G| > 4(g-1)$$

if we impose the additional condition that $\gcd(p-1, E) = 2$.

List of Possible Signatures

- Let $(g; m_1; \ldots; m_r)$ be the signature of a Fuchsian group Γ. Then

$$\frac{1}{\pi}\mu(\Gamma) = 4(g-1) + \sum_{k=1}^{r}\left(1 - \frac{1}{m_k}\right) < 1 \tag{2}$$

has no solution unless $g = 0$.

List of Possible Signatures

- Let $(g; m_1; \ldots; m_r)$ be the signature of a Fuchsian group Γ. Then

$$\frac{1}{\pi}\mu(\Gamma) = 4(g-1) + \sum_{k=1}^{r}\left(1 - \frac{1}{m_k}\right) < 1 \tag{2}$$

has no solution unless $g = 0$.

- If $g = 0$, then since $m_k \geq 2$, we must have $r < 5$, so all signatures have length 3 or 4.

List of Possible Signatures

- Let $(g; m_1; \ldots; m_r)$ be the signature of a Fuchsian group Γ. Then
$$\frac{1}{\pi}\mu(\Gamma) = 4(g-1) + \sum_{k=1}^{r}\left(1 - \frac{1}{m_k}\right) < 1 \qquad (2)$$
has no solution unless $g = 0$.
- If $g = 0$, then since $m_k \geq 2$, we must have $r < 5$, so all signatures have length 3 or 4.
- Takeuchi gave a complete list of cocompact arithmetic triangle groups; almost all of these have volume less than π.

List of Possible Signatures

- The only other possible candidates are $(2,2,3,3)$,$(2,2,3,4)$,$(2,2,3,5)$ and $(2,2,2,n)$, for $n \geq 3$.

List of Possible Signatures

- The only other possible candidates are $(2,2,3,3)$,$(2,2,3,4)$,$(2,2,3,5)$ and $(2,2,2,n)$, for $n \geq 3$.
- It can be shown that there are only 12 signatures for which $(2,2,2,n)$ is arithmetic.

Sufficiently Large Primes

- Note that the orders of the elliptic elements are either 2,3,4,5 or 7, so $\Pi = \{2, 3, 5, 7\}$.

Sufficiently Large Primes

- Note that the orders of the elliptic elements are either 2,3,4,5 or 7, so $\Pi = \{2, 3, 5, 7\}$.
- Further examining the list of possible signatures, and putting $\frac{\mu(\Gamma)}{4\pi}$ into lowest terms, we find that $R = 4 \cdot 3 \cdot 5 \cdot 7$ is the least common multiple of the numerators of all $\frac{\mu(\Gamma_\sigma)}{4\pi}$ and $s = 84$ is the largest occurring denominator.

Sufficiently Large Primes

- Note that the orders of the elliptic elements are either 2,3,4,5 or 7, so $\Pi = \{2, 3, 5, 7\}$.
- Further examining the list of possible signatures, and putting $\frac{\mu(\Gamma)}{4\pi}$ into lowest terms, we find that $R = 4 \cdot 3 \cdot 5 \cdot 7$ is the least common multiple of the numerators of all $\frac{\mu(\Gamma_\sigma)}{4\pi}$ and $s = 84$ is the largest occurring denominator.
- To deal with the last condition $\gcd(p - 1, E) = 2$, we need a lemma:

Sufficiently Large Primes

- Note that the orders of the elliptic elements are either 2,3,4,5 or 7, so $\Pi = \{2, 3, 5, 7\}$.
- Further examining the list of possible signatures, and putting $\frac{\mu(\Gamma)}{4\pi}$ into lowest terms, we find that $R = 4 \cdot 3 \cdot 5 \cdot 7$ is the least common multiple of the numerators of all $\frac{\mu(\Gamma_\sigma)}{4\pi}$ and $s = 84$ is the largest occurring denominator.
- To deal with the last condition $\gcd(p - 1, E) = 2$, we need a lemma:

Lemma

If S is a Riemann surface of genus $\gamma \geq 2$, then it has no automorphisms of prime order greater than $2\gamma + 1$.

Sufficiently Large Primes

Proof.

Sufficiently Large Primes

Proof.

If f is an automorphism of S of order p, let T be the Riemann surface corresponding to S modulo $< f >$, and γ' its genus.

Sufficiently Large Primes

Proof.

If f is an automorphism of S of order p, let T be the Riemann surface corresponding to S modulo $< f >$, and γ' its genus. Then $f : S \longrightarrow T$ is a smooth p-sheeted covering of T, so the Riemann-Hurwitz formula reads:

$$2(\gamma - 1) = 2p(\gamma' - 1) + m(p - 1)$$

Sufficiently Large Primes

Proof.

If f is an automorphism of S of order p, let T be the Riemann surface corresponding to S modulo $< f >$, and γ' its genus. Then $f : S \longrightarrow T$ is a smooth p-sheeted covering of T, so the Riemann-Hurwitz formula reads:

$$2(\gamma - 1) = 2p(\gamma' - 1) + m(p - 1)$$

where m is the number of fixed points of f.

Sufficiently Large Primes

Proof.

If f is an automorphism of S of order p, let T be the Riemann surface corresponding to S modulo $< f >$, and γ' its genus. Then $f : S \longrightarrow T$ is a smooth p-sheeted covering of T, so the Riemann-Hurwitz formula reads:

$$2(\gamma - 1) = 2p(\gamma' - 1) + m(p - 1)$$

where m is the number of fixed points of f. Assume that $p \geq 2\gamma$, then

Sufficiently Large Primes

Proof.

If f is an automorphism of S of order p, let T be the Riemann surface corresponding to S modulo $< f >$, and γ' its genus. Then $f : S \longrightarrow T$ is a smooth p-sheeted covering of T, so the Riemann-Hurwitz formula reads:

$$2(\gamma - 1) = 2p(\gamma' - 1) + m(p - 1)$$

where m is the number of fixed points of f. Assume that $p \geq 2\gamma$, then

- for $\gamma' \geq 2$, $2(\gamma - 1) \geq 2p + m(p - 1) \geq 2p$, a contradiction

Sufficiently Large Primes

Proof.

If f is an automorphism of S of order p, let T be the Riemann surface corresponding to S modulo $< f >$, and γ' its genus. Then $f : S \longrightarrow T$ is a smooth p-sheeted covering of T, so the Riemann-Hurwitz formula reads:

$$2(\gamma - 1) = 2p(\gamma' - 1) + m(p - 1)$$

where m is the number of fixed points of f. Assume that $p \geq 2\gamma$, then

- for $\gamma' \geq 2$, $2(\gamma - 1) \geq 2p + m(p - 1) \geq 2p$, a contradiction
- for $\gamma' = 1$, $2(\gamma - 1) = m(p - 1) \geq p - 1 \geq 2\gamma - 1$, a contradiction.

$\square$

Sufficiently Large Primes

- For $\gamma' = 0$, $2(\gamma - 1) = -2pg + m(p-1)$, we have $m = \frac{2\gamma}{p-1} + 2 \leq \frac{p}{p-1} + 2 \leq 3$, so $m = 3$.

Sufficiently Large Primes

- For $\gamma' = 0$, $2(\gamma - 1) = -2pg + m(p-1)$, we have $m = \frac{2\gamma}{p-1} + 2 \leq \frac{p}{p-1} + 2 \leq 3$, so $m = 3$.
- In this case, $2\gamma - 2 = -2p + 3(p-1)$, so $p = 2\gamma + 1$.

Sufficiently Large Primes

- For $\gamma' = 0$, $2(\gamma - 1) = -2pg + m(p-1)$, we have $m = \frac{2\gamma}{p-1} + 2 \leq \frac{p}{p-1} + 2 \leq 3$, so $m = 3$.
- In this case, $2\gamma - 2 = -2p + 3(p-1)$, so $p = 2\gamma + 1$. Hence it follows that $p \leq 2\gamma + 1$.

Sufficiently Large Primes

- For $\gamma' = 0$, $2(\gamma - 1) = -2pg + m(p-1)$, we have $m = \frac{2\gamma}{p-1} + 2 \leq \frac{p}{p-1} + 2 \leq 3$, so $m = 3$.
- In this case, $2\gamma - 2 = -2p + 3(p-1)$, so $p = 2\gamma + 1$. Hence it follows that $p \leq 2\gamma + 1$.
- So if S is a surface of genus 2, it cannot have automorphisms of prime order q for any $q > 5$. Thus the exponent of $Aut(S)$ is not divisible by any prime other than 2,3 or 5.

Sufficiently Large Primes

- For $\gamma' = 0$, $2(\gamma - 1) = -2pg + m(p-1)$, we have $m = \frac{2\gamma}{p-1} + 2 \leq \frac{p}{p-1} + 2 \leq 3$, so $m = 3$.
- In this case, $2\gamma - 2 = -2p + 3(p-1)$, so $p = 2\gamma + 1$. Hence it follows that $p \leq 2\gamma + 1$.
- So if S is a surface of genus 2, it cannot have automorphisms of prime order q for any $q > 5$. Thus the exponent of $Aut(S)$ is not divisible by any prime other than 2,3 or 5.

Sufficiently Large Primes

- **Conclusion:** No prime other than $\{2, 3, 5\}$ divides E, the least common multiple of the exponents of automorphism groups of surfaces of genus 2. Thus the condition that $\gcd(p - 1, E) = 2$ is satisfied by all p such that $p - 1$ is not divisible by $3, 4, 5$.

Sufficiently Large Primes

- **Conclusion:** No prime other than $\{2, 3, 5\}$ divides E, the least common multiple of the exponents of automorphism groups of surfaces of genus 2. Thus the condition that $\gcd(p-1, E) = 2$ is satisfied by all p such that $p-1$ is not divisible by $3, 4, 5$.
- Since we also require that $p \not\equiv 0 \mod q$ for $q = 2,3,5$, this leaves the possibilities that $p \equiv 2 \pmod 3$, $p \equiv 3 \mod 4$ and $p \equiv 2, 3, 4 \mod 5$. The first two lift to the congruence $p \equiv 11 \pmod{12}$; combining with the last one gives $p \equiv 23, 47, 59 \pmod{60}$ as the equivalent congruence.

Sufficiently large Primes/Smaller Primes

- We have shown that any prime $p > 84$ congruent to one of 23,47,59 modulo 60 satisfies the conditions of the Main Theorem.

Sufficiently large Primes/Smaller Primes

- We have shown that any prime $p > 84$ congruent to one of 23,47,59 modulo 60 satisfies the conditions of the Main Theorem.
- Thus, surfaces of genus $p+1$ for any such p satisfy the lower bound: $N_g = 4(g-1)$.

Sufficiently large Primes/Smaller Primes

- We have shown that any prime $p > 84$ congruent to one of 23,47,59 modulo 60 satisfies the conditions of the Main Theorem.
- Thus, surfaces of genus $p + 1$ for any such p satisfy the lower bound: $N_g = 4(g - 1)$.
- What about $p = 23, 47, 59$ or 83?

Smaller Primes: p=59

- $p = 59$, S of genus $g = 60$:

Smaller Primes: p=59

- $p = 59$, S of genus $g = 60$:
- 59 is coprime to R, so $|Aut(S)| = |G| = (g - 1)s = 59s$ for some s.

Smaller Primes: p=59

- $p = 59$, S of genus $g = 60$:
- 59 is coprime to R, so $|Aut(S)| = |G| = (g-1)s = 59s$ for some s.
- By inspection, s is coprime to 59, so a 59-Sylow subgroup is of order 59. Letting n_{59} be the number of 59-Sylow subgroups, we must have $n_{59}|s$ and $n_{59} \equiv 1 \pmod{59} \Rightarrow n_{59} = 1$. So the 59-Sylow subgroup P_{59} is unique.

Smaller Primes: p=59

- $p = 59$, S of genus $g = 60$:
- 59 is coprime to R, so $|Aut(S)| = |G| = (g-1)s = 59s$ for some s.
- By inspection, s is coprime to 59, so a 59-Sylow subgroup is of order 59. Letting n_{59} be the number of 59-Sylow subgroups, we must have $n_{59}|s$ and $n_{59} \equiv 1 \pmod{59} \Rightarrow n_{59} = 1$. So the 59-Sylow subgroup P_{59} is unique.
- $p \notin \Pi = \{2, 3, 5, 7\}$, the set of primes dividing an element of order in some Γ_σ.

Smaller Primes: p=59

- $p = 59$, S of genus $g = 60$:
- 59 is coprime to R, so $|Aut(S)| = |G| = (g-1)s = 59s$ for some s.
- By inspection, s is coprime to 59, so a 59-Sylow subgroup is of order 59. Letting n_{59} be the number of 59-Sylow subgroups, we must have $n_{59}|s$ and $n_{59} \equiv 1 \pmod{59} \Rightarrow n_{59} = 1$. So the 59-Sylow subgroup P_{59} is unique.
- $p \notin \Pi = \{2, 3, 5, 7\}$, the set of primes dividing an element of order in some Γ_σ.
- $p - 1 = 58 = 2 \cdot 19$, so $\gcd(p-1, E) = 2$.

Smaller Primes: p=59

- $p = 59$, S of genus $g = 60$:
- 59 is coprime to R, so $|Aut(S)| = |G| = (g-1)s = 59s$ for some s.
- By inspection, s is coprime to 59, so a 59-Sylow subgroup is of order 59. Letting n_{59} be the number of 59-Sylow subgroups, we must have $n_{59}|s$ and $n_{59} \equiv 1 \pmod{59} \Rightarrow n_{59} = 1$. So the 59-Sylow subgroup P_{59} is unique.
- $p \notin \Pi = \{2, 3, 5, 7\}$, the set of primes dividing an element of order in some Γ_σ.
- $p - 1 = 58 = 2 \cdot 19$, so $\gcd(p-1, E) = 2$.
- Conclusion: $g = 60$ attains the lower bound.

Smaller Primes: p=83

- $p = 83$, S of genus $g = 84$:

Smaller Primes: p=83

- $p = 83$, S of genus $g = 84$:
- 83 is coprime to R, so $|Aut(S)| = |G| = (g-1)s = 83s$ for some s. By inspection, s is coprime to 83, so if P_{83} is a 83-Sylow subgroup, then $|P_{83}| = 83$. Letting n_{83} be the number of 83-Sylow subgroups, we must have $n_{83}|s$ and $n_{59} \equiv 1 \pmod{59}$.

Smaller Primes: p=83

- $p = 83$, S of genus $g = 84$:
- 83 is coprime to R, so $|Aut(S)| = |G| = (g-1)s = 83s$ for some s. By inspection, s is coprime to 83, so if P_{83} is a 83-Sylow subgroup, then $|P_{83}| = 83$. Letting n_{83} be the number of 83-Sylow subgroups, we must have $n_{83}|s$ and $n_{59} \equiv 1 \pmod{59}$.
- Claim: P_{83} is normal in G.

Smaller Primes: p=83

- $p = 83$, S of genus $g = 84$:
- 83 is coprime to R, so $|Aut(S)| = |G| = (g-1)s = 83s$ for some s. By inspection, s is coprime to 83, so if P_{83} is a 83-Sylow subgroup, then $|P_{83}| = 83$. Letting n_{83} be the number of 83-Sylow subgroups, we must have $n_{83}|s$ and $n_{59} \equiv 1 \pmod{59}$.
- Claim: P_{83} is normal in G.

Proof:

Smaller Primes: p=83

- $p = 83$, S of genus $g = 84$:
- 83 is coprime to R, so $|Aut(S)| = |G| = (g-1)s = 83s$ for some s. By inspection, s is coprime to 83, so if P_{83} is a 83-Sylow subgroup, then $|P_{83}| = 83$. Letting n_{83} be the number of 83-Sylow subgroups, we must have $n_{83}|s$ and $n_{59} \equiv 1 \pmod{59}$.
- Claim: P_{83} is normal in G.

Proof:

- The only possibility for the 83-Sylow subgroup P_{83} not being unique is if $n_{83} = s = 84$.

Smaller Primes: p=83

- $p = 83$, S of genus $g = 84$:
- 83 is coprime to R, so $|Aut(S)| = |G| = (g-1)s = 83s$ for some s. By inspection, s is coprime to 83, so if P_{83} is a 83-Sylow subgroup, then $|P_{83}| = 83$. Letting n_{83} be the number of 83-Sylow subgroups, we must have $n_{83}|s$ and $n_{59} \equiv 1 \pmod{59}$.
- Claim: P_{83} is normal in G.

Proof:

- The only possibility for the 83-Sylow subgroup P_{83} not being unique is if $n_{83} = s = 84$.
- Then the normaliser of P_{83} is just P, so G acts faithfully and transitively on P_{83} (Frobenius action).
  $\Rightarrow$ There exists a normal subgroup N of G such that G is the semidirect product of N and P_{83}.

Smaller Primes: p=83,47,23

- In particular, there exists an epimorphism $G \to \mathbb{Z}_{83}$.

Smaller Primes: p=83,47,23

- In particular, there exists an epimorphism $G \to \mathbb{Z}_{83}$.
- But since $s = 84$, $\Gamma = \Gamma(2, 3, 7)$ is a triangle group, this is impossible. Thus P_{83} must be normal as required.

Smaller Primes: p=83,47,23

- In particular, there exists an epimorphism $G \to \mathbb{Z}_{83}$.
- But since $s = 84$, $\Gamma = \Gamma(2, 3, 7)$ is a triangle group, this is impossible. Thus P_{83} must be normal as required.
- Also, $p - 1 = 82 = 2 \cdot 41$, so $\gcd(p - 1, E) = 2$.

Smaller Primes: p=83,47,23

- In particular, there exists an epimorphism $G \to \mathbb{Z}_{83}$.
- But since $s = 84$, $\Gamma = \Gamma(2,3,7)$ is a triangle group, this is impossible. Thus P_{83} must be normal as required.
- Also, $p - 1 = 82 = 2 \cdot 41$, so $\gcd(p-1, E) = 2$. Therefore, $p = 83$ satisfies all required conditions to exclude that $|G| > 4(g-1) = 4 \cdot 83$.

Smaller Primes: p=83,47,23

- In particular, there exists an epimorphism $G \to \mathbb{Z}_{83}$.
- But since $s = 84$, $\Gamma = \Gamma(2,3,7)$ is a triangle group, this is impossible. Thus P_{83} must be normal as required.
- Also, $p - 1 = 82 = 2 \cdot 41$, so $\gcd(p-1, E) = 2$. Therefore, $p = 83$ satisfies all required conditions to exclude that $|G| > 4(g-1) = 4 \cdot 83$.
- Conclusion: $g = 60$ attains the lower bound.

Smaller Primes: p=83,47,23

- In particular, there exists an epimorphism $G \to \mathbb{Z}_{83}$.
- But since $s = 84$, $\Gamma = \Gamma(2,3,7)$ is a triangle group, this is impossible. Thus P_{83} must be normal as required.
- Also, $p - 1 = 82 = 2 \cdot 41$, so $\gcd(p-1, E) = 2$. Therefore, $p = 83$ satisfies all required conditions to exclude that $|G| > 4(g-1) = 4 \cdot 83$.
- Conclusion: $g = 60$ attains the lower bound.
- Similarly, one can show that for $p = g - 1 = 47$, there exists a unique normal subgroup of order 47, and satisfies the other conditions of the Main Theorem as well.

Smaller Primes: p=83,47,23

- In particular, there exists an epimorphism $G \to \mathbb{Z}_{83}$.
- But since $s = 84$, $\Gamma = \Gamma(2,3,7)$ is a triangle group, this is impossible. Thus P_{83} must be normal as required.
- Also, $p - 1 = 82 = 2 \cdot 41$, so $\gcd(p-1, E) = 2$. Therefore, $p = 83$ satisfies all required conditions to exclude that $|G| > 4(g-1) = 4 \cdot 83$.
- Conclusion: $g = 60$ attains the lower bound.
- Similarly, one can show that for $p = g - 1 = 47$, there exists a unique normal subgroup of order 47, and satisfies the other conditions of the Main Theorem as well.
- Using more results from group theory, one can show that $p = 23$ attains the lower bound as well.

Smaller Primes: p=83,47,23

- In particular, there exists an epimorphism $G \to \mathbb{Z}_{83}$.
- But since $s = 84$, $\Gamma = \Gamma(2,3,7)$ is a triangle group, this is impossible. Thus P_{83} must be normal as required.
- Also, $p - 1 = 82 = 2 \cdot 41$, so $\gcd(p-1, E) = 2$. Therefore, $p = 83$ satisfies all required conditions to exclude that $|G| > 4(g-1) = 4 \cdot 83$.
- Conclusion: $g = 60$ attains the lower bound.
- Similarly, one can show that for $p = g - 1 = 47$, there exists a unique normal subgroup of order 47, and satisfies the other conditions of the Main Theorem as well.
- Using more results from group theory, one can show that $p = 23$ attains the lower bound as well.
- In fact, one can show that $g = 24$ is the smallest prime such that $N_{ar}(g) = 4(g-1)$.

Explicit Sequence Theorem

Theorem (Explicit Sequence Theorem)

For all primes $p \equiv 23, 47, 59 \pmod{6}0$, *we have* $N_{ar}(g) = 4(g-1)$. *The least genus* g *for which the the lower bound* $N_{ar}(g) = 4(g-1)$ *is attained is* $g = 24$.

References I

- Farkas, H.M., Kra, I.
  Riemann Surfaces.
  New York: Springer, 1980.
- Jones, G., Singerman, D.
  Complex Functions.
  Cambridge: Cambridge UP, 1987.
- Katok, S.
  Fuchsian Groups.
  Chicago: U Chicago Press, 1992.

References II

Belolipetsky, M., Jones, G.
A bound for the number of automorphisms of an arithmetic Riemann surface.
Math. Proc. Cambridge Philos. Soc., **138** (2005), no. 2, 289-299.

Sah, C.H.
Groups related to compact Riemann surfaces.
Acta Math. **123** (1969), 13-42.

Takeuchi, K.
Arithmetic Triangle Groups
J. Math. Soc. Japan **29** (1977), 91-106.