<table>
<thead>
<tr>
<th>Title</th>
<th>On the Galois images associated to QM-abelian surfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>ARAI, Keisuke</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録別冊 = RIMS Kokyuroku Bessatsu (2007), B4: 165-187</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2007-12</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/174164">http://hdl.handle.net/2433/174164</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
On the Galois images associated to QM-abelian surfaces

By

Keisuke ARAI*

Abstract

Let $\rho_{E/K,p} : G_K \rightarrow \text{Aut}(T_pE) \cong \text{GL}_2(\mathbb{Z}_p)$ be the Galois representation determined by the Galois action on the $p$-adic Tate module of an elliptic curve $E$ over a number field $K$. Serre showed that $\rho_{E/K,p}$ has an open image if $E$ has no complex multiplication. The author showed that $\rho_{E/K,p}(G_K)$ have a uniform lower bound when we fix $K$, $p$ and vary $E$. In this paper, we give a similar result on uniform boundedness of the Galois images associated to abelian surfaces with quaternionic multiplication.

§1. Introduction

Let $k$ be a field of characteristic 0, and let $G_k = \text{Gal}(\overline{k}/k)$ be the absolute Galois group of $k$ where $\overline{k}$ is an algebraic closure of $k$. Let $p$ be a prime number. For an elliptic curve $E$ over $k$, let $T_pE$ be the $p$-adic Tate module of $E$, and let

$$\rho_{E/k,p} : G_k \rightarrow \text{Aut}(T_pE) \cong \text{GL}_2(\mathbb{Z}_p)$$

be the $p$-adic representation determined by the action of $G_k$ on $T_pE$. By a number field we mean a finite extension of $\mathbb{Q}$.

We recall a famous theorem proved by Serre.

Theorem 1.1. ([Se1], IV-11) Let $K$ be a number field and $E$ be an elliptic curve over $K$ without complex multiplication. Take a prime $p$. Then the image $\rho_{E/K,p}(G_K)$ is open in $\text{GL}_2(\mathbb{Z}_p)$ i.e. there exists a positive integer $n$ depending on $p, K$ and $E$ such that $\rho_{E/K,p}(G_K) \supseteq 1 + p^n\mathbb{M}_2(\mathbb{Z}_p)$.

The author showed that the image $\rho_{E/K,p}(G_K)$ has a uniform lower bound.

*Graduate School of Mathematical Sciences, The University of Tokyo, 8-1 Komaba 3-chome, Meguro-ku, Tokyo 153-8914, Japan. E-mail: araik@ms.u-tokyo.ac.jp

© 2007 Research Institute for Mathematical Sciences, Kyoto University. All rights reserved.
Theorem 1.2. ([A], Theorem 1.2) Let $K$ be a number field and $p$ be a prime. Then there exists a positive integer $n$ depending on $p$ and $K$ satisfying the following. For any elliptic curve $E$ over $K$ without complex multiplication, we have $\rho_{E/K,p}(G_K) \supseteq 1 + p^nM_2(\mathbb{Z}_p)$.

Remark 1.3. In the above theorem, the integer $n$ is effectively estimated if $j(E)$ is not contained in an exceptional finite set ([A], Theorem 1.3).

The author hopes to give a similar result in a higher dimensional case. In this paper, we treat so-called QM-abelian surfaces. We will give the main results in Theorem 2.3 and Theorem 5.1.

I would like to thank Professor F. Momose and Doctor T. Yamauchi for suggesting this subject to me. I would like to thank Professor T. Saito for advice and comments. I would also like to thank the referee for comments and suggestions. This work was partly supported by 21st Century COE Program in The University of Tokyo, A Base for New Developments of Mathematics into Science and Technology.

§ 2. QM-abelian surfaces and the main theorem

Let $Q$ be an indefinite quaternion division algebra over $\mathbb{Q}$. Let $d = \text{disc}(Q)$ be the discriminant of $Q$. We know that $d$ is the product of an even number of primes, and $d > 1$. Choose a maximal order $R$ of $Q$. It is known that $R$ is unique up to conjugation by an element of $Q^\times$. For a prime $p$, put $R_p := R \otimes_{\mathbb{Z}} \mathbb{Z}_p$. If $p$ does not divide $d$, fix an isomorphism $R_p \cong \mathrm{M}_2(\mathbb{Z}_p)$.

Definition 2.1. (cf. [Bu], p.591) Let $S$ be a scheme over $\mathbb{Q}$. A QM-abelian surface (by $R$) over $S$ is a pair $(A, i)$ where $A$ is an abelian surface over $S$ (i.e. $A$ is an abelian scheme over $S$ of relative dimension 2), and $i : R \hookrightarrow \text{End}_S(A)$ is an injective ring homomorphism (sending 1 to id). We say two QM-abelian surfaces $(A, i)$, $(A', i')$ over $S$ are isomorphic if there is an isomorphism $A \cong A'$ of abelian schemes over $S$ and the following diagram is commutative:

\[
\begin{array}{ccc}
R & \xrightarrow{i} & \text{End}_S(A) \\
\downarrow{\text{id}} & & \downarrow{\cong} \\
R & \xrightarrow{i'} & \text{End}_S(A'),
\end{array}
\]

where the right vertical map is induced by the isomorphism $A \cong A'$.

Let $k$ be a field of characteristic 0. It is known that a QM-abelian surface $(A, i)$ over $k$ where $i$ is an isomorphism has a Galois representation which looks like that of
an elliptic curve ([O], §1). By this reason, a QM-abelian surface is also called a fake elliptic curve or a false elliptic curve.

Let \((A, i)\) be a QM-abelian surface over \(k\). Suppose the following:

\[(2.1) \quad i : R \rightarrow^\simeq \End_k(A) = \End(A).\]

Note that the condition (2.1) corresponds to "no complex multiplication" in the case of elliptic curves. Take a prime \(p\) not dividing \(d\). Then the \(p\)-adic Tate module \(T_pA\) of \(A\) is a free \(R_p\)-module of rank 1. Thus we have a Galois representation

\[\rho_{(A,i)/k,p} : \mathbb{G}_k \rightarrow \Aut_{R_p}(T_pA) \cong R_p^\times \cong \GL_2(\mathbb{Z}_p).\]

The first isomorphism is not canonical, and the second is induced from the isomorphism \(R_p \cong \M_2(\mathbb{Z}_p)\) fixed above. Let

\[\overline{\rho}_{(A,i)/k,p^n} : \mathbb{G}_k \rightarrow \GL_2(\mathbb{Z}/p^n\mathbb{Z})\]

be the reduction of \(\rho_{(A,i)/k,p}\) modulo \(p^n\). Note that the determinant

\[\det \rho_{(A,i)/k,p} : \mathbb{G}_k \rightarrow \mathbb{Z}_p^\times\]

is the \(p\)-adic cyclotomic character.

The representation \(\rho_{(A,i)/k,p}\) has an open image just as in the case of an elliptic curve.

**Theorem 2.2.** ([O], Theorem 2.8) Let \(K\) be a number field and \((A, i)\) be a QM-abelian surface over \(K\) satisfying (2.1) (with \(k = K\)). Take a prime \(p\) not dividing \(d\). Then the representation \(\rho_{(A,i)/K,p}\) has an open image i.e. there exists a positive integer \(n\) depending on \(p, K, R\) and \((A, i)/K\) such that \(\rho_{(A,i)/K,p}(\mathbb{G}_K) \supseteq 1 + p^nM_2(\mathbb{Z}_p)\).

We will show the following theorem asserting that the representation \(\rho_{(A,i)/K,p}\) has a uniform lower bound. This is one of the main result of this paper.

**Theorem 2.3.** Let \(K\) be a number field and \(p\) be a prime not dividing \(d\). Then there exists a positive integer \(n\) depending on \(p, K, R\) satisfying the following: For any QM-abelian surface \((A, i)\) over \(K\) having the property (2.1) (with \(k = K\)), we have \(\rho_{(A,i)/K,p}(\mathbb{G}_K) \supseteq 1 + p^nM_2(\mathbb{Z}_p)\).

Let \((A, i), (A', i')\) be QM-abelian surfaces over \(k\). Take a field extension \(k'/k\). We say \((A, i)\) and \((A', i')\) are \(k'\)-isomorphic if their base changes \((A \times_{\ Spec(k)} \ Spec(k'), i)\) and \((A' \times_{\ Spec(k)} \ Spec(k'), i')\) are isomorphic. Note that the last "i" is the composite

\[R \rightarrow^i \End_k(A) \rightarrow^\text{canonical} \End_{k'}(A \times_{\ Spec(k)} \ Spec(k')),\]
and similar for the last \( "i" \).

In Section 5, we will give an effective bound for \( \rho_{(A,i)/K,p}(G_K) \) except a finite number of \( \overline{K} \)-isomorphism classes of QM-abelian surfaces.

\section{3. Moduli of QM-abelian surfaces}

Let

\[ M^R : (\text{Sch}/\mathbb{Q}) \rightarrow (\text{Sets}) \]

be the contravariant functor defined as follows:

(1) For any scheme \( S \) over \( \mathbb{Q} \),

\[ M^R(S) = \{ \text{isomorphism classes of QM-abelian surfaces } (A, i) \text{ over } S \} . \]

(2) For any morphism of schemes \( f : S' \rightarrow S \) over \( \mathbb{Q} \),

\[ M^R(f) : M^R(S) \rightarrow M^R(S') ; [(A, i)] \mapsto [(A \times_S S', i)] \]

where the last \( "i" \) is the composite

\[ R \rightarrow^i \text{End}_S(A) \rightarrow^{\text{canonical}} \text{End}_{S'}(A \times_S S') . \]

The functor \( M^R \) has a coarse moduli scheme \( X^R \) over \( \mathbb{Q} \). The scheme \( X^R \) is a proper smooth curve with constant field \( \mathbb{Q} \), called a Shimura curve (cf. [Bu]). Let \( g^R := g(X^R) \) be the genus of \( X^R \). For a prime \( p \), put

\[ \left( \frac{-1}{p} \right) := \begin{cases} 
1 & \text{if } p \equiv 1 \mod 4, \\
-1 & \text{if } p \equiv -1 \mod 4, \\
0 & \text{if } p = 2,
\end{cases} \]

\[ \left( \frac{-3}{p} \right) := \begin{cases} 
1 & \text{if } p \equiv 1 \mod 3, \\
-1 & \text{if } p \equiv -1 \mod 3, \\
0 & \text{if } p = 3.
\end{cases} \]

\textbf{Lemma 3.1.} \([\text{[Shimi], Chapter 2, Chapter 3}]\) We have

\[ g^R = 1 + \frac{1}{12} \prod_{p|d} (p-1) - \frac{1}{4} \prod_{p|d} \left( 1 - \left( \frac{-1}{p} \right) \right) - \frac{1}{3} \prod_{p|d} \left( 1 - \left( \frac{-3}{p} \right) \right) . \]

In particular, \( g^R = 0 \) if and only if \( d \in \{6, 10, 22\} \), and \( g^R = 1 \) if and only if \( d \in \{14, 15, 21, 33, 34, 46\} \).
Faltings proved the following celebrated theorem known as Mordell's conjecture.

**Theorem 3.2.** ([F], Theorem 7) Let $K$ be a number field and $X$ be a proper smooth curve over $K$. If the genus $g(X) \geq 2$, then $X(K)$ consists of only finitely many elements.

**Corollary 3.3.** Let $K$ be a number field. If $g^R \geq 2$, then there are only finitely many $\bar{K}$-isomorphism classes of QM-abelian surfaces over $K$.

§ 4. Twists and Galois images

When $g^R \geq 2$, we show Theorem 2.3 by using the theory of twists.

**Lemma 4.1.** (cf. [St], X, §2, §5) Let $k$ be a field of characteristic 0, and $(A, i), (A', i')$ be QM-abelian surfaces satisfying (2.1). If $(A, i)$ and $(A', i')$ are $\bar{k}$-isomorphic, then there exists a field extension $L$ with $[L : k] \leq 2$ such that $(A, i)$ and $(A', i')$ are $L$-isomorphic.

**Proof.** Put $Twist((A, i), k) := \{(A'', i'')\}/k$-isomorphism, where $(A'', i'')$ is a QM-abelian surface over $k$ satisfying (2.1) and isomorphic to $(A, i)$ over $\bar{k}$. Then we have a natural inclusion $Twist(\circlearrowright)$ which is defined as follows. Take a $\bar{k}$-isomorphism $\phi : (A'', i'') \mapsto (A, i)$. Let $\xi : G_k \mapsto \text{Aut}(A, i)$ be the map sending $\sigma$ to $\phi^\sigma \circ \phi^{-1}$. Then $\xi$ represents an element of $H^1(G_k, \text{Aut}(A, i))$, which is independent of the choice of $\phi$.

Next we show $\text{Aut}(A, i) = \{\pm 1\}$. The inclusion $\text{Aut}(A, i) \supseteq \{\pm 1\}$ is obvious. To see the other inclusion, we have $\text{Aut}(A, i) = \text{Aut}(A) \cap \text{End}(A, i) \subseteq R^x \cap (\text{center of } \text{End}(A) \otimes \mathbb{Q}) = R^x \cap \mathbb{Q} = Z^x = \{\pm 1\}$. Thus $\text{Aut}(A, i) = \{\pm 1\}$, on which $G_k$ acts trivially. Hence we have an isomorphism $H^1(G_k, \text{Aut}(A, i)) \cong k^x/(k^x)^2; (\xi : \sigma \mapsto \sigma(\overline{m})/\overline{m} \leftrightarrow m)$. This $\xi$ is trivialized by the corresponding extension $k(\overline{m})/k$.

**Lemma 4.2.** ([A], Lemma 2.3) Let $n \geq 1$ be an integer. Let $H$ be a subgroup of $GL_2(\mathbb{Z}_p)$ containing $1 + p^nM_2(\mathbb{Z}_p)$, and $H'$ be a closed subgroup of $GL_2(\mathbb{Z}_p)$ which is a subgroup of $H$ of index 2. If $p \geq 3$, then $H' \supseteq 1 + p^nM_2(\mathbb{Z}_p)$; if $p = 2$ and $n \geq 2$, $H' \supseteq 1 + p^{n+1}M_2(\mathbb{Z}_p)$.

**Corollary 4.3.** Let $K$ be a number field and $(A, i)$ be a QM-abelian surface over $K$ with the property (2.1). Then there exists a positive integer $n$ depending on $p, K, R$ and $(A, i)/K$ satisfying the following: For any QM-abelian surface $(A', i')$ over $K$ that is $\bar{K}$-isomorphic to $(A, i)$ (such an $(A', i')$ automatically satisfies (2.1)), we have $\rho_{(A', i')/K, p}(G_K) \supseteq 1 + p^nM_2(\mathbb{Z}_p)$.
Proof. Combining Lemma 4.1, 4.2 and Theorem 2.2, we get the result. \qed

By Corollary 3.3 and 4.3, we get the following.

**Proposition 4.4.** If $g^R \geq 2$, then Theorem 2.3 is true.

§ 5. Effective version

We give an effective version of Theorem 2.3, though we admit finitely many exceptions. We use the following conventions:

\begin{align*}
1 + p^0\mathbb{Z}_p & := \mathbb{Z}_p^\times, \\
1 + p^0\text{M}_2(\mathbb{Z}_p) & := \text{GL}_2(\mathbb{Z}_p), \\
1 + p^0\text{M}_2(\mathbb{Z}/p\mathbb{Z}) & := \text{GL}_2(\mathbb{Z}/p\mathbb{Z}).
\end{align*}

**Theorem 5.1.** Suppose $g^R \leq 1$, so that $d \in \{6, 10, 22, 14, 15, 21, 33, 34, 46\}$. For a prime $p$ not dividing $d$, there exists an integer $n \geq 0$ satisfying the following condition $(C)_{R,p}$. $(C)_{R,p}$: Let $K$ be a number field. Then for all QM-abelian surfaces $(A, i)$ over $K$ with (2.1) but a finite number of $\overline{K}$-isomorphism classes, we have

\[ \rho_{(A,i)/K,p}(G_K) \supseteq (1 + p^n\text{M}_2(\mathbb{Z}_p))^{\det=1}. \]

Let $n(R,p) \geq 0$ be the minimum integer $n$ satisfying $(C)_{R,p}$. Then $n(R,p)$ is estimated as follows. When $d = 6$, we have

\[
n(R,p) \begin{cases} 
\in \{1, 2\} & \text{if } p = 5, \\
= 1 & \text{if } p = 7, \\
\leq 1 & \text{if } p = 11, \\
= 1 & \text{if } p = 13, \\
= 0 & \text{if } p \geq 17.
\end{cases}
\]

When $d = 10$, we have

\[
n(R,p) \begin{cases} 
\leq 3 & \text{if } p = 3, \\
= 1 & \text{if } p = 7, \\
= 0 & \text{if } p \geq 11.
\end{cases}
\]

When $d = 22$, we have

\[
n(R,p) \begin{cases} 
\leq 2 & \text{if } p = 3, \\
\leq 1 & \text{if } p = 5, \\
= 0 & \text{if } p \geq 7.
\end{cases}
\]
When \( d \in \{14, 21, 33, 34, 46\} \), we have
\[
n(R, p) = \begin{cases} 
\leq 3 & \text{if } p = 2, \\
\leq 1 & \text{if } p = 3, \\
= 0 & \text{if } p \geq 5.
\end{cases}
\]

When \( d = 15 \), we have
\[
n(R, p) = \begin{cases} 
\leq 5 & \text{if } p = 2, \\
= 0 & \text{if } p \geq 7.
\end{cases}
\]

To deduce \( \rho_{G_K} \geq 1 + p^nM_2(\mathbb{Z}/p) \) from Theorem 5.1, we use the following.

**Lemma 5.2.** ([A], Corollary 2.7) Let \( H \subseteq GL_2(\mathbb{Z}/p) \) be a closed subgroup and \( n, r \geq 0 \) be integers. Assume \( r \geq 2 \) if \( p = 2 \). If \( H \supseteq 1 + p^nM_2(\mathbb{Z}/p)^{\det=1} \) and \( \det(H) \supseteq 1 + p^r \mathbb{Z}/p \), then \( H \supseteq 1 + p^{n+r}M_2(\mathbb{Z}/p) \).

Corollary 4.3, Theorem 5.1 and Lemma 5.2 imply Theorem 2.3 for \( g^R \leq 1 \).

§ 6. Level structure on QM-abelian surfaces

To construct a curve with genus at least 2, we introduce a level structure on a QM-abelian surface.

**Definition 6.1.** (cf. [Bu], Definition 1.1, [Bo], §13) Take an integer \( N \geq 1 \) prime to \( d \). Let \( S \) be a scheme over \( \mathbb{Q} \) and \((A, i)\) be a QM-abelian surface over \( S \). A level \( N \)-structure on \((A, i)\) is an isomorphism of \( S \)-group schemes
\[
\gamma : R \otimes \mathbb{Z}/NZ \xrightarrow{\cong} A[N]
\]
which is compatible with the action of \( R \).

Take two QM-abelian surfaces with level \( N \)-structure \((A, i, \gamma), (A', i', \gamma')\). We say \((A, i, \gamma)\) and \((A', i', \gamma')\) are isomorphic if there is an isomorphism \((A, i) \cong (A', i')\) of QM-abelian surfaces and the isomorphism is compatible with \( \gamma \) and \( \gamma' \).

Let \( X^R(N) \) be the moduli scheme over \( \mathbb{Q} \) associated to the contravariant functor
\[
\mathcal{M}^R(N) : (\text{Sch}/\mathbb{Q}) \rightarrow (\text{Sets})
\]
defined as follows:
(1) For any scheme \( S \) over \( \mathbb{Q} \),
\[
\mathcal{M}^R(N)(S) = \{\text{isomorphism classes of } (A, i, \gamma)\},
\]
where $(A, i)$ is a QM-abelian surface over $S$ and $\gamma$ a level $N$-structure on it.

(2) For any morphism of schemes $f : S' \rightarrow S$ over $\mathbb{Q}$,

$$\mathcal{M}^R(N)(f) : \mathcal{M}^R(N)(S) \rightarrow \mathcal{M}^R(N)(S'); [(A, i, \gamma)] \mapsto [(A \times_S S', i, \gamma \times_S S')].$$

Then $X^R(N)$ is a proper smooth curve with constant field $\mathbb{Q}(\zeta_N)$. To see this, first we define a morphism

$$X^R(N) \rightarrow \text{Spec}(\mathbb{Q}(\zeta_N)).$$

For simplicity, suppose $N$ is odd. Take an element $\alpha \in Q$ such that $\alpha^2 = -d$ (such an element exists). We may assume $\alpha \in R$ and $\alpha$ maps to \( \begin{pmatrix} 0 & -1 \\ d & 0 \end{pmatrix} \) via the isomorphism $R \otimes \mathbb{Z} \cong M_2(\mathbb{Z})$. Let $*: Q \rightarrow Q$ be the involution defined by $x^* = \alpha^{-1} x^\iota \alpha$, where $\iota$ is the canonical involution on $Q$. Then $*$ stabilizes $R$. For any QM-abelian surface $(A, i)$, there exists a unique principal polarization $\lambda : A \rightarrow A^\vee$ making the following diagram commutative ([BC], Proposition (1.5)):

\[
\begin{array}{ccc}
A & \xrightarrow{\lambda} & A^\vee \\
\downarrow i(r^*) & & \downarrow i(r)^\vee \\
A & \xrightarrow{\lambda} & A^\vee.
\end{array}
\]

Let $e_N: A[N] \times A^\vee[N] \rightarrow \mu_N$ be the Weil pairing, and define a pairing $\langle , \rangle : A[N] \times A[N] \rightarrow \mu_N$ by $\langle x, y \rangle = e_N(x, \lambda(y))$. Then $\langle , \rangle$ is bilinear, alternating, non-degenerate and satisfies $\langle rx, y \rangle = \langle x, r^* y \rangle$ for every $r \in R$ ([Bu], p.592). Take a level $N$-structure $\gamma$ on $(A, i)$ and identify $A[N] \cong R \otimes \mathbb{Z} \cong M_2(\mathbb{Z})$ by using $\gamma$. Define a morphism $X^R(N) \rightarrow \text{Spec}(\mathbb{Q}(\zeta_N))$ by $(A, i, \gamma) \mapsto \langle \begin{pmatrix} 10 \\ 00 \end{pmatrix}, \begin{pmatrix} 01 \\ 00 \end{pmatrix} \rangle$.

Note that $\langle \begin{pmatrix} 10 \\ 00 \end{pmatrix}, \begin{pmatrix} 01 \\ 00 \end{pmatrix} \rangle$ generates $\mu_N$. In fact, we have $\begin{pmatrix} 10 \\ 00 \end{pmatrix}^* = \begin{pmatrix} 10 \\ 00 \end{pmatrix}$, hence $\langle \begin{pmatrix} 10 \\ 00 \end{pmatrix}, \begin{pmatrix} 00 \\ uv \end{pmatrix} \rangle = 0$ for any $u, v \in \mathbb{Z}$. Since $\langle , \rangle$ is alternating, $\langle \begin{pmatrix} 10 \\ 00 \end{pmatrix}, \begin{pmatrix} 10 \\ 00 \end{pmatrix} \rangle = 0$. As $\langle , \rangle$ is non-degenerate, $\langle \begin{pmatrix} 10 \\ 00 \end{pmatrix}, \begin{pmatrix} 01 \\ 00 \end{pmatrix} \rangle$ must generate $\mu_N$.

Next consider the $\mathbb{C}$-valued points of $X^R(N)$ (cf. [Be], §3, §4, [DR], IV.5). Put $\mathbb{H} := \{ z \in \mathbb{C} | \text{Im} z > 0 \}$ and write $SR^\times := \{ c \in R | Nrd(c) = 1 \}$, where $\text{Nrd}$ is the reduced norm. We have an isomorphism of complex manifolds

$$\text{Hom}_{\text{Spec}(\mathbb{Q})}(\text{Spec}(\mathbb{C}), X^R(N)) \cong SR^\times \backslash (\mathbb{H} \times \text{GL}_2(\mathbb{Z}/NZ)),$$

and the set of connected components of this manifold is identified with $(\mathbb{Z}/NZ)^\times$ via
determinant. We also have

$$\text{Hom}_{\text{Spec}(\mathbb{Q}(\zeta_N))}(\text{Spec}(\mathbb{C}), X^R(N)) \cong SR^\times(N) \backslash \mathbb{H},$$

where $SR^\times(N) := \{ c \in SR^\times | c \equiv 1 \text{ mod } N \}$. Therefore the constant field of $X^R(N)$ is $\mathbb{Q}(\zeta_N)$ because $SR^\times(N) \backslash \mathbb{H}$ is connected.

Put

$$G := \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \subseteq (R \otimes_\mathbb{Z} \mathbb{Z}/N\mathbb{Z})^\times.$$  

We have a right action of $G$ on $X^R(N)$:

$$[(A, i, \gamma)] \mapsto [(A, i, \gamma \circ g)]$$

where $(A, i)$ is a QM-abelian surface, $\gamma$ a level $N$-structure on $(A, i)$ and $g \in G$. For a subgroup $H \subseteq G$, put

$$X^R_H := X^R(N)/H.$$  

Then $X^R_H$ is a proper smooth curve with constant field $\mathbb{Q}(\zeta_N)$. Let $g^R_H$ be the genus of $X^R_H$.

**Lemma 6.2.** Let $K$ be a number field. If $g^R_H \geq 2$, then there are only finitely many $\overline{K}$-isomorphism classes of QM-abelian surfaces $(A, i)$ over $K$ with the property (2.1) and satisfying: A conjugate of $\overline{\rho}_{(A, i)/K,N}(\text{G}_K)$ is contained in $H$.

The genus $g^R_H$ is expressed by using $g^R$. Put

$$\sigma := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tau := \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in \text{SL}_2(\mathbb{Z}).$$

For $\alpha \in \text{SL}_2(\mathbb{Z})$ or $R$, we also use the same letter to denote the reduction of $\alpha$. Put

$$\text{Fix}_H := \{ gH \in G/H | gH = gH \}.$$  

Let $SR^\times_H$ be the inverse image of $H$ by the natural surjection

$$SR^\times \twoheadrightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

**Lemma 6.3.** (cf. [Shimu, Proposition 1.40]) We have

$$g^R_H = 1 + (g - 1)\mu_H + \frac{1}{4}(r\mu_H - \nu_2) + \frac{1}{3}(s\mu_H - \nu_3)$$

$$= 1 + (g - 1 + \frac{1}{4}r + \frac{1}{3}s)\mu_H - \frac{1}{4}\nu_2 - \frac{1}{3}\nu_3,$$

where

$$r := \prod_{p \mid d} \left(1 - \left(\frac{-1}{p}\right)\right), s := \prod_{p \mid d} \left(1 - \left(\frac{-3}{p}\right)\right),$$

$$\nu_2 := r\#\text{Fix}_\sigma, \nu_3 := s\#\text{Fix}_\tau,$$

$$\mu_H := [SR^\times/\{\pm 1\} : (SR^\times_H, -1)/\{\pm 1\}].$$
Proof. We show the formula over $\mathbb{C}$. We call $c \in SR^\times$ an elliptic element if $|\text{Tr}(c)| < 2$, where $\text{Tr}$ is the reduced trace. For a subgroup $U \subseteq SR^\times$, a point $z \in \mathbb{H}$ is called an elliptic point of $U$ if there exists an elliptic element $c \in U$ such that $c(z) = z$.

By abuse of language, we sometimes call a point on $U \setminus \mathbb{H}$ an elliptic point if it is the image of an elliptic point on $\mathbb{H}$ of $U$. It is known that $r$ (resp. $s$) is the number of elliptic points of order 2 (resp. 3) on $SR^\times \setminus \mathbb{H}$. The index $\mu_H$ is the degree of the quotient map $\phi : SR^\times_H \setminus \mathbb{H} \rightarrow SR^\times \setminus \mathbb{H}$, because the group of all holomorphic automorphisms of $\mathbb{H}$ is $\text{SL}_2(\mathbb{R})/\{\pm 1\}$. We show $\nu_2$ (resp. $\nu_3$) is the number of elliptic points of order 2 (resp. 3) on $SR^\times_H \setminus \mathbb{H}$. Let $P_1, \ldots, P_r$ (resp. $Q_1, \ldots, Q_s$) be the elliptic points of order 2 (resp. 3) on $SR^\times \setminus \mathbb{H}$. We have a decomposition

$$\{\text{elliptic points of order 2 of } SR^\times_H \}$$

$$= \prod_{i=1}^{r} \{\text{elliptic points of order 2 of } SR^\times_H \text{ above } P_i \}$$

$$\subseteq \{\text{elliptic points of order 2 of } SR^\times \} \subseteq \mathbb{H}.$$

Let $\widetilde{P}_i \in \mathbb{H}$ be a lift of $P_i$. Choose a generator $\sigma_i$ of the cyclic group $\{g \in SR^\times | g \widetilde{P}_i = \widetilde{P}_i \} \cong \mathbb{Z}/4\mathbb{Z}$. The map

$$\{\text{elliptic points of order 2 of } SR^\times_H \text{ above } P_i \}$$

$$\rightarrow \{g \in SR^\times | g^{-1}\sigma_i g \in SR^\times_H \}/SR^\times_H :$$

$$g \widetilde{P}_i \mapsto g^{-1}SR^\times_H$$

is well-defined, and it induces a bijection

$$SR^\times_H \setminus \{\text{elliptic points of order 2 of } SR^\times_H \text{ above } P_i \}$$

$$\cong \{g \in SR^\times | g^{-1}\sigma_i g \in SR^\times_H \}/SR^\times_H.$$

The mod $N$ map induces a bijection $\{g \in SR^\times | g^{-1}\sigma_i g \in SR^\times_H \}/SR^\times_H \cong \text{Fix}_{\sigma_i}$. Hence we have

$$\{\text{elliptic points of order 2 on } SR^\times_H \}$$

$$= SR^\times_H \setminus \{\text{elliptic points of order 2 of } SR^\times_H \}$$

$$= \prod_{i=1}^{r} \{\text{elliptic points of order 2 of } SR^\times_H \text{ above } P_i \}$$

$$\cong \prod_{i=1}^{r} \text{Fix}_{\sigma_i}.$$
Thus \( \nu_2 \) is the number of elliptic points of order 2 on \( SR_H^\times \backslash \mathbb{H} \) since \( \sigma_i \) is conjugate to \( \sigma \) in \( G \). The assertion for \( \nu_3 \) is verified in the same way.

Applying Hurwitz’ formula to the map \( \phi \), we have

\[
2g_H^R - 2 = (2g^R - 2)\mu_H + \sum_{X \mapsto P_1, \ldots, P_r} (e_X - 1) + \sum_{Y \mapsto Q_1, \ldots, Q_s} (e_Y - 1)
\]

where \( e_X \) (resp. \( e_Y \)) is the ramification index of \( \phi \) at \( X \) (resp. \( Y \)). Let \( P \in SR_X^\times \backslash \mathbb{H} \) be an elliptic point of order \( e \) where \( e \) is 2 or 3. Let \( X_1, \ldots, X_a \in SR_H^\times \backslash \mathbb{H} \) (resp. \( X_{a+1}, \ldots, X_{a+b} \in SR_H^\times \backslash \mathbb{H} \)) be the elliptic points of order \( e \) (resp. non-elliptic points) lying over \( P \). Then we have \( \mu_H = a + eb \). Thus \( \sum_{X \mapsto P}(e_X - 1) = \sum_{j=1}^{a}(e_{X_j} - 1) + \sum_{j=a+1}^{a+b}(e_{X_j} - 1) = 0 + (e - 1)b = \frac{e-1}{e}(\mu_H - a) \). Let \( a_i \) be the number of elliptic points of order 2 on \( SR_H^\times \backslash \mathbb{H} \) above \( P_i \). Then \( \nu_2 = \sum_{i=1}^{r} a_i \). Hence \( \sum_{X \mapsto P_1, \ldots, P_r}(e_X - 1) = \sum_{i=1}^{r}(\mu_H - a_i) = \frac{1}{2}(r\mu_H - \nu_2) \). Similarly \( \sum_{Y \mapsto Q_1, \ldots, Q_s}(e_Y - 1) = \frac{5}{3}(s\mu_H - \nu_3) \). Therefore \( g_H^R = 1 + (g^R - 1)\mu_H + \frac{1}{2}\sum_{X \mapsto P_1, \ldots, P_r}(e_X - 1) + \frac{1}{2}\sum_{Y \mapsto Q_1, \ldots, Q_s}(e_Y - 1) = 1 + (g^R - 1)\mu_H + \frac{1}{2}r\mu_H - \nu_2 + \frac{5}{3}s\mu_H - \nu_3 \).

Note that if \( H \) contains \(-1\), then \( \mu_H = [G : H] \).

§ 7. Conjugate elements in \( \text{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \)

We refer to the results of [A] in order to estimate the genus \( g_H^R \).

**Lemma 7.1.** ([A], Lemma 2.1) Let \( H \) be a closed subgroup of \( \text{GL}_2(\mathbb{Z}_p) \). Then \( H \) contains \( \text{SL}_2(\mathbb{Z}_p) \) if and only if \( H \mod p^3 \) contains \( \text{SL}_2(\mathbb{Z}/p^2\mathbb{Z}) \).

Assume \( p \geq 5 \). Then \( H \) contains \( \text{SL}_2(\mathbb{Z}_p) \) if and only if \( H \mod p \) contains \( \text{SL}_2(\mathbb{Z}/p\mathbb{Z}) \).

**Lemma 7.2.** ([A], Lemma 2.2) Let \( n \geq 1 \) be an integer. If \( p = 2 \), assume \( n \geq 2 \). Let \( H \) be a closed subgroup of \( \text{GL}_2(\mathbb{Z}_p) \). Then \( H \) contains \( 1 + p^n\text{M}_2(\mathbb{Z}_p) \) (resp. \( (1 + p^n\text{M}_2(\mathbb{Z}_p))^{\text{det}=1} \)) if and only if \( H \mod p^{n+1} \) contains \( 1 + p^n\text{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}) \) (resp. \( (1 + p^n\text{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}))^{\text{det}=1} \)).

**Definition 7.3.** (cf. [A], Definition 3.7) Let \( n \geq 1 \) be an integer and \( H \subseteq \text{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \) be a subgroup. We call \( H \) a slim subgroup if

\[ H \not\supseteq (1 + p^{n-1}\text{M}_2(\mathbb{Z}/p^n\mathbb{Z}))^{\text{det}=1}. \]

Note that a slim subgroup of \( \text{SL}_2(\mathbb{Z}/p\mathbb{Z}) \) is just a proper subgroup.

Consider subgroups of \( \text{GL}_2(\mathbb{Z}/p\mathbb{Z}) \). A Borel subgroup is a subgroup which is conjugate to \( \{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \} \); the normalizer of a split Cartan subgroup is conjugate to
When $p \geq 3$, the normalizer of a non-split Cartan subgroup is conjugate to
\[ \left\{ \begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}, \begin{pmatrix} x & y \\ -\lambda y & -x \end{pmatrix} \right| (x, y) \in \mathbb{F}_p \times \mathbb{F}_p \setminus \{(0,0)\}, \] where $\lambda \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$ is a fixed element. Assume $p \geq 5$. The quotient group $\text{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ of $GL_2(\mathbb{Z}/p\mathbb{Z})$ has a subgroup which is isomorphic to $S_4$; it has a subgroup which is isomorphic to $A_5$ if and only if $p \equiv 0, \pm 1 \mod 5$. Take a subgroup $H$ (of $GL_2(\mathbb{Z}/p\mathbb{Z})$) whose order is prime to $p$. We call $H$ an exceptional subgroup if it is the inverse image of a subgroup which is isomorphic to $A_4$, $S_4$ or $A_5$ by the natural surjection $GL_2(\mathbb{Z}/p\mathbb{Z}) \rightarrow \text{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.

Put
\[
B := \left\{ \begin{pmatrix} ** \\ 0* \end{pmatrix} \right\} \cap \text{SL}_2(\mathbb{Z}/p\mathbb{Z}),
\]
\[
C := \left\{ \begin{pmatrix} *0 \\ 0* \end{pmatrix}, \begin{pmatrix} 0* \\ *0 \end{pmatrix} \right\} \cap \text{SL}_2(\mathbb{Z}/p\mathbb{Z}),
\]
\[
D := \left\{ \begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}, \begin{pmatrix} x & y \\ -\lambda y & -x \end{pmatrix} \right\} \cap \text{SL}_2(\mathbb{Z}/p\mathbb{Z}),
\]
\[
E := \text{(an exceptional subgroup)} \cap \text{SL}_2(\mathbb{Z}/p\mathbb{Z}).
\]

**Proposition 7.4.** ([Se2], p.284) Let $H$ be a maximal subgroup of $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$. If $p \geq 5$, then $H$ is $GL_2(\mathbb{Z}/p\mathbb{Z})$-conjugate to $B, C, D$ or $E$. If $p = 3$, then $H$ is $GL_2(\mathbb{Z}/3\mathbb{Z})$-conjugate to $B, C$ or $D$.

We review the number of elements conjugate to $\sigma, \tau$ in the maximal subgroups $B, C, D, E$ of $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

**Lemma 7.5.** ([A], Lemma 4.9) In $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$, the number of elements conjugate
to \(\sigma, \tau\) in \(B, C, D, E\) is as follows.

\[
\# B \cap \text{Conj}(\sigma) = \begin{cases} 
2p & \text{if } p \equiv 1 \mod 4, \\
0 & \text{if } p \equiv -1 \mod 4, \\
1 & \text{if } p = 2. 
\end{cases}
\]

\[
\# B \cap \text{Conj}(\tau) = \begin{cases} 
2p & \text{if } p \equiv 1 \mod 3, \\
0 & \text{if } p \equiv -1 \mod 3, \\
1 & \text{if } p = 3. 
\end{cases}
\]

\[
\# C \cap \text{Conj}(\sigma) = \begin{cases} 
p + 1 & \text{if } p \equiv 1 \mod 4, \\
p - 1 & \text{if } p \equiv -1 \mod 4, \\
1 & \text{if } p = 2. 
\end{cases}
\]

\[
\# C \cap \text{Conj}(\tau) = \begin{cases} 
2 & \text{if } p \equiv 1 \mod 3, \\
0 & \text{if } p \not\equiv 1 \mod 3, 
\end{cases}
\]

\[
\# D \cap \text{Conj}(\sigma) = \begin{cases} 
p + 1 & \text{if } p \equiv 1 \mod 4, \\
p + 3 & \text{if } p \equiv -1 \mod 4, 
\end{cases}
\]

\[
\# D \cap \text{Conj}(\tau) = \begin{cases} 
0 & \text{if } p = 3 \text{ or } p \equiv 1 \mod 3, \\
2 & \text{if } p \geq 5 \text{ and } p \equiv -1 \mod 3. 
\end{cases}
\]

\[
\# E \cap \text{Conj}(\sigma) \leq \begin{cases} 
30 & \text{if } p \equiv \pm 1 \mod 5, \\
18 & \text{if } p \geq 5 \text{ and } p \not\equiv \pm 1 \mod 5. 
\end{cases}
\]

\[
\# E \cap \text{Conj}(\tau) \leq \begin{cases} 
20 & \text{if } p \equiv \pm 1 \mod 5, \\
8 & \text{if } p \geq 5 \text{ and } p \not\equiv \pm 1 \mod 5. 
\end{cases}
\]

Now we recall maximal subgroups of \(\text{SL}_2(\mathbb{Z}/4\mathbb{Z})\) whose image mod 2 is \(\text{SL}_2(\mathbb{Z}/2\mathbb{Z})\).

**Lemma 7.6.** ([A], Lemma 4.7) Let \(A \subsetneq \text{SL}_2(\mathbb{Z}/4\mathbb{Z})\) be a proper subgroup. Assume \(A\) maps surjectively mod 2 onto \(\text{SL}_2(\mathbb{Z}/2\mathbb{Z})\). Then \(A\) is conjugate to

\[
A_1 := \left\langle \sigma, \left(\begin{array}{cc}
1 & 1 \\
2 & -1
\end{array}\right) \right\rangle,
\]

which is a maximal subgroup, and is not a normal subgroup.

We review the number of elements conjugate to \(\sigma, \tau\) in \(A_1 \subseteq \text{SL}_2(\mathbb{Z}/4\mathbb{Z})\).
Lemma 7.7. ([A], Lemma 4.10) In $\text{SL}_2(\mathbb{Z}/4\mathbb{Z})$, we have

$$
\# A_1 \cap \text{Conj}(\sigma) = 3,
\quad \# A_1 \cap \text{Conj}(\tau) = 2.
$$

We review the number of elements conjugate to $\sigma, \tau$ in $\text{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

Lemma 7.8. ([A], Lemma 5.1) Let $n \geq 1$ be an integer. In $\text{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ we have

$$\#	ext{Conj}(\sigma) = \begin{cases}
(p + 1)p^{2n-1} & \text{if } p \equiv 1 \text{ mod } 4, \\
(p - 1)p^{2n-1} & \text{if } p \equiv -1 \text{ mod } 4, \\
3 & \text{if } p = 2 \text{ and } n = 1, \\
3 \cdot 2^{2n-3} & \text{if } p = 2 \text{ and } n \geq 2,
\end{cases}
$$

$$\#	ext{Conj}(\tau) = \begin{cases}
(p + 1)p^{2n-1} & \text{if } p \equiv 1 \text{ mod } 3, \\
(p - 1)p^{2n-1} & \text{if } p \equiv -1 \text{ mod } 3, \\
4 \cdot 3^{2n-2} & \text{if } p = 3.
\end{cases}
$$

We control the number of elements conjugate to $\sigma, \tau$ contained in a slim subgroup. Let $n \geq 1$ be an integer and let $H$ be a subgroup of $\text{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. For an integer $1 \leq i \leq n$, put

$$H_i := H \cap (1 + p^i \mathbb{M}_2(\mathbb{Z}/p^n\mathbb{Z})) = \text{Ker } (\text{mod } p^i : H \rightarrow \text{SL}_2(\mathbb{Z}/p^i\mathbb{Z})).$$

We identify $H/H_i$ with $H \mod p^i$.

For $p \geq 3$, define a sequence $\{a(\sigma,p)_n\}_{n \geq 2}$ as follows:

$$a(\sigma,p)_n := 2p^{2(n-l)} + 2(l-1)(p^2 - 1)p^{n-1},$$

where $n = 2l$ or $2l + 1$. For $p \geq 5$, define a sequence $\{a(\tau,p)_n\}_{n \geq 2}$ by

$$a(\tau,p)_n := a(\sigma,p)_n.$$

Proposition 7.9. ([A], Corollary 6.9, 6.10) Let $n \geq 2$ be an integer and let $H \subseteq \text{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be a slim subgroup. If $p \geq 3$, then we have

$$\# H \cap \text{Conj}(\sigma) \leq a(\sigma,p)_n + p^{n-1}(\#(H/H_1) \cap \text{Conj}(\sigma) - 2).$$

If $p \geq 5$, then we have

$$\# H \cap \text{Conj}(\tau) \leq a(\tau,p)_n + p^{n-1}(\#(H/H_1) \cap \text{Conj}(\tau) - 2).$$
Define a sequence \( \{a(\tau, 3)_n\}_{n \geq 2} \) as follows:
\[
a(\tau, 3)_n := \begin{cases} 
3^2 & \text{if } n = 2, \\
(4n - 11) \cdot 3^n & \text{if } n = 2l \geq 4, \\
(4n - 9) \cdot 3^n & \text{if } n = 2l + 1.
\end{cases}
\]

**Proposition 7.10.** ([A], Corollary 6.11) Let \( n \geq 2 \) be an integer and let \( H \subseteq \text{SL}_2(\mathbb{Z}/3^n\mathbb{Z}) \) be a slim subgroup. Then we have
\[
\# H \cap \text{Conj}(\tau) \leq a(\tau, 3)_n + 3^{n-1} \left( \#(H/H_1) \cap \text{Conj}(\tau) - 1 \right).
\]

Define a sequence \( \{a(\tau, 2)_n\}_{n \geq 5} \) as follows:
\[
a(\tau, 2)_n := \begin{cases} 
(31^\circ - 5) \cdot 2^{n+1} & \text{if } n = 2l', \\
(31^\circ - 7) \cdot 2^{n+1} & \text{if } n = 2l' - 1.
\end{cases}
\]

**Proposition 7.11.** ([A], Proposition 6.16) Let \( n \geq 5 \) be an integer and let \( H \subseteq \text{SL}_2(\mathbb{Z}/2^n\mathbb{Z}) \) be a slim subgroup. Then we have
\[
\# H \cap \text{Conj}(\tau) \leq a(\tau, 2)_n + 2^{n-2} \left( \#(H/H_3) \cap \text{Conj}(\tau) - 8 \right).
\]

§ 8. Proof of the effective version

For each \( d \) and \( p \), we find a suitable \( n \) and show \( g_H^R \geq 2 \) for any slim subgroup \( H \subseteq \text{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \) (with \( H \ni -1 \)), and prove Theorem 5.1.

Case \( d = 6 \). If \( H \) contains \(-1\), then
\[
g_H^R = 1 + \frac{1}{6} [G : H] \left( 1 - 3 \frac{\# \text{Fix}_\sigma}{[G : H]} - 4 \frac{\# \text{Fix}_\tau}{[G : H]} \right)
\]
by Lemma 6.3. Put
\[
\delta := 1 - 3 \frac{\# H \cap \text{Conj}(\sigma)}{[G : H]} - 4 \frac{\# H \cap \text{Conj}(\tau)}{[G : H]}.
\]
An easy group theory (cf. [A] Lemma 4.1) shows
\[
\delta = 1 - 3 \frac{\# H \cap \text{Conj}(\sigma)}{\# \text{Conj}(\sigma)} - 4 \frac{\# H \cap \text{Conj}(\tau)}{\# \text{Conj}(\tau)}.
\]

Now we find a suitable \( n \) and show \( \delta > 0 \) for any slim subgroup \( H \subseteq \text{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \).

**Proposition 8.1.** Assume \( p \geq 17 \). For any slim subgroup \( H \subseteq \text{SL}_2(\mathbb{Z}/p\mathbb{Z}) \), we have \( \delta > 0 \).
Proof. In $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have $\# \text{Conj}(\sigma) \geq (p-1)p$ and $\# \text{Conj}(\tau) \geq (p-1)p$ by Lemma 7.8. Suppose $H \subseteq B$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 2p$ and $\# H \cap \text{Conj}(\tau) \leq 2p$. Therefore $\delta \geq 1 - 3 \cdot \frac{2p}{(p-1)p} - 4 \cdot \frac{2p}{(p-1)p} = \frac{p-15}{p-1} > 0$.

Next suppose $H \subseteq C,D$ or $E$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) < 2p$ and $\# H \cap \text{Conj}(\tau) < 2p$. The calculation in the case $H \subseteq B$ shows $\delta > 0$.

**Proposition 8.2.** Assume $p = 13$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/13\mathbb{Z})$. If $H$ is contained in $C,D$ or $E$, then $\delta > 0$.

Proof. In $\text{SL}_2(\mathbb{Z}/13\mathbb{Z})$, we have $\# \text{Conj}(\sigma) = \# \text{Conj}(\tau) = 14 \cdot 13$ by Lemma 7.8. Suppose $H \subseteq E$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 18$ and $\# H \cap \text{Conj}(\tau) \leq 8$. Therefore $\delta \geq 1 - 3 \cdot \frac{18}{14 \cdot 13} - 4 \cdot \frac{8}{14 \cdot 13} = \frac{48}{91} > 0$.

Next suppose $H \subseteq C$ or $D$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 14 < 18$ and $\# H \cap \text{Conj}(\tau) \leq 2 < 8$. The calculation in the case $H \subseteq E$ shows $\delta > 0$.

**Proposition 8.3.** Assume $p = 13$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/13^2\mathbb{Z})$. If $H/H_1$ is contained in $B$, then $\delta > 0$.

Proof. In $\text{SL}_2(\mathbb{Z}/13^2\mathbb{Z})$, we have $\# \text{Conj}(\sigma) = \# \text{Conj}(\tau) = 14 \cdot 13^3$ by Lemma 7.8. Lemma 7.5 shows that in $\text{SL}_2(\mathbb{Z}/13\mathbb{Z})$ we have $\# B \cap \text{Conj}(\sigma) = \# B \cap \text{Conj}(\tau) = 26$. By Proposition 7.9, we have $\# H \cap \text{Conj}(\sigma) \leq a(\sigma,13)_2 + 13(26 - 2) = 50 \cdot 13$ and $\# H \cap \text{Conj}(\tau) \leq a(\tau,13)_2 + 13(26 - 2) = 50 \cdot 13$. Therefore $\delta \geq 1 - 3 \cdot \frac{50 \cdot 13}{14 \cdot 13^3} - 4 \cdot \frac{50 \cdot 13}{14 \cdot 13^3} = \frac{144}{169} > 0$.

**Proposition 8.4.** Assume $p = 11$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/11\mathbb{Z})$. If $H$ is contained in $B,C$ or $D$, then $\delta > 0$.

Proof. In $\text{SL}_2(\mathbb{Z}/11\mathbb{Z})$, we have $\# \text{Conj}(\sigma) = \# \text{Conj}(\tau) = 110$ by Lemma 7.8. Suppose $H \subseteq D$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 14$ and $\# H \cap \text{Conj}(\tau) \leq 2$. Therefore $\delta \geq 1 - 3 \cdot \frac{14}{110} - 4 \cdot \frac{2}{110} = \frac{6}{11} > 0$.

Next suppose $H \subseteq B$ or $C$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 10 < 14$ and $\# H \cap \text{Conj}(\tau) = 0 < 2$. The calculation in the case $H \subseteq D$ shows $\delta > 0$.

**Proposition 8.5.** Assume $p = 11$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/11^2\mathbb{Z})$. If $H/H_1$ is contained in $E$, then $\delta > 0$.

Proof. In $\text{SL}_2(\mathbb{Z}/11^2\mathbb{Z})$, we have $\# \text{Conj}(\sigma) = \# \text{Conj}(\tau) = 10 \cdot 11^3$ by Lemma 7.8. Lemma 7.5 shows that in $\text{SL}_2(\mathbb{Z}/11\mathbb{Z})$ we have $\# E \cap \text{Conj}(\sigma) \leq 30$ and $\# E \cap \text{Conj}(\tau) \leq 20$. By Proposition 7.9, we have $\# H \cap \text{Conj}(\sigma) \leq a(\sigma,11)_2 + 11(30 - 2) = 50 \cdot 11$ and $\# H \cap \text{Conj}(\tau) \leq a(\tau,11)_2 + 11(20 - 2) = 40 \cdot 11$. Therefore $\delta \geq 1 - 3 \cdot \frac{50 \cdot 11}{10 \cdot 11^3} - 4 \cdot \frac{40 \cdot 11}{10 \cdot 11^3} = \frac{90}{121} > 0$. 

□
Proposition 8.6. Assume \( p = 7 \). Take a slim subgroup \( H \subseteq \text{SL}_2(\mathbb{Z}/7\mathbb{Z}) \). If \( H \) is contained in \( C \) or \( D \), then \( \delta > 0 \).

Proof. In \( \text{SL}_2(\mathbb{Z}/7\mathbb{Z}) \), we have \( \# \text{Conj}(\sigma) = 42 \) and \( \# \text{Conj}(\tau) = 56 \) by Lemma 7.8.

Suppose \( H \subseteq C \). Lemma 7.5 shows \( \# H \cap \text{Conj}(\sigma) \leq 6 \) and \( \# H \cap \text{Conj}(\tau) \leq 2 \). Therefore \( \delta \geq 1 - 3 \cdot \frac{3}{42} - 4 \cdot \frac{2}{56} = \frac{2}{7} > 0 \).

Next suppose \( H \subseteq D \). Lemma 7.5 shows \( \# H \cap \text{Conj}(\sigma) \leq 10 \) and \( \# H \cap \text{Conj}(\tau) = 0 \). Therefore \( \delta \geq 1 - 3 \cdot \frac{10}{42} - 4 \cdot 0 = \frac{2}{7} > 0 \). \( \square \)

Proposition 8.7. Assume \( p = 7 \). Take a slim subgroup \( H \subseteq \text{SL}_2(\mathbb{Z}/7^2\mathbb{Z}) \). If \( H/H_1 \) is contained in \( B \) or \( E \), then \( \delta > 0 \).

Proof. In \( \text{SL}_2(\mathbb{Z}/7^2\mathbb{Z}) \), we have \( \# \text{Conj}(\sigma) = 6 \cdot 7^3 \) and \( \# \text{Conj}(\tau) = 8 \cdot 7^3 \) by Lemma 7.8.

Suppose \( H/H_1 \subseteq B \). Lemma 7.5 shows that in \( \text{SL}_2(\mathbb{Z}/7\mathbb{Z}) \) we have \( \# B \cap \text{Conj}(\sigma) = 0 \) and \( \# B \cap \text{Conj}(\tau) = 14 \). Thus \( \# H \cap \text{Conj}(\sigma) = 0 \). By Proposition 7.9, we have \( \# H \cap \text{Conj}(\tau) \leq a(\tau, 7)_2 + 7(14 - 2) = 26 \cdot 7 \). Therefore \( \delta \geq 1 - 3 \cdot 0 - 4 \cdot \frac{26 \cdot 7}{8 \cdot 7^3} = \frac{36}{49} > 0 \).

Next suppose \( H/H_1 \subseteq E \). Lemma 7.5 shows that in \( \text{SL}_2(\mathbb{Z}/7\mathbb{Z}) \) we have \( \# E \cap \text{Conj}(\sigma) \leq 18 \) and \( \# E \cap \text{Conj}(\tau) \leq 8 \). By Proposition 7.9, we have \( \# H \cap \text{Conj}(\sigma) \leq a(\sigma, 7)_2 + 7(18 - 2) = 30 \cdot 7 \) and \( \# H \cap \text{Conj}(\tau) \leq a(\tau, 7)_2 + 7(8 - 2) = 20 \cdot 7 \). Therefore \( \delta \geq 1 - 3 \cdot \frac{30 \cdot 7}{6 \cdot 7^3} - 4 \cdot \frac{20 \cdot 7}{8 \cdot 7^3} = \frac{24}{49} > 0 \). \( \square \)

Proposition 8.8. Assume \( p = 5 \). Take a slim subgroup \( H \subseteq \text{SL}_2(\mathbb{Z}/5\mathbb{Z}) \). If \( H \) is contained in \( C \), then \( \delta > 0 \).

Proof. In \( \text{SL}_2(\mathbb{Z}/5\mathbb{Z}) \), we have \( \# \text{Conj}(\sigma) = 30 \) and \( \# \text{Conj}(\tau) = 20 \) by Lemma 7.8. Lemma 7.5 shows that in \( \text{SL}_2(\mathbb{Z}/5\mathbb{Z}) \) we have \( \# C \cap \text{Conj}(\sigma) = 6 \) and \( \# C \cap \text{Conj}(\tau) = 0 \). Therefore \( \delta \geq 1 - 3 \cdot \frac{6}{30} - 4 \cdot 0 = \frac{2}{5} > 0 \). \( \square \)

Proposition 8.9. Assume \( p = 5 \). Take a slim subgroup \( H \subseteq \text{SL}_2(\mathbb{Z}/5^2\mathbb{Z}) \). If \( H/H_1 \) is contained in \( B \) or \( D \), then \( \delta > 0 \).

Proof. In \( \text{SL}_2(\mathbb{Z}/5^2\mathbb{Z}) \), we have \( \# \text{Conj}(\sigma) = 6 \cdot 5^3 \) and \( \# \text{Conj}(\tau) = 4 \cdot 5^3 \) by Lemma 7.8.

Suppose \( H/H_1 \subseteq B \). Lemma 7.5 shows that in \( \text{SL}_2(\mathbb{Z}/5\mathbb{Z}) \) we have \( \# B \cap \text{Conj}(\sigma) = 10 \) and \( \# B \cap \text{Conj}(\tau) = 0 \). Thus \( \# H \cap \text{Conj}(\sigma) = 0 \). By Proposition 7.9, we have \( \# H \cap \text{Conj}(\tau) \leq a(\sigma, 5)_2 + 5(10 - 2) = 90 \). Therefore \( \delta \geq 1 - 3 \cdot \frac{90}{6 \cdot 5^3} - 4 \cdot 0 = \frac{16}{25} > 0 \).

Next suppose \( H/H_1 \subseteq D \). Lemma 7.5 shows that in \( \text{SL}_2(\mathbb{Z}/5\mathbb{Z}) \) we have \( \# D \cap \text{Conj}(\sigma) = 6 \) and \( \# D \cap \text{Conj}(\tau) = 2 \). By Proposition 7.9, we have \( \# H \cap \text{Conj}(\sigma) \leq a(\sigma, 5)_2 + 5(6 - 2) = 70 \) and \( \# H \cap \text{Conj}(\tau) \leq a(\sigma, 5)_2 + 5(2 - 2) = 50 \). Therefore \( \delta \geq 1 - 3 \cdot \frac{70}{6 \cdot 5^3} - 4 \cdot \frac{50}{4 \cdot 5^3} = \frac{8}{25} > 0 \). \( \square \)
Proposition 8.10. Assume $p = 5$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/5^3\mathbb{Z})$. If $H/H_1$ is contained in $E$, then $\delta > 0$.

Proof. In $\text{SL}_2(\mathbb{Z}/5^3\mathbb{Z})$, we have $\#\text{Conj}(\sigma) = 6 \cdot 5^5$ and $\#\text{Conj}(\tau) = 4 \cdot 5^5$ by Lemma 7.8. Lemma 7.5 shows that in $\text{SL}_2(\mathbb{Z}/5\mathbb{Z})$ we have $\#E \cap \text{Conj}(\sigma) \leq 18$ and $\#E \cap \text{Conj}(\tau) \leq 8$. By Proposition 7.9, we have $\#H \cap \text{Conj}(\sigma) \leq a(\sigma, 5)_3 + 5^2(18 - 2) = 66 \cdot 5^2$ and $\#H \cap \text{Conj}(\tau) \leq a(\tau, 5)_{\text{S}} + 5^2(8 - 2) = 56 \cdot 5^2$. Therefore $\delta \geq 1 - 3 \cdot \frac{66 \cdot 5^2}{65^5} - 4 \cdot \frac{56 \cdot 5^2}{45^5} = \frac{36}{125} > 0$. \hfill $\square$

(Proof of Theorem 5.1 when $d = 6$) Put

$$n'(R, p) := \begin{cases} 2 & \text{if } p = 5, \\ 1 & \text{if } p \in \{7, 11, 13\}, \\ 0 & \text{if } p \geq 17. \end{cases}$$

Let $(A, i)$ be a QM-abelian surface over $K$ satisfying (2.1) and $\rho_{(A, i)/K, p}(G_K) \not\simeq (1 + p^{n'(R, p)} \text{M}_2(\mathbb{Z}_p))^\det=1$. By Lemma 7.1 and 7.2, we have $\overline{\rho}_{(A, i)/K, p^{n'(R, p)+1}}(G_K) \not\simeq (1 + p^{n'(R, p)} \text{M}_2(\mathbb{Z}/p^{n'(R, p)+1}\mathbb{Z}))^{\det=1}$. (More precisely, we should replace $n'(R, p)$ by $n'(R, p) - 1, n'(R, p) - 2$ according to the shape of $\overline{\rho}_{(A, i)/K, p}$. Replacing $K$ by $K(\zeta_{p^{n'(R, p)+1}})$, we may assume $\overline{\rho}_{(A, i)/K, p^{n'(R, p)+1}}(G_K) \subseteq \text{SL}_2(\mathbb{Z}/p^{n'(R, p)+1}\mathbb{Z})$. We may also assume that $\overline{\rho}_{(A, i)/K, p^{n'(R, p)+1}}(G_K)$ is contained in a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/p^{n'(R, p)+1}\mathbb{Z})$ satisfying $H \ni -1$ (see [A], proof of Proposition 3.8). By Lemma 6.2, we know that there are only finitely many $\overline{K}$-isomorphism classes of such $(A, i)$'s. Therefore $n(R, p) \leq n'(R, p)$. To exclude $n(R, p) = 0$ for $p = 5$ (resp. $p = 7$, resp. $p = 13$), we have only to see $g_B^R = g_D^R = 1$ (resp. $g_B^R = 1$, resp. $g_B^R = 1$) where $n = 1$.

Case $d = 10$. If $H$ contains $-1$, then

$$g_H^R = 1 + \frac{1}{3}[G : H] \left(1 - 4 \frac{\#\text{Fix}_\tau}{[G : H]}\right)$$

by Lemma 6.3. Put

$$\delta := 1 - 4 \frac{\#\text{Fix}_\tau}{[G : H]} = 1 - 4 \frac{\#H \cap \text{Conj}(\tau)}{\#\text{Conj}(\tau)}.$$

Proposition 8.11. Assume $p \geq 11$. For any slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have $\delta > 0$.

Proof. In $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have $\#\text{Conj}(\tau) \geq (p - 1)p$ by Lemma 7.8. Suppose $H \subseteq B$. Lemma 7.5 shows $\#H \cap \text{Conj}(\tau) \leq 2p$. Therefore $\delta \geq 1 - 4 \cdot \frac{2p}{(p-1)p} = \frac{p-9}{p-1} > 0$. \hfill $\square$
Next suppose $H \subseteq C, D$ or $E$. Lemma 7.5 shows $\# H \cap \text{Conj}(\tau) < 2p$. The calculation in the case $H \subseteq B$ shows $\delta > 0$.

**Proposition 8.12.** Assume $p = 7$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/7\mathbb{Z})$. If $H$ is contained in $C, D$ or $E$, then $\delta > 0$.

**Proof.** In $\text{SL}_2(\mathbb{Z}/7\mathbb{Z})$, we have $\# \text{Conj}(\tau) = 56$ by Lemma 7.8. Since $H \subseteq C, D$ or $E$, Lemma 7.5 shows $\# H \cap \text{Conj}(\tau) \leq 8$. Therefore $\delta \geq 1 - 4 \cdot \frac{8}{56} = \frac{3}{7} > 0$. \hfill $\square$

**Proposition 8.13.** Assume $p = 7$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/7^2\mathbb{Z})$. If $H/H_1$ is contained in $B$, then $\delta > 0$.

**Proof.** In $\text{SL}_2(\mathbb{Z}/7^2\mathbb{Z})$, we have $\# \text{Conj}(\tau) = 8 \cdot 7^3$ by Lemma 7.8. Lemma 7.5 shows that in $\text{SL}_2(\mathbb{Z}/7\mathbb{Z})$ we have $\# B \cap \text{Conj}(\tau) = 14$. By Proposition 7.9, we have $\# H \cap \text{Conj}(\tau) \leq a(\tau, 7) = 26 \cdot 7$. Therefore $\delta \geq 1 - 4 \cdot \frac{267}{8 \cdot 7^3} = \frac{36}{49} > 0$. \hfill $\square$

**Proposition 8.14.** Assume $p = 3$. For any slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/3^4\mathbb{Z})$, we have $\delta > 0$.

**Proof.** In $\text{SL}_2(\mathbb{Z}/3^4\mathbb{Z})$, we have $\# \text{Conj}(\tau) = 4 \cdot 3^6$ by Lemma 7.8. Similarly $\# \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \cap \text{Conj}(\tau) = 4$. By Proposition 7.10, we have $\# H \cap \text{Conj}(\tau) \leq a(\tau, 3) = 2 \cdot 3^5$. Therefore $\delta \geq 1 - 4 \cdot \frac{2 \cdot 3^5}{4 \cdot 3^6} = \frac{1}{3} > 0$. \hfill $\square$

Case $d = 22$. If $H$ contains $-1$, then

$$g_{H}^{R} = 1 + \frac{1}{6}[G : H]\left(5 - 3 \frac{\# \text{Fix}_\sigma}{[G : H]} - 8 \frac{\# \text{Fix}_\tau}{[G : H]}\right)$$

by Lemma 6.3. Put

$$\delta := 5 - 3 \frac{\# \text{Fix}_\sigma}{[G : H]} - 8 \frac{\# \text{Fix}_\tau}{[G : H]} = 5 - 3 \frac{\# H \cap \text{Conj}(\sigma)}{\# \text{Conj}(\sigma)} - 8 \frac{\# H \cap \text{Conj}(\tau)}{\# \text{Conj}(\tau)}.$$

**Proposition 8.15.** Assume $p \geq 7$. For any slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have $\delta > 0$.

**Proof.** In $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have $\# \text{Conj}(\sigma) \geq (p - 1)p$ and $\# \text{Conj}(\tau) \geq (p - 1)p$ by Lemma 7.8.

Suppose $H \subseteq B$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 2p$ and $\# H \cap \text{Conj}(\tau) \leq 2p$. Therefore $\delta \geq 5 - 3 \frac{2p}{(p - 1)p} - 8 \cdot \frac{2p}{(p - 1)p} = \frac{5p - 27}{p - 1} > 0$.

Next suppose $H \subseteq C$ or $D$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) < 2p$ and $\# H \cap \text{Conj}(\tau) < 2p$. The calculation in the case $H \subseteq B$ shows $\delta > 0$. 

Finally suppose $H \subseteq E$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 30$ and $\# H \cap \text{Conj}(\tau) \leq 20$. Therefore $\delta \geq 5 - 3 \cdot \frac{30}{(p-1)p} - 8 \cdot \frac{20}{(p-1)p} = \frac{46}{21} > 0$ if $p \geq 8$. When $p = 7$, we have $\# H \cap \text{Conj}(\sigma) \leq 18$ and $\# H \cap \text{Conj}(\tau) \leq 8$ by Lemma 7.5. Thus $\delta \geq 5 - 3 \cdot \frac{18}{6 \cdot 7} - 8 \cdot \frac{8}{6 \cdot 7} = \frac{46}{21} > 0$. \qed

**Proposition 8.16.** Assume $p = 5$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/5\mathbb{Z})$. If $H$ is contained in $B$, $C$ or $D$, then $\delta > 0$.

**Proof.** In $\text{SL}_2(\mathbb{Z}/5\mathbb{Z})$, we have $\# \text{Conj}(\sigma) = 30$ and $\# \text{Conj}(\tau) = 20$ by Lemma 7.8. Suppose $H \subseteq B$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 10$ and $\# H \cap \text{Conj}(\tau) = 0$. Therefore $\delta \geq 5 - 3 \cdot \frac{10}{30} - 8 \cdot 0 = 4 > 0$.

Next suppose $H \subseteq C$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 6 < 10$ and $\# H \cap \text{Conj}(\tau) = 0$. The calculation in the case $H \subseteq B$ shows $\delta > 0$.

Finally suppose $H \subseteq D$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 6$ and $\# H \cap \text{Conj}(\tau) \leq 2$. Therefore $\delta \geq 5 - 3 \cdot \frac{6}{30} - 8 \cdot \frac{2}{20} = \frac{18}{5} > 0$. \qed

**Proposition 8.17.** Assume $p = 5$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/5^2\mathbb{Z})$. If $H/H_1$ is contained in $E$, then $\delta > 0$.

**Proof.** In $\text{SL}_2(\mathbb{Z}/5^2\mathbb{Z})$, we have $\# \text{Conj}(\sigma) = 6 \cdot 5^3$ and $\# \text{Conj}(\tau) = 4 \cdot 5^3$ by Lemma 7.8. Lemma 7.5 shows that in $\text{SL}_2(\mathbb{Z}/5\mathbb{Z})$ we have $\# E \cap \text{Conj}(\sigma) \leq 18$ and $\# E \cap \text{Conj}(\tau) \leq 8$. By Proposition 7.9, we have $\# H \cap \text{Conj}(\sigma) \leq a(\sigma,5) \cdot 5(18 - 2) = 26 \cdot 5$ and $\# H \cap \text{Conj}(\tau) \leq a(\tau,5) \cdot 5(8 - 2) = 16 \cdot 5$. Therefore $\delta \geq 5 - 3 \cdot \frac{26 \cdot 5}{6 \cdot 5^3} - 8 \cdot \frac{16 \cdot 5}{4 \cdot 5^3} = \frac{10}{9} > 0$. \qed

**Proposition 8.18.** Assume $p = 3$. For any slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/3^3\mathbb{Z})$, we have $\delta > 0$.

**Proof.** In $\text{SL}_2(\mathbb{Z}/3^3\mathbb{Z})$, we have $\# \text{Conj}(\sigma) = 2 \cdot 3^5$ and $\# \text{Conj}(\tau) = 4 \cdot 3^4$ by Lemma 7.8. Similarly $\# \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \cap \text{Conj}(\sigma) = 6$ and $\# \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \cap \text{Conj}(\tau) = 4$. By Proposition 7.9, we have $\# H \cap \text{Conj}(\sigma) \leq a(\sigma,3) \cdot 3^2(6 - 2) = 22 \cdot 3^2$. By Proposition 7.10, we have $\# H \cap \text{Conj}(\tau) \leq a(\tau,3) \cdot 3^2(4-1) = 4 \cdot 3^3$. Therefore $\delta \geq 5 - 3 \cdot \frac{22 \cdot 3^2}{2 \cdot 3^5} - 8 \cdot \frac{4 \cdot 3^3}{4 \cdot 3^3} = \frac{10}{9} > 0$. \qed

Case $g^R = 1$ (equivalently $d \in \{14, 15, 21, 33, 34, 46\}$). If $H$ contains $-1$, then we know

$$g^R_H = 1 + \frac{1}{12} [G : H] \left(3r \left(1 - \frac{\# \text{Fix}_{\sigma}}{[G : H]} \right) + 4s \left(1 - \frac{\# \text{Fix}_{\tau}}{[G : H]} \right) \right)$$

$$= 1 + \frac{1}{12} [G : H] \left(3r \left(1 - \frac{\# H \cap \text{Conj}(\sigma)}{\# \text{Conj}(\sigma)} \right) + 4s \left(1 - \frac{\# H \cap \text{Conj}(\tau)}{\# \text{Conj}(\tau)} \right) \right)$$

from Lemma 6.3. Thus we have $g^R_H \geq 2$ if at least one of the following two conditions is satisfied:
• $r > 0$ and $\# H \cap \text{Conj}(\sigma) < \# \text{Conj}(\sigma)$.

• $s > 0$ and $\# H \cap \text{Conj}(\tau) < \# \text{Conj}(\tau)$.

The values of $r, s$ depending on $d$ are as follows:

<table>
<thead>
<tr>
<th>$d$</th>
<th>$r$</th>
<th>$s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>21</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>33</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>34</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>46</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

Note that in any case we have $(r, s) \neq (0, 0)$.

**Proposition 8.19.** Assume $p \geq 5$. For any slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have $\delta > 0$.

**Proof.** In $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have $\# \text{Conj}(\sigma) = (p \pm 1)p$ and $\# \text{Conj}(\tau) = (p \pm 1)p$ by Lemma 7.8.

Suppose $H \subseteq B, C$ or $D$. Lemma 7.5 shows $\# H \cap \text{Conj}(\sigma) \leq 2p < \# \text{Conj}(\sigma)$ and $\# H \cap \text{Conj}(\tau) \leq 2p < \# \text{Conj}(\tau)$. Therefore $g_H^R \geq 2$.

Next suppose $H \subseteq E$. Lemma 7.5 shows

$$\# H \cap \text{Conj}(\sigma) \leq \begin{cases} 30 < \# \text{Conj}(\sigma) & \text{if } p \geq 7, \\ 18 < \# \text{Conj}(\sigma) & \text{if } p = 5, \end{cases}$$

and

$$\# H \cap \text{Conj}(\tau) \leq \begin{cases} 20 < \# \text{Conj}(\tau) & \text{if } p \geq 7, \\ 8 < \# \text{Conj}(\tau) & \text{if } p = 5. \end{cases}$$

Therefore $g_H^R \geq 2$. $\square$

**Proposition 8.20.** Assume $p = 3$. For any slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/3^2\mathbb{Z})$, we have $g_H^R \geq 2$.

**Proof.** In $\text{SL}_2(\mathbb{Z}/3^2\mathbb{Z})$, we have $\# \text{Conj}(\sigma) = 54$ and $\# \text{Conj}(\tau) = 36$ by Lemma 7.8. Similarly $\# \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \cap \text{Conj}(\sigma) = 6$ and $\# \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \cap \text{Conj}(\tau) = 4$. By Proposition 7.9, we have $\# H \cap \text{Conj}(\sigma) \leq a(\sigma, 3)_2 + 3(6 - 2) = 30 < \# \text{Conj}(\sigma)$. By Proposition 7.10, we have $\# H \cap \text{Conj}(\tau) \leq a(\tau, 3)_2 + 3(4 - 1) = 18 < \# \text{Conj}(\tau)$. Therefore $g_H^R \geq 2$. $\square$
Proposition 8.21. Assume $p = 2$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/2\mathbb{Z})$. If $H$ is contained in $B$, then $g_H^R \geq 2$.

Proof. In $\text{SL}_2(\mathbb{Z}/2\mathbb{Z})$, we have $\#\text{Conj}(\sigma) = 3$ and $\#\text{Conj}(\tau) = 2$ by Lemma 7.8. Lemma 7.5 shows $\#H \cap \text{Conj}(\sigma) \leq 1 < \#\text{Conj}(\sigma)$ and $\#H \cap \text{Conj}(\tau) = 0 < \text{Conj}(\tau)$. Therefore $g_H^R \geq 2$. \hfill \Box

Proposition 8.22. Assume $p = 2$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/2^2\mathbb{Z})$. If $H/H_1$ is equal to the whole $\text{SL}_2(\mathbb{Z}/2\mathbb{Z})$, then $g_H^R \geq 2$.

Proof. In $\text{SL}_2(\mathbb{Z}/2^2\mathbb{Z})$, we have $\#\text{Conj}(\sigma) = 6$ and $\#\text{Conj}(\tau) = 8$ by Lemma 7.8. By Lemma 7.6, we may assume $H \subseteq A_1$. Lemma 7.7 shows $\#H \cap \text{Conj}(\sigma) \leq 3 < \#\text{Conj}(\sigma)$ and $\#H \cap \text{Conj}(\tau) \leq 2 < \text{Conj}(\tau)$. Therefore $g_H^R \geq 2$. \hfill \Box

Proposition 8.23. Assume $p = 2$ and $d \in \{21, 33\}$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/2\mathbb{Z})$. If $H$ is contained in $F$, then $g_H^R \geq 2$.

Proof. In $\text{SL}_2(\mathbb{Z}/2\mathbb{Z})$, we have $\#\text{Conj}(\sigma) = 3$ by Lemma 7.8. We can easily see $\#H \cap \text{Conj}(\sigma) = 0 < \#\text{Conj}(\sigma)$. Since $d \in \{21, 33\}$, we have $r > 0$. Therefore $g_H^R \geq 2$. \hfill \Box

Proposition 8.24. Assume $p = 2$ and $d = 15$. Take a slim subgroup $H \subseteq \text{SL}_2(\mathbb{Z}/2^5\mathbb{Z})$. If $H/H_1$ is contained in $F$, then $g_H^R \geq 2$.

Proof. In $\text{SL}_2(\mathbb{Z}/2^5\mathbb{Z})$, we have $\#\text{Conj}(\tau) = 2^9$ by Lemma 7.8. Similarly $\#(H/H_3) \cap \text{Conj}(\tau) \leq \#\text{SL}_2(\mathbb{Z}/2^3\mathbb{Z}) \cap \text{Conj}(\tau) = 2^5$. By Proposition 7.11, we have $\#H \cap \text{Conj}(\tau) \leq a(\tau, 2)_5 + 2^3(2^5 - 8) = 5 \cdot 2^6 < \#\text{Conj}(\tau)$. Since $d = 15$, we have $s > 0$. Therefore $g_H^R \geq 2$. \hfill \Box

This completes the proof of Theorem 5.1. When $p = 2$, a slight difference occurs between the power of 2 in Proposition 8.21-8.24 and $n(R, 2)$ in Theorem 5.1. See [A], proof of Proposition 3.8 for details.

References


ON THE GALOIS IMAGES ASSOCIATED TO QM-ABELIAN SURFACES


