PACIFIC JOURNAL OF MATHEMATICS
Vol. 114, No. 2, 1984

# REPRESENTATIONS ASSOCIATED WITH ELLIPTIC SURFACES

DAVID A. COX AND WALTER R. PARRY

**An elliptic surface (over C) $f$: $X \to S$ with a section has two representations naturally associated to it: the first, the monodromy representation, is determined by the topology of $f$, while the second, the Galois representation, is determined by the arithmetic of the general fiber of $f$. The purpose of this paper is to study and compare the properties of these representations.**

We will always assume that $f$: $X \to S$ is relatively minimal and that the $j$-invariant is nonconstant. We let $K$ denote the function field of $S$ and $E$ the general fiber of $f$. Then $E/K$ is an elliptic curve with $f$: $X \to S$ as its Néron model.

The Galois representation given by the action of $\mathrm{Gal}(\bar{K}/K)$ on the torsion points of $E(\bar{K})$ is studied first. Since $\mathbf{C}$ contains all roots of unity, this representation can be regarded as a continuous homomorphism

$$\rho_{E/K}\colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{SL}(2, \hat{\mathbf{Z}}) = \prod_{p\,\text{prime}} \mathrm{SL}(2, \mathbf{Z}_p).$$

With the above hypothesis on $E/K$, it is known that the image of $\rho_{E/K}$, denoted $\mathrm{Im}(\rho_{E/K})$, is open in $\mathrm{SL}(2, \hat{\mathbf{Z}})$ (see **[5]**). This naturally leads to the notion of *level* of $E/K$. In §1 we introduce this and study its basic properties. Then, in §2, we show how to bound the level in terms of the behavior of the $j$-invariant and also in terms of the genus $g$ of $K$.

The monodromy representation (also called the homological invariant) of $f$: $X \to S$ is studied in §3. If $S_0 = \{s \in S\colon f \text{ is smooth above } s\}$ and $X_t$ is the fiber over $t \in S_0$, then $\pi_1(S_0, t)$ acts on $H^1(X_t, \mathbf{Z})$, giving us the monodromy representation

$$\rho_{X/S}\colon \pi_1(S_0, t) \to \mathrm{SL}(2, \mathbf{Z}).$$

(The image is in $\mathrm{SL}(2, \mathbf{Z})$ because of Poincaré duality.) We will show that the monodromy determines the Galois representation and that in some respects the monodromy is the more subtle invariant.

**1.** We will work in a slightly more general context than that of the introduction. Here, $K$ will be a field of characteristic zero containing all roots of unity, and $E/K$ will be an elliptic curve such that $\mathrm{Im}(\rho_{E/K})$ is open in $\mathrm{SL}(2, \hat{\mathbf{Z}})$. This means that for some integer $n \geq 1$,

$$\hat{\Gamma}(n) \subseteq \mathrm{Im}(\rho_{E/K}), \tag{1.1}$$

where

$$\hat{\Gamma}(n) = \{\gamma \in \mathrm{SL}(2, \hat{\mathbf{Z}}) \colon \gamma \equiv 1 \bmod n\}.$$

The *level* of $E/K$ is the smallest integer $n$ for which (1.1) holds. It can be shown that the level is actually the greatest common divisor of all such integers.

The level influences many things associated with $E/K$, as the next proposition shows.

PROPOSITION 1.1. *Let $E/K$ have level $n$.*
(i) $\mathrm{End}_K(E) = \mathrm{End}_{\overline{K}}(E) = \mathbf{Z}$.
(ii) *Let $\lambda\colon E \to E'$ be a $K$-isogeny.*
(a) *If $\lambda$ is cyclic, then* $\deg(\lambda) \mid n$.
(b) *$E'/K$ has level $n'$, where $n' \mid \deg(\lambda) n$. Thus $n' \mid n^2$.*
(iii) *$E(K)_{\mathrm{tor}}$ is $n$-torsion.*
(iv) *Let $p$ be prime and let*

$$\rho_{E/K,p}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{SL}(2, \mathbf{F}_p)$$

*be the Galois representation on $p$-torsion points. If $p \nmid n$, then $\rho_{E/K,p}$ is surjective, and, if $p > 5$, the converse is true.*

*Proof.* Let $T(E) = \varprojlim E_m$, where $E_m = \{x \in E(\overline{K}) \colon mx = 0\}$. Then $T(E) = \prod_p T_p(E) \cong \hat{\mathbf{Z}}^2$, where $T_p(E)$ is the usual Tate module over $\mathbf{Z}_p$. Every $K$-isogeny $\lambda\colon E \to E'$ induces a map $T(E) \to T(E')$ which is represented by a matrix $A \in M(2, \hat{\mathbf{Z}})$ such that $\det(A) = \deg(\lambda)$ for some choice of bases. Also, if a positive integer $k$ divides the entries of $A$, then $E_k \subseteq \mathrm{Ker}(\lambda)$. Since $\lambda$ is a $K$-isogeny,

$$A \cdot \rho_{E/K}(\sigma) = \rho_{E'/K}(\sigma) \cdot A \tag{1.2}$$

for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

To prove (i), take $\lambda \in \mathrm{End}_K(E)$. Since $\hat{\Gamma}(n) \subseteq \mathrm{Im}(\rho_{E/K})$, (1.2) implies that $A$ centralizes $\hat{\Gamma}(n)$. Thus, $A$ is a homothety, which easily implies that $\mathrm{End}_K(E) = \mathbf{Z}$. Since this is true for all finite extensions of $K$, $\mathrm{End}_{\overline{K}}(E) = \mathbf{Z}$.

We now prove (ii). Since two isogenous elliptic curves are isogenous via a cyclic isogeny, $\lambda$ may be taken to be cyclic. This implies that bases of

$T(E)$ and $T(E')$ can be chosen such that $A = \left(\begin{smallmatrix}1 & 0\\ 0 & N\end{smallmatrix}\right)$, where $N = \deg(\lambda)$. Since $\hat{\Gamma}(n) \subseteq \operatorname{Im}(\rho_{E/K})$, (1.2) implies

$$A\hat{\Gamma}(n)A^{-1} \subseteq \operatorname{Im}(\rho_{E'/K}).$$

Thus $N \mid n$ because $A\hat{\Gamma}(n)A^{-1} \subseteq \mathrm{SL}(2,\hat{\mathbf{Z}})$, and $n' \mid Nn$ because $\hat{\Gamma}(Nn) \subseteq A\hat{\Gamma}(n)A^{-1} \subseteq \operatorname{Im}(\rho_{E'/K})$.

Now (iii) is clear because any element of $E(K)_{\mathrm{tor}}$ defines a cyclic $K$-isogeny whose degree is the order of the element.

To prove (iv), note that $\hat{\Gamma}(n) = \prod_p \Gamma(p^{v_p(n)})_p$, where $\Gamma(p^r)_p = \{\gamma \in \mathrm{SL}(2,\mathbf{Z}_p)\colon \gamma \equiv 1 \bmod p^r\}$. Thus the natural map

$$\hat{\Gamma}(n) \to \mathrm{SL}(2,\mathbf{F}_p)$$

is surjective when $p \nmid n$. The converse follows easily from [**10**, IV.3, Lemma 5].

If $E/K$ has finite level and $L$ is a finite extension of $K$, then $E/L$ clearly also has finite level. It is possible to estimate how much the level can change as follows.

PROPOSITION 1.2. *Let $E/K$ have level $n$, and let $L$ be a finite extension of $K$. Then $E/L$ has level $n'$, where $n' \leq [L\colon K]n$.*

*Proof.* Let $G = \operatorname{Im}(\rho_{E/L}) \cap \hat{\Gamma}(n)$. Since $\hat{\Gamma}(n) \subseteq \operatorname{Im}(\rho_{E/K})$, it follows that $[\hat{\Gamma}(n) : G]$ divides $[\operatorname{Im}(\rho_{E/K})\colon \operatorname{Im}(\rho_{E/L})] = [L\colon K]$. However:

(1.3) The map $G \to G \cap \mathrm{SL}(2,\mathbf{Z})$ gives a bijection between open subgroups of $\mathrm{SL}(2,\hat{\mathbf{Z}})$ and congruence subgroups of $\mathrm{SL}(2,\mathbf{Z})$. This bijection preserves level, index, normal subgroups and quotients.

Let $\Gamma = G \cap \mathrm{SL}(2,\mathbf{Z})$. Then $\Gamma \subseteq \Gamma(n)$ and $\Gamma$ has level $n'$, hence it suffices to prove that

$$n' \leq [\Gamma(n) : \Gamma]n. \tag{1.4}$$

When $n = 1$, (1.4) is proved in [**2**, Theorem 4.2], and the proof easily generalizes to the case when $n > 1$. □

Sometimes $E/L$ has finite level even when $L$ is an infinite extension of $K$. The most interesting example is when $L = K_{\mathrm{ab}}$, the maximal Abelian extension of $K$. In this case, Serre noticed (see [**11**, Remark, p. 300]) that $E/K_{\mathrm{ab}}$ has finite level. We can estimate the level of $E/K_{\mathrm{ab}}$ as follows.

THEOREM 1.3. *Let $E/K$ have level $n$. Then $E/K_{\text{ab}}$ has level $n'$, where $n' \mid 12n^2$.*

*Proof.* By Serre's result, $\text{Im}(\rho_{E/K_{\text{ab}}})$ is a normal subgroup of $\text{Im}(\rho_{E/K})$ of finite index and Abelian qotient. Since $\hat{\Gamma}(n) \subseteq \text{Im}(\rho_{E/K})$, we see that $G = \text{Im}(\rho_{E/K_{\text{ab}}}) \cap \hat{\Gamma}(n)$ is normal in $\hat{\Gamma}(n)$, again with finite index and Abelian quotient. It suffices to prove that $\hat{\Gamma}(12n^2) \subseteq G$.

We may assume that $G$ is the closure of the commutator subgroup of $\hat{\Gamma}(n)$. Using the notation of the proof of Proposition 1.1(iv), we have $\hat{\Gamma}(n) = \prod_p \Gamma(p^{v_p(n)})_p$. Then $G$ is also a product: $G = \prod_p G_p$.

Let $H$ be the closure of the commutator subgroup of $\text{SL}(2, \hat{\mathbf{Z}})$. One easily sees that $H = \prod_p H_p$, where

(1.5) $H_p = \text{SL}(2, \mathbf{Z}_p)$ for $p > 3$;

(1.6) $H_3$ has index 3 in $\text{SL}(2, \mathbf{Z}_3)$ and is generated by $\Gamma(3)_3$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$; and

(1.7) $H_2$ has index 4 in $\text{SL}(2, \mathbf{Z}_2)$ and is generated by $\Gamma(4)_2$, $\left(\begin{smallmatrix} 0 & -1 \\ 0 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 2 \\ 0 & -1 \end{smallmatrix}\right)$.

Fix a prime $p$ and let $r = v_p(n)$. Then $G_p$ is the closure of the commutator subgroup of $\Gamma(p^r)_p$. We will show that

$$(1.8) \qquad G_p = \begin{cases} H_p \cap \Gamma(p^{2r})_p & \text{if } p \neq 2 \text{ or } r = 0 \\ \Gamma(2^{2r})_2 \cap \Gamma_0(2^{2r+1})_2 \cap \Gamma_0(2^{2r+1})_2^t & \text{if } p = 2 \text{ and } r > 0, \end{cases}$$

where the subscript "0" has the usual meaning and the superscript "$t$" means transpose. The theorem follows immediately from (1.8), and by computing indices, one also obtains the inequality

$$(1.9) \qquad \left[\hat{\Gamma}(n) \colon \text{Im}(\rho_{E/K_{\text{ab}}}) \cap \hat{\Gamma}(n)\right] \leq 12n^3.$$

This will be useful later.

Before proving (1.8), note that it is closely related to a result of Lang and Trotter which describes the closure of the commutator subgroup of $\{\gamma \in \text{GL}(2, \mathbf{Z}_p) \colon \gamma \equiv 1 \bmod p^r\}$ (see [**8**, p. 95 and pp. 163–173]). The only difference occurs when $p = 2$.

Let $\tilde{G}_p$ denote the right hand side of (1.8). The case $r = 0$ is trivial. To handle the case $r > 0$, we start with the following three simple observations.

(1.10) The commutators of $\text{sl}(2, \mathbf{Z}_p)$ generate the subgroup

$$\Lambda = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{sl}(2, \mathbf{Z}_p) \colon b \equiv c \equiv 0 \bmod 2 \right\}.$$

(1.11) If $1 + p^rA$ is in $\Gamma(p^r)_p$, then $\mathrm{tr}(A) \equiv 0 \bmod p^r$.

(1.12) If $x = 1 + p^rA$ and $y = 1 + p^rB$ are in $\Gamma(p^r)_p$, then

$$xyx^{-1}y^{-1} = 1 + p^{2r}[A, B] + p^{3r}[A, B]\left(\sum_{k=1}^{\infty} (-1)^k p^{(k-1)r}\left(\sum_{i+j=k} A^iB^j\right)\right).$$

These facts immediately imply that $G_p \subseteq \tilde{G}_p$. For the opposite inclusion, we will show that if $1 + p^{kr}A$ is in $\tilde{G}_p$, $k \geq 2$, then there are $x_i, y_i \in \Gamma(p^r)_p$, $1 \leq i \leq 3$, such that

$$(1.13) \qquad 1 + p^{kr}A = \prod_{i=1}^{3} x_iy_ix_i^{-1}y_i^{-1} \qquad \bmod p^{(k+1)r}.$$

This implies that $\tilde{G}_p$ consists of convergent infinite products of commutators of elements of $\Gamma(p^r)_p$, proving (1.8).

To show that (1.13) holds, first note that $p^{(k-2)r}A \equiv \tilde{A} \bmod p^{(k-1)r}$ for some $\tilde{A} \in \Lambda$. By (1.10), $\tilde{A} = \Sigma_{i=1}^3[A_i, B_i]$, where $A_i$ and $B_i$ are nilpotent and $[A_i, B_i] \equiv 0 \bmod p^{(k-2)r}$. Then $x_i = 1 + p^rA_i$ and $y_i = 1 + p^rB_i$ lie in $\Gamma(p^r)_p$, and (1.13) follows from (1.12). □

Since $E/K_{\mathrm{ab}}$ has finite level, it follows that $E(K_{\mathrm{ab}})_{\mathrm{tor}}$ is finite. This fact was noticed by Mazur in [**9**, Proposition 6.12]. Combining Theorem 1.3 and Proposition 1.1(iii), we get the following more explicit result.

COROLLARY 1.4. *If $E/K$ has level $n$, then $E(K_{\mathrm{ab}})_{\mathrm{tor}}$ is $12n^2$-torsion.*

We next cast our results in field theoretic terms. Let $K_{\mathrm{tor}}$ be the field obtained from $K$ by adjoining the coordinates of points in $E(\bar{K})_{\mathrm{tor}}$.

COROLLARY 1.5. *If $E/K$ has level $n$, then*

$$[K_{\mathrm{ab}} \cap K_{\mathrm{tor}} : K] \leq 12n^5 \prod_{p|n} (1 - p^{-2}).$$

*Proof.* Let $L = K_{\mathrm{ab}} \cap K_{\mathrm{tor}}$. Then $[L : K] = [\mathrm{Gal}(K_{\mathrm{tor}}/K) : \mathrm{Gal}(K_{\mathrm{tor}}/L)]$. It is well-known that $\mathrm{Gal}(K_{\mathrm{tor}}/K) \cong \mathrm{Im}(\rho_{E/K})$ and $\mathrm{Gal}(K_{\mathrm{tor}}/L) \cong \mathrm{Im}(\rho_{E/K_{\mathrm{ab}}})$. Thus $[L : K] = [\mathrm{Im}(\rho_{E/K}) : \mathrm{Im}(\rho_{E/K_{\mathrm{ab}}})]$. Since $\hat{\Gamma}(n) \subseteq \mathrm{Im}(\rho_{E/K})$, we get

$$[L : K] \leq \left[\mathrm{Im}(\rho_{E/K}) : \hat{\Gamma}(n)\right]\left[\hat{\Gamma}(n) : \mathrm{Im}(\rho_{E/K_{\mathrm{ab}}}) \cap \hat{\Gamma}(n)\right],$$

and then (1.9) implies

$$(1.14) \qquad [L:K] \leq \left[\mathrm{Im}(\rho_{E/K}) : \hat{\Gamma}(n)\right] \cdot (12n^3).$$

But $\mathrm{Im}(\rho_{E/K}) \subseteq \mathrm{SL}(2, \hat{\mathbf{Z}}) = \hat{\Gamma}(1)$, so that by (1.3) and (1.4) we have

$$n \leq \left[\mathrm{SL}(2, \hat{\mathbf{Z}}) : \mathrm{Im}(\rho_{E/K})\right].$$

The index of $\hat{\Gamma}(n)$ in $\mathrm{SL}(2, \hat{\mathbf{Z}})$ is known, yielding

$$\left[\mathrm{Im}(\rho_{E/K}) : \hat{\Gamma}(n)\right] \leq n^2 \prod_{p|n} (1 - p^{-2}).$$

This formula and (1.14) give the desired estimate for $[L:K]$. □

Besides the level, there are other invariants of $\mathrm{Im}(\rho_{E/K})$. One of the most natural is the index of $\mathrm{Im}(\rho_{E/K})$ in $\mathrm{SL}(2, \hat{\mathbf{Z}})$. We have the following relation between level and index.

PROPOSITION 1.6.
(i) *If $E/K$ has level $n$, then*

$$n \leq \left[\mathrm{SL}(2, \hat{\mathbf{Z}}) : \mathrm{Im}(\rho_{E/K})\right] \leq n^3 \prod_{p|n} (1 - p^{-2}).$$

(ii) *The index* $[\mathrm{SL}(2, \hat{\mathbf{Z}}) : \mathrm{Im}(\rho_{E/K})]$ *is an isogeny invariant of $E/K$; the level is not.*

*Proof.* The proof of Corollary 1.5 gives (i). To prove (ii), suppose that $E$ and $E'$ are $K$-isogenous. By (1.3), $\Gamma = \mathrm{Im}(\rho_{E/K}) \cap \mathrm{SL}(2, \mathbf{Z})$ and $\Gamma' = \mathrm{Im}(\rho_{E'/K}) \cap \mathrm{SL}(2, \mathbf{Z})$ are congruence subgroups, and we need only show that they have the same index in $\mathrm{SL}(2, \mathbf{Z})$. From (1.2) it follows that $\Gamma$ and $\Gamma'$ are conjugate in $\mathrm{SL}(2, \mathbf{R})$. Thus their fundamental domains have the same volume, therefore $\pm\Gamma$ and $\pm\Gamma'$ have the same index in $\mathrm{SL}(2, \mathbf{Z})$ and thus $\Gamma$ and $\Gamma'$ have the same index in $\mathrm{SL}(2, \mathbf{Z})$. In §3, we will give examples to show that the level is not an isogeny invariant. □

While we are principally concerned with elliptic curves over function fields, we now comment on the arithmetic case. An elliptic curve $E$ over a number field $K$ has a Galois representation

$$\rho_{E/K} \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \hat{\mathbf{Z}}),$$

and Serre has proved that $\mathrm{Im}(\rho_{E/K}) \cong \mathrm{GL}(2, \hat{\mathbf{Z}})$ has finite index when $E$ has no complex multiplication (see **[11]**). If $K_{\mathrm{cyc}}$ is $K$ with all roots of unity adjoined, it follows that $E/K_{\text{cyc}}$ has finite level, which we may define to be the level of $E/K$. The results of this section then provide useful information about the arithmetic of $E/K$. (Lang and Trotter have defined an invariant of $\text{Im}(\rho_{E/K}) \subseteq \text{GL}(2, \hat{\mathbf{Z}})$ analogous to the level: in the language of [**8**, p. 18], one takes the smallest integer which is stable and splitting for $G = \text{Im}(\rho_{E/K})$.)

**2.** In this section we return to the situation of the introduction, where $E$ is an elliptic curve over a function field $K$ in one variable over $\mathbf{C}$, and the $j$-invariant is nonconstant. The Néron model of $E/K$ is an elliptic surface $f\colon X \to S$. Our goal here is to get effectively computable bounds for the level of $E/K$.

We first show how the $j$-invariant influences the level.

PROPOSITION 2.1. *Let $E/K$ have level $n$. Then*
(i) $n \le 2\deg(j)$,
(ii) $n \mid 2\text{LCM}\{b\colon j \text{ has a pole of order } b\}$.

*Proof.* Let $H$ be the image of $\text{Im}(\rho_{E/K})$ in $\text{SL}(2, \mathbf{Z}/n\mathbf{Z})$. Then $E/K$ has a level $H$-structure in the sense of [**3**, §3.1]. Since $\Gamma = \text{Im}(\rho_{E/K}) \cap \text{SL}(2, \mathbf{Z})$ is the inverse image of $H$ in $\text{SL}(2, \mathbf{Z})$, [**3**, §5] gives us a commutative diagram

$$(2.1) \qquad \begin{array}{ccc} & & X(\Gamma) \\ & \pi\nearrow & \\ S & & \downarrow J \\ & j\searrow & \\ & & \mathbf{P}^1 \end{array},$$

where $X(\Gamma) = \Gamma\backslash\mathfrak{H}^*$, and $J$ is the natural map induced by $\Gamma \subseteq \text{SL}(2, \mathbf{Z})$.

From (2.1), we see that $\deg(J) \mid \deg(j)$. Since $\deg(J) = [\text{SL}(2, \mathbf{Z})\colon \pm\Gamma]$, it follows from (1.4) that

$$m \le [\text{SL}(2, \mathbf{Z})\colon \pm\Gamma] \le \deg(j),$$

where $m$ is the level of $\pm\Gamma$.

By [**15**, Theorem 2], we have

$$\begin{aligned} m &= \text{LCM}\{\text{widths of cusps of } \pm\Gamma\} \\ &= \text{LCM}\{b\colon J \text{ has a pole of order } b\}. \end{aligned}$$

Then (2.1) implies that $m \mid \text{LCM}\{b\colon j \text{ has a pole of order } b\}$.

It remains to relate $m$, the level of $\pm\Gamma$, to $n$, the level of $\Gamma$. Since $[\pm\Gamma : \Gamma] \leq 2$, it follows that $[\Gamma(m) : \Gamma \cap \Gamma(m)] \leq 2$, and since $\Gamma \cap \Gamma(m)$ has level $n$, (1.4) gives that

$$n \leq [\Gamma(m) : \Gamma \cap \Gamma(m)] \cdot m \leq 2m.$$

Hence $n = m$ or $n = 2m$, and the proposition follows. □

In §3, we will give examples to show that the factor of 2 is necessary in both parts of Proposition 2.1.

A more striking result is that the level of $E/K$ is bounded by a constant depending only on the genus of the base field $K$. Recall that $K$ is the function field of the Riemann surface $S$.

THEOREM 2.2. *Let $E/K$ have level $n$, and let $S$ have genus $g$.*
(i) *If $g = 0$, then $n = O(1)$.*
(ii) *If $g \geq 1$, then $n = 24g + O(g^{1/2})$.*
(iii) *If $p$ is a prime dividing $n$, then $p \leq 12g + 13$.*

*Proof.* By (1.3), $\Gamma = \mathrm{Im}(\rho_{E/K}) \cap \mathrm{SL}(2, \mathbf{Z})$ is a congruence subgroup of level $n$. Since $j$ is nonconstant, the map $\pi$: $S \to X(\Gamma)$ of (2.1) is surjective. Thus, letting $\bar{g}$ denote the genus of $X(\Gamma)$, we have

$$\bar{g} \leq g. \tag{2.2}$$

Let $\overline{\Gamma}$ be the image of $\Gamma$ in PSL(2, **Z**), and let its level be $\bar{n}$. Then $\bar{g}$ is also the genus of $X(\overline{\Gamma})$, and we can use the following results of [**2**] to relate $\bar{g}$ and $\bar{n}$.

THEOREM 2.3. *Let $\overline{\Gamma} \subseteq \mathrm{PSL}(2, \mathbf{Z})$ be a congruence subgroup of level $\bar{n}$, and let $\bar{g}$ be the genus of $X(\overline{\Gamma})$.*
(i) *If $\bar{g} = 0$, then $\bar{n} = O(1)$.*
(ii) *If $\bar{g} \geq 1$, then $\bar{n} = 12\bar{g} + O(\bar{g}^{1/2})$.*
(iii) *If $p$ is a prime dividing $\bar{n}$, then $p \leq 12\bar{g} + 13$.*

*Proof.* See Corollary 4.7 (when $\bar{g} = 0$), Corollary 4.8 and Proposition 4.9 in [**2**]. □

Since $\bar{n}$ is also the level of $\pm\Gamma$, $\bar{n} = n$ or $\bar{n} = n/2$, and the theorem follows immediately from (2.2) and Theorem 2.3. □

More precise versions of (i) and (ii) in Theorem 2.2 may be stated as follows.

(i)′ If $g = 0$, then $n \leq 64$.

(ii)′ If $g \geq 1$, then

$$n \leq 24g + 13(48g + 121)^{1/2} + 145.$$

These statements follow from a more precise version of Theorem 2.3 which appears in the preprint version of [**2**]. (Specifically, see Corollary 4.11 and Table 5.1 in the preprint, and note that the group of level 36, resp. 48, in PSL(2, **Z**) in Table 5.1 is not the image of a group of level 72, resp. 96, in SL(2, **Z**).)

Here is a corollary of Theorem 2.2(iii) and Proposition 1.1(iv).

COROLLARY 2.4. *With the above notation, the Galois representation on p-torsion points*

$$\rho_{E/K,p}: \mathrm{Gal}(\overline{K}/K) \to \mathrm{SL}(2, \mathbf{F}_p)$$

*is surjective for all primes* $p > 12g + 13$. □

Another corollary of Theorem 2.2 is the following finiteness result.

COROLLARY 2.5. *For a fixed function field K over* **C**, *there are only finitely many possibilities for the image of the Galois representation* $\rho_{E/K}$. □

Since there are only finitely many congruence subgroups $\Gamma$ of SL(2, **Z**) such that $X(\Gamma)$ has a given genus (proved by Thompson in [**14**]), this corollary was already known.

Given the strength of these theorems, one might hope for similar results in the number field case. Here, recall that $E$ is an elliptic curve without complex multiplication over a number field $K$. Little is known about the size of $\mathrm{Im}(\rho_{E/K}) \subseteq \mathrm{GL}(2, \hat{\mathbf{Z}})$, although some examples have been computed (see [**8**] and [**11**]). In analogy with Proposition 2.1, Serre (see [**11**, §5]) has shown, when $K = \mathbf{Q}$, how to bound the primes dividing the level in terms of the reduction data of $E/\mathbf{Q}$. It should be possible to bound the level itself using the reduction data. The analog of Theorem 2.2 is quite a different matter. Given the present state of knowledge, one cannot even reasonably conjecture such a result. The number field case is much deeper than the function field case.

**3.** Let $E/K$ be as in §2, and let $f: X \to S$ be its Néron model. We now study the monodromy representation

$$\rho_{X/S}: \pi_1(S_0, t) \to \mathrm{SL}(2, \mathbf{Z})$$

defined in the introduction. The image $\Gamma$ of $\rho_{X/S}$ in $\mathrm{SL}(2,\mathbf{Z})$ is called the *global monodromy group* of $f\colon X \to S$. Both $\rho_{X/S}$ and $\Gamma$ are topological invariants in the sense that they are uniquely determined up to $\mathrm{SL}(2,\mathbf{Z})$-conjugacy by the topology of $f\colon X \to S$ and the orientation induced on the smooth fibers of $f$. Stiller has studied the basic properties of $\Gamma$:

PROPOSITION 3.1. *Let* $\Gamma$ *be the global monodromy group of* $f\colon X \to S$.

(i) $\Gamma$ *has finite index in* $\mathrm{SL}(2,\mathbf{Z})$.

(ii) *There is a commutative diagram*

$$\begin{array}{ccc} & & X(\Gamma) \\ & \pi \nearrow & \\ S & & \downarrow J \\ & j \searrow & \\ & & \mathbf{P}^1 \end{array}$$

*where* $J$ *is the natural map induced by* $\Gamma \subseteq \mathrm{SL}(2,\mathbf{Z})$.

(iii) $[\mathrm{SL}(2,\mathbf{Z})\colon \pm\Gamma] \mid \deg(j)$.

(iv) $[\mathrm{SL}(2,\mathbf{Z})\colon \pm\Gamma]$ *is an isogeny invariant of* $E/K$.

*Proof.* See [**13**, §§1 and 2]. □

Stiller also shows that other interesting invariants of $E/K$ are isogeny invariants. Propositions 1.6(ii) and 2.1(i) were inspired by parts (iii) and (iv) of Proposition 3.1.

Results such as the above lead one to expect a close relation between the Galois and monodromy representations. To state the relation precisely, we need to recall some facts.

(3.1) There is a continuous homomorphism

$$(\rho_{X/S})\hat{}\colon \pi_1(S_0, t)\hat{} \to \mathrm{SL}(2,\hat{\mathbf{Z}})$$

(where $\hat{}$ denotes profinite completion) such that the diagram

$$\begin{array}{ccc} \pi_1(S_0, t) & \overset{\rho_{X/S}}{\to} & \mathrm{SL}(2,\mathbf{Z}) \\ \cap| & & \cap| \\ \pi_1(S_0, t)\hat{} & \overset{(\rho_{X/S})\hat{}}{\to} & \mathrm{SL}(2,\hat{\mathbf{Z}}) \end{array}$$

commutes.

(3.2) $\pi_1(S_0, t)\hat{}$ is isomorphic to the étale fundamental group $\pi_1^{\mathrm{et}}(S_0, t)$.

(3.3) There is a continuous surjection

$$g\colon \mathrm{Gal}(\overline{K}/K) \to \pi_1^{\mathrm{et}}(S_0, t).$$

Our basic result is that $\rho_{X/S}$ determines $\rho_{E/K}$ as follows.

THEOREM 3.2. *The diagram*

$$\begin{array}{ccc} \mathrm{Gal}(\bar{K}/K) & \overset{\rho_{E/K}}{\to} & \mathrm{Sl}(2,\hat{\mathbf{Z}}) \\ g\downarrow & & \uparrow(\rho_{X/S})\hat{} \\ \pi_1^{\mathrm{et}}(S_0, t) & \overset{\sim}{\to} & \pi_1(S_0, t)\hat{} \end{array}$$

*is commutative.*

*Proof.* Let $X_t$ be the fiber of $f\colon X \to S$ over $t$, and let $E_n = \{x \in E(\bar{K})\colon nx = 0\}$. Then it suffices to find isomorphisms

$$\phi_n\colon E_n \overset{\sim}{\to} H^1(X_t, \mathbf{Z}/n\mathbf{Z}),$$

compatible with the natural inclusions $\mathbf{Z}/n\mathbf{Z} \subseteq \mathbf{Z}/m\mathbf{Z}$ and $E_n \subseteq E_m$ (when $n \mid m$), such that the diagrams

$$(3.4)\qquad \begin{array}{ccc} \mathrm{Gal}(\bar{K}/K) & \overset{\rho_1}{\to} & \mathrm{Aut}(E_n) \\ \downarrow & & \downarrow\wr\ \mathrm{Aut}(\phi_n) \\ \pi_1(S_0, t)\hat{} & \overset{\rho_2}{\to} & \mathrm{Aut}(H^1(X_t, \mathbf{Z}/n\mathbf{Z})) \end{array}$$

commute for all $n$, where $\rho_1$ and $\rho_2$ are determined by $\rho_{E/K}$ and $\rho_{X/S}$ respectively.

The map sending 1 to $e^{2\pi i/n}$ induces compatible isomorphisms $\mathbf{Z}/n\mathbf{Z} \cong \boldsymbol{\mu}_n$. Thus, in (3.4), we can replace $\mathbf{Z}/n\mathbf{Z}$ by $\boldsymbol{\mu}_n$.

The map $\rho_2$, restricted to $\pi_1(S_0, t)$, describes the locally constant sheaf $R^1 f_* \boldsymbol{\mu}_n$ on $S_0$. Working in the étale topology, there is a locally constant sheaf $R^1_{\mathrm{et}} f_* \boldsymbol{\mu}_n$ which is described by a map

$$\rho_3\colon \pi_1^{\mathrm{et}}(S_0, t) \to \mathrm{Aut}(H^1_{\mathrm{et}}(X_t, \boldsymbol{\mu}_n)).$$

The comparison theorem of [**1**, XVI 4.1] gives us compatible commutative diagrams

$$(3.5)\qquad \begin{array}{ccc} \pi_1^{\mathrm{et}}(S_0, t) & \overset{\rho_3}{\to} & \mathrm{Aut}(H^1_{\mathrm{et}}(X_t, \boldsymbol{\mu}_n)) \\ \downarrow\wr & & \downarrow\wr \\ \pi_1(S_0, t)\hat{} & \overset{\rho_2}{\to} & \mathrm{Aut}(H^1(X_t, \boldsymbol{\mu}_n)). \end{array}$$

Next, let the map $\xi\colon \mathrm{Spec}(\bar{K}) \to S_0$ be induced by the inclusion $K \subseteq \bar{K}$. Then the geometric point $t \in S_0$ gives us a specialization $\xi \to t$.

The specialization morphisms

$$\begin{aligned} &\pi_1^{\text{et}}(S_0, t) \to \pi_1^{\text{et}}(S_0, \xi) \\ &H^1_{\text{et}}(X_\xi, \mu_n) \to H^1_{\text{et}}(X_t, \mu_n) \end{aligned} \tag{3.6}$$

are isomorphisms by [**1**, XVI 2.2 and 2.3], and we can replace $t$ by $\xi$ in the bottom row of (3.5).

Finally, note that $\pi_1^{\text{et}}(\text{Spec}(K), \xi) \cong \text{Gal}(\bar{K}/K)$, and that the isomorphism

$$H^1_{\text{et}}(X_\xi, \mu_n) \cong E_n \tag{3.7}$$

of [**1**, IX 4.7] is compatible with the Galois action (and also with the usual maps $\mu_n \subseteq \mu_m$ and $E_n \subseteq E_m$). This implies that $\rho_1$ can be identified in a natural way with $\rho_3 \circ \delta$, where

$$\delta\colon \pi_1^{\text{et}}(\text{Spec}(K), \xi) \to \pi_1^{\text{et}}(S_0, \xi)$$

is induced by the map $\text{Spec}(K) \to S_0$. Then (3.5)–(3.7) give us the desired maps $\phi_n$, and the theorem follows. □

This theorem also proves the well-known fact that the Galois representation is unramified over $S_0$ (i.e., where $E/K$ has good reduction).

Here are some simple corollaries of Theorem 3.2.

COROLLARY 3.3. *Given $E/K$, let $\Gamma$ be the global monodromy group of its Néron model.*

(i) $\text{Im}(\rho_{E/K})$ *is the closure of* $\Gamma$ *in* $\text{SL}(2, \hat{\mathbf{Z}})$.

(ii) $\text{Im}(\rho_{E/K}) \cap \text{SL}(2, \mathbf{Z})$ *is the smallest congruence subgroup of* $\text{SL}(2, \mathbf{Z})$ *containing* $\Gamma$. □

COROLLARY 3.4. $\text{Im}(\rho_{E/K})$ *and the level of $E/K$ are topological invariants of the Néron model of $E/K$.* □

We can now give the example promised in Proposition 1.6(ii). In [**13**, §3], Stiller constructs isogenous elliptic curves $E$ and $\tilde{E}$ over $\mathbf{C}(t)$ such that their Néron models have global monodromy groups $\Gamma(2)$ and $\Gamma_0(4)$ respectively. It follows from Corollary 3.3 that $E/\mathbf{C}(t)$ has level 2, while $\tilde{E}/\mathbf{C}(t)$ has level 4. Note that this is the maximum change of level allowed by Proposition 1.1(ii).

Since the global monodromy group $\Gamma$ determines $\text{Im}(\rho_{E/K})$, it is natural to ask if the converse is true. If $\Gamma$ were always a congruence subgroup of $\text{SL}(2, \mathbf{Z})$, then the converse would follow immediately from Corollary 3.3. However, the following shows that $\Gamma$ can be *any* subgroup of $\text{SL}(2, \mathbf{Z})$ of finite index.

PROPOSITION 3.5. *Let $\Gamma$ be a subgroup of finite index in* $\mathrm{SL}(2, \mathbf{Z})$. *Then there is an elliptic curve $E/K$, where $K$ is the function field of $X(\Gamma)$, whose Néron model has $\Gamma$ as its global monodromy group.*

*Proof.* Let $\overline{\Gamma}$ be the image of $\Gamma$ in $\mathrm{PSL}(2, \mathbf{Z})$, and let $\mathfrak{E}$ be the set of elliptic points of $\mathrm{SL}(2, \mathbf{Z})$ acting on $\mathfrak{H}$. Then $\overline{\Gamma}$ acts freely on $\mathfrak{H}$-$\mathfrak{E}$ with quotient, say, $S_0$, giving us a surjective homomorphism

$$\bar{\rho}\colon \pi_1(S_0) \to \overline{\Gamma}.$$

Suppose there is a commutative diagram

$$\begin{array}{ccc} & & \Gamma \\ & {\scriptstyle\rho}\nearrow & \\ \pi_1(S_0) & & \downarrow \\ & {\scriptstyle\bar\rho}\searrow & \\ & & \overline{\Gamma} \end{array} \tag{3.8}$$

Let $J\colon X(\overline{\Gamma}) \to \mathbf{P}^1$ be the natural map. Then $\rho$ belongs to $J$ in the sense of [7, §8], so we can let $f\colon X \to X(\overline{\Gamma})$ be the basic member of $\mathfrak{F}(\rho, J)$ (again, see [7, §8]). One easily checks that $\mathrm{Im}(\rho)$ is the global monodromy group. Thus, the generic fiber of $f$ will give the desired example, provided we can find a *surjective* map $\rho$ satisfying (3.8).

If $-1 \notin \Gamma$, then $\Gamma \to \overline{\Gamma}$ is an isomorphism, so that $\rho$ exists and is clearly surjective. (It is clear from [**12**, §4] that this gives us the elliptic modular surface of $\Gamma$.)

Suppose that $-1 \in \Gamma$. Our above construction gives us a commutative diagram

$$\begin{array}{ccc} \pi_1(S_0) & \xrightarrow{\bar\rho} & \overline{\Gamma} \\ \cap| & & \cap| \\ \pi_1(\mathbf{P}^1 - \{0, 1, \infty\}) & \xrightarrow{\bar\rho_1} & \mathrm{PSL}(2, \mathbf{Z}). \end{array}$$

where $\bar{\rho}_1$ is surjective. Since $\pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$ is free, $\bar{\rho}_1$ lifts to a homomorphism

$$\rho_1\colon \pi_1(\mathbf{P}^1 - \{0, 1, \infty\}) \to \mathrm{SL}(2, \mathbf{Z})$$

which is easily seen to be surjective. Then $\rho = \rho_{1|\pi_1(S_0)}$ gives the desired surjective lift of $\bar{\rho}$. □

We can now give the examples promised in the remarks following the proof of Proposition 2.1. Let $\Gamma$ be the commutator subgroup of $\mathrm{SL}(2, \mathbf{Z})$.

Then (1.3) and (1.5)–(1.7) show that $-1 \notin \Gamma$, $[\mathrm{SL}(2,\mathbf{Z}):\Gamma] = 12$ and, contrary to the claim of [**12**, Ex. 5.9], $\Gamma$ has level 12. The proof of Proposition 3.5 shows that the elliptic modular surface of $\Gamma$ has $\Gamma$ as its global monodromy group. Then the corresponding elliptic curve $E/K$ has level 12 by Corollary 3.3. The $j$-invariant of $E/K$ has only one pole, which is of order 6 (see [**12**, Ex. 5.9]), so that $6 = \deg(j) = \mathrm{LCM}\{b: j \text{ has a pole of order } b\}$. Thus, the factors of 2 in Proposition 2.1 are necessary.

A final question to ask is if the analog of Corollary 2.5 holds for the global monodromy group $\Gamma$: for elliptic surfaces over a fixed Riemann surface $S$, are there only finitely many possibilities for $\Gamma$? The answer is no. To see this, note that by [**6**], there are infinitely many subgroups $\Gamma \subseteq \mathrm{SL}(2,\mathbf{Z})$ of finite index such that $X(\Gamma) \cong \mathbf{P}^1$. Given such a $\Gamma$, Proposition 3.5 gives us an elliptic surface $f: X \to \mathbf{P}^1$ with monodromy representation

$$\rho_{X/\mathbf{P}^1}: \pi_1(S_0) \to \Gamma$$

where $S_0 \subseteq \mathbf{P}^1$ and $\rho_{X/\mathbf{P}^1}$ is surjective. If $S$ is any Riemann surface, we can find a map $\pi: S \to \mathbf{P}^1$ which is unramified above $\mathbf{P}^1 - S_0$. Then the pullback of $f: X \to \mathbf{P}^1$ via $\pi$ gives us an elliptic surface over $S$ with $\Gamma$ as global monodromy group. This gives us infinitely many global monodromy groups $\Gamma$. Combining this with Corollary 2.5, we get infinitely many elliptic surfaces over $S$ with distinct $\Gamma$'s and the same $\mathrm{Im}(\rho_{E/K})$. Thus, we see that the global monodromy group is a much more subtle invariant than the image of the Galois representation.

## REFERENCES


[1] M. Artin, A. Grothendieck, and J. L. Verdier, *Théorie des Topos et Cohomologie Étale des Schémas* (*SGA*4), Lecture Notes in Math., vol. 305, Springer, New York, 1973.

[2] D. Cox and W. Parry, *Genera of congruence subgroups in* **Q**-*quaternion algebras*, J. Reine Angew. Math., to appear.

[3] P. Deligne and M. Rapoport, *Les schémas de modules des courbes elliptiques*, in *Modular Functions of One Variable* II, Lecture Notes in Math., vol. 349, Springer, New York, 1973.

[4] A. Grothendieck, *Revêtements Étales et Groupe Fondemental* (*SGA*1), Lecture Notes in Math., vol. 224, Springer, New York, 1971.

[5] J. Igusa, *Fiber systems of Jacobian varieties III*, Amer. J. Math., **81** (1959), 453–476.

[6] G. Jones, *Triangular maps and non-congruence subgroups of the modular group*, Bull. London Math. Soc., **11** (1979), 117–123.

[7] K. Kodaira, *On compact analytic surfaces II*, Annals of Math., **77** (1963), 563–626.

[8] S. Lang and H. Trotter, *Frobenius Distributions in $GL_2$-extensions*, Lecture Notes in Math., vol. 504, Springer, New York, 1976.

[9] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Inv. Math., **18** (1972), 183–266.

[10] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, Benjamin, New York, 1968.

[11] _____, *Proprietes galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math., **15** (1972), 259–331.

[12] T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan, **24** (1972), 20–59.

[13] P. Stiller, *Monodromy and invariants of elliptic surfaces*, Pacific J. Math., **92** (1981), 433–452.

[14] J. Thompson, *A finiteness theorem for subgroups of* PSL(2, **R**) *which are commensurable with* PSL(2, **Z**), in *The Santa Cruz conference on finite groups*, Proceedings of Symposia in Pure Math., vol. 37, AMS, Providence, 1980.

[15] K. Wohlfahrt, *An extension of F. Klein's level concept*, Illinois J. Math., **8** (1964), 529–535.

Received September 3, 1982. First author's research supported by NSF Grant MCS-8002276. Second author's research supported by NSF Grant MCS-8003600 A02.

AMHERST COLLEGE
AMHERST, MA 01002

AND

SUNY
STONY BROOK, NY 11794