Abstract. Let $A$ be an elliptic curve over a number field $K$, let $p \geq 7$ be a prime and let $\wp$ be a prime ideal of $K$ lying above $p$, such that the $j$-invariant of $A$ is non-integral at $\wp$. We extend a result of Rohrlich to show that a certain deformation of the Galois representation attached to the Tate module of $A$ is surjective, under some restrictions involving the ramification index of $\wp$, $p$ and $j(A)$.

1. Surjectivity of a Galois Representation

Let $K$ be a number field, fix $\overline{K}$, an algebraic closure of $K$, and let $j$ be transcendental over $K$. Let $E$ be an elliptic curve defined over the field $\overline{K}(j)$ such that $j(E) = j$. Given a prime number $p \geq 7$, the natural action of $\text{Gal}(\overline{K}(j)/K(j))$ on the group of $p$-torsion points of $E$ induces a representation $\tilde{\pi}_E : \text{Gal}(\overline{K}(j)/K(j)) \to \text{SL}(2, \mathbb{F}_p)$. The universal deformation of $\tilde{\pi}_E$, with respect to certain ramification conditions (see [Roh], [Roh04]), is an epimorphism $\pi_E : \text{Gal}(\overline{K}(j)/\tilde{K}(j)) \to \text{SL}(2, \mathbb{Z}_p[[X]])$.

Let $\tilde{K}$ be the extension of $K$ generated by all roots of unity of $p$-power order. In [Roh00a], [Roh00b], D. E. Rohrlich showed that $\pi_E$ descends to an epimorphism $\rho_E : \text{Gal}(\overline{K}(j)/\tilde{K}(j)) \to \text{SL}(2, \mathbb{Z}_p[[X]])$.

Notice that $\rho_E$ encapsulates arithmetic information which was not present in $\pi_E$.

Let $A$ be an elliptic curve defined over $K$ with $j$-invariant $j(A) \neq 0, 1728$ and suppose that $A$ coincides with the fiber of $E$ at $j = j(A)$. Choose a place $\sigma$ of $\overline{K}(j)$ extending the place $j = j(A)$ of $\tilde{K}(j)$, and write $D$ and $I$ for the corresponding decomposition and inertia subgroups of $\text{Gal}(\overline{K}(j)/\tilde{K}(j))$. We “specialize” the representation $\rho_E$ to $j = j(A)$ by restricting the map to
the decomposition group $D$. By the ramification constraints of the universal deformation (see [Roh00b]), the map $\rho_E$ is unramified outside $\{0, 1728, \infty\}$, thus $\rho_E|_D$ factors through $D/I \cong \text{Gal}(\bar{K}/\tilde{K})$. We obtain a representation:

$$\rho_A : \text{Gal}(\bar{K}/\tilde{K}) \rightarrow \text{SL}(2, \mathbb{Z}_p[[X]])$$

If we write $\overline{\rho}_A : \text{Gal}(\bar{K}/\tilde{K}) \rightarrow \text{SL}(2, \mathbb{Z}_p)$ for the representation determined up to equivalence by the natural action of $\text{Gal}(\bar{K}/\tilde{K})$ on the Tate module of $A$, then, by construction, $\rho_A$ is a deformation of $\overline{\rho}_A$, and in particular $\rho_A|_{X=0} = \overline{\rho}_A$. The image of $\overline{\rho}_A$, which has been characterized by M. Deuring [Deu53], [Deu58], J.-P. Serre [Ser72], J. Tate [ST68] and others, depends drastically on whether the elliptic curve $A$ has complex multiplication or not.

In light of the results of Deuring, Serre and Tate, one would naturally want to know how large is the image of the representation $\rho_A$. Let

$$\overline{\rho}_A : \text{Gal}(\bar{K}/\tilde{K}) \rightarrow \text{SL}(2, \mathbb{F}_p)$$

be the representation induced by the action of Galois on the points of order $p$ on $A$. In [Roh04], Rohrlich proved in the case $K = \mathbb{Q}$ that if $\overline{\rho}_A$ is surjective and $\nu_p(j(A)) = -1$ then $\rho_A$ is surjective, where $\nu_p$ is the usual $p$-adic valuation on $\mathbb{Q}$. In this note we generalize Rohrlich’s results to more general number fields.

Fix $\wp$, a prime of $K$ lying above a prime $p \geq 7$. We write $\nu_\wp$ for the standard $\wp$-adic valuation on $K$, so that, for a uniformizer $\pi$ of $\wp$, $\nu_\wp(\pi) = 1$ and $\nu_\wp(p) = e$, where $e = e(\wp | p)$ is the ramification index.

**Theorem 1.1.** If $\overline{\rho}_A$ is surjective, $e$ is not divisible by $p-1$, $\nu_\wp(j(A)) = -t$ with $t \in \mathbb{N}$, $\gcd(p, t) = 1$, and

$$t < \frac{ep}{p-1} = e + \frac{e}{p-1};$$

then $\rho_A$ is surjective.

**Proof.** The strategy of the proof is the same as in [Roh04], proof of Theorem 1 (which shows the case $K = \mathbb{Q}$). We summarize it here and point out where the proof diverges for a number field $K$ as in the statement of Theorem 1.1.

It suffices to verify the surjectivity of the projective representation

$$P\overline{\rho}_A : \text{Gal}(\bar{K}/\tilde{K}) \rightarrow \text{PSL}(2, \Lambda)$$

because the only subgroup of $\text{SL}(2, \Lambda)$ with projective image $\text{PSL}(2, \Lambda)$ is the full group $\text{SL}(2, \Lambda)$. We similarly define projective maps $P\rho_E$ and $P\overline{\rho}_A$. By the definition of $\rho_A$, in order to verify the surjectivity of $P\rho_A$ it suffices to show that the image via $P\rho_E$ of the decomposition group $D$ is the full group $\text{PSL}(2, \Lambda)$.
The kernel of $\rho_E$ determines a fixed field $L$, in particular $\text{Gal}(L/\tilde{K}(j)) \cong \text{PSL}(2, \mathbb{Z}_p[[X]])$. For $i \geq 1$, let $L_i \subseteq L$ be the fixed field determined by the kernel of the reduction map

$$\text{Gal}(L/\tilde{K}(j)) \cong \text{PSL}(2, \mathbb{Z}_p[[X]]) \to \text{PSL}(2, \mathbb{Z}_p[[X]]/(p, X)^t).$$

Recall that we have chosen a place $\sigma$ of $K(j)$ extending $j = j(A)$. Let $\ell_\nu$ be the residue class field of $\sigma |_{L_\nu}$, i.e. $\ell_\nu = \sigma(L_\nu)\setminus\{\infty\}$.

A criterion of Boston ([Bos86], Prop. 2, p. 262) reduces the problem to proving that the image of $D$ in $\text{Gal}(L_2/\tilde{K}(j))$ maps to all of $\text{PSL}(2, \Lambda/(p, X)^2)$. Equivalently, one needs to show that $[L_2 : \tilde{K}(j)] = [\ell_2 : \tilde{K}]$. Notice that the assumption on the surjectivity of $\tilde{\rho}_A$ implies that $\rho_A$ is surjective (see, for example, [Ser68], IV-23, Lemma 3), and so is $\text{P}\rho_A$, the projectivization of $\tilde{\rho}_A$. It follows that $[L_1 : \tilde{K}(j)] = [\ell_1 : \tilde{K}]$, therefore it suffices to prove that

(1) $[L_2 : L_1] = [\ell_2 : \ell_1].$

1.1. Siegel Functions. We follow the definitions established in [Roh04].

Definition 1.2. Let $p \geq 7$ be a prime and define $R = \mathbb{F}_p^2 \setminus \{(0, 0)\}$.

(1) $M$ is the set of all functions $m: R \to \mathbb{Z}$ with $m(r) = m(-r)$. $M$ is clearly a $\mathbb{Z}$-module.

(2) We write $N$ for the $\mathbb{Z}$-submodule of $M$ consisting of all those $m \in M$ that reduce modulo $p$ to a function defined by a homogeneous polynomial of degree two over $\mathbb{F}_p$.

Let $r \in R$ and let $s = (s_1, s_2) \in \mathbb{Z}^2$ be any lift of $r$, i.e. $s = (s_1, s_2) \equiv r \mod p$ and put $a = a_s = \frac{1}{p}(s_1, s_2)$, then the symbol $f_r$ represents any Siegel function $g_a^2$ (see [KL81], p. 29). If $s \in \mathbb{Z}^2$ is replaced by another lift of $r$ then $f_r$ is multiplied by a $p$th root of unity (for this see [KL81], Remark on p. 30), so the symbol $f_r(\tau)$ is only well defined up to $p$th roots of unity. For $m \in M$ we also define the symbolic $m$th power:

$$f^m = \prod_{r \in R} f_r^{m(r)}.$$

The key ingredient in the proof of Theorem 1.1 is given by the following result of Rohrlich ([Roh04], Theorem 2).

Theorem 1.3. The extension $L_2/L_1$ is generated by $p$th roots of Siegel units. More precisely, $L_2 = L_1\{((f^m)^{1/p} : m \in N}\}$.

Using the previous theorem, Rohrlich reduces the proof of (1) to the following local statement (see [Roh04], p. 19, 20; the argument is valid in our case, by simply replacing $\mathbb{Q}$ by $\tilde{K}$). Since $\nu_p(j(A)) = -t < 0$ there is a unique Tate curve $B$ over $K$, with $j(B) = j(A)$. Suppose there is a
$m \in \mathbb{N}$ such that $\sigma(f^m)^{1/p} \notin K_{\wp}(B[p^\nu])$ for all sufficiently large $\nu \in \mathbb{N}$, then equality (1) follows.

Let $O_{\wp}$ be the ring on integers in $K_{\wp}$ and let $q$ be the unique element of $\pi O_{\wp}$ such that $j(q) = j(B)$, where $\pi$, as before, is a uniformizer of $\wp$. Proposition 8 of [Roh04], can be generalized to:

**Proposition 1.4.** There exists $m \in \mathbb{N}$ such that:

$$\sigma(f^m) = q^\mu(1 - uq)(1 - vq^2) = q^\mu(1 + wq)$$

with $\mu \in \mathbb{Z}$, $u, w \in O_{\wp}^\times$, and $v \in O_{\wp}$. In particular, $\sigma(f^m) \in K_{\wp}$.

The proof found in [Roh04] is valid without change. Let $f = f^m$ with $m$ as in the previous proposition. Hence, in order to finish the proof of Theorem 1.1, we need to show:

**Proposition 1.5.** Suppose that $v_{\wp}(j(A)) = -t$ with $t \in \mathbb{N}$, $e$ is not divisible by $p - 1$, $\gcd(p, t) = 1$, and

$$t < \frac{ep}{p - 1} = e + \frac{e}{p - 1};$$

then $\sigma(f)^{1/p} \notin K_{\wp}(B[p^\nu])$ for all sufficiently large $\nu \in \mathbb{N}$.

**Proof.** It suffices to show that $\sigma(f)^{1/p}$ has degree $p$ over $K_{\wp}(B[p^\nu])$ for all sufficiently large $\nu$. Note that $K_{\wp}(B[p^\nu]) = K_{\wp}(\zeta, q^{1/p^\nu})$ where $\zeta$ is a primitive $p^\nu$th root of unity (see [Lan87], Chapter 15, Theorem 3).

Since $v_{\wp}(j(A)) = -t$, then $v_{\wp}(q) = t$ (and by assumption $\gcd(p, t) = 1$). It follows that $\gcd(v_{\wp}(q), p^\nu) = 1$ and the order of $q$ in $K_{\wp}^\times/K_{\wp}^{p^\nu}$ is $p^\nu$.

Recall that by Proposition 1.4 we can write $\sigma(f)$ as $q^\mu(1 - uq)(1 - vq^2) = q^\mu(1 + wq)$ with $\mu \in \mathbb{Z}$, $u, w \in O_{\wp}^\times$, and $v \in O_{\wp}$. We claim that $\alpha := q^{-p}\sigma(f)$ has degree $p^\nu$ in $K_{\wp}^\times/K_{\wp}^{p^\nu}$. For suppose the contrary, i.e. $\alpha^{p^\nu-1} = \beta^{p^\nu}$ for some $\beta \in K_{\wp}$. Then $\beta^p = \xi\alpha$ with $\xi$ a $p^{\nu-4}$th root of unity and $\xi = \beta^p\alpha^{-1} \in K_{\wp}$. Since $K_{\wp}$ cannot contain nontrivial $p$th roots of unity (or $p - 1$ would divide $e$), it follows that $\xi = 1$.

Hence $\alpha = \beta^p$. Let $\beta = 1 + b\pi$ for some $b \in O_{\wp}$, $\pi$ a uniformizer for $\wp$. By the binomial theorem:

$$(1 + b\pi)^p = \sum_{h=0}^{p} \binom{p}{h} b^h \pi^h$$

so the terms in $\beta^p - 1$ have $\wp$-adic valuations in the list

$$p(v_{\wp}(b) + 1), i(v_{\wp}(b) + 1) + e \text{ with } 1 \leq i \leq p - 1$$

and the minimum non-zero valuation is either $p(v_{\wp}(b) + 1)$ or $v_{\wp}(b) + 1 + e$ (and both cannot be equal, since that implies that $p - 1$ divides $e$). This value
must equal $t$ since we are assuming $\alpha = 1 + wq = \beta^p$, but $t$ is not divisible by $p$ by hypothesis, so the minimum valuation must be $t = \nu_\wp(b) + 1 + e$.

First suppose $t < e + 1$. This implies that $\nu_\wp(b) < 0$ which is contradictory since $b \in \mathcal{O}_\wp$. Otherwise $e + 1 \leq t < \frac{ep}{p-1}$ and the fact that $\nu_\wp(b) + 1 + e < p \cdot (\nu_\wp(b) + 1)$ implies that

$$p > \frac{\nu_\wp(b) + 1 + e}{\nu_\wp(b) + 1}.$$ 

Substituting $\nu_\wp(b) = t - e - 1$ we obtain $p > \frac{e}{t-e}$ and hence $t > \frac{ep}{p-1}$ (since $t > e$) which contradicts our assumption on $t$. Therefore, we conclude that $\alpha$ is not a $p$-th power.

Remark 1.6. Using the $\wp$-adic logarithm and exponential maps one can prove that if $\nu_\wp(\gamma) > e + \frac{e}{p-1}$ then $(1 + \gamma)^{1/p} \in K_\wp$. So the bound on $t$ in the theorem is best possible, at least for this method of proof.

Thus we have proved that the order of $\alpha$ in $K_\wp^\times/K_\wp^{\times p^\nu}$ is exactly $p^\nu$. Therefore, the subgroup of $K_\wp^\times/K_\wp^{\times p^\nu}$ generated by the cosets of $q$ and $\sigma(f)$ has order $p^{2\nu}$.

Lemma 1.7. Let $L$ be a field with $\text{char}(L) = 0$, and let $\zeta$ be a primitive $p^\nu$th root of unity. Let $M = L(\zeta)$. Then the following natural map is injective:

$$L^\times/L^{\times p^\nu} \rightarrow M^\times/M^{\times p^\nu}.$$ 

We claim that Proposition 1.5 follows using the previous lemma (which we will prove below). Indeed, let $F_\nu = K_\wp(\zeta)$ where $\zeta$ is a primitive $p^\nu$th root of unity. The natural map

$$K_\wp^\times/K_\wp^{\times p^\nu} \rightarrow F_\nu^\times/F_\nu^{\times p^\nu}$$

is injective by the previous Lemma, so the image of the group generated by the cosets of $q$ and $\sigma(f)$ also has order $p^{2\nu}$.

It follows that $[F_\nu(q^{1/p^\nu}, \sigma(f)^{1/p^\nu}): F_\nu] = p^{2\nu}$ and we can deduce that

$$[F_\nu(q^{1/p^\nu}, \sigma(f)^{1/p^\nu}): F_\nu(q^{1/p^\nu})] = p^\nu.$$ 

Hence $\sigma(f)^{1/p^\nu}$ has degree $p^\nu$ over $F_\nu(q^{1/p^\nu}) = K_\wp(B[p^\nu])$, so $\sigma(f)^{1/p}$ has degree $p$ over $K_\wp(B[p^\nu])$. $\square$

Proof of Lemma 1.7. As a consequence of Hilbert Theorem 90 we obtain:

$$H^1(\text{Gal}(\overline{L}/L), \mu_{p^\nu}) = L^\times/L^{\times p^\nu}, \quad \text{and} \quad H^1(\text{Gal}(\overline{M}/M), \mu_{p^\nu}) = M^\times/M^{\times p^\nu}.$$ 

Moreover, the natural map $L^\times/L^{\times p^\nu} \rightarrow M^\times/M^{\times p^\nu}$ corresponds to the restriction map in cohomology, which fits in the exact sequence:

$$0 \rightarrow H^1(\text{Gal}(M/L), \mu_{p^\nu}) \rightarrow H^1(\text{Gal}(\overline{L}/L), \mu_{p^\nu}) \rightarrow H^1(\text{Gal}(\overline{M}/M), \mu_{p^\nu}) \rightarrow H^2(\text{Gal}(\overline{L}/L), \mu_{p^\nu})$$

and the exact sequence:

$$0 \rightarrow H^1(\text{Gal}(\overline{M}/M), \mu_{p^\nu}) \rightarrow H^1(\text{Gal}(\overline{L}/L), \mu_{p^\nu}) \rightarrow H^1(\text{Gal}(M/L), \mu_{p^\nu}) \rightarrow H^2(\text{Gal}(\overline{L}/L), \mu_{p^\nu}).$$
Thus, in order to show that the map is injective, is enough to show that

\[ H^1(\text{Gal}(M/L), \mu_{p^r}) = 0. \]

Since \( M = L(\zeta) \) where \( \zeta \) is a primitive \( p^r \)th root of unity, we can think of \( \text{Gal}(M/L) \) as a subgroup of \( (\mathbb{Z}/p^r\mathbb{Z})^\times \) acting on \( \mu_{p^r} \cong \mathbb{Z}/p^r\mathbb{Z} \) via multiplication, and to finish the proof, we must prove:

**Lemma 1.8.** \( H^1(G, \mathbb{Z}/p^r\mathbb{Z}) = 0 \) for any \( G \leq (\mathbb{Z}/p^r\mathbb{Z})^\times \).

Statements similar to this one can be found in the literature (see e.g. [Rub99], Lemma 6.1), but for the convenience of the reader we include a proof of the precise statement needed here.

**Proof.** For this, let \( \psi : G \to \mathbb{Z}/p^r\mathbb{Z} \) be a cocycle. We would like to prove that \( \psi \) is actually a coboundary. Since \( G \leq (\mathbb{Z}/p^r\mathbb{Z})^\times \), \( G \) is cyclic, \( G = \langle a \rangle \) for some \( a \). Moreover, suppose that the order of \( G \) is \( n_0 \). Since \( \psi \) is a cocycle \( \psi(1) = 0 \) and, inductively, one can show that

\[ \psi(a^t) = (a^{t-1} + a^{t-2} + ... + 1)\psi(a) = \left( \frac{a^{t} - 1}{a - 1} \right) \psi(a). \]

Note that \( \frac{1}{a-1} \) might not make sense in \( \mathbb{Z}/p^r\mathbb{Z} \), so we also let \( a \) be an integer representative of the congruence class, and we write \( \left( \frac{a^{t-1}}{a-1} \right) \) for the congruence class of \( \frac{a^{t-1}}{a-1} \in \mathbb{Z} \) modulo \( p^r\mathbb{Z} \).

Note that \( n_0 \), the order of \( G \), divides \( p^{r-1}(p-1) \), the order of \( (\mathbb{Z}/p^r\mathbb{Z})^\times \). First, suppose that \( \gcd(n_0, p-1) > 1 \). Then \( a \not\equiv 1 \mod p \), since the elements which are congruent to 1 modulo \( p \) generate subgroups with order a power of \( p \). Since \( a \not\equiv 1 \mod p \), \( a - 1 \in (\mathbb{Z}/p^r\mathbb{Z})^\times \) and it follows that:

\[ \psi(a^t) = \left( \frac{a^{t} - 1}{a - 1} \right) \psi(a) = (a^{t-1} + a^{t-2} + ... + 1)\psi(a) = a^{t-1} \psi(a) \frac{a^{t} - 1}{a - 1} = \frac{\psi(a)}{a - 1} \psi(a) = \psi(a) \left( \frac{a^{t-1}}{a - 1} \right) \]

with \( \frac{\psi(a)}{a-1} \in \mathbb{Z}/p^r\mathbb{Z} \). Hence \( \psi \) is a coboundary in this case.

Only the case \( n_0 = p^{r-m} \) remains, where \( m \) is an integer satisfying \( 1 \leq m < \nu \). This corresponds to the case \( G = \{ \alpha \in (\mathbb{Z}/p^r\mathbb{Z})^\times : \alpha \equiv 1 \mod p^m \} \). Thus \( a \), the chosen generator of \( G \), satisfies \( a \equiv 1 + up^m \mod p^r \), with \( u \not\equiv 0 \mod p \). It suffices to show that \( \psi(a) \equiv 0 \mod p^m \) since that would imply that \( \psi(a) \equiv 0 \mod p^m \mathbb{Z}/p^r\mathbb{Z} \) and we can proceed as in (♠) to prove that \( \psi \) is a coboundary. We start with:

\[ 0 \equiv \psi(1) \equiv \psi(a \cdot a^{p^{r-m}-1}) \equiv \psi(a) + a \cdot \psi(a^{p^{r-m}-1}) \mod p^r \]

and

\[ \psi(a^{p^{r-m}-1}) \equiv \left( \frac{a^{p^{r-m}-1} - 1}{a - 1} \right) \psi(a) \mod p^r \]
thus
\[ 0 \equiv \psi(a) + a \cdot \left( \frac{a^{p^\nu-1} - 1}{a - 1} \right) \psi(a) \mod p^\nu. \quad (\mathfrak{H}) \]

It is easy to see that \((1 + up^\nu)^p = 1 + u'p^\nu\), with \(u \equiv u' \mod p\). Hence:
\[ a \cdot \left( \frac{a^{p^\nu-1} - 1}{a - 1} \right) = \frac{a^{p^\nu-1} - 1}{a - 1} - 1 \equiv p^{\nu-m} - 1 \mod p^{\nu+1} \]

and the congruence remains true modulo \(p^\nu\). Finally, substituting in \((\mathfrak{H})\) above, we obtain:
\[ 0 \equiv \psi(a) + (p^{\nu-m} - 1)\psi(a) \equiv p^{\nu-m}\psi(a) \mod p^\nu. \]

Therefore, \(\psi(a) \equiv 0 \mod p^m\), which concludes the proof of the Lemma. \(\square\)

2. Example

Let \(K = \mathbb{Q}(\sqrt{-11})\), \(p = 11\) and set \(\tau = \frac{1+\sqrt{-11}}{2}\). We write \(\varphi\) for the unique prime ideal of \(K\) lying above 11, thus the ramification index \(e = e(\varphi \mid p) = 2\). Let \(A/K\) be the curve:
\[ A: y^2 + (2\tau - 1)y = x^3 + \tau x^2, \quad j(A) = \frac{-61440 - 851968\tau}{11 \cdot 4931} \]

\[ \Delta_A = -3795 - 352\tau, \quad N_{K/\mathbb{Q}}(\Delta_A) = 3^3 \cdot 11^2 \cdot 3941, \quad N_{K/\mathbb{Q}}(j(A)) = \frac{2^{24} \cdot 3^3}{11^2 \cdot 3941} \]

In particular, \(t = -v_p(j(A)) = 2\). Note that \(e = 2\) is not divisible by \(p - 1 = 10\); \(\gcd(p, t) = \gcd(11, 2) = 1\) and \(\frac{ep}{p-1} = \frac{11}{5} > 2 = t\).

Hence it remains to check that the representation \(\tilde{\rho}_A: \text{Gal}(\overline{K}/\overline{K}) \to \text{SL}(2, \mathbb{F}_p)\) is surjective. In [Ser72], Proposition 19, J-P. Serre gives conditions for a subgroup \(G\) of \(\text{SL}(2, \mathbb{F}_p)\) to be the full group \(\text{SL}(2, \mathbb{F}_p)\). We reproduce the result here for the reader’s convenience:
Proposition. Suppose $p \geq 5$ and the following hypotheses are satisfied:

1. The subgroup $G$ contains a matrix $s_1$ such that $\text{Tr}(s_1)^2 - 4 \det(s_1)$ is a non-zero quadratic residue modulo $p$, and $\text{Tr}(s_1) \not\equiv 0 \mod p$;
2. $G$ contains a matrix $s_2$ such that $\text{Tr}(s_2)^2 - 4 \det(s_2)$ is not a quadratic residue modulo $p$, and $\text{Tr}(s_2) \not\equiv 0 \mod p$;
3. $G$ contains a matrix $s_3$ such that $u = \text{Tr}(s_3)^2/\det(s_3)$ is not 0, 1, 2 or 4 modulo $p$ and $u^2 - 3u + 1 \not\equiv 0 \mod p$.

Then $G$ is the full group $\text{SL}(2, \mathbb{F}_p)$.

Let $G < \text{SL}(2, \mathbb{F}_p)$ be the image of the representation $\widetilde{\rho}_A$. Let $S_A$ denote the set of all prime ideals of $K$ such that $A$ has bad reduction. $S_A$ is the set of prime ideals which divide $\Delta_A$, i.e. $S_A = \{3, 11, 3941\}$. Then, for every $\nu \not\in S_A \cup \{\wp\}$ the image via $\widetilde{\rho}_A$ of a Frobenius element $\pi_\nu \in \text{Gal}(\overline{K}/K)$ is a matrix that we also denote by $\pi_\nu$ such that:

1. $\text{Tr}(\pi_\nu) \equiv a_\nu \mod p$ where $a_\nu$ is the trace of the Frobenius automorphism of $A$ at the place $\nu$;
2. $\det(\pi_\nu) \equiv N(\nu) \mod p$.

In order to conclude that $G = \text{SL}(2, \mathbb{F}_p)$ we exhibit three Frobenius elements $s_1, s_2, s_3$ ($s_3 = s_2$) that satisfy the conditions in the proposition above. The trace of the Frobenius automorphism was calculated using the computer software PARI [Pari00].

- The prime number 5 is split in $K$. Let $\nu_5$ be one of the prime ideals of $K$ lying above 5 (so $N(\nu_5) = 5$). The trace of the Frobenius automorphism is $a_{\nu_5} = -1$. Let $s_1 = \pi_{\nu_5}$. Then:

$$\text{Tr}(s_1)^2 - 4 \det(s_1) \equiv (-1)^2 - 4 \cdot 5 \equiv -19 \equiv 5^2 \mod 11.$$ 

- The prime number 13 is inert in $K$. Let $\nu_{13}$ be the prime ideal of $K$ lying above 13 (so $N(\nu_{13}) = 169$). The trace of the Frobenius automorphism is $a_{\nu_{13}} = 10$. Let $s_2 = \pi_{\nu_{13}}$. Then:

$$\text{Tr}(s_2)^2 - 4 \det(s_2) \equiv (10)^2 - 4 \cdot 169 \equiv -576 \equiv 7 \mod 11$$

and 7 is not a quadratic residue modulo 11.

- Let $s_3 = s_2$ and let $u = \text{Tr}(s_3)^2/\det(s_3) \equiv \frac{100}{169} \equiv 3 \mod 11$. Then $u^2 - 3u + 1 \equiv 1 \mod 11$.

Therefore $\widetilde{\rho}_A$ is surjective and all conditions of Theorem 1.1 have been verified, thus the map $\rho_A: \text{Gal}(\overline{K}/K) \to \text{SL}(2, \mathbb{Z}_{11}[[X]])$ is surjective. □

Acknowledgements

I would like to thank David Rohrlich for his dedication as my advisor.
References


E-mail address: alozano@colby.edu

Department of Mathematics, Colby College, 8800 Mayflower Hill, Waterville, ME 04901.