ACTA ARITHMETICA
117.3 (2005)

On the surjectivity of Galois representations attached to elliptic curves over number fields

by

Álvaro Lozano-Robledo (Waterville, ME)

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 $K(j)$ such that $j(E) = j$. Given a prime number $p \geq 7$, the natural action of $\mathrm{Gal}(\overline{K(j)}/\overline{K}(j))$ on the group of p-torsion points of E induces a representation $\widetilde{\pi}_E\colon\ \mathrm{Gal}(\overline{K(j)}/\overline{K}(j)) \to \mathrm{SL}(2, \mathbb{F}_p)$. The universal deformation of $\widetilde{\pi}_E$, with respect to certain ramification conditions (see [Roh], [Roh04]), is an epimorphism

$$\pi_E\colon\ \mathrm{Gal}(\overline{K(j)}/\overline{K}(j)) \to \mathrm{SL}(2, \mathbb{Z}_p[[X]]).$$

Let $\widetilde{K}$ be the extension of K generated by all roots of unity of p-power order. In [Roh00a], [Roh00b], D. E. Rohrlich showed that π_E descends to an epimorphism

$$\varrho_E\colon\ \mathrm{Gal}(\overline{K(j)}/\widetilde{K}(j)) \to \mathrm{SL}(2, \mathbb{Z}_p[[X]]).$$

Notice that ϱ_E encapsulates arithmetic information which was not present in π_E.

Let A be an elliptic curve defined over K with j-invariant $j(A) \notin \{0, 1728\}$ and suppose that A coincides with the fiber of E at $j = j(A)$. Choose a place σ of $\overline{K(j)}$ extending the place $j = j(A)$ of $\widetilde{K}(j)$, and write D and I for the corresponding decomposition and inertia subgroups of $\mathrm{Gal}(\overline{K(j)}/\widetilde{K}(j))$. We "specialize" the representation ϱ_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 ϱ_E is unramified outside $\{0, 1728, \infty\}$, thus $\varrho_E|_D$ factors through $D/I \cong \mathrm{Gal}(\overline{K}/\widetilde{K})$. We obtain a representation

$$\varrho_A\colon\ \mathrm{Gal}(\overline{K}/\widetilde{K}) \to \mathrm{SL}(2, \mathbb{Z}_p[[X]]).$$

2000 *Mathematics Subject Classification*: Primary 11F80; Secondary 11G05.

Key words and phrases: p-adic Galois representations, deformations, surjectivity, elliptic curves.

If we write $\bar{\varrho}_A\colon\ \mathrm{Gal}(\overline{K}/\widetilde{K}) \to \mathrm{SL}(2,\mathbb{Z}_p)$ for the representation determined up to equivalence by the natural action of $\mathrm{Gal}(\overline{K}/\widetilde{K})$ on the Tate module of A, then, by construction, ϱ_A is a deformation of $\bar{\varrho}_A$, and in particular $\varrho_A|_{X=0} = \bar{\varrho}_A$. The image of $\bar{\varrho}_A$, 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 ϱ_A. Let

$$\widetilde{\varrho}_A\colon\ \mathrm{Gal}(\overline{K}/\widetilde{K}) \to \mathrm{SL}(2,\mathbb{F}_p)$$

be the representation induced by the Galois action on the points of order p on A. In [Roh04], Rohrlich proved in the case $K=\mathbb{Q}$ that if $\widetilde{\varrho}_A$ is surjective and $\nu_p(j(A)) = -1$ then ϱ_A is surjective, where ν_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 π of $\wp$, $\nu_\wp(\pi) = 1$ and $\nu_\wp(p) = e$, where $e = e(\wp \,|\, p)$ is the ramification index.

THEOREM 1.1. *If $\widetilde{\varrho}_A$ 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 ϱ_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

$$P\varrho_A\colon\ \mathrm{Gal}(\overline{K}/\widetilde{K}) \to \mathrm{PSL}(2,\Lambda)$$

because the only subgroup of $\mathrm{SL}(2,\Lambda)$ with projective image $\mathrm{PSL}(2,\Lambda)$ is the full group $\mathrm{SL}(2,\Lambda)$. We similarly define projective maps $P\varrho_E$ and $P\bar{\varrho}_A$. By the definition of ϱ_A, in order to verify the surjectivity of $P\varrho_A$ it suffices to show that the image via $P\varrho_E$ of the decomposition group D is the full group $\mathrm{PSL}(2,\Lambda)$.

The kernel of ϱ_E determines a fixed field $\mathbf{L}$, in particular $\mathrm{Gal}(\mathbf{L}/\widetilde{K}(j)) \cong \mathrm{PSL}(2,\mathbb{Z}_p[[X]])$. For $i \geq 1$, let $\mathbf{L}_i \subseteq \mathbf{L}$ be the fixed field determined by the kernel of the reduction map

$$\mathrm{Gal}(\mathbf{L}/\widetilde{K}(j)) \cong \mathrm{PSL}(2,\mathbb{Z}_p[[X]]) \to \mathrm{PSL}(2,\mathbb{Z}_p[[X]]/(p,X)^i).$$

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

A criterion of Boston ([Bos86, Prop. 2, p. 262]) reduces the problem to proving that the image of D in $\mathrm{Gal}(\mathbf{L}_2/\widetilde{K}(j))$ maps to all of $\mathrm{PSL}(2, \Lambda/(p, X)^2)$. Equivalently, one needs to show that $[\mathbf{L}_2 : \widetilde{K}(j)] = [\ell_2 : \widetilde{K}]$. Notice that the assumption on the surjectivity of $\widetilde{\varrho}_A$ implies that $\bar{\varrho}_A$ is surjective (see, for example, [Ser68, IV-23, Lemma 3]), and so is $P\bar{\varrho}_A$, the projectivization of $\bar{\varrho}_A$. It follows that $[\mathbf{L}_1 : \widetilde{K}(j)] = [\ell_1 : \widetilde{K}]$, therefore it suffices to prove that

$$[\mathbf{L}_2 : \mathbf{L}_1] = [\ell_2 : \ell_1]. \tag{1}$$

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 $m\colon R \to \mathbb{Z}$ 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. $s = (s_1, s_2) \equiv r \bmod p$, and put $a = a_s = p^{-1}(s_1, s_2)$. Then the symbol f_r represents any Siegel function g_a^{12} (see [KL81, p. 29]). If $s \in \mathbb{Z}^2$ is replaced by another lift of r then f_r is multiplied by a pth root of unity ([KL81, Remark on p. 30]), so the symbol $f_r(\tau)$ is only well defined up to pth roots of unity. For $m \in M$ we also define the symbolic mth 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 $\mathbf{L}_2/\mathbf{L}_1$ is generated by pth roots of Siegel units. More precisely, $\mathbf{L}_2 = \mathbf{L}_1(\{(f^m)^{1/p} : m \in N\})$.*

Using the previous theorem, Rohrlich reduces the proof of (1) to the following local statement (see [Roh04, pp. 19, 20]; the argument is valid in our case, by simply replacing $\mathbb{Q}$ by K). Since $\nu_\wp(j(A)) = -t < 0$ there is a unique Tate curve B over $K_\wp$ with $j(B) = j(A)$. Suppose there is an $m \in N$ 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 $\mathcal{O}_\wp$ be the ring on integers in $K_\wp$ and let q be the unique element of $\pi\mathcal{O}_\wp$ such that $j(q) = j(B)$, where π, as before, is a uniformizer of $\wp$. Proposition 8 of [Roh04] can be generalized to:

PROPOSITION 1.4. *There exists $m \in N$ such that*:

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

with $\mu \in \mathbb{Z}$, $u, w \in \mathcal{O}_\wp^\times$, and $v \in \mathcal{O}_\wp$. 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 ν. Note that $K_\wp(B[p^\nu]) = K_\wp(\zeta, q^{1/p^\nu})$ where ζ is a primitive p^νth root of unity (see [Lan87, Chapter 15, Theorem 3]).

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

Recall that by Proposition 1.4 we can write $\sigma(f)$ as $q^\mu(1-uq)(1-vq^2) = q^\mu(1+wq)$ with $\mu \in \mathbb{Z}$, $u, w \in \mathcal{O}_\wp^\times$, and $v \in \mathcal{O}_\wp$. We claim that $\alpha := q^{-\mu}\sigma(f)$ has degree p^ν in $K_\wp^\times / K_\wp^{\times p^\nu}$. 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 ξ a $p^{\nu-1}$th root of unity and $\xi = \beta^p\alpha^{-1} \in K_\wp$. Since $K_\wp$ cannot contain nontrivial pth 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 $b \in \mathcal{O}_\wp$, π 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

$$p(\nu_\wp(b)+1), \qquad i(\nu_\wp(b)+1)+e \quad \text{ with } 1 \le i \le p-1$$

and the minimum nonzero valuation is either $p(\nu_\wp(b)+1)$ or $\nu_\wp(b)+1+e$ (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 $e+1 \le t < ep/(p-1)$ and the fact that $\nu_\wp(b)+1+e < p(\nu_\wp(b)+1)$ implies that

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

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

REMARK 1.6. Using the $\wp$-adic logarithm and exponential maps one can prove that if $\nu_\wp(\gamma) > e + e/(p-1)$ 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 α in $K_\wp^\times / K_\wp^{\times p^\nu}$ is exactly p^ν. 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* $\mathrm{char}(L) = 0$, *and let ζ be a primitive p^νth root of unity. Let $M = L(\zeta)$. Then the following natural map is injective*:

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

We claim that Proposition 1.5 follows from the previous lemma (which we will prove below). Indeed, let $\mathbf{F}_\nu = K_\wp(\zeta)$ where ζ is a primitive p^νth root of unity. The natural map

$$K_\wp^\times / K_\wp^{\times p^\nu} \to \mathbf{F}_\nu^\times / \mathbf{F}_\nu^{\times p^\nu}$$

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

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

Hence $\sigma(f)^{1/p^\nu}$ has degree p^ν over $\mathbf{F}_\nu(q^{1/p^\nu}) = K_\wp(B[p^\nu])$, so $\sigma(f)^{1/p}$ has degree p over $K_\wp(B[p^\nu])$. ∎

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

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

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

$$0 \to H^1(\mathrm{Gal}(M/L), \mu_{p^\nu}) \to H^1(\mathrm{Gal}(\overline{L}/L), \mu_{p^\nu}) \to H^1(\mathrm{Gal}(\overline{M}/M), \mu_{p^\nu}).$$

Thus, in order to show that the map is injective, is enough to show that

$$H^1(\mathrm{Gal}(M/L), \mu_{p^\nu}) = 0.$$

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

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

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 $\psi : G \to \mathbb{Z}/p^\nu\mathbb{Z}$ be a cocycle. We wish to prove that ψ is actually a coboundary. Since $G \leq (\mathbb{Z}/p^\nu\mathbb{Z})^\times$, G is cyclic, that is, $G = \langle a \rangle$ for some a. Moreover, suppose that the order of G is n_0. Since ψ is a cocycle $\psi(1) = 0$ and, inductively, one can show that

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

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

Note that n_0, the order of G, divides $p^{\nu-1}(p-1)$, the order of $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$. First, suppose that $\gcd(n_0, p-1) > 1$. Then $a \neq 1 \bmod p$, since the elements which are congruent to 1 modulo p generate subgroups with order a power of p. Since $a \neq 1 \bmod p$, $a - 1 \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times$ and it follows that

$$(\clubsuit) \qquad \psi(a^t) = \left(\frac{a^t - 1}{a - 1}\right)\psi(a) = (a^t - 1)\,\frac{\psi(a)}{a-1} = a^t\,\frac{\psi(a)}{a-1} - \frac{\psi(a)}{a-1}$$

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

Only the case $n_0 = p^{\nu-m}$ remains, where m is an integer satisfying $1 \leq m < \nu$. This corresponds to the case $G = \{\alpha \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times : \alpha \equiv 1 \bmod p^m\}$. Thus a, the chosen generator of G, satisfies $a \equiv 1 + up^m \bmod p^\nu$, with $u \neq 0 \bmod p$. It suffices to show that $\psi(a) \equiv 0 \bmod p^m$ since that will imply that $\psi(a)/(a-1) \in \mathbb{Z}/p^\nu\mathbb{Z}$ and we can proceed as in ($\clubsuit$) to prove that ψ is a coboundary. We start with

$$0 \equiv \psi(1) \equiv \psi(a \cdot a^{p^{\nu-m}-1}) \equiv \psi(a) + a \cdot \psi(a^{p^{\nu-m}-1}) \bmod p^\nu$$

and

$$\psi(a^{p^{\nu-m}-1}) \equiv \left(\frac{a^{p^{\nu-m}-1} - 1}{a-1}\right)\psi(a) \bmod p^\nu,$$

thus

$$(\maltese) \qquad 0 \equiv \psi(a) + a\left(\frac{a^{p^{\nu-m}-1} - 1}{a-1}\right)\psi(a) \bmod p^\nu.$$

It is easy to see that $(1+up^\eta)^{p^\kappa} = 1 + u'p^{\eta+\kappa}$, with $u \equiv u' \bmod p$. Hence

$$a\left(\frac{a^{p^{\nu-m}-1} - 1}{a-1}\right) = \frac{a^{p^{\nu-m}} - 1}{a-1} - 1 \equiv p^{\nu-m} - 1 \bmod p^{\nu+1}$$

and the congruence remains true modulo p^ν. Finally, substituting in ($\maltese$) above, we obtain

$$0 \equiv \psi(a) + (p^{\nu-m} - 1)\psi(a) \equiv p^{\nu-m}\psi(a) \bmod p^{\nu}.$$

Therefore, $\psi(a) \equiv 0 \bmod p^m$, which concludes the proof of the lemma. ∎

We have thus finished the proof of Theorem 1.1. ∎

2. Example. Let $K = \mathbb{Q}(\sqrt{-11})$, $p = 11$ and set $\tau = (1 + \sqrt{-11})/2$. We write $\wp$ for the unique prime ideal of K lying above 11, thus the ramification index $e = e(\wp \,|\, p)$ is 2. Let A/K be the curve

$$A\colon\ y^2 + (2\tau - 1)y = x^3 + \tau x^2, \qquad j(A) = \frac{-61440 - 851968\tau}{11 \cdot 4931},$$

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

In particular, $t = -v_\wp(j(A)) = 2$. Note that $e = 2$ is not divisible by $p - 1 = 10$; $\gcd(p, t) = \gcd(11, 2) = 1$ and $ep/(p-1) = 11/5 > 2 = t$.

Hence it remains to check that the representation $\widetilde{\varrho}_A\colon\ \mathrm{Gal}(\overline{K}/\widetilde{K}) \to \mathrm{SL}(2, \mathbb{F}_p)$ is surjective. In [Ser72, Proposition 19], J.-P. Serre gives conditions for a subgroup G of $\mathrm{SL}(2, \mathbb{F}_p)$ to be the full group $\mathrm{SL}(2, \mathbb{F}_p)$. 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 $\mathrm{Tr}(s_1)^2 - 4\det(s_1)$ is a nonzero quadratic residue modulo p, and $\mathrm{Tr}(s_1) \neq 0 \bmod p$;*
(2) *G contains a matrix s_2 such that $\mathrm{Tr}(s_2)^2 - 4\det(s_2)$ is not a quadratic residue modulo p, and $\mathrm{Tr}(s_2) \neq 0 \bmod p$;*
(3) *G contains a matrix s_3 such that $u = \mathrm{Tr}(s_3)^2/\det(s_3)$ is not 0, 1, 2 or 4 modulo p and $u^2 - 3u + 1 \neq 0 \bmod p$.*

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

Let $G < \mathrm{SL}(2, \mathbb{F}_p)$ be the image of the representation $\widetilde{\varrho}_A$. 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 Δ_A, i.e. $S_A = \{3, 11, 3941\}$. Then, for every $\nu \notin S_A \cup \{\wp\}$, the image via $\widetilde{\varrho}_A$ of a Frobenius element $\pi_\nu \in \mathrm{Gal}(\overline{K}/\widetilde{K})$ is a matrix that we also denote by π_ν such that:

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

In order to conclude that $G = \mathrm{SL}(2, \mathbb{F}_p)$ 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 ν_5 be one of the prime ideals of K lying above 5 (so $\mathbf{N}(\nu_5) = 5$). The trace of the Frobenius automorphism is $a_{\nu_5} = -1$. Let $s_1 = \pi_{\nu_5}$. Then
$$\mathrm{Tr}(s_1)^2 - 4\det(s_1) \equiv (-1)^2 - 4 \cdot 5 \equiv -19 \equiv 5^2 \bmod 11.$$
- The prime number 13 is inert in K. Let ν_{13} be the prime ideal of K lying above 13 (so $\mathbf{N}(\nu_{13}) = 169$). The trace of the Frobenius automorphism is $a_{\nu_{13}} = 10$. Let $s_2 = \pi_{\nu_{13}}$. Then
$$\mathrm{Tr}(s_2)^2 - 4\det(s_2) \equiv (10)^2 - 4 \cdot 169 \equiv -576 \equiv 7 \bmod 11$$
and 7 is not a quadratic residue modulo 11.
- Let $s_3 = s_2$ and let $u = \mathrm{Tr}(s_3)^2/\det(s_3) \equiv \frac{100}{169} \equiv 3 \bmod 11$. Then $u^2 - 3u + 1 \equiv 1 \bmod 11$.

Therefore $\widetilde{\varrho}_A$ is surjective and all conditions of Theorem 1.1 have been verified, thus the map $\varrho_A\colon\ \mathrm{Gal}(\overline{K}/\widetilde{K}) \to \mathrm{SL}(2, \mathbb{Z}_{11}[[X]])$ is surjective. ∎

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

References

[Bos86] N. Boston, *Appendix to* [MW86], Compositio Math. 59 (1986), 261–264.

[Deu53] M. Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. IIa 1953, 85–94; *II*, ibid. 1955, 13–42; *III*, ibid. 1956, 37–76; *IV*, ibid. 1957, 55–80.

[Deu58] —, *Die Klassenkörper der komplexen Multiplikation*, in: Enzyklopädie der mathematischen Wissenschaften: Mit Einschluss ihrer Anwendungen, Band I-2, Heft 10, Teil II, Teubner, Stuttgart, 1958.

[KL81] D. S. Kubert and S. Lang, *Modular Units*, Grundlehren Math. Wiss. 244, Springer, New York, 1981.

[Lan87] S. Lang, *Elliptic Functions*, 2nd ed., Springer, New York, 1987.

[MW86] B. Mazur and A. Wiles, *On p-adic analytic families of Galois representations*, Compositio Math. 59 (1986), 231–264.

[Pari00] The PARI Group, PARI/GP, Version 2.1.1, 2000, Bordeaux, available from http://www.parigp-home.de/

[Roh] D. E. Rohrlich, *Universal deformation rings and universal elliptic curves*, unpublished note (available at his website).

[Roh00a] —, *False division towers of elliptic curves*, J. Algebra 229 (2000), 249–279.

[Roh00b] —, *A deformation of the Tate module*, ibid. 229 (2000), 280–313.

[Roh04] —, *Modular units and the surjectivity of a Galois representation*, J. Number Theory 107 (2004), 8–24.

[Rub99] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, in: Arithmetic Theory of Elliptic Curves (Cetraro, 1997), Lecture Notes in Math. 1716, Springer, Berlin, 1999, 167–234.

[Ser68] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, W. A. Benjamin, New York, 1968.

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. 88 (1968), 492–517.

Department of Mathematics
Colby College
8800 Mayflower Hill
Waterville, ME 04901, U.S.A.
E-mail: alozano@colby.edu

Received on 6.9.2004
and in revised form on 18.11.2004 (4844)