

Galois properties of elliptic curves with an isogeny

Ralph Greenberg[†]

1 Introduction

Suppose that E is an elliptic curve defined over \mathbf{Q} . Consider the homomorphism

$$\rho_{E,p} : G_{\mathbf{Q}} \longrightarrow \text{Aut}_{\mathbf{Z}_p}(T_p(E))$$

giving the action of $G_{\mathbf{Q}}$ on $T_p(E)$, the p -adic Tate module for E and for a prime p . If E doesn't have complex multiplication, then a famous theorem of Serre [Ser2] asserts that the image of $\rho_{E,p}$ has finite index in $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$ for all p and that the index is 1 for all but finitely many p . This paper concerns some of the exceptional cases where the index is not 1. If E has a cyclic isogeny of degree p defined over \mathbf{Q} , then $T_p(E)/pT_p(E)$ is isomorphic to $E[p]$ and has a 1-dimensional \mathbf{F}_p -subspace which is invariant under the action of $G_{\mathbf{Q}}$. Hence $\rho_{E,p}$ can't be surjective if such an isogeny exists. Our primary objective in this paper is to show that, under various assumptions, the image of $\rho_{E,p}$ is as large as allowed by the p -power isogenies defined over \mathbf{Q} .

Assume that E has a \mathbf{Q} -isogeny of degree p and let Φ denote its kernel. Let $\Psi = E[p]/\Phi$. The actions of $G_{\mathbf{Q}}$ on Φ and Ψ are given by two characters $\varphi, \psi : G_{\mathbf{Q}} \rightarrow \mathbf{F}_p^\times$, respectively. Our main result is the following.

Theorem 1. *Assume that $p \geq 7$. Assume also that $\varphi\psi^{-1}$ is not of order 2. Then the image of $\rho_{E,p}$ contains a Sylow pro- p subgroup of $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$.*

One can identify $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$ with $GL_2(\mathbf{Z}_p)$ by choosing a basis for $T_p(E)$ over \mathbf{Z}_p . One Sylow pro- p subgroup of $GL_2(\mathbf{Z}_p)$ is the set of matrices whose reduction modulo p is upper triangular and unipotent, which we will denote by $S_2(\mathbf{Z}_p)$ in this paper. The conclusion in the proposition is that, for some choice of basis, the image of $\rho_{E,p}$ contains $S_2(\mathbf{Z}_p)$. One can then determine the image of $\rho_{E,p}$ precisely. It is determined by the two characters φ and ψ .

[†]Research supported in part by National Science Foundation grant DMS-0200785.

It is worth pointing out that the validity of the assumptions or the conclusion in the above proposition is unaffected by quadratic twists, and so depends only on the j -invariant of the elliptic curve E . (Note that elliptic curves with automorphisms of order 3 or 4 are excluded since $p > 3$.) If E is replaced by the quadratic twist E_d for some squarefree integer d , then the characters φ and ψ themselves are changed to $\varphi\chi$ and $\psi\chi$, where χ is the character corresponding to the quadratic field $\mathbf{Q}(\sqrt{d})$.

If $K = \mathbf{Q}(\sqrt{-p})$ has class number 1 and E is an elliptic curve over \mathbf{Q} whose endomorphism ring R is an order in K , then E has an isogeny of degree p over \mathbf{Q} . For $p \geq 5$, this is so because it turns out that $\sqrt{-p} \in R$ and so E has an endomorphism defined over K of degree p whose kernel is $G_{\mathbf{Q}}$ -invariant. This endomorphism corresponds to a \mathbf{Q} -isogeny from E to the quadratic twist E_{-p} . One sees easily that the ratio $\varphi\psi^{-1}$ is the quadratic character corresponding to K . Thus, $\varphi\psi^{-1}$ has order 2. The image of $\rho_{E,p}$ is a two-dimensional p -adic Lie group and hence cannot even be open in $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$.

A famous theorem of Mazur [Maz] asserts that non-CM elliptic curves over \mathbf{Q} which have a \mathbf{Q} -isogeny of prime degree p exist only for p in the set $\{2, 3, 5, 7, 11, 13, 17, 37\}$. For such elliptic curves, it turns out that the order of $\varphi\psi^{-1}$ is at least 4 if $p \geq 11$ or if $p = 5$, as explained in remark 4.2.1. Something rather special happens for $p = 7$. There are non-CM elliptic curves over \mathbf{Q} with a \mathbf{Q} -isogeny of degree 7 where $\varphi\psi^{-1}$ has order 2. For example, the curves in the isogeny classes 637A and 637C have those properties. The set of j -invariants corresponding to such elliptic curves turns out to be infinite. In [GRS], Rubin, Silverberg, and the author will prove that the conclusion in theorem 1 is still true for all but finitely many of those j -invariants. The obvious exceptions are CM-elliptic curves. Up to quadratic twists, they are represented by the elliptic curves of conductor 49. There are four such elliptic curves. They have complex multiplication by either the maximal order of $\mathbf{Q}(\sqrt{-7})$ or the order $\mathbf{Z}[\sqrt{-7}]$, and correspond to two j -invariants. We do not know if any non-CM exceptions actually exist.

The assumption in theorem 1 that $p \geq 7$ is needed. The conclusion can certainly fail to be true if $p = 5$, even though the ratio $\varphi\psi^{-1}$ must then have order 4. (See remark 4.2.1.) For example, if E is defined by $y^2 + y = x^3 - x^2 - 10x - 20$, which is 11A1 in [Cre], then $E[5]$ is isomorphic to $\Phi \oplus \Psi$, a direct sum of two 1-dimensional \mathbf{F}_5 -representation spaces for $G_{\mathbf{Q}}$. Thus, E has two independent isogenies of degree 5 over \mathbf{Q} . Obviously, the image of $\rho_{E,5}$ cannot contain $S_2(\mathbf{Z}_5)$ in that case. The index of the image will clearly be divisible by 5. Fisher [Fis] shows that the image of $\rho_{E,5}$ contains the kernel of the map $\text{Aut}_{\mathbf{Z}_5}(T_5(E)) \rightarrow \text{Aut}_{\mathbf{F}_5}(E[5])$. The same thing is actually true for any elliptic curve over \mathbf{Q} with two independent \mathbf{Q} -isogenies of degree 5, a consequence of the last part of the following result.

Theorem 2. *Suppose that E has an isogeny of degree 5 defined over \mathbf{Q} . If none of the elliptic curves in the \mathbf{Q} -isogeny class of E has two independent isogenies of degree 5, then the image of $\rho_{E,5}$ contains a Sylow pro-5 subgroup of $\text{Aut}_{\mathbf{Z}_5}(T_5(E))$. Otherwise, the index of the image of $\rho_{E,5}$ in $\text{Aut}_{\mathbf{Z}_5}(T_5(E))$ is divisible by 5, but not by 25.*

Thus, the power of 5 dividing the index $[\text{Aut}_{\mathbf{Z}_5}(T_5(E)) : \text{im}(\rho_{E,5})]$ is either 1 or 5. In general, as we explain in section 2, if E is any non-CM elliptic curve and p is any prime, then the index $[\text{Aut}_{\mathbf{Z}_p}(T_p(E)) : \text{im}(\rho_{E,p})]$ depends only on the isogeny class of E over \mathbf{Q} . This fact is a special case of a very general observation. Apart from the cases considered in theorems 1 and 2, and restricting attention to elliptic curves with a \mathbf{Q} -isogeny of degree p , we have not been able to determine all the possibilities for that index. It is just the power of p which leads to serious difficulties, and the issue remains unresolved only for the primes $p \in \{2, 3, 7\}$.

The case $p = 7$ will be studied in [GRS]. However, for $p \in \{2, 3\}$, many of the ingredients in the proofs break down. Obviously, $\varphi\psi^{-1}$ will be of order 1 or 2. Furthermore, it is possible for elliptic curves over \mathbf{Q} to have cyclic \mathbf{Q} -isogenies of 2-power degree up to 16, which is one of the numerous difficulties for $p = 2$. As for $p = 3$, one can prove some sufficient conditions for the conclusion in theorem 1 to hold, but certain cases will not be covered. One natural question is the following: Is the index $[\text{Aut}_{\mathbf{Z}_p}(T_p(E)) : \text{im}(\rho_{E,p})]$ bounded when E varies over some class of non-CM elliptic curves? We wonder if this question is approachable when $p = 2$ and E is allowed to vary over all non-CM elliptic curves defined over \mathbf{Q} .

Theorem 1 was originally motivated by a project concerning non-commutative Iwasawa theory. It was of interest to construct p -adic Lie extensions whose Galois group is isomorphic to a specific subgroup H_∞ of $PGL_2(\mathbf{Z}_p)$, namely the subgroup represented by matrices which are upper triangular modulo p . Elliptic curves with an isogeny of degree p provides a possible source of such examples and the above proposition confirms this for $p \in \{7, 11, 13, 17, 37\}$. All one needs is for $\varphi\psi^{-1}$ to have order $p - 1$, and this can happen for each of the listed primes, as we explain in remark 4.2.1. The p -adic representations associated to modular forms give other examples for certain primes p . Results in [Gre] provide another source of such examples for many more primes.

The proof of theorem 1 actually also proves the first part of theorem 2. However, the proof of the second part of theorem 2 remained elusive for some time. I suspected at first that the index would sometimes be divisible by 25. Alice Silverberg and Karl Rubin provided me with a parametric description of the family of elliptic curves over \mathbf{Q} with two independent \mathbf{Q} -isogenies of degree 5. Attempts to use that description to find such examples failed. In the end, very helpful discussions with Silverberg and Rubin at UC Irvine led to completing the proof. Two crucial ingredients are due to them, namely that all the elliptic curves E in the above family are potentially ordinary at 5 and that this could force some prime $\ell \neq 5$ to have

ramification index divisible by 5 in a certain cyclic extension of \mathbf{Q} contained in $\mathbf{Q}(E[25])$. I am grateful for the invitation to visit UC Irvine and for the long and fruitful discussions about this topic that took place there.

A number of computations were useful as a guide. I am grateful to Robert Bradshaw for showing me how to use Sage for some of those computations. I also want to thank William Stein and Soroosh Yazdani for finding an elliptic curve with a \mathbf{Q} -isogeny of degree 13 where the ratio $\varphi\psi^{-1}$ turns out to have order 4. That example settles the only unresolved question concerning the possible orders of that ratio, as explained in remark 4.2.1.

Section 2 of this paper contains a proof of the fact that the index of the image of $\rho_{E,p}$ is an isogeny invariant. Various other useful isogeny invariants are also discussed. Section 3 contains the group theoretic ingredients that we need, mainly observations concerning the structure of certain pro- p subgroups of $GL_2(\mathbf{Z}_p)$. Theorems 1 and 2 are proved in sections 4 and 5, respectively. We prove more general versions for elliptic curves over a number field F , but special considerations when $F = \mathbf{Q}$, and when $p = 5$ in the case of theorem 2, are needed.

An earlier version of this paper contained a discussion of the p -adic representation $\rho_{\Delta,p}$ associated to the cusp form Δ of weight 12 and level 1 for the two primes $p = 691$ and $p = 7$. If T is a $G_{\mathbf{Q}}$ -invariant \mathbf{Z}_p -lattice in the underlying representation space for $\rho_{\Delta,p}$, then it turns out that T/pT is reducible for those primes, corresponding to the existence of certain classical congruences for Ramanujan's τ -function. (This connection is discussed in [Ser1].) The point of view of this paper shows that the conclusion in theorem 1 holds for $\rho_{\Delta,691}$. The case $p = 7$ is more interesting. We are able to determine the image of $\rho_{\Delta,7}$ modulo 7^2 , which turns out to be a subgroup of $GL_2(\mathbf{Z}/7^2\mathbf{Z})$ of order $6 \cdot 7^3$. Consequently, we can derive a certain classical congruence for $\tau(q)$ modulo 7^2 , where q is any prime. This congruence is given as (8.6) in [BeOn]. The discussion we had originally included sheds light on the nature of that congruence and why it exists. However, we then found that these things have already been discussed by Swinnerton-Dyer in [SwD]. His result concerning the image of $\rho_{\Delta,7}$ even gives a congruence for $\tau(q)$ modulo 7^3 , a refinement of the congruence modulo 7^2 . Our point of view is rather different than the one in [SwD] and should hopefully also be able explain that refinement. We hope to pursue this interesting example at another time.

2 Isogeny invariants.

Suppose that F is a number field and that E is an elliptic curve defined over F . We collect here a number of quantities defined in terms of E , but which turn out to depend only on the

F -isogeny class of E . The first was already mentioned in the introduction, but we consider it in a very general form.

2.1. The index of the image. As mentioned in the introduction, if E is a non-CM elliptic curve over \mathbf{Q} , p is any prime, and E' is isogenous to E over \mathbf{Q} , then the images of $\rho_{E,p}$ and $\rho_{E',p}$ in $GL_2(\mathbf{Z}_p)$ (after choosing bases for their respective Tate modules) have the same index. The analogous fact is true over any number field and follows from the following general result. Let \mathcal{F} be a finite extension of \mathbf{Q}_p and let \mathcal{O} be the maximal order in \mathcal{F} .

Proposition 2.1.1. *Suppose that V is a finite-dimensional \mathcal{F} -vector space and that G is a compact, open subgroup of $\text{Aut}_{\mathcal{F}}(V)$. If T and T' are any two G -invariant \mathcal{O} -lattices in V , then $[\text{Aut}_{\mathcal{O}}(T) : G] = [\text{Aut}_{\mathcal{O}}(T') : G]$.*

Proof. If one chooses a basis for V over \mathcal{F} , then $\text{Aut}_{\mathcal{F}}(V)$ is identified with $GL_n(\mathcal{F})$, where $n = \dim_{\mathcal{F}}(V)$. Thus, we can regard $\text{Aut}_{\mathcal{F}}(V)$ as a locally compact topological group. We can choose a left Haar measure μ on $\text{Aut}_{\mathcal{F}}(V)$ such that $\mu(G) = 1$. Both $\text{Aut}_{\mathcal{O}}(T)$ and $\text{Aut}_{\mathcal{O}}(T')$ can be regarded as subgroups of $\text{Aut}_{\mathcal{F}}(V)$. They are compact, open subgroups and contain G as a subgroup of finite index. Furthermore, if $\sigma \in \text{Aut}_{\mathcal{F}}(V)$ and T is any \mathcal{O} -lattice in V , then so is $\sigma(T)$. Thus, we have an action of $\text{Aut}_{\mathcal{F}}(V)$ on the set of \mathcal{O} -lattices in V . This action is easily seen to be transitive. Also, the stabilizer of T for this action is just $\text{Aut}_{\mathcal{O}}(T)$. Choosing σ so that $\sigma(T) = T'$, we have $\text{Aut}_{\mathcal{O}}(T') = \sigma \text{Aut}_{\mathcal{O}}(T) \sigma^{-1}$. We want to show that both of those open sets have the same measure with respect to μ .

It suffices to show that μ is a right Haar measure too. If $\sigma \in \text{Aut}_{\mathcal{F}}(V)$ and if U is any open subset of $\text{Aut}_{\mathcal{F}}(V)$, then we define the measure μ_{σ} by $\mu_{\sigma}(U) = \mu(U\sigma^{-1})$. Clearly, μ_{σ} is a left Haar measure on $\text{Aut}_{\mathcal{F}}(V)$ and so we have $\mu_{\sigma} = c(\sigma)\mu$ for some positive real constant $c(\sigma)$. The map c is a homomorphism from $\text{Aut}_{\mathcal{F}}(V)$ to the multiplicative group $\mathbf{R}_{pos}^{\times}$. It is trivial on the center of $\text{Aut}_{\mathcal{F}}(V)$ and hence factors through the corresponding quotient group, which is isomorphic to $PGL_n(\mathcal{F})$. However, $PGL_n(\mathcal{F})$ contains the simple, nonabelian group $PSL_n(\mathcal{F})$ as a normal subgroup of finite index. Hence c factors through a finite quotient group of $\text{Aut}_{\mathcal{F}}(V)$. Since $\mathbf{R}_{pos}^{\times}$ is torsion-free, c must be trivial. Therefore, it follows that μ is also right translation-invariant, i.e., μ is indeed a right Haar measure on $\text{Aut}_{\mathcal{F}}(V)$. As a consequence, we have

$$\mu(\text{Aut}_{\mathcal{O}}(T)) = \mu(\text{Aut}_{\mathcal{O}}(T')) \quad .$$

Every coset of G in $\text{Aut}_{\mathcal{O}}(V)$ has measure 1 with respect to μ and hence each of the above quantities is just the respective index in the proposition. ■

The assertion about elliptic curves follows by taking $\mathcal{F} = \mathbf{Q}_p$ and $V = T_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, which we denote by $V_p(E)$. Suppose that E is defined over a number field F and is non-CM.

Then G_F acts on $V_p(E)$. Let G denote the image of G_F in $\text{Aut}_{\mathbf{Q}_p}(V_p(E))$. Thus, G is a compact subgroup of $\text{Aut}_{\mathbf{Q}_p}(V_p(E))$. According to a theorem of Serre [Ser2], G is open. If E' is F -isogenous to E , then its Tate module $T_p(E')$ can be regarded as another G -invariant \mathbf{Z}_p -lattice in V . For the special case where $F = \mathbf{Q}$, and where E has an isogeny of degree p over \mathbf{Q} , it is not difficult to determine all the possibilities for the prime-to- p part of the index. It amounts to determining the possibilities for the degrees of the extension K/\mathbf{Q} , where $K = \mathbf{Q}(\Phi, \Psi)$, the fixed field for $\ker(\varphi) \cap \ker(\psi)$. Since $\mathbf{Q}(\mu_p) \subseteq K$, the degree in question is of the form $k(p-1)$, where k divides $p-1$. The prime-to- p part of the index is then $(p^2-1)/k$. It is not hard to show that $k \in \{1, 2, 3, 4, 6\}$. For $p \leq 7$, each k dividing $p-1$ can occur.

As an illustration, consider the three elliptic curves E over \mathbf{Q} of conductor 11, which we denote by E_1, E_2 , and E_3 (for 11A1, 11A2, and 11A3, respectively). They have \mathbf{Q} -isogenies of degree 5. One has $\Phi \cong \mu_5$ and $\Psi \cong \mathbf{Z}/5\mathbf{Z}$, or the reverse. In terms of a suitable basis for $T_5(E_i)$, where $1 \leq i \leq 3$, the image of $\rho_{E_i,5}$ turns out to be the subgroup G_i of $GL_2(\mathbf{Z}_5)$, where

$$G_1 = \begin{bmatrix} \mathbf{Z}_5^\times & 5\mathbf{Z}_5 \\ 5\mathbf{Z}_5 & 1 + 5\mathbf{Z}_5 \end{bmatrix}, \quad G_2 = \begin{bmatrix} \mathbf{Z}_5^\times & \mathbf{Z}_5 \\ 5^2\mathbf{Z}_5 & 1 + 5\mathbf{Z}_5 \end{bmatrix}, \quad G_3 = \begin{bmatrix} 1 + 5\mathbf{Z}_5 & \mathbf{Z}_5 \\ 5^2\mathbf{Z}_5 & \mathbf{Z}_5^\times \end{bmatrix} .$$

All of these subgroups have index 120 in $GL_2(\mathbf{Z}_5)$. The assertion that $\text{im}(\rho_{E_1,5}) = G_1$ is verified by Fisher in [Fis]. The fact that G_1 contains $\text{im}(\rho_{E_1,5})$ is clear because $E_1[5] \cong \Phi \oplus \Psi$. The equality then means that $[\text{Aut}_{\mathbf{Z}_5}(T_5(E_1)) : \text{im}(\rho_{E_1,5})] = 120$. Now E_2 and E_3 both have just one independent \mathbf{Q} -isogeny of degree 5, whose kernel Φ is isomorphic to μ_5 for E_2 and to $\mathbf{Z}/5\mathbf{Z}$ for E_3 . In addition, both have cyclic \mathbf{Q} -isogenies of degree 25. Thus, for $i \in \{2, 3\}$, it is clear that G_i at least contains the image of $\rho_{E_i,5}$. Equality then follows because G_i and $\text{im}(\rho_{E_i,5})$ both have the same index in $GL_2(\mathbf{Z}_5)$.

2.2. A more general version. Suppose that f is a cuspidal eigenform for $\Gamma_0(N)$ of weight k and some level $N \geq 1$. Consider the two-dimensional π -adic representation associated to f which was constructed by Deligne. Here π is a prime above p of the field generated by the Hecke eigenvalues of f . The representation is defined over the π -adic completion of that field, which we denote by \mathcal{F} . The determinant of that representation is then χ_p^{k-1} , where χ_p is the p -power cyclotomic character, and has values in \mathbf{Q}_p^\times . Therefore, if $\mathcal{F} \neq \mathbf{Q}_p$, then the image of the representation cannot be open. However, the image will be open in a certain subgroup, as was proved by Serre. One can easily generalize proposition 2.1.1 to cover such cases.

Suppose that $m \geq 0$. If V is as in proposition 2.1.1, and T is an \mathcal{O} -lattice in V , we define

$$\text{Aut}_{\mathcal{F}}^*(V) = \{ \sigma \in \text{Aut}_{\mathcal{F}}(V) \mid \det(\sigma) \in (\mathbf{Q}_p^\times)^m \}, \quad \text{Aut}_{\mathcal{O}}^*(T) = \text{Aut}_{\mathcal{F}}^*(V) \cap \text{Aut}_{\mathcal{O}}(T) .$$

The special case $m = 0$ will be of interest later. In that case, $\text{Aut}_{\mathcal{F}}^*(V)$ is isomorphic to $SL_n(\mathcal{F})$ and $\text{Aut}_{\mathcal{O}}^*(T)$ is isomorphic to $SL_n(\mathcal{O})$, where $n = \dim_{\mathcal{F}}(V)$. In general, note that if $\sigma \in \text{Aut}_{\mathcal{O}}(T)$, then $\sigma \in \text{Aut}_{\mathcal{O}}^*(T)$ if and only if $\det(\sigma) \in (\mathbf{Z}_p^\times)^m$. Assume that G is a compact, open subgroup of $\text{Aut}_{\mathcal{F}}^*(V)$. Let T and T' be G -invariant \mathcal{O} -lattices in V . Thus, $\text{Aut}_{\mathcal{O}}^*(T)$ and $\text{Aut}_{\mathcal{O}}^*(T')$ contain G as a subgroup of finite index. We will show that the corresponding indices are the same.

Let μ^* be a left Haar measure on $\text{Aut}_{\mathcal{F}}^*(V)$. We can assume that $\mu^*(G) = 1$. It is useful to note that $\text{Aut}_{\mathcal{F}}^*(V)$ is a normal subgroup of $\text{Aut}_{\mathcal{F}}(V)$. If $\sigma \in \text{Aut}_{\mathcal{F}}(V)$, then we define μ_σ^* by $\mu_\sigma^*(U) = \mu^*(\sigma U \sigma^{-1})$ for every open subset U of $\text{Aut}_{\mathcal{F}}^*(V)$. One sees easily that μ_σ^* is also a left Haar measure on $\text{Aut}_{\mathcal{F}}^*(V)$ and therefore one has $\mu_\sigma^* = c(\sigma)\mu^*$ for some positive real constant $c(\sigma)$. As previously, c defines a homomorphism from $\text{Aut}_{\mathcal{F}}(V)$ to \mathbf{R}_{pos}^\times , and must be trivial. Hence, $\mu_\sigma^* = \mu^*$. Also, it is clear that if $T' = \sigma(T)$, then

$$\text{Aut}_{\mathcal{O}}^*(T') = \sigma \text{Aut}_{\mathcal{O}}^*(T) \sigma^{-1} .$$

Since $\mu_\sigma^* = \mu^*$, those two sets have the same measure with respect to μ^* . As before, those measures coincide with the indices $[\text{Aut}_{\mathcal{O}}^*(T') : G]$ and $[\text{Aut}_{\mathcal{O}}^*(T) : G]$, respectively, which must therefore indeed be equal.

Consider the case where $m = 0$. Suppose we are in the situation of proposition 2.1.1. Then G is an open subgroup of $\text{Aut}_{\mathcal{F}}(V)$. Let $\text{Aut}_{\mathcal{F}}^{(0)}(V)$ denote the kernel of the determinant map $\det : \text{Aut}_{\mathcal{F}}(V) \rightarrow \mathcal{F}^\times$. We also write $\text{Aut}_{\mathcal{O}}^{(0)}(T)$ when T is an \mathcal{O} -lattice in V for the kernel of \det on $\text{Aut}_{\mathcal{O}}(T)$. Let $G^{(0)} = G \cap \text{Aut}_{\mathcal{F}}^{(0)}(V)$, the kernel of $\det|_G$. Then $G^{(0)}$ is an open subgroup of $\text{Aut}_{\mathcal{F}}^{(0)}(V)$. The above result shows that if T and T' are two G -invariant \mathcal{O} -lattices in V , then $[\text{Aut}_{\mathbf{Z}_p}^{(0)}(T) : G^{(0)}] = [\text{Aut}_{\mathbf{Z}_p}^{(0)}(T') : G^{(0)}]$.

2.3. An index formula. In the rest of this section, we just consider the p -adic Tate module for elliptic curves. We assume that E is an elliptic curve defined over a number field F and that p is any prime. As before, we let G be the image of G_F in $\text{Aut}_{\mathbf{Q}_p}(V_p(E))$. Of course, one simple invariant of the F -isogeny class for E is the isomorphism class of the group G . This is obvious because $G \cong \text{Gal}(F(E[p^\infty])/F)$, and the field $F(E[p^\infty])$ is unchanged by an F -isogeny. Now assume that E is non-CM. Serre's theorem [Ser2] implies that G is an open subgroup of $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$. Define $G^{(0)}$ and $\text{Aut}_{\mathbf{Z}_p}^{(0)}(T_p(E))$ as in section 2.2. Thus, $\text{Aut}_{\mathbf{Z}_p}^{(0)}(T_p(E))$ is isomorphic to $SL_2(\mathbf{Z}_p)$. Recalling that $\det \circ \rho_{E,p}$ is just the p -power cyclotomic character $\chi_p : G_F \rightarrow \mathbf{Z}_p^\times$ giving the action of G_F on μ_{p^∞} , we see that $\det(G)$, the image of G under the determinant map, is just $\chi_p(G_F)$. It follows that

$$(1) \quad [\text{Aut}_{\mathbf{Z}_p}(T_p(E)) : G] = [\text{Aut}_{\mathbf{Z}_p}^{(0)}(T_p(E)) : G^{(0)}][\mathbf{Z}_p^\times : \chi_p(G_F)] .$$

To see this, let $A = \text{Aut}_{\mathbf{Z}_p}(T_p(E))$ and $A^{(0)} = \text{Aut}_{\mathbf{Z}_p}^{(0)}(T_p(E))$. Let $B \subseteq A$ be the inverse image of $\det(G)$ under the map $\det : A \rightarrow \mathbf{Z}_p^\times$. Then one has $B = A^{(0)}G$ and one sees easily that the obvious map $A^{(0)}/G^{(0)} \rightarrow B/G$ of left coset spaces is a bijection. Also, it is obvious that $[A : B] = [\mathbf{Z}_p^\times : \chi_p(G_F)]$. The index relation (1) follows immediately. As a consequence, we see again that the index $[\text{Aut}_{\mathbf{Z}_p}^{(0)}(T_p(E)) : G^{(0)}]$ depends only on the F -isogeny class of E .

2.4. The center of the image. With the same assumptions and notation as in **2.3**, we now consider the index of the center of G in the center of $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$. We continue to assume that E is non-CM. The center of $\text{Aut}_{\mathbf{Q}_p}(V_p(E))$ is $\mathbf{Q}_p^\times I$, where I is the identity map on $V_p(E)$. Since G is open, the center of G is $G \cap \mathbf{Q}_p^\times I$. On the other hand, if E' is any elliptic curve which is F -isogenous to E , then the center of $\text{Aut}_{\mathbf{Z}_p}(T_p(E'))$ is simply $\mathbf{Z}_p^\times I$ and doesn't depend on E' . Thus, neither does the index of $G \cap (\mathbf{Q}_p^\times I) = G \cap (\mathbf{Z}_p^\times I)$ in $\mathbf{Z}_p^\times I$.

The prime-to- p part of the index $[\mathbf{Z}_p^\times I : G \cap (\mathbf{Z}_p^\times I)]$ is determined by the action of G_F on $E[p]$. It is equal to the index $[\mathbf{F}_p^\times I : \overline{G} \cap \mathbf{F}_p^\times I]$, where \overline{G} is the image of G_F in $\text{Aut}_{\mathbf{F}_p}(E[p])$. To justify this, first note that the kernel of the map $G \cap \mathbf{Z}_p^\times I \rightarrow \overline{G} \cap \mathbf{F}_p^\times I$ is a pro- p group. It therefore suffices to show the surjectivity of that map. We can assume that p is odd. To verify the surjectivity, note that the map $G \rightarrow \overline{G}$ (which is reduction modulo p) is surjective. Now suppose that $g \in G$ is such that its image \overline{g} in \overline{G} is in $\mathbf{F}_p^\times I$. Then $g = a(I + pA)$ for some $a \in \mathbf{Z}_p^\times$ and some endomorphism A of $T_p(E)$. Clearly, $g^{p^n} \rightarrow bI$ as $n \rightarrow \infty$, where b is the $(p-1)$ -st root of unity in $a + p\mathbf{Z}_p$. Thus, $bI \in G \cap \mathbf{Z}_p^\times I$ is also mapped to \overline{g} .

If E has an F -isogeny of degree p , then $[\mathbf{F}_p^\times I : \overline{G} \cap \mathbf{F}_p^\times I]$ is determined by φ and ψ . To see this, note that \overline{G} consists of upper triangular matrices (in terms of a suitable basis for $E[p]$). Also, if \overline{G} contains an element of the form au , where $a \in \mathbf{F}_p^\times$ and u is upper triangular and unipotent, then \overline{G} contains $(au)^p = aI$. It follows that $\overline{G} \cap \mathbf{F}_p^\times I$ consists of elements aI , where $a = \varphi(\sigma) = \psi(\sigma)$ for some $\sigma \in G_F$. That is, $a = \varphi(\sigma)$, where $\sigma \in \ker(\varphi\psi^{-1})$. Thus, $\overline{G} \cap \mathbf{F}_p^\times I$ is isomorphic to $\varphi(\ker(\varphi\psi^{-1}))$. For example, if $E(F)$ has a point of order p , then one can take φ to be trivial and we have $[\mathbf{F}_p^\times I : \overline{G} \cap \mathbf{F}_p^\times I] = p - 1$.

2.5. The set of Galois-invariant cyclic subgroups. Suppose that E is a non-CM elliptic curve defined over F . Another invariant of the F -isogeny class of E is the cardinality of the set of G_F -invariant cyclic subgroups of $E[p^\infty]$. We denote that set by $\mathcal{C}_{E,p}(F)$. To explain the F -isogeny invariance of $|\mathcal{C}_{E,p}(F)|$, first note that if Θ is in that set, then there exist an elliptic curve E' defined over F and an F -isogeny $f : E \rightarrow E'$ whose kernel is Θ . The degree of the isogeny is $|\Theta|$, a power of p . Of course, Θ determines the F -isomorphism class of $E' = E/\Theta$. A standard type of argument shows that, conversely, the F -isomorphism class of E' determines Θ . We present this next.

Let $f' : E' \rightarrow E$ denote the dual isogeny to f . Let $\iota : E \rightarrow E$ be the identity map. Let $p^t = |\Theta|$. The endomorphism of E defined by multiplication by p^t is $p^t \iota$. Thus, $f' \circ f = p^t \iota$. Suppose that $g : E \rightarrow E'$ is another F -isogeny with a cyclic kernel of p -power order. Then, $f' \circ g$ is an endomorphism of E of p -power degree. Hence, $f' \circ g = \pm p^u \iota$ for some $u \geq 0$. Assume that $u \geq t$. Then $f' \circ (f \circ p^{u-t} \iota) = \pm f' \circ g$. This implies that $f \circ p^{u-t} \iota = \pm g$. Since $\ker(g)$ is cyclic, it follows that $u = t$ and that $f = \pm g$. Therefore, $\ker(g) = \Theta$. A similar argument works if $t \leq u$, using the assumption that $\ker(f)$ is cyclic.

We say that two elliptic curves E and E' defined over F are (F, p) -isogenous if there exists an isogeny $E \rightarrow E'$ whose degree is a power of p . This defines an equivalence relation. The F -isogeny class for E is partitioned into (F, p) -isogeny classes, all of the same cardinality as one easily sees. Also, it is easy to verify that if E and E' are (F, p) -isogenous, then there exists an isogeny $f : E \rightarrow E'$ with cyclic kernel. It follows from these observations that there is a 1-1 correspondence between the set $\mathcal{C}_{E,p}(F)$ and the (F, p) -isogeny class of E . Therefore, the cardinality of $\mathcal{C}_{E,p}(F)$ indeed depends only on the F -isogeny class of E .

The orders of the groups that occur in $\mathcal{C}_{E,p}(F)$ may depend on E itself. Suppose that the largest order of a group in $\mathcal{C}_{E',p}(F)$, as E' varies over the F -isogeny class of E , is p^e . That is, at least one elliptic curve F -isogenous to E has a cyclic G_F -invariant subgroup Θ of order p^e , but none of those curves have a cyclic G_F -invariant subgroup of order p^{e+1} . Obviously, e is determined just by the F -isogeny class of E . Since Θ will have $e + 1$ distinct subgroups, all G_F -invariant, it follows that $|\mathcal{C}_{E,p}(F)| \geq e + 1$. We will prove the following result.

Proposition 2.5.1. *Assume that $\varphi \neq \psi$. We then have $|\mathcal{C}_{E,p}(F)| = e + 1$.*

Proof. Equality is trivial if $e = 0$ and so we assume that $e \geq 1$. Thus, E has a cyclic F -isogeny of degree p with kernel Φ , say. Nothing is lost if we just assume that $E[p^\infty]$ itself has a cyclic G_F -invariant subgroup Θ of order p^e and that $\Theta[p] = \Phi$. It follows that all the composition factors in Θ are isomorphic to Φ . The G_F -module $E[p^e]$ has $2e$ -composition factors, half isomorphic to Φ and half isomorphic to Ψ . It follows that all the composition factors in $E[p^e]/\Theta$ will be isomorphic to Ψ . Suppose that we have $|\mathcal{C}_{E,p}(F)| > e + 1$. Then $E[p^e]$ would contain a cyclic G_F -invariant subgroup Ξ not contained in Θ . The composition factors for Ξ must include Ψ at least once. But they are all isomorphic to $\Xi[p]$. Hence $\Xi[p] \cong \Psi$ and so $\Xi[p] \neq \Theta[p]$. It follows that $E[p]$ has two distinct G_F -invariant subgroups of order p , Φ itself and another which we simply denote by Ψ . Thus, the sequence (5) splits.

Now $E[p^{e+1}]/E[p]$ is isomorphic to $E[p^e]$ and therefore contains a G_F -invariant subgroup isomorphic to Θ . Since $E[p]/\Psi \cong \Phi$, it follows that $E[p^{e+1}]/\Psi$ has a G_F -invariant subgroup Θ' of order p^{e+1} whose composition factors are all isomorphic to Φ . Note that Θ' can be regarded as a subgroup of $E'[p^{e+1}]$, where $E' = E/\Psi$. It is G_F -invariant. Since $E'[p]$ has a composition factor isomorphic to Ψ , it follows that $\Theta'[p] \neq E'[p]$. Hence Θ' is cyclic.

Its order is p^{e+1} . This contradicts the definition of e , showing that we do indeed have the equality $|\mathcal{C}_{E,p}(F)| = e + 1$. ■

The assumption that $\varphi \neq \psi$ in proposition 2.5.1 is needed. Consider the elliptic curves in the \mathbf{Q} -isogeny class 15A in [Cre]. That isogeny class has cardinality 8 and all the curves in it are related by cyclic \mathbf{Q} -isogenies of 2-power degree. The kernels have orders 1, 2, 4, 8, and 16. None have order 2^7 . Of course, we still have $|\mathcal{C}_{E,2}(\mathbf{Q})| = 8$. Following Cremona's ordering, we give here the number of cyclic subgroups of each of the orders 2, 4, 8, 16, respectively, for each of the curves in 15A. The numbers are 3, 4, 0, 0 for A1, 3, 2, 2, 0 for A2 and A3, and 1, 2, 2, 2 for the remaining five curves.

With proposition 2.5.1 in mind, we want to single out two types of behavior concerning (F, p) -isogeny when E has a nontrivial F -isogeny of degree p . These types are determined just by the F -isogeny class of E . We continue to assume that $\varphi \neq \psi$.

Type I. We just require that $e = 1$. That is, the (F, p) -isogeny class of E contains just one other elliptic curve E' . Both E and E' have just one independent cyclic isogeny of degree p , and none of degree p^2 .

Type II. This just means that $e = 2$. That is, the (F, p) -isogeny class for E contains three elliptic curves, at least one of which has a cyclic F -isogeny of degree p^2 . Suppose that E_1 is one such elliptic curve and that Θ_1 is a cyclic, G_F -invariant subgroup of $E_1[p^2]$ of order p^2 . Of course, $E_2 = E_1/\Theta_1$ will be another such elliptic curve since the image of $E_1[p^2]$ in $E_2[p^2]$ is G_F -invariant and cyclic of order p^2 . Finally, $E_3 = E_1/\Theta_1[p]$ has two independent F -isogenies of degree p . One with kernel $\Theta_1/\Theta_1[p]$, the other with kernel $E_1[p]/\Theta_1[p]$. Those two subgroups of $E_3[p]$ are obviously distinct. Now E_3 cannot also have a cyclic isogeny of degree p^2 because $|\mathcal{C}_{E_3,p}(F)| = 3$. For the same reason, E_1 and E_2 cannot have two independent F -isogenies of degree p .

If E has an F -isogeny of degree p , but none of the elliptic curves in the F -isogeny class of E has a cyclic F -isogeny of degree p^2 , then that F -isogeny class is of type **I**. If E has either a cyclic F -isogeny of degree p^2 or two independent F -isogenies of degree p , but none of the elliptic curves in the F -isogeny class of E has a cyclic F -isogeny of degree p^3 , then that F -isogeny class is of type **II**.

As an illustration, if $p = 5$, then the \mathbf{Q} -isogeny class 11A is of type **II** and the \mathbf{Q} -isogeny class 38B is of type **I**. Both of those \mathbf{Q} -isogeny classes consist of one $(\mathbf{Q}, 5)$ -isogeny class. The \mathbf{Q} -isogeny class 66C has cardinality 4 and is a union of two $(\mathbf{Q}, 5)$ -isogeny classes. It is of type **I**. For $p \geq 7$, elliptic curves over \mathbf{Q} can't have cyclic \mathbf{Q} -isogenies of degree p^2 , a result due to Mazur [Maz], Ligozat [Lig], and Kenku [Ken1,2]. Thus, if E is defined over \mathbf{Q} and has a cyclic \mathbf{Q} -isogeny of degree p , then the \mathbf{Q} -isogeny class of E is of type **I**.

3 Pro- p subgroups of $GL_2(\mathbf{Z}_p)$.

3.1. *A Sylow pro- p subgroup.* We just assume at first that p is an odd prime. Let $U_2(\mathbf{F}_p)$ denote the group of upper triangular, unipotent matrices in $GL_2(\mathbf{F}_p)$, which is a cyclic subgroup of order p . Of course, $U_2(\mathbf{F}_p)$ is a Sylow p -subgroup of $GL_2(\mathbf{F}_p)$. Let

$$S_2(\mathbf{Z}_p) = \begin{bmatrix} 1 + p\mathbf{Z}_p & \mathbf{Z}_p \\ p\mathbf{Z}_p & 1 + p\mathbf{Z}_p \end{bmatrix} .$$

Then $S_2(\mathbf{Z}_p)$ is the inverse image of $U_2(\mathbf{F}_p)$ under the obvious map $GL_2(\mathbf{Z}_p) \rightarrow GL_2(\mathbf{F}_p)$. The kernel of that map will be denoted by $C_2(p)$. Since $C_2(p)$ is a pro- p group, it follows that $S_2(\mathbf{Z}_p)$ is a Sylow pro- p subgroup of $GL_2(\mathbf{Z}_p)$. Furthermore, $S_2^{(0)}(\mathbf{Z}_p) = S_2(\mathbf{Z}_p) \cap SL_2(\mathbf{Z}_p)$ is a Sylow pro- p subgroup of $SL_2(\mathbf{Z}_p)$. The following result will be a crucial part of proving theorem 1.

Proposition 3.1.1. *Suppose that $A, B \in S_2^{(0)}(\mathbf{Z}_p)$, that $C \in S_2(\mathbf{Z}_p)$, and that these matrices have the following properties:*

- (a) *The image of A in $GL_2(\mathbf{F}_p)$ is nontrivial.*
- (b) *The image of B in $GL_2(\mathbf{F}_p)$ is trivial and the image of B in $GL_2(\mathbf{Z}/p^2\mathbf{Z})$ is not upper triangular.*
- (c) *$\text{Det}(C) \not\equiv 1 \pmod{p^2}$.*

Then $\{A, B\}$ generates a dense subgroup of $S_2^{(0)}(\mathbf{Z}_p)$ and $\{A, B, C\}$ generates a dense subgroup of $S_2(\mathbf{Z}_p)$.

The conclusion gives what we call “*topological generating sets*” for the pro- p groups $S_2^{(0)}(\mathbf{Z}_p)$ and $S_2(\mathbf{Z}_p)$. Note that property (a) means that the image of A in $U_2(\mathbf{F}_p)$ generates that group. Letting $M_2(\mathbf{Z}_p)$ denote the ring of 2×2 matrices over \mathbf{Z}_p , $M_2(\mathbf{F}_p)$ denote that ring over \mathbf{F}_p , and I_2 denote the 2×2 identity matrix, property (b) means that $B = I_2 + pX$, where $X \in M_2(\mathbf{Z}_p)$ and the image of X in $M_2(\mathbf{F}_p)$ is not upper triangular. Finally, property (c) simply means that $\text{det}(C) = 1 + px$, where $x \in \mathbf{Z}_p, x \notin p\mathbf{Z}_p$. If we replace C by CA^u for a suitable u , we can assume that $C \in C_2(p)$.

The proof is based on the following lemma. It is a special case of proposition 5.3.1 in [Gre], which is the analogue for $n \times n$ matrices, but can also be easily verified directly when $n = 2$. However, we will state it here in a more detailed form. Let $M^{(0)}(\mathbf{F}_p)$ denote the subspace of $M_2(\mathbf{F}_p)$ consisting of matrices of trace 0. The group $U_2(\mathbf{F}_p)$ acts on both of these \mathbf{F}_p -vector spaces by conjugation. Hence, they can be regarded as modules over the group

ring $\mathbf{F}_p[U_2(\mathbf{F}_p)]$. The matrix with a 1 in row i , column j , and 0's for its other entries will be denoted by E_{ij} . We will use this notation for that specific matrix over various rings.

Lemma 3.1.2. *Suppose that $p \geq 3$. Let $U_2(\mathbf{F}_p)$ act on $M^{(0)}(\mathbf{F}_p)$ by conjugation. Then $M^{(0)}(\mathbf{F}_p)$ is a cyclic module over $\mathbf{F}_p[U_2(\mathbf{F}_p)]$. The only proper $\mathbf{F}_p[U_2(\mathbf{F}_p)]$ -submodules of $M^{(0)}(\mathbf{F}_p)$ are $\mathbf{F}_p E_{12}$ and $\mathbf{F}_p E_{12} + \mathbf{F}_p(E_{11} - E_{22})$. If $m \in M^{(0)}(\mathbf{F}_p)$ is not upper triangular, then m is a generator of $M^{(0)}(\mathbf{F}_p)$ as an $\mathbf{F}_p[U_2(\mathbf{F}_p)]$ -module.*

The ring $\mathbf{F}_p[U_2(\mathbf{F}_p)]$ is a local ring. If u is a generator for $U_2(\mathbf{F}_p)$, then the nontrivial ideals in $\mathbf{F}_p[U_2(\mathbf{F}_p)]$ are powers of the maximal ideal J , the ideal generated by $u - 1$. It is the augmentation ideal of $\mathbf{F}_p[U_2(\mathbf{F}_p)]$. Thus, the first assertion in the lemma implies that $M^{(0)}(\mathbf{F}_p) \cong \mathbf{F}_p[U_2(\mathbf{F}_p)]/J^3$. The proper submodules mentioned in the lemma correspond to J^2/J^3 and J/J^3 , respectively, in that isomorphism. The second submodule has \mathbf{F}_p -dimension 2 and is just the subspace of upper triangular matrices in $M^{(0)}(\mathbf{F}_p)$. The first is 1-dimensional and is just the subspace of “strictly” upper triangular matrices.

Proof of proposition 3.1.1. The argument is based on the above lemma and the isomorphisms (3) below, which we state in a more general form than we now need. They concern the Frattini quotients $\widetilde{\Pi}$ of certain pro- p groups Π . (We recall the general definition of the Frattini quotient below.) Let $C_2(p^k) = I_2 + p^k M_2(\mathbf{Z}_p)$ for any $k \geq 1$ and let $C_2^{(0)}(p^k)$ denote the intersection of $C_2(p^k)$ with $SL_2(\mathbf{Z}_p)$. Their Frattini quotients are given by

$$(2) \quad \widetilde{C_2(p^k)} = C_2(p^k)/C_2(p^{k+1}), \quad \widetilde{C_2^{(0)}(p^k)} = C_2^{(0)}(p^k)/C_2^{(0)}(p^{k+1}) \quad .$$

We then have the isomorphisms

$$(3) \quad \widetilde{C_2(p^k)} \cong M_2(\mathbf{F}_p), \quad \widetilde{C_2^{(0)}(p^k)} \cong M_2^{(0)}(\mathbf{F}_p) \quad ,$$

which are induced by the map sending $I_2 + p^k X$ to the image of X in $M_2(\mathbf{F}_p)$, where X is in $M_2(\mathbf{Z}_p)$. This map is an isomorphism of \mathbf{F}_p -representation spaces for $GL_2(\mathbf{F}_p)$, where $GL_2(\mathbf{F}_p)$ acts on $M_2(\mathbf{F}_p)$ by conjugation. As for the action on $\widetilde{C_2(p^k)}$, note first that $GL_2(\mathbf{Z}/p^{k+1}\mathbf{Z})$ acts on that group by conjugation. One sees easily that this action factors through the quotient group $GL_2(\mathbf{F}_p)$, and thus defines an action of that group on $\widetilde{C_2(p^k)}$.

Now $B \in C_2^{(0)}(p)$. Let \widetilde{B} denote its image in $\widetilde{C_2^{(0)}(p)}$. Lemma 3.1.2 and the assumption about B imply that the image of \widetilde{B} under the map (3) generates $M_2^{(0)}(\mathbf{F}_p)$ as an $\mathbf{F}_p[U_2(\mathbf{F}_p)]$ -module. It follows that the orbit of \widetilde{B} under the action of $U_2(\mathbf{F}_p)$ generates the group $\widetilde{C_2^{(0)}(p)}$. The Burnside Basis Theorem (which is recalled below) then implies that the set

$\{A^i B A^{-i}\}_{0 \leq i < p}$ is a topological generating set for $C_2^{(0)}(p)$. Consequence, it indeed follows that $\{A, B\}$ is a topological generating set for $S_2^{(0)}(\mathbf{Z}_p)$. Finally, consider the determinant map $\det : S_2(\mathbf{Z}_p) \rightarrow 1 + p\mathbf{Z}_p$. This map is surjective and the image of C under that map generates $1 + p\mathbf{Z}_p$ topologically. The final assertion in the proposition then follows. ■

3.2. Ω -groups and the Ω -type. A more detailed discussion of this topic can be found in sections 2 and 5 of [Gre]. We assume that Ω is a finite subgroup of the group of diagonal matrices in $GL_2(\mathbf{Z}_p)$. Thus, Ω is an abelian group and its exponent divides $p - 1$. Suppose that Π is a pro- p subgroup of $GL_2(\mathbf{Z}_p)$ and that $\alpha\Pi\alpha^{-1} = \Pi$ for all α in Ω . We then have a homomorphism $\Omega \rightarrow \text{Aut}(\Pi)$, where $\text{Aut}(\Pi)$ denotes the group of continuous automorphisms of Π . This homomorphism is defined by letting $\alpha \in \Omega$ act on Π by conjugation. Thus, in the terminology of [Gre], Π is an Ω -group. For example, $S_2(\mathbf{Z}_p)$ and $S_2^{(0)}(\mathbf{Z}_p)$ are Ω -groups, as are the groups $C_2(p^k)$ and $C_2^{(0)}(p^k)$ for $k \geq 1$. Furthermore, letting Ω acts on $M_2(\mathbf{F}_p)$ and $M_2^{(0)}(\mathbf{F}_p)$ by conjugation, it is obvious that the isomorphisms (3) are Ω -equivariant.

In general, suppose that Π is a topologically finitely generated pro- p group. We let $\tilde{\Pi}$ denote the Frattini quotient of Π . Thus, $\tilde{\Pi} = \Pi/\Theta$, where Θ is the intersection of all closed subgroups of Π of index p . Thus, $\tilde{\Pi}$ is a finite-dimensional \mathbf{F}_p -vector space. According to the Burnside Basis Theorem, a set of elements $\Sigma = \{\pi_1, \dots, \pi_t\}$ in Π is a topological generating set for Π (i.e., the subgroup generated by Σ is dense in Π) if and only if the set $\tilde{\Sigma} = \{\tilde{\pi}_1, \dots, \tilde{\pi}_t\}$ is a generating set for $\tilde{\Pi}$. Here we denote the image of an element $\pi \in \Pi$ under the map $\Pi \rightarrow \tilde{\Pi}$ by $\tilde{\pi}$. The minimal cardinality of a topological generating set for Π is $\dim_{\mathbf{F}_p}(\tilde{\Pi})$.

Suppose that we have a homomorphism $\Omega \rightarrow \text{Aut}(\Pi)$, where $\text{Aut}(\Pi)$ denotes the group of continuous automorphisms of Π . We then say that Π is an Ω -group. The Frattini quotient $\tilde{\Pi}$ is then a representation space for Ω over \mathbf{F}_p . Since Ω is abelian and has exponent dividing $p - 1$, $\tilde{\Pi}$ is isomorphic to a direct sum of 1-dimensional representation spaces of Ω . Each such summand corresponds to an \mathbf{F}_p^\times -valued character ξ of Ω and occurs as a constituent in $\tilde{\Pi}$ with a certain multiplicity $m_\xi(\tilde{\Pi})$. That multiplicity is the \mathbf{F}_p -dimension of the maximal subspace $\tilde{\Pi}^{(\xi)}$ of $\tilde{\Pi}$ on which Ω acts by the character ξ . Let $\hat{\Omega} = \text{Hom}(\Omega, \mathbf{F}_p^\times)$, the group of \mathbf{F}_p^\times -valued characters of Ω . The isomorphism class of $\tilde{\Pi}$ as a representation space for Ω is determined by the multiplicities $(m_\xi(\tilde{\Pi}))_{\xi \in \hat{\Omega}}$, which we will refer to as the Ω -type of Π .

We can identify $\hat{\Omega}$ with $\text{Hom}(\Omega, \mathbf{Z}_p^\times)$. Suppose that Π is an Ω -group, $\pi \in \Pi$, $\xi \in \hat{\Omega}$, and $\alpha \in \Omega$. It makes sense to write $\pi^{\xi(\alpha)}$, which is an element in the closure $\overline{\langle \pi \rangle}$ of the cyclic subgroup of Π generated by π . We say that π is a ξ -element if $\alpha(\pi) = \pi^{\xi(\alpha)}$ for all $\alpha \in \Omega$. We also say that such an element π is an Ω -element if we don't specify ξ . That just means that the subgroup $\overline{\langle \pi \rangle}$ is Ω -invariant. The first part of the following lemma is proposition 2.1.1 in [Gre]. The second part then follows from the Burnside Basis Theorem. Essentially the

same result is also proven in [Bos]. (See page 184.) This lemma will be useful in verifying the hypotheses in proposition 3.1.1.

Lemma 3.2.1. *If $x \in \tilde{\Pi}$ is a ξ -element, then there exists a ξ -element $\pi \in \Pi$ such that $\tilde{\pi} = x$. In particular, Π has a minimal topological generating set consisting of Ω -elements.*

Now we consider certain special elements in $GL_2(\mathbf{Z}_p)$. We also use the notation E_{ij} for the matrices defined just as before, but with entries in \mathbf{Z}_p . Let $D_2(\mathbf{Z}_p)$ denote the subgroup of diagonal matrices in $GL_2(\mathbf{Z}_p)$. If $d = d_1E_{11} + d_2E_{22}$ is in $D_2(\mathbf{Z}_p)$, if $a \in \mathbf{Z}_p$, and if $1 \leq i, j \leq 2$, then

$$(4) \quad d(I_2 + aE_{ij})d^{-1} = I_2 + d_i d_j^{-1} a E_{ij} = (I_2 + aE_{ij})^{d_i d_j^{-1}}.$$

These identities are trivial if $i = j$ and easily verified for $i \neq j$. In the latter case, the third expression is defined because the closure of the subgroup generated by $I_2 + aE_{ij}$ is a pro- p group. Note also that if $b \in \mathbf{Z}_p$, then $I_2 + baE_{ij} = (I_2 + aE_{ij})^b$ when $i \neq j$. One verifies this first for $b \in \mathbf{Z}$, and then for $b \in \mathbf{Z}_p$ using a continuity argument.

Now any $\alpha \in \Omega$ can be written as $\alpha = \varphi(\alpha)E_{11} + \psi(\alpha)E_{22}$, and we have thus defined two elements φ and ψ in $\widehat{\Omega}$. With this notation, α is the diagonal matrix whose diagonal entries are $\varphi(\alpha), \psi(\alpha)$, in order. Now if we take $\Pi = S^{(0)}(\mathbf{Z}_p)$, then the set $\{A, B\}$, where $A = I_2 + E_{12}$ and $B = I_2 + pE_{21}$, is a topological generating set consisting of Ω -elements. Those two elements do indeed generate Π topologically, as follows from proposition 3.1.1. It is clear from (4) that A and B are Ω -elements and that the corresponding characters are $\varphi\psi^{-1}$ and its inverse $\psi\varphi^{-1}$, respectively. The Ω -type of $S^{(0)}(\mathbf{Z}_p)$ is thus determined. As for $\Pi = S_2(\mathbf{Z}_p)$, that group is the direct product $S_2^{(0)}(\mathbf{Z}_p) \times (1 + p\mathbf{Z}_p)I_2$, the corresponding Frattini quotient has \mathbf{F}_p -dimension 3, and the set $\{I_2 + E_{12}, I_2 + pE_{21}, (1 + p)I_2\}$ will topologically generate $S_2(\mathbf{Z}_p)$. The last generator is fixed by Ω and so is a ξ_0 -element, where ξ_0 denotes the trivial character of Ω . Thus, the Ω -type of $S_2(\mathbf{Z}_p)$ is given by the characters $\varphi\psi^{-1}$, $\psi\varphi^{-1}$, and ξ_0 . Of course, in general, these characters are not necessarily distinct.

3.3. Other pro- p subgroups of $GL_2(\mathbf{Z}_p)$. Finally, we will list and discuss various other pro- p groups which occur later in this paper. All of them are invariant under conjugation by $D_2(\mathbf{Z}_p)$ and hence are Ω -groups.

For any $k \geq 1$, define $T_2(p^k) = \begin{bmatrix} 1 + p\mathbf{Z}_p & \mathbf{Z}_p \\ p^k\mathbf{Z}_p & 1 + p\mathbf{Z}_p \end{bmatrix}$. Thus, $T_2(p^k)$ is the subgroup of $S_2(\mathbf{Z}_p)$ consisting of matrices which are upper triangular modulo p^k . We let $T_2^{(0)}(p^k)$ denote its intersection with $SL_2(\mathbf{Z}_p)$. Obviously, $T_2(p) = S_2(\mathbf{Z}_p)$. The case where $k = 2$ will be

especially useful. Note that $T_2(p^2)$ is a subgroup of $S_2(\mathbf{Z}_p)$ of index p and hence is a normal subgroup. There is an action of Ω on the quotient group $S_2(\mathbf{Z}_p)/T_2(p^2)$. That group is cyclic and is generated by the image of $I_2 + pE_{21}$, and so Ω acts by the character $\psi\varphi^{-1}$ on it. Of course, the same statements obviously apply to the quotient group $S_2^{(0)}(\mathbf{Z}_p)/T_2^{(0)}(p^2)$. In contrast, note that $C_2^{(0)}(p)$ is a subgroup of $S_2^{(0)}(\mathbf{Z}_p)$ of index p , the quotient group $S_2^{(0)}(\mathbf{Z}_p)/C_2^{(0)}(p)$ (which can be identified with $U_2(\mathbf{F}_p)$) is generated by the image of $I_2 + E_{12}$, and Ω therefore acts on that quotient group by the character $\varphi\psi^{-1}$.

For any $k \geq 1$, let $N_2(p^k) = \begin{bmatrix} 1 + p^k\mathbf{Z}_p & \mathbf{Z}_p \\ p^k\mathbf{Z}_p & 1 + p^k\mathbf{Z}_p \end{bmatrix}$. We have $N_2(p) = T_2(p) = S_2(\mathbf{Z}_p)$.

Assume now that $k \geq 2$. Then $N_2(p^k)$ is the kernel of the obvious homomorphism from $T_2(p^k)$ to $((1 + p\mathbf{Z}_p)/(1 + p^k\mathbf{Z}_p))^2$ (projection to the diagonal). That homomorphism is surjective and hence $N_2(p^k)$ is a normal subgroup of $T_2(p^k)$ of index $p^{2(k-1)}$. In particular, the quotient $T_2(p^2)/N_2(p^2)$ is a 2-dimensional \mathbf{F}_p -vector space on which Ω acts trivially. Let $N_2^{(0)}(p^k) = N_2(p^k) \cap SL_2(\mathbf{Z}_p)$ for $k \geq 1$. Then, $N_2^{(0)}(p^k)$ is a normal subgroup of $T_2^{(0)}(p^k)$. The \mathbf{F}_p -dimension of $T_2^{(0)}(p^2)/N_2^{(0)}(p^2)$ is 1 and the action of Ω is again trivial.

4 The proof of theorem 1.

4.1. A general result. We assume that E is an elliptic curve defined over a number field F and that E has an isogeny of degree p defined over F , where p is an odd prime. Thus, we have an exact sequence

$$(5) \quad 0 \longrightarrow \Phi \longrightarrow E[p] \longrightarrow \Psi \longrightarrow 0$$

of \mathbf{F}_p -representation spaces for G_F . The actions of G_F on Φ and Ψ are given by two homomorphisms $\varphi, \psi : G_F \rightarrow \mathbf{F}_p^\times$. We can regard φ and ψ as \mathbf{F}_p^\times -valued characters of $\Omega = \text{Gal}(K/F)$, where $K = F(\Phi, \Psi)$, the fixed field for $\ker(\varphi) \cap \ker(\psi)$. Thus, Ω is a finite, abelian group of exponent dividing $p-1$. Also, we have $F(\mu_p) \subseteq K$ and $\varphi\psi = \omega$, where $\omega : \Omega \rightarrow \mathbf{F}_p^\times$ gives the action of Ω on μ_p . We can lift φ, ψ , and ω uniquely to \mathbf{Z}_p^\times -valued characters of Ω . The liftings will also be denoted by φ, ψ , and ω .

Let $G = \text{Gal}(F(E[p^\infty])/F)$. The representation $\rho_{E,p}$ giving the action of G_F on $T_p(E)$ induces a faithful representation of G . To simplify the discussion, we will identify G with its image under $\rho_{E,p}$. It is clear that $P = \text{Gal}(F(E[p^\infty])/K)$ is a normal, pro- p subgroup of G and that $G/P \cong \Omega$. The Schur-Zassenhaus theorem implies that G contains a subgroup isomorphic to Ω , unique up to conjugacy. We will fix a choice of such a subgroup, which

we also denote by Ω . Thus, since G has been identified with a subgroup of $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$, so is Ω . Assume that $\varphi \neq \psi$. Regarding (5) as an exact sequence of representation spaces for Ω , it splits and we have a unique splitting homomorphism. Thus, $E[p] \cong \Phi \oplus \Psi$, and the two summands are just $e_\varphi E[p]$ and $e_\psi E[p]$, where e_φ and e_ψ are the idempotents in $\mathbf{F}_p[\Omega]$ for φ and ψ , respectively. We also regard φ and ψ as \mathbf{Z}_p^\times -valued characters and the corresponding idempotents as elements of $\mathbf{Z}_p[\Omega]$. We can then decompose $T_p(E)$ as a direct sum of $e_\varphi T_p(E)$ and $e_\psi T_p(E)$. Both those summands are free \mathbf{Z}_p -modules of rank 1. We let v_φ and v_ψ be generators. Thus, $\{v_\varphi, v_\psi\}$ is a \mathbf{Z}_p -module basis for $T_p(E)$. Their images \bar{v}_φ and \bar{v}_ψ under the canonical homomorphism $T_p(E) \rightarrow E[p]$ will be generators for $e_\varphi E[p]$ and $e_\psi E[p]$, respectively.

We use the basis $\{v_\varphi, v_\psi\}$ to identify $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$ with $GL_2(\mathbf{Z}_p)$. Thus, we now regard G, P , and Ω as subgroups of $GL_2(\mathbf{Z}_p)$. If $\alpha \in \Omega$, then α is identified with the diagonal matrix whose diagonal entries are $\varphi(\alpha)$ and $\psi(\alpha)$, in order, just as in section 3. We will use the notation from that section for various other subgroups of $GL_2(\mathbf{Z}_p)$. It is clear that P is a subgroup of $S_2(\mathbf{Z}_p)$. Letting $P^{(0)}$ denote the intersection of P with $SL_2(\mathbf{Z}_p)$, we have $P^{(0)} \subseteq S_2^{(0)}(\mathbf{Z}_p)$. Since $\Omega \subset G$ and P is a normal subgroup of G , the pro- p groups P and $P^{(0)}$ are both invariant under conjugation by Ω and hence are Ω -groups.

Recall that we are assuming that $\varphi \neq \psi$. Hence, $\varphi\psi^{-1}$ has order at least 2. We will prove the following result.

Proposition 4.1.1. *Assume that the exact sequence (5) of \mathbf{F}_p -representation spaces for G_F is nonsplit, that E has no cyclic isogeny of degree p^2 over F , and that $\varphi\psi^{-1}$ is of order at least 3. Then $P^{(0)} = S_2^{(0)}(\mathbf{Z}_p)$. In addition, if we assume that $[F(\mu_{p^2}) : F]$ is divisible by p , then $P = S_2(\mathbf{Z}_p)$.*

Note that the assumption about $\varphi\psi^{-1}$ implies that $p \geq 5$. Also, the first two assumptions are obviously necessary for the conclusions to hold.

Proof. For brevity, let $\xi = \varphi\psi^{-1}$. Then $\xi^{-1} = \psi\varphi^{-1}$ and we are assuming that $\xi \neq \xi^{-1}$. The assumption that (5) is nonsplit means that the image of P in $GL_2(\mathbf{F}_p)$ is the cyclic group $U_2(\mathbf{F}_p)$. Thus, viewing P as an Ω -group, there is a surjective Ω -homomorphism $\tilde{P} \rightarrow U_2(\mathbf{F}_p)$. Now Ω acts on $U_2(\mathbf{F}_p)$ by the character ξ , as pointed out in section 3.3. Hence Ω acts on a certain quotient of \tilde{P} by ξ . It follows that $e_\xi \tilde{P}$ maps surjectively onto that quotient. Therefore, \tilde{P} has a nontrivial ξ -element x whose image in $U_2(\mathbf{F}_p)$ generates that group. By lemma 3.2.1, P itself has a ξ -element A such that $\tilde{A} = x$. It is clear that $\det(A) = 1$ since if we let Ω acts trivially on $1 + p\mathbf{Z}_p$, then the determinant map is an Ω -homomorphism from $S_2(\mathbf{Z}_p)$ to $1 + p\mathbf{Z}_p$. Hence $A \in P^{(0)}$.

The additional assumption that E has no cyclic \mathbf{Q} -isogeny of degree p^2 implies that $P \not\subseteq T_2(p^2)$. Hence P maps surjectively to the quotient group $S_2(\mathbf{Z}_p)/T_2(p^2)$, which is cyclic of order p . As mentioned in section 3.3, Ω acts on that quotient group by the character ξ^{-1} . Therefore, Ω acts on the corresponding quotient of \tilde{P} by the character ξ^{-1} . Now $e_{\xi^{-1}}\tilde{P}$ maps surjectively onto that quotient. As before, lemma 3.2.1 then implies that P has a ξ^{-1} -element B with a nontrivial image in $S_2(\mathbf{Z}_p)/T_2(p^2)$. Thus, B is not upper triangular modulo p^2 . Just as for A , we have $B \in P^{(0)}$. Also, the image of B in $U_2(\mathbf{F}_p)$ will be trivial since Ω acts by ξ on that group, and by ξ^{-1} on the image of B . (This is where the assumption that $\xi \neq \xi^{-1}$ is needed.) It follows that $B \in C_2(p)$.

The elements $A, B \in P^{(0)}$ satisfy the properties (a) and (b) stated in proposition 3.1.1. It follows that they generate $S_2^{(0)}(\mathbf{Z}_p)$ topologically. Since $P^{(0)}$ is a closed subgroup of $S_2^{(0)}(\mathbf{Z}_p)$, we must indeed have $P^{(0)} = S_2^{(0)}(\mathbf{Z}_p)$. As for the final assertion, the additional assumption implies that there exists a matrix $C \in P$ such that $\det(C)$ is a topological generator of $1 + p\mathbf{Z}_p$. Thus, C satisfies property (c) in proposition 3.1.1. The equality $P = S_2(\mathbf{Z}_p)$ therefore follows. Alternatively, one can use formula (1). \blacksquare

4.2. The proof of theorem 1. We assume that E is defined over \mathbf{Q} and has a \mathbf{Q} -isogeny of degree p , that $p \geq 7$, and that $\varphi\psi^{-1}$ is not of order 2. We must just verify the assumptions in proposition 4.1.1 when we take $F = \mathbf{Q}$. We then can conclude that the image of $\rho_{E,p}$ contains $S_2(\mathbf{Z}_p)$, which is what theorem 1 asserts.

First of all, we have $\varphi\psi = \omega$, the character giving the action of $G_{\mathbf{Q}}$ on μ_p . Since ω is odd, it is clear that $\varphi \neq \psi$. Hence $\xi = \varphi\psi^{-1}$ has order at least 3. It therefore suffices to verify the two assumptions in proposition 3.1 about isogenies. It is known that elliptic curves over \mathbf{Q} cannot have \mathbf{Q} -isogenies of degree p^2 when $p \geq 7$. That assertion follows from [Maz] for most primes, from [Lig] or [Ken2] for $p = 7$, and from [Ken1] for $p = 13$. This justifies one assumption. However, it also follows that the \mathbf{Q} -isogeny class of E is of type **I** in the terminology of section 2.5. Consequently, the sequence (5) is nonsplit, verifying the other assumption.

Remark 4.2.1. If $p \equiv 1 \pmod{4}$, then the hypothesis in theorem 1 that $\varphi\psi^{-1}$ not be of order 2 is automatically satisfied. To see this, note that

$$(6) \quad (\varphi\psi^{-1})^{\frac{p-1}{2}} = (\omega\psi^{-2})^{\frac{p-1}{2}} = \omega^{\frac{p-1}{2}},$$

which is a character of order 2. Hence the order of $\varphi\psi^{-1}$ is not a divisor of $\frac{p-1}{2}$, and so must be divisible by the highest power of 2 dividing $p-1$. In particular, the hypothesis in theorem 1 concerning $\varphi\psi^{-1}$ is automatically satisfied for $p \in \{13, 17, 37\}$, and also for $p = 5$. Those are the only primes satisfying $p \equiv 1 \pmod{4}$ for which cyclic \mathbf{Q} -isogenies of degree p

can exist according to the results in [Maz]. The statements about j -invariants and isogenies mentioned in the rest of this remark are also from Mazur's paper.

If E has good, ordinary reduction or multiplicative reduction at p , then $\varphi\psi^{-1}$ has order $p-1$. This is clear since the restriction of that ratio to the inertia subgroup of $G_{\mathbf{Q}_p}$ will then coincide with $\omega^{\pm 1}$. Now $\varphi\psi^{-1}$ is unchanged by quadratic twists and so depends only on the j -invariant of E (at least for $p \geq 5$). In particular, for $p = 37$, there are just two j -invariants of elliptic curves over \mathbf{Q} which have \mathbf{Q} -isogenies of degree 37. They are represented by two elliptic curves E of conductor 1225. Since $37 \nmid 1225$, E has good reduction at 37. The reduction must be ordinary because the $G_{\mathbf{Q}_{37}}$ -module $E[37]$ is reducible. Hence $\varphi\psi^{-1}$ has order 36 when $p = 37$.

There are two j -invariants of elliptic curves over \mathbf{Q} with a cyclic \mathbf{Q} -isogeny of degree 17. In this case, (6) implies that $\varphi\psi^{-1}$ has order 16. There are infinitely many distinct j -invariants for elliptic curves E over \mathbf{Q} with a \mathbf{Q} -isogeny of degree $p = 13$. The order of $\varphi\psi^{-1}$ is either 4 or 12. If E has good reduction at 13, or multiplicative reduction, then $\varphi\psi^{-1}$ has order 12, as explained above. The first such examples are the curves in the isogeny classes 147B,C in [Cre]. In response to my query, W. Stein and S. Yazdani found the example $y^2 = x^3 - 338x + 2392$, a curve of conductor $2^8 \cdot 5 \cdot 13^2$. It has a \mathbf{Q} -isogeny of degree 13 and $\varphi\psi^{-1}$ turns out to have order 4.

As for $p = 11$, any non-CM elliptic curve over \mathbf{Q} with a \mathbf{Q} -isogeny of degree 11 is isomorphic to a quadratic twist of one of the two elliptic curves in the isogeny class 121A. Thus, it suffices to consider an elliptic curve E in 121A. The characters φ and ψ can only be ramified at 11 for such an E . Hence, those characters are powers of ω , say $\varphi = \omega^a$ and $\psi = \omega^b$, where $a, b \geq 0$ satisfy $a + b \equiv 1 \pmod{11}$. As a consequence, we obtain a congruence of the form

$$a_q(E) \equiv q^a + q^b \pmod{11}$$

for all primes $q \neq 11$. Here $a_q(E)$ is the Hecke eigenvalue associated to q . One can interpret $a_q(E)$ as the trace of $\rho_{E,11}(g_q)$, where g_q is the Frobenius element for a prime of $\mathbf{Q}(E[11^\infty])$ lying above q . The above congruence follows immediately from that interpretation. The table of Hecke eigenvalues in [Cre] shows that $a_2(E) = -1$. One deduces easily that $\{\varphi, \psi\} = \{\omega^2, \omega^9\}$. Thus, the ratio $\varphi\psi^{-1}$ has order 10 and theorem 1 applies to E , and to all quadratic twists of E , when $p = 11$.

In summary, for $p \geq 11$, the assumption in theorem 1 that $\varphi\psi^{-1}$ is not of order 2 is automatically satisfied if E is non-CM. In contrast, if $p = 7$, then $\varphi\psi^{-1}$ can have order 6 or order 2, both cases occurring for infinitely many distinct j -invariants. Of course, theorem 1 applies if the order is 6. It will be shown in [GRS] that the conclusion in theorem 1 is still valid for $p = 7$ when $\varphi\psi^{-1}$ has order 2, except for finitely many of the possible j -invariants. The elliptic curves of conductor 49 give obvious exceptions because they have

complex multiplication. Apart from the two j -invariants for elliptic curves of conductor 49, it is likely that no other exceptions exist. \diamond

Remark 4.2.2. Our first proof of theorem 1 was somewhat different. It also made use of the same results from [Gre] that have been already used here. The original argument showed that $P^{(0)}$ must contain the specific set

$$\{I_2 + E_{12}, I_2 + pE_{21}\} ,$$

and therefore the subgroup $S_2^{(0)}(\mathbf{Z}_p)$ topologically generated by that set. The additional ingredient in that argument will be useful itself and so we give it here as a lemma.

Lemma. *Suppose that $\xi = \varphi\psi^{-1}$ has order at least 3. If A is a ξ -element of $S_2(\mathbf{Z}_p)$, then $A = (I_2 + E_{12})^a$ for some $a \in \mathbf{Z}_p$. If B is a ξ^{-1} -element of $S_2(\mathbf{Z}_p)$, then $B = (I_2 + pE_{21})^b$ for some $b \in \mathbf{Z}_p$.*

Proof. Suppose that $\chi \in \widehat{\Omega}$ has order at least 3, that C is a χ -element in $S_2(\mathbf{Z}_p)$, and that $C \neq I_2$. Let λ be an eigenvalue for C in $\overline{\mathbf{Q}_p}$. Then λ is a principal unit in $\mathbf{Q}_p(\lambda)$, an extension of \mathbf{Q}_p of degree at most 2. Also, for any $\alpha \in \Omega$, the matrices C and $C^{\chi(\alpha)}$ are conjugate and hence $\lambda^{\chi(\alpha)}$ is also an eigenvalue for C . Since the character χ has at least three distinct values, and C has at most two distinct eigenvalues, it follows that λ is a p -power root of unity. Also, the assumption about ξ implies that $p > 3$ and therefore that $[\mathbf{Q}_p(\mu_p) : \mathbf{Q}_p] = p - 1 > 2$. Therefore, we must have $\lambda = 1$. That is, C must be a unipotent matrix.

Since $C \neq I_2$, the kernel of $C - I_2$ has \mathbf{Z}_p -rank 1. Let v be a generator of that kernel. All the eigenvectors for C are in $\mathbf{Z}_p v$. Suppose that $\alpha \in \Omega$. The fact that C is an Ω -element implies that αv is also an eigenvector for C and hence a multiple of v . Therefore, $\mathbf{Z}_p v$ is an Ω -invariant \mathbf{Z}_p -submodule of $T_p(E)$. It follows that v is either in $\mathbf{Z}_p v_\varphi$ or in $\mathbf{Z}_p v_\psi$. That is, either v_φ or v_ψ is an eigenvector for C . More precisely, either $Cv_\varphi = v_\varphi$ or $Cv_\psi = v_\psi$. In the first case, C is upper triangular and hence of the form $C = I_2 + aE_{12}$ for some $a \in \mathbf{Z}_p$. In this case, $\chi = \xi$. In the second case, C is lower triangular and hence of the form $C = I_2 + aE_{21}$ for some $a \in \mathbf{Z}_p$. But $C \in S_2(\mathbf{Z}_p)$ and hence $a = pb$ for some $b \in \mathbf{Z}_p$. In this case, $\chi = \xi^{-1}$. The stated assertions about A and B follow immediately. \blacksquare

It is worth pointing out the following example which shows the importance of the assumption about $\xi = \varphi\psi^{-1}$ in the above lemma. Suppose that ξ has order 2. Thus, Ω consists of matrices which are scalar multiples of $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ or of I_2 . One can verify that the matrix

$$(7) \quad A = \begin{bmatrix} \sqrt{1+p} & 1 \\ p & \sqrt{1+p} \end{bmatrix}$$

is a ξ -element of $S_2(\mathbf{Z}_p)$. The images of A in $S_2(\mathbf{Z}_p)/C^{(0)}(p)$ and in $S_2(\mathbf{Z}_p)/T_2(p^2)$ are generators of each of those groups. Thus, A has a nontrivial image in $U_2(\mathbf{F}_p)$ and A is not upper triangular modulo p^2 . In this example, Ω acts by ξ on a 2-dimensional \mathbf{F}_p -subspace W of $\widetilde{S_2(\mathbf{Z}_p)}$. The images of $C_2(p)$ and of $T_2(p^2)$ are 1-dimensional subspaces of W as is the subspace generated by the image of A , but they are all different subspaces.

The above lemma justifies the statements mentioned at the beginning of this remark. The matrix A occurring in the proof of proposition 4.1.1 must have the form $A = (I_2 + E_{12})^a$. Since A has a nontrivial image in $U_2(\mathbf{F}_p)$, we have $a \in \mathbf{Z}_p^\times$. Since $P^{(0)}$ contains A , it also contains $I_2 + E_{12}$. The matrix B occurring in the proof has the form $B = (I_2 + pE_{21})^b$. Since B is not upper triangular modulo p^2 , we have $b \in \mathbf{Z}_p^\times$. Since $P^{(0)}$ contains B , it also contains $I_2 + pE_{21}$. \diamond

Remark 4.2.3. Suppose that $p \geq 3$, that $F = \mathbf{Q}$, that E has a \mathbf{Q} -isogeny of degree p , and that we actually have $P = S_2(\mathbf{Z}_p)$. The last assumption implies easily that the \mathbf{Q} -isogeny class of E is of type **I**. Let $E' = E/\Phi$, the other elliptic curve in the (\mathbf{Q}, p) -isogeny class of E . Thus, $E'[p]$ contains a $G_{\mathbf{Q}}$ -invariant subgroup Ψ' isomorphic to Ψ as a $G_{\mathbf{Q}}$ -module. Note that both $\mathbf{Q}(E[p])$ and $\mathbf{Q}(E'[p])$ are cyclic extensions of $K = \mathbf{Q}(\Phi, \Psi)$ of degree p .

Let $K_\infty = \mathbf{Q}(E[p^\infty])$. Now P was defined at first as a subgroup of $G = \text{Gal}(K_\infty/\mathbf{Q})$, namely $P = \text{Gal}(K_\infty/K)$. Thus, we can interpret the Frattini quotient as a Galois group: $\tilde{P} = \text{Gal}(L/K)$, where L is a finite extension of K and $\text{Gal}(L/K)$ is an abelian group of exponent p . Our assumption implies that \tilde{P} has \mathbf{F}_p -dimension 3. Hence L is a compositum of three cyclic extensions of K of degree p . In fact, we can take the three extensions of K which are the fixed fields for the subgroups $C_2(p)$, $T_2(p^2)$ (both of which have index p in P), and the unique subgroup of P which contains $P^{(0)}$ and has index p . That last subfield of K_∞ is easy to identify. It is just $K(\mu_{p^2})$.

To be clear, we will write C and T for the subgroups of P which have been identified with $C_2(p)$ and $T_2(p^2)$, respectively. Thus, C and T are Galois groups. It is obvious that the fixed field for C is $\mathbf{Q}(E[p])$. As for T , it turns out that its fixed field is $\mathbf{Q}(E'[p])$. There are several ways to explain this. With the set-up of this section, we can argue as follows. Let Θ denote the image of $\mathbf{Z}_p v_\phi$ in $E[p^2]$. Thus, Θ is cyclic of order p^2 , contains Φ , and is invariant under the action of T . Let Φ' denote the image of Θ under the \mathbf{Q} -isogeny $E \rightarrow E'$. Then Φ' is also invariant under the action of T . Clearly, Φ' has order p and hence the pro- p group T acts trivially on Φ' . Also, Ω acts on Φ' by the character φ . Since $p \geq 3$, we have $\psi \neq \varphi$, and hence $\Phi' \neq \Psi'$. Also, P must act trivially on Ψ' . It follows that T acts trivially on both Φ' and Ψ' and therefore on $E'[p]$. Thus, the fixed field for T contains $\mathbf{Q}(E'[p])$. The two fields have the same degree over \mathbf{Q} and hence must coincide.

Thus, assuming that $P = S_2(\mathbf{Z}_p)$, the above discussion shows that

$$(8) \quad L = \mathbf{Q}(E[p], E'[p], \mu_{p^2})$$

and that the action of Ω on $\text{Gal}(L/K)$ has the characters $\varphi\psi^{-1}$, $\psi\varphi^{-1}$, and ξ_0 as constituents. More precisely, Ω acts by $\varphi\psi^{-1}$ on $\text{Gal}(\mathbf{Q}(E[p])/K)$, by $\psi\varphi^{-1}$ on $\text{Gal}(\mathbf{Q}(E'[p])/K)$, and by ξ_0 on $\text{Gal}(K(\mu_{p^2})/K)$. If $\varphi\psi^{-1}$ has order at least 3, then those three characters are distinct. If $\varphi\psi^{-1}$ has order 2, then that character has multiplicity 2 for the action of Ω on $\text{Gal}(L/K)$. One should note that $\mathbf{Q}(E'[p]) \neq \mathbf{Q}(E[p])$ under the assumption that $P = S_2(\mathbf{Z}_p)$. This is clear simply because $T_2(p^2) \neq C_2(p)$, and hence $T \neq C$.

The above facts about L/K have interesting consequences in certain situations. As an extreme example (which can occur when $p \in \{3, 7\}$), suppose that φ and ψ are powers of ω and that $\xi = \varphi\psi^{-1}$ has order 2. Suppose also that the image of $\rho_{E,p}$ contains a Sylow pro- p subgroup of $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$, which means that $P = S_2(\mathbf{Z}_p)$. We then have $K = \mathbf{Q}(\mu_p)$ and ξ occurs with multiplicity 2 when $\Omega = \text{Gal}(K/\mathbf{Q})$ acts on $\text{Gal}(L/K)$. Now let L_p be the maximal extension of K contained in L which is unramified outside the unique prime of K above p . If p is a regular prime (or even just a properly irregular prime), then a standard Kummer theory argument shows that when one views $\text{Gal}(L_p/K)$ as an \mathbf{F}_p -representation space for Ω , an odd character ξ of Ω occurs with multiplicity at most 1. Therefore, in this hypothetical situation, it would follow that at least one prime $\ell \neq p$ is ramified in L/K . This means that the ramification index for ℓ in at least one of the extensions $\mathbf{Q}(E[p])/\mathbf{Q}$ or $\mathbf{Q}(E'[p])/\mathbf{Q}$ is equal to p . \diamond

5 The case $p = 5$.

5.1. A general result. We first prove a result for $p \geq 5$. We will follow the set-up and notation of section 4. In particular, we continue to assume that $\varphi \neq \psi$, we identify Ω with a subgroup of $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$ and we pick a basis $\{v_\varphi, v_\psi\}$ for $T_p(E)$ as before. We then identify $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$ with $GL_2(\mathbf{Z}_p)$. We have various subgroups of $GL_2(\mathbf{Z}_p)$ to consider, which we continue to denote by G , P , $P^{(0)}$, etc., defined exactly as previously. The terminology and observations in section 2.5 will be helpful. The hypotheses in proposition 4.1.1 are satisfied if the (F, p) -isogeny class of E is of type **I** and $\varphi\psi^{-1}$ has order at least 3. As for type **II**, we have the following result.

Proposition 5.1.1. *Assume that the F -isogeny class of E is of type **II** and that $\varphi\psi^{-1}$ has order at least 3. Then the image of $\rho_{E,p}$ contains $C_2^{(0)}(p^2)$. Furthermore, we have*

$$[S_2^{(0)}(\mathbf{Z}_p) : P^{(0)}] = p^i \quad ,$$

where $1 \leq i \leq 2$. If we assume in addition that $[F(\mu_{p^2}) : F]$ is divisible by p , then we have $[S_2(\mathbf{Z}_p) : P] = p^i$, with the same value of i as above, and the image of $\rho_{E,p}$ contains $C_2(p^2)$.

Proof. First of all, assume that (5) is nonsplit. According to section 2.5, E will have a cyclic F -isogeny of degree p^2 , but none of degree p^3 . Furthermore, Ω acts on the kernel of that isogeny by φ and hence that kernel is generated by the image of v_φ in $E[p^2]$. It follows that $P \subseteq T_2(p^2)$, but $P \not\subseteq T_2(p^3)$. Now, $T_2(p^3)$ has index p in $T_2(p^2)$ and hence must be a normal subgroup. The action of Ω on the quotient $T_2(p^2)/T_2(p^3)$ is by the character ξ^{-1} . This last statement is clear since $I_2 + p^2E_{21}$ is a ξ^{-1} -element and its image generates that quotient. Now P maps surjectively to $T_2(p^2)/T_2(p^3)$ and therefore \tilde{P} has a nontrivial quotient on which Ω acts by ξ^{-1} . It follows that $e_{\xi^{-1}}\tilde{P}$ is mapped surjectively to $T_2(p^2)/T_2(p^3)$. Thus, \tilde{P} contains a ξ^{-1} -element x whose image in $T_2(p^2)/T_2(p^3)$ generates that group. Lemma 3.2.1 implies that P itself contains a ξ^{-1} -element B such that the image of B in $T_2(p^2)/T_2(p^3)$ is nontrivial. That is, B is upper triangular modulo p^2 , but not modulo p^3 .

The lemma in remark 4.2.2 implies that B is a power of $I_2 + pE_{21}$ and hence has the form $B = I_2 + cE_{21}$, where $c = p^2a$ and $a \in \mathbf{Z}_p^\times$. Note that $\det(B) = 1$. Therefore, we see that $B \in C_2^{(0)}(p^2) \cap P$. Let \tilde{B} denote the image of B in the Frattini quotient of $C_2^{(0)}(p^2)$. Then the map (3) (for $k = 2$) sends \tilde{B} to an element of $M_2^{(0)}(\mathbf{F}_p)$ which is not upper triangular.

Lemma 3.1.2 implies that $\widetilde{C_2^{(0)}(p^2)}$ is generated by \tilde{B} as an $\mathbf{F}_p[U_2(\mathbf{F}_p)]$ -module. Since $P^{(0)}$ contains an element A whose image in $U_2(\mathbf{F}_p)$ is nontrivial, it follows that $C_2^{(0)}(p^2)$ has a topologically generating set consisting of matrices of the form A^iBA^{-i} , where $0 \leq i \leq p-1$. Therefore, $P^{(0)}$ indeed contains $C_2^{(0)}(p^2)$ in the case where (5) is nonsplit. Although it wasn't needed above, one can see that P contains the specific matrices $I_2 + E_{12}$ and $I_2 + p^2E_{21}$.

Continuing to assume that (5) is nonsplit, the fact that $I_2 + E_{12}$ is in $P^{(0)}$ implies that $(I_2 + E_{12})^a = I_2 + aE_{12}$ is in $P^{(0)}$ for all $a \in \mathbf{Z}_p$. Therefore, $P^{(0)}$ contains $N_2^{(0)}(p^2)$, a subgroup defined in section 3.3. Since $[T_2^{(0)}(p^2) : N_2^{(0)}(p^2)] = p$, it follows that either $P^{(0)} = T_2^{(0)}(p^2)$ or $P^{(0)} = N_2^{(0)}(p^2)$. Thus, the index of $P^{(0)}$ in $T_2^{(0)}(p^2)$ is either 1 or p . Since $T^{(0)}(p^2)$ itself has index p in $S^{(0)}(\mathbf{Z}_p)$, the index $[S^{(0)}(\mathbf{Z}_p) : P^{(0)}]$ will indeed be either p or p^2 .

Now assume that E has two independent F -isogenies of degree p , i.e., that (5) is split. According to section 2.3, the index $[SL_2(\mathbf{Z}_p) : P^{(0)}]$ is the same as in the case where (5) is nonsplit. Hence the index $[S^{(0)}(\mathbf{Z}_p) : P^{(0)}]$ will also be either p or p^2 . However, we now have $P^{(0)} \subseteq C_2^{(0)}(p)$, a subgroup of $S_2(\mathbf{Z}_p)$ of index p . Thus, the index $[C^{(0)}(p) : P^{(0)}]$ will be either 1 or p . One verifies easily that $C^{(0)}(p^2)$ is generated topologically by p -th powers of elements in $C^{(0)}(p)$, all of which are clearly contained in $P^{(0)}$. It follows that we indeed have the inclusion $C^{(0)}(p^2) \subset P^{(0)}$.

The last statement in proposition 5.1.1 follows because the assumption about $[F(\mu_{p^2}) : F]$

means that the image of G_F under the homomorphism χ_p contains $1 + p\mathbf{Z}_p$. One can then use section 2.3 to prove the index statement, applying it to P instead of G . The inclusion $C_2(p^2) \subset P$ can then be deduced just as above. ■

Note that, under the first assumptions in the proposition, the above proof shows that $P^{(0)}$ contains $N_2^{(0)}(p^2)$ and, if we make the additional assumption about $[F(\mu_{p^2}) : F]$, then P contains $N_2(p^2)$.

5.2. *The proof of theorem 2.* The first part of theorem 2 follows from proposition 4.1.1 and remark 4.2.1 (which shows that $\varphi\psi^{-1}$ has order 4). The assumptions imply that the \mathbf{Q} -isogeny class of E is of type **I** (as defined in section 2.5). For the second part of theorem 2, we use the fact that elliptic curves over \mathbf{Q} have no cyclic isogenies of degree 125, a theorem of Kenku [Ken2]. Hence, we can assume that the \mathbf{Q} -isogeny class of E is of type **II**. In the notation of proposition 5.1.1, we want to prove that $i = 1$. We need two lemmas.

Lemma 5.2.1. *Suppose that $p \geq 5$, that E is an elliptic curve defined over \mathbf{Q}_p which has potentially supersingular reduction. Suppose that \mathcal{F} is an abelian extension of \mathbf{Q}_p and that the ramification index for \mathcal{F}/\mathbf{Q}_p is 12. Then $|E(\mathcal{F})[p]| \leq 12$.*

We will apply this for $p = 5$, but here is an illustration for $p = 13$. Suppose that E is an elliptic curve defined over \mathbf{Q}_{13} which has an isogeny of degree 13 defined over \mathbf{Q}_{13} . Suppose that Φ is the kernel of that isogeny. Thus, $[\mathbf{Q}_{13}(\Phi) : \mathbf{Q}_{13}]$ obviously divides 12. One can choose an \mathcal{F} which contains $\mathbf{Q}_{13}(\Phi)$ and satisfies the hypothesis in lemma 5.2.1. But the inequality stated in the lemma will obviously not be satisfied. Therefore, E must have (potentially) ordinary or multiplicative reduction.

Proof. Since $p \geq 5$, E achieves good reduction over the cyclic extension of \mathbf{Q}_p^{unr} of degree 12. Thus, replacing \mathcal{F} by an unramified extension if necessary, we can assume that E achieves good supersingular reduction over \mathcal{F} . Let \mathcal{O} denote the maximal order in \mathcal{F} , \mathfrak{m} denote its maximal ideal, and $\overline{\mathfrak{m}}$ denote the maximal ideal of the algebraic closure $\overline{\mathbf{Q}}_p$. Let \widehat{E} denote the formal group for E over \mathcal{O} , a formal group of height p^2 in a parameter t . Note that $E(\mathcal{F})[p] = \widehat{E}(\mathfrak{m})[p]$.

Multiplication by p on \widehat{E} is given by a power series $F(t)$ with coefficients in \mathcal{O} , the coefficient of t being p . Writing $F(t) = tG(t)$, the constant term of $G(t)$ is p . The roots of $G(t)$ in $\overline{\mathfrak{m}}$ are the values of t giving the points of order p on $\widehat{E}(\overline{\mathfrak{m}})$. By the Weierstrass Preparation Theorem, there exists a monic polynomial $g(t) \in \mathcal{O}[t]$ of degree $p^2 - 1$ which has the same roots $t \in \overline{\mathfrak{m}}$ as $G(t)$, whose constant term c satisfies $\text{ord}_p(c) = 1$, and whose nonleading terms are all in \mathfrak{m} . Here ord_p is the valuation on \mathcal{F} normalized so that $\text{ord}_p(p) = 1$.

The roots of $g(t)$ are distinct. The points of $\widehat{E}(\mathfrak{m})$ of order p correspond to the roots of $g(t)$ in \mathfrak{m} . The above remarks imply that the number of roots of $g(t)$ in \mathfrak{m} is precisely $|E(\mathcal{F})[p]| - 1$.

If one expresses $g(t)$ as a product of irreducible polynomials in $\mathcal{F}[t]$, then each factor has its constant term in \mathfrak{m} . Thus, the number of irreducible factors of $g(t)$ is at most 12. They cannot all be linear because $g(t)$ has degree $p^2 - 1$, which is at least 24. Thus, $g(t)$ has at most 11 linear factors over \mathcal{F} , and hence at most 11 roots in \mathfrak{m} . The bound on the cardinality of $\widehat{E}(\mathfrak{m})[p]$ follows from this. \blacksquare

Lemma 5.2.2. *Suppose that E is an elliptic curve over \mathbf{Q}_5 and that E has two independent cyclic isogenies of degree 5 defined over \mathbf{Q}_5 . Then E has either potentially ordinary or potentially multiplicative reduction. Consequently, $E[5^\infty]$ contains a $G_{\mathbf{Q}_5}$ -invariant subgroup C isomorphic to $\mathbf{Q}_5/\mathbf{Z}_5$ as a group. The action of the inertia subgroup $I_{\mathbf{Q}_5}$ of $G_{\mathbf{Q}_5}$ on $D = E[5^\infty]/C$ is through a quotient group of order dividing 4.*

Proof. The assumption about isogenies implies that $\text{Gal}(\mathbf{Q}_5(E[5])/\mathbf{Q}_5)$ is an abelian group of exponent dividing 4. Since $\mathbf{Q}_5(\mu_5)$ is a subfield of $\mathbf{Q}_5(E[5])$, the exponent is exactly 4. By local class field theory (or Kummer theory), one sees that $\mathbf{Q}_5(E[5])$ is contained in the compositum of $\mathbf{Q}_5(\mu_5)$ and the unramified extension of \mathbf{Q}_5 of degree 4. Now the unramified quadratic extension of \mathbf{Q}_5 has a cyclic extension of degree 3 which is totally ramified. Let \mathcal{F} be the compositum of all of these fields.

The ramification index of \mathcal{F}/\mathbf{Q}_5 is 12. Note that $E[5] \subset E(\mathcal{F})$. Thus, $|E(\mathcal{F})[5]| = 25$. Lemma 5.2.1 implies that E can't have potentially supersingular reduction. It follows that $E[5^\infty]$ indeed has a subgroup almost as described, namely $C = \widehat{E}(\overline{\mathfrak{m}})[5^\infty]$, which is at least invariant under the action of $G_{\mathcal{F}}$. Since \widehat{E} has height 1, we have $C \cong \mathbf{Q}_5/\mathbf{Z}_5$ and hence $D = E[5^\infty]/C \cong \mathbf{Q}_5/\mathbf{Z}_5$ too. The action of the inertia subgroup $I_{\mathcal{F}}$ of $G_{\mathcal{F}}$ on D is trivial. The action of $I_{\mathcal{F}}$ on C is given by the 5-power cyclotomic character χ_5 , restricted to $I_{\mathcal{F}}$, which has infinite order. Note that D is the maximal quotient of $E[5^\infty]$ on which $I_{\mathcal{F}}$ acts trivially. This action of $I_{\mathcal{F}}$ uniquely determines C .

Since \mathcal{F}/\mathbf{Q}_5 is normal, it is clear that C is actually $G_{\mathbf{Q}_5}$ -invariant. The action of $I_{\mathbf{Q}_5}$ on D is given by a homomorphism $I_{\mathbf{Q}_5} \rightarrow \mathbf{Z}_5^\times$ which factors through $\text{Gal}(\mathcal{F}/\mathbf{Q}_5)$. Since the torsion subgroup of \mathbf{Z}_5^\times has order 4, that homomorphism indeed factors through a quotient of $I_{\mathbf{Q}_5}$ of order dividing 4. \blacksquare

Lemma 5.2.2 was pointed out to the author by Karl Rubin and Alice Silverberg. They verified it by using a parametric description of elliptic curves over \mathbf{Q} which have two independent \mathbf{Q} -isogenies of degree 5. The j -invariants of curves in the family are values of a certain rational function. They could explicitly verify that the values which are 5-integral reduce modulo 5 to non-supersingular j -invariants in \mathbf{F}_5 . The usefulness of the above lemma in the following proof was also pointed out by Rubin and Silverberg.

Proof of the second part of theorem 2. Let $\gamma, \delta : G_{\mathbf{Q}_5} \rightarrow \mathbf{F}_5^\times$ be the characters giving the action of $G_{\mathbf{Q}_5}$ on $C[5]$ and $D[5] \cong E[5]/C[5]$, respectively. One has $\gamma\delta = \omega$, where ω is now considered as a character of $G_{\mathbf{Q}_5}$. Consequently, one sees easily that $\gamma \neq \delta$. Thus, the composition factors $C[5]$ and $D[5]$ in $E[5]$ are nonisomorphic.

Since the index in question is unchanged by a \mathbf{Q} -isogeny, we are free to choose E so that it has a cyclic \mathbf{Q} -isogeny of degree 25. We denote the kernel of such an isogeny by Φ^\sharp and assume that $\Phi = \Phi^\sharp[5]$. If we regard Φ and Ψ as $G_{\mathbf{Q}_5}$ -modules, then they must be isomorphic to $C[5]$ and $D[5]$ in some order. Replacing E by a \mathbf{Q} -isogenous curve if necessary, we can assume that $\Phi \cong D[5]$. (If $\Phi \cong C[5]$, replace E by E/Φ^\sharp .) Since $C[5] \not\cong D[5]$, it is clear that $\Phi \cap C$ is trivial. It follows that $\Phi^\sharp \cap C$ is trivial too. Therefore, the map $E[5^\infty] \rightarrow D$ induces an isomorphism

$$\Phi^\sharp \cong D[25]$$

for the action of $G_{\mathbf{Q}_5}$. Hence the ramification index of 5 in $\mathbf{Q}(\Phi^\sharp)/\mathbf{Q}$ divides 4.

Obviously, $\mathbf{Q}(\Phi^\sharp)$ is a cyclic extension of \mathbf{Q} of degree dividing 20. We now show that this degree is divisible by 5. Assume to the contrary that $[\mathbf{Q}(\Phi^\sharp) : \mathbf{Q}]$ divides 4. Now $\mathbf{Q}(\Phi^\sharp) \neq \mathbf{Q}$ because $E(\mathbf{Q})$ can't have a point of order 25. Thus, $\mathbf{Q}(\Phi^\sharp)$ contains a quadratic field F over which it has degree 1 or 2. The action of G_F on $\mathbf{Q}(\Phi^\sharp)$ is given by a character of order 1 or 2. It follows that either E , or a quadratic twist of E over F , has a rational point over F of order 25. This contradicts a theorem of Kenku [Ken2] which asserts that the modular curve $X_1(25)$ has no noncuspidal rational points over quadratic extensions of \mathbf{Q} .

Hence $\mathbf{Q}(\Phi^\sharp)$ is a cyclic extension of \mathbf{Q} of degree divisible by 5. Its unique subfield of degree 5 over \mathbf{Q} is unramified at 5. It must therefore be ramified at some prime $\ell \neq 5$. Let $\Psi^\sharp = E[25]/\Phi^\sharp$ and let $K^\sharp = \mathbf{Q}(\Phi^\sharp, \Psi^\sharp)$. The ramification index for ℓ in the extension K^\sharp/\mathbf{Q} will be divisible by 5. Of course, $K = \mathbf{Q}(\Phi, \Psi)$ is a subfield of K^\sharp , we have $5 \nmid [K : \mathbf{Q}]$, and hence the ramification index for ℓ in the extension K^\sharp/K is divisible by 5.

The action of $\text{Gal}(K^\sharp/\mathbf{Q})$ on Φ^\sharp and Ψ^\sharp is given by homomorphisms

$$\varphi^\sharp, \psi^\sharp : \text{Gal}(K^\sharp/\mathbf{Q}) \longrightarrow (\mathbf{Z}/25\mathbf{Z})^\times \quad ,$$

respectively. Thus, we obtain an injective homomorphism $\varphi^\sharp \times \psi^\sharp$ from $\text{Gal}(K^\sharp/\mathbf{Q})$ to $(\mathbf{Z}/25\mathbf{Z})^\times \times (\mathbf{Z}/25\mathbf{Z})^\times$. Since $\text{Gal}(K^\sharp/K)$ acts trivially on $\Phi \times \Psi$, its image under $\varphi^\sharp \times \psi^\sharp$ is contained in the Sylow 5-subgroup of $(\mathbf{Z}/25\mathbf{Z})^\times \times (\mathbf{Z}/25\mathbf{Z})^\times$, which has order 25. Thus, $\text{Gal}(K^\sharp/K)$ has exponent 5 and order dividing 25.

The product $\varphi^\sharp\psi^\sharp$ is the homomorphism ω^\sharp giving the Galois action on μ_{25} . It follows that $K(\mu_{25}) \subseteq K^\sharp$. It is clear that $[K(\mu_{25}) : K] = 5$. Furthermore, the above prime ℓ is unramified in $K(\mu_{25})/K$, and therefore its ramification index for the extension $[K^\sharp : K(\mu_{25})]$ is divisible by 5. Hence, $[K^\sharp : K]$ must be divisible by 25. It follows that $[K^\sharp : K] = 25$, that $\text{Gal}(K^\sharp/K)$ is the Sylow 5-subgroup of $\text{Gal}(K^\sharp/\mathbf{Q})$, and is isomorphic to $(\mathbf{Z}/5\mathbf{Z})^2$.

By definition, there is a surjective map from P to $\text{Gal}(K^\sharp/K)$. It is given by the action of P on $\Phi^\sharp \times \Psi^\sharp$, i.e., by the restrictions of φ^\sharp and ψ^\sharp to P . Now we have the inclusions

$$N_2(25) \subseteq P \subseteq T_2(25) \quad .$$

The first was pointed out after the proof of proposition 5.1.1. The second inclusion is due to the choice of E , just as at the beginning of that proof. The natural action of $T_2(25)$ on $\Phi^\sharp \times \Psi^\sharp$ is just the map from $T_2(25)$ to $((1 + 5\mathbf{Z}_5)/(1 + 25\mathbf{Z}_5))^2$, the map to the diagonal. The kernel of that map is $N_2(25)$. The restriction of that map to P gives the action of P mentioned above. The image of P and $T_2(25)$ both have order 25. The maps are surjective. It follows that $P = T_2(25)$. Therefore, we indeed have $[S_2(\mathbf{Z}_5) : P] = 5$. The assertion in theorem 2 follows from this together with the invariance of that index under \mathbf{Q} -isogeny. ■

References

- [BeOn] B. C. Berndt, K. Ono, *Ramanujan's Unpublished Manuscript On The Partition And Tau Functions With Proofs And Commentary*, in the Andrews Festschrift, Séminaire Lotharingien de Combinatoire **42** (2001), 39-110.
- [Bos] N. Boston, *Explicit deformations of Galois representations*, Invent. Math. **103**, 181-196 (1991).
- [Cre] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press (1992).
- [Fis] T. Fisher, *Descent calculations for the elliptic curves of conductor 11*, Proc. London Math. Soc. **86** (2003), 583-606.
- [Gre] R. Greenberg, *Galois representations with open image*, preprint.
- [GRS] R. Greenberg, K. Rubin, A. Silverberg, in preparation.
- [Ken1] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. **22** (1981), 239-244.
- [Ken2] M. A. Kenku, *On the modular curves $X_0(125)$, $X_1(25)$, and $X_1(49)$* , J. London Math. Soc. **23** (1981), 415-427.
- [Lig] G. Ligozat, *Courbes modulaires de genre 1*, Bull. Soc. Math. France, Mémoire **43** (1975), 1-80.

- [Maz] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129-162.
- [Rib] K. Ribet, *On ℓ -adic representations attached to modular forms*, Invent. Math. **28** (1975), 245-275.
- [Ser1] J. P. Serre, *Une interprétation des congruences relative à la fonction τ de Ramanujan*, Séminaire Delange-Pisot-Poitou, 1967/68, no. 14.
- [Ser2] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.
- [SwD] H. P. F. Swinnerton-Dyer, *On ℓ -adic representations and congruences for coefficients of modular forms II*, Lecture Notes in Math. **601** (1977), 63-90.