AN OVERVIEW OF A THEOREM OF FLACH

TOM WESTON

In recent years, the study of the deformation theory of Galois representations has become of central importance in arithmetic algebraic geometry. The most fundamental question in this field is the explicit determination of universal deformation rings associated to given residual representations. It was observed by Mazur in his first paper [Maz90, Section 1.6] on the subject that the solution of this problem is immediate if a certain Galois cohomology group associated to the residual representation vanishes.

The goal of this paper is to provide an overview of a theorem of Flach which yields the vanishing of this cohomology group for many mod l representations coming from rational elliptic curves. We do not seek to give a complete proof; we hope only to make clear the main ideas. In the process we will touch on many facets of arithmetic algebraic geometry, including Tate's duality theorems in Galois cohomology, generalized Selmer groups, Kolyvagin's theory of Euler systems and the geometry of modular curves.

The work we will describe actually has another, more direct, application: it can be used in many cases to prove the Taylor-Wiles isomorphism between a certain universal deformation ring and a certain Hecke algebra. We will not touch on this aspect; for details, see [Maz94] or [Wes00].

We have tried to keep the prerequisites to a minimum. The main requirement is a good familiarity with Galois cohomology. The algebraic geometry we use is mostly at the level of [Sil86, Chapters 1 and 2], which the exception of Appendix B, which is significantly more advanced. Some familiarity with elliptic curves is helpful, although with the exception of Appendix A we will use little more than the Tate module and the existence of the Weil pairing.

I would like to thank Brian Conrad, Matthew Emerton and Karl Rubin for teaching me much of the material presented here. I would also like to thank Fernando Gouvea for encouraging the writing of this paper. Above all, I would like to thank Barry Mazur for his constant help and insights; I can only hope that his point of view is visible in the mathematics below.

1. Unobstructed deformation problems

Let $G_{\mathbf{Q},S}$ be the maximal quotient of the absolute Galois group of $\mathbf{Q}$ unramified away from a finite set of places S. Let l be a prime number and let $\bar{\rho} : G_{\mathbf{Q},S} \to \mathrm{GL}_2(\mathbf{F}_l)$ be a Galois representation. Under certain additional hypotheses (for example, if $\bar{\rho}$ is irreducible) we can associate a *universal deformation ring* $\mathcal{R}(\bar{\rho})$ to such a residual representation; see [Gou], [Maz90] or [Maz97] for details.

In general the determination of the structure of the ring $\mathcal{R}(\bar{\rho})$ is quite difficult. However, in at least one case the determination is easy: let $\mathrm{ad}(\bar{\rho})$ be the $G_{\mathbf{Q},S}$-module of 2×2 matrices over $\mathbf{F}_l$ on which $\gamma \in G_{\mathbf{Q},S}$ acts via conjugation by $\bar{\rho}(\gamma)$.

If

$$H^2(G_{\mathbf{Q},S}, \mathrm{ad}(\bar{\rho})) = 0,$$

then $\mathcal{R}(\bar{\rho})$ is isomorphic to a power series ring in $\dim_{\mathbf{F}_l} H^1(G_{\mathbf{Q},S}, \mathrm{ad}(\bar{\rho}))$ variables over $\mathbf{Z}_l$; see [Maz90, Section 1.6, Proposition 2]. If this is the case, we say that the deformation problem for $\bar{\rho}$ is *unobstructed*.

Our goal in this paper is to explain the main ideas of the proof of the following theorem of Flach.

Theorem 1. *(* [Fla92, Theorem 2]*) Let E be an elliptic curve over $\mathbf{Q}$, let $l \geq 5$ be a prime and let S be the set of places of $\mathbf{Q}$ at which E has bad reduction, together with l and ∞. Let $\rho : G_{\mathbf{Q},S} \to \mathrm{GL}_2(\mathbf{Z}_l)$ be the representation of $G_{\mathbf{Q},S}$ on the l-adic Tate module of E and let $\bar{\rho} : G_{\mathbf{Q},S} \to \mathrm{GL}_2(\mathbf{F}_l)$ be the residual representation. Assume further that:*

- *E has good reduction at l;*
- *ρ is surjective;*
- *For all $p \in S - \{\infty\}$, $E[l] \otimes E[l]$ has no $G_{\mathbf{Q}_p}$-invariants;*
- *l does not divide the rational number $L(\mathrm{Sym}^2 T_l E, 0)/\Omega$, where $\mathrm{Sym}^2 T_l E$ is the symmetric square of the l-adic Tate module of E and Ω is a certain period.*

Then the deformation problem for $\bar{\rho}$ is unobstructed.

In Appendix A we discuss precisely how stringent these hypotheses are; the main result is that for fixed E which does not have complex multiplication, then they are satisfied for a set of primes l of density 1. We will explain the fourth hypothesis in Section 5.

We should note that this theorem uses in a crucial way the fact that E is modular, and thus stating it in the form above relies heavily on the recent proof of the Taniyama-Shimura conjecture.

2. Galois modules and the calculus of Tate twists

We begin with some formalities on Galois actions and certain commutative algebra operations. Let S be a finite set of places of $\mathbf{Q}$ including the prime l. Let M and N be $\mathbf{Z}_l$-modules with $G_{\mathbf{Q},S}$-actions. We make the tensor product $M \otimes_{\mathbf{Z}_l} N$ a $G_{\mathbf{Q},S}$-module via the diagonal action: $\gamma(m \otimes n) = \gamma m \otimes \gamma n$. We make $\mathrm{Hom}_{\mathbf{Z}_l}(M, N)$ a $G_{\mathbf{Q},S}$-module via the adjoint action: $\gamma f(m) = \gamma \cdot f(\gamma^{-1} m)$ for $f \in \mathrm{Hom}_{\mathbf{Z}_l}(M, N)$. Note that the $G_{\mathbf{Q},S}$-invariants of $\mathrm{Hom}_{\mathbf{Z}_l}(M, N)$ are precisely the $G_{\mathbf{Q},S}$-equivariant homomorphisms $\mathrm{Hom}_{\mathbf{Z}_l[G_{\mathbf{Q},S}]}(M, N)$. Throughout this paper we assume that the base ring for any of these constructions is $\mathbf{Z}_l$; we will usually omit it from the notation.

Now assume that M is free over $\mathbf{Z}_l$ of rank 2. We define the *symmetric square* $\mathrm{Sym}^2 M$ of M to be the submodule of $M \otimes M$ which is invariant under the automorphism of $M \otimes M$ interchanging the two factors. If x, y is a basis for M, then $x \otimes x, x \otimes y + y \otimes x, y \otimes y$ is a basis for $\mathrm{Sym}^2 M$, so that $\mathrm{Sym}^2 M$ is free over $\mathbf{Z}_l$ of rank 3. In fact, if $l \neq 2$, then $\mathrm{Sym}^2 M$ is a direct summand of $M \otimes M$; the complimentary summand is the alternating square $\wedge^2 M$, which has basis $x \otimes y - y \otimes x$:

$$M \otimes M = \wedge^2 M \oplus \mathrm{Sym}^2 M. \tag{1}$$

One checks easily that $\mathrm{Sym}^2 M$ is stable under the action of $G_{\mathbf{Q},S}$, so that it can also be considered as a $G_{\mathbf{Q},S}$-module. We also have an induced action of $G_{\mathbf{Q},S}$ on

$\wedge^2 M$, and with these actions the decomposition (1) is a decomposition of $G_{\mathbf{Q},S}$-modules.

The module of endomorphisms $\mathrm{End}(M)$ admits a similar decomposition. (As always we let $G_{\mathbf{Q},S}$ act on $\mathrm{End}(M)$ via the adjoint action.) The scalar matrices in $\mathrm{End}(M)$ are a free $\mathbf{Z}_l$-module of rank 1 with trivial Galois action, since conjugation is trivial on scalars. Thus we have a canonical decomposition

$$\mathrm{End}(M) = \mathbf{Z}_l \oplus \mathrm{End}^0(M)$$

where $\mathrm{End}^0(M)$ denotes the trace zero matrices in $\mathrm{End}(M)$ and the first summand corresponds to the scalar matrices. (We always take $\mathbf{Z}_l$ itself to have trivial $G_{\mathbf{Q},S}$-action.)

Now let E be a rational elliptic curve and let l be an odd prime. Recall that the *l-adic Tate module* of E is the free $\mathbf{Z}_l$-module of rank 2 defined by

$$T_l E = \varprojlim E[l^n].$$

If S is any set of places of $\mathbf{Q}$ including l and the places where E has bad reduction, then $T_l E$ carries a natural action of $G_{\mathbf{Q},S}$. Upon choosing a basis for $T_l E$ we can view this as a representation

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l).$$

The Galois module which will actually prove most relevant to the proof of Theorem 1 is the symmetric square of $T_l E$.

We can perform a similar construction with the l-power roots of unity: this Tate module, $\varprojlim \mu_{l^n}$, is written as $\mathbf{Z}_l(1)$. Thus $\mathbf{Z}_l(1)$ is a free $\mathbf{Z}_l$-module of rank 1 on which $G_{\mathbf{Q},S}$ acts via the cyclotomic character

$$\varepsilon : G_{\mathbf{Q},S} \to \mathbf{Z}_l^*;$$

here S is any set of places of $\mathbf{Q}$ containing l. For any $n > 0$, define $\mathbf{Z}_l(n)$ to be the tensor product (over $\mathbf{Z}_l$) of $\mathbf{Z}_l(1)$ with itself n times. Define $\mathbf{Z}_l(-1)$ to be the integral Pontrjagin dual $\mathrm{Hom}(\mathbf{Z}_l(1), \mathbf{Z}_l)$ of $\mathbf{Z}_l(1)$, and define $\mathbf{Z}_l(-n)$ as the tensor product of $\mathbf{Z}_l(-1)$ with itself n times. Thus $\mathbf{Z}_l(n)$ is a free $\mathbf{Z}_l$-module of rank one on which $G_{\mathbf{Q},S}$ acts via ε^n. If M is any $\mathbf{Z}_l$-module with an action of $G_{\mathbf{Q}}$, we define its n^{th} *Tate twist* by

$$M(n) = M \otimes_{\mathbf{Z}_l} \mathbf{Z}_l(n).$$

$M(n)$ is isomorphic to M as a $\mathbf{Z}_l$-module, but they usually have different $G_{\mathbf{Q}}$-actions.

A key property of the Tate module of an elliptic curve is that the Weil pairings

$$E[l^n] \otimes E[l^n] \to \mu_{l^n}$$

compile to yield a perfect, skew-symmetric, Galois equivariant pairing

$$e : T_l E \otimes T_l E \to \mathbf{Z}_l(1).$$

See [Sil86, Proposition III.8.3]. Since e is skew-symmetric, this implies that $\wedge^2 T_l E \cong \mathbf{Z}_l(1)$. We record some additional consequences below.

Lemma 2. *The Weil pairing induces a Galois equivariant isomorphism*

$$\mathrm{End}(T_l E)(1) \cong T_l E \otimes T_l E.$$

This isomorphism restricts to an isomorphism

$$\mathrm{End}^0(T_l E)(1) \cong \mathrm{Sym}^2 T_l E$$

of direct summands.

Proof. The Weil pairing yields a duality isomorphism

$$T_l E \cong \mathrm{Hom}(T_l E, \mathbf{Z}_l(1)),$$

essentially by the definition of a perfect pairing. Galois equivariance of the Weil pairing implies precisely that this identification respects Galois action, thanks to the definition of the adjoint Galois action. Tensoring with $T_l E$ now yields the first statement of the lemma, since $\mathrm{Hom}(T_l E, T_l E(1))$ is visibly isomorphic to $\mathrm{End}(T_l E)(1)$.

Explicitly, the above isomorphism sends $t \otimes t' \in T_l E \otimes T_l E$ to the function $t' \otimes e(t, \cdot) \in \mathrm{Hom}(T_l E, T_l E \otimes \mathbf{Z}_l(1))$. To check the second statement, we can ignore Galois actions and we simply have to check that symmetric elements of $T_l E \otimes T_l E$ correspond to trace zero matrices in $\mathrm{End}(T_l E)$. This follows immediately from the fact that the Weil pairing is alternating; we leave it as an exercise. □

If M is any free $\mathbf{Z}_l$-module with an action of $G_{\mathbf{Q},S}$, we define its *integral Cartier dual* M^* to be the $G_{\mathbf{Q},S}$-module $\mathrm{Hom}(M, \mathbf{Z}_l(1))$. (Often the term *Cartier dual* is used for the module $\mathrm{Hom}(M, \mathbf{Q}_l/\mathbf{Z}_l(1))$.)

Lemma 3. *The Weil pairing induces an isomorphism*

$$(T_l E \otimes T_l E)^* \cong T_l E \otimes T_l E(-1).$$

This isomorphism restricts to an isomorphism

$$(\mathrm{Sym}^2 T_l E)^* \cong (\mathrm{Sym}^2 T_l E)(-1).$$

Proof. In general, if A and B are any free $\mathbf{Z}_l$-modules with $G_{\mathbf{Q},S}$-actions, then $(A \otimes B)^* \cong A^* \otimes B^*(-1)$, as one checks easily from the definition. In our case, the Weil pairing shows that $(T_l E)^* \cong T_l E$, and the first statement follows. The second statement is immediate once the first isomorphism has been made explicit; we omit the details. □

3. First reductions

In this section we will use various global duality theorems of Tate to reduce our calculation of $H^2(G_{\mathbf{Q},S}, \mathrm{ad}(\bar{\rho}))$ to the vanishing of a certain Shafarevich-Tate group. For the remainder of the paper we fix a rational elliptic curve E and a prime l satisfying the hypotheses of Theorem 1. Let S be the corresponding set of places of $\mathbf{Q}$. Note that as Galois modules $\mathrm{ad}(\bar{\rho}) \cong \mathrm{End}(E[l])$; we will use the notation $\mathrm{End}(E[l])$ from now on.

We begin with the following small piece of the Poitou-Tate exact sequence (see [Was97b, Section 8] for statements and [Mil86, Chapter 1, Section 4] for a proof; here we are using the fact that $l \neq 2$ to eliminate the terms at infinity):

$$\prod_{p \in S - \{\infty\}} H^0(\mathbf{Q}_p, E[l] \otimes E[l]) \to \mathrm{Hom}\big(H^2(G_{\mathbf{Q},S}, (E[l] \otimes E[l])^*), \mathbf{Z}/l\mathbf{Z}\big) \to$$
$$H^1(G_{\mathbf{Q},S}, E[l] \otimes E[l]) \to \prod_{p \in S} H^1(\mathbf{Q}_p, E[l] \otimes E[l]).$$

Tensoring the first isomorphism of Lemma 2 with $\mathbf{Z}/l\mathbf{Z}$ yields an isomorphism

$$E[l] \otimes E[l] \cong \mathrm{End}(E[l])(1).$$

Together with Lemma 3, this implies that

$$(E[l] \otimes E[l])^* \cong \mathrm{End}(E[l]).$$

Thus the above exact sequence contains a term which is (only non-canonically) isomorphic to $H^2(G_{\mathbf{Q},S}, \mathrm{End}(E[l]))$; since to prove Theorem 1 we need to show that this group vanishes, we see that it will suffice to show that the two groups

$$\prod_{p \in S - \{\infty\}} H^0(\mathbf{Q}_p, E[l] \otimes E[l])$$

$$Ш^1(G_{\mathbf{Q},S}, E[l] \otimes E[l])) = \ker \left(H^1(G_{\mathbf{Q},S}, E[l] \otimes E[l]) \to \prod_{p \in S} H^1(\mathbf{Q}_p, E[l] \otimes E[l]) \right)$$

both vanish.

The vanishing of the first of these groups is the third hypothesis in the statement of Theorem 1. For the second, we first write

$$E[l] \otimes E[l] = \wedge^2 E[l] \oplus \mathrm{Sym}^2 E[l] \cong \mu_l \oplus \mathrm{Sym}^2 E[l].$$

(The isomorphism of $\wedge^2 E[l]$ and μ_l comes from the Weil pairing.) One sees immediately from this that there is a corresponding decomposition

$$Ш^1(G_{\mathbf{Q},S}, E[l] \otimes E[l]) \cong Ш^1(G_{\mathbf{Q},S}, \mu_l) \oplus Ш^1(G_{\mathbf{Q},S}, \mathrm{Sym}^2 E[l]).$$

The first term is easily dealt with. We will need the following results, which will also be useful later when dealing with Selmer groups.

Lemma 4. *Let A be a $G_{\mathbf{Q}}$-module which is unramified away from a finite set of primes S. Then*

$$H^1(G_{\mathbf{Q},S}, A) \cong \ker \left(H^1(\mathbf{Q}, A) \to \prod_{p \notin S} H^1(I_p, A) \right).$$

Here $I_p \subseteq G_{\mathbf{Q}}$ is the inertia group at p.

Proof. See [Was97b, Proposition 6] for a proof. The idea is simply that cohomology classes for $G_{\mathbf{Q},S}$ are automatically unramified away from S and therefore are trivial when restricted to the corresponding inertia groups. □

Lemma 5. *Let p be a prime different from l. Then the maximal pro-l quotient of the inertia group I_p is isomorphic to $\mathbf{Z}_l$ as an abelian group. If $G_{\mathbf{Q}_p}$ is made to act on I_p by conjugation, then the maximal pro-l quotient of I_p is isomorphic to $\mathbf{Z}_l(1)$ as a $G_{\mathbf{Q}_p}$-module.*

Proof. Recall that $I_p = \mathrm{Gal}(\bar{\mathbf{Q}}_p / \mathbf{Q}_p^{\mathrm{ur}})$. It is shown in [Frö67, Section 8, Corollary 3] that the maximal pro-l quotient of this group is $\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ur}}(p^{1/l^\infty})/\mathbf{Q}_p^{\mathrm{ur}})$. This is seen to be isomorphic to $\mathbf{Z}_l$ using the isomorphisms

$$\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ur}}(p^{1/l^\infty})/\mathbf{Q}_p^{\mathrm{ur}}) \cong \varprojlim \mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ur}}(p^{1/l^n})/\mathbf{Q}_p^{\mathrm{ur}}) \cong \varprojlim \mathbf{Z}/l^n\mathbf{Z} \cong \mathbf{Z}_l.$$

We leave the verification that the conjugation action is cyclotomic as an exercise. □

Lemma 6. $Ш^1(G_{\mathbf{Q},S}, \mu_l) = 0$.

Proof. By definition,

$$Ш^1(G_{\mathbf{Q},S}, \mu_l) = \ker\left(H^1(G_{\mathbf{Q},S}, \mu_l) \to \prod_{p \in S} H^1(\mathbf{Q}_p, \mu_l) \right).$$

Lemma 4 shows that we can rewrite this as

$$Ш^1(G_{\mathbf{Q},S}, \mu_l) = \ker\left(H^1(\mathbf{Q}, \mu_l) \to \prod_{p \notin S} H^1(I_p, \mu_l) \times \prod_{p \in S} H^1(\mathbf{Q}_p, \mu_l) \right).$$

We will compute these groups.

We begin by working in some generality. Let K be any perfect field of characteristic different from l, and consider the exact sequence

$$0 \to \mu_l \to \bar{K}^* \xrightarrow{l} \bar{K}^* \to 0$$

of G_K-modules. Hilbert's theorem 90 (see [Ser97, Chapter II.1, Proposition 1]) says that $H^1(K, \bar{K}^*) = 0$, so the long exact sequence in G_K-cohomology coming from the short exact sequence above yields an isomorphism

$$K^* \otimes_{\mathbf{Z}} \mathbf{Z}/l\mathbf{Z} \cong H^1(K, \mu_l).$$

This applies in particular to the fields $\mathbf{Q}_p$:

$$\mathbf{Q}_p^* \otimes_{\mathbf{Z}} \mathbf{Z}/l\mathbf{Z} \cong H^1(\mathbf{Q}_p, \mu_l).$$

For $p \notin S$ we also need to compute $H^1(I_p, \mu_l)$. Since $p \notin S$, we know that $p \neq l$; thus I_p acts trivially on μ_l. Thus $H^1(I_p, \mu_l) \cong \mathrm{Hom}(I_p, \mu_l)$. Any such homomorphism must factor through the maximal pro-l quotient of I_p, and now Lemma 5 shows that this group is just $\mathbf{Z}/l\mathbf{Z}$. It is easily checked that the restriction map

$$H^1(\mathbf{Q}_p, \mu_l) \to H^1(I_p, \mu_l) \cong \mathbf{Z}/l\mathbf{Z}$$

is just the natural map

$$\mathbf{Q}_p^\times \otimes_{\mathbf{Z}} \mathbf{Z}/l\mathbf{Z} \cong (\mathbf{Z} \times \mathbf{Z}_p^\times) \otimes_{\mathbf{Z}} \mathbf{Z}/l\mathbf{Z} \to \mathbf{Z}/l\mathbf{Z}$$

which is trivial on $\mathbf{Z}_p^\times$; that is, it is the p-adic valuation map modulo l.

The group $Ш^1(G_{\mathbf{Q},S}, \mu_l)$ is therefore the kernel of the map

$$\mathbf{Q}^\times \otimes_{\mathbf{Z}} \mathbf{Z}/l\mathbf{Z} \to \prod_{p \notin S} \mathbf{Z}/l\mathbf{Z} \times \prod_{p \in S - \{\infty\}} \mathbf{Q}_p^\times \otimes_{\mathbf{Z}} \mathbf{Z}/l\mathbf{Z}.$$

(Since $l \neq 2$ the term at ∞ vanishes.) Over calculations above show that this kernel consists only of elements of $\mathbf{Q}^\times \otimes_{\mathbf{Z}} \mathbf{Z}/l\mathbf{Z}$ which have p-adic valuation divisible by l for all primes p. (In fact, at $p \in S$ the conditions are even stronger, but we won't need that.) Unique factorization in $\mathbf{Z}$ implies that any such rational number is an l^{th}-power in $\mathbf{Q}^\times$, and therefore is zero in $\mathbf{Q}^\times \otimes \mathbf{Z}/l\mathbf{Z}$. (Here we also need to use the fact that the units $\mathbf{Z}^\times$ are just ± 1 and disappear on tensoring with $\mathbf{Z}/l\mathbf{Z}$.) Thus $Ш^1(G_{\mathbf{Q},S}, \mu_l) = 0$, as claimed. Note that the fact that $\mathbf{Z}$ has unit rank 0 and class number 1 was essential to this argument. □

We have now reduced the proof of Theorem 1 to showing that the Shafarevich-Tate group $Ш^1(G_{\mathbf{Q},S}, \mathrm{Sym}^2 E[l])$ is trivial. We will first show that it embeds into an a priori larger group. Before we can do this, however, we need to define the Selmer groups of our Galois modules.

4. Selmer groups

Recall that the Selmer group of an elliptic curve over $\mathbf{Q}$ is defined to be the subgroup of $H^1(\mathbf{Q}, T_l E \otimes \mathbf{Q}_l/\mathbf{Z}_l)$ of cohomology classes which for all p are locally in the image of $E(\mathbf{Q}_p)$ under the Kummer map. (See [Gre].) We will be working with $\mathrm{Sym}^2 T_l E \otimes \mathbf{Q}_l/\mathbf{Z}_l$, but here we no longer have any natural geometric object on which to base our local conditions in the definition of the Selmer group. The key to the general definition of a Selmer group is the fact that the image of the local Kummer map consists precisely of those cohomology classes which are unramified, in a sense which we shall make precise below.

Let us fix some notation for the remainder of the paper: set $T = \mathrm{Sym}^2 T_l E$ (a free $\mathbf{Z}_l$-module of rank 3), $V = T \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$ (a 3 dimensional $\mathbf{Q}_l$-vector space) and $A = V/T = \mathrm{Sym}^2 T_l E \otimes_{\mathbf{Z}_l} \mathbf{Q}_l/\mathbf{Z}_l$ (which is isomorphic as an abelian group to $(\mathbf{Q}_l/\mathbf{Z}_l)^3$). T, V and A are to be regarded as three different incarnations of the same Galois module. We will also need to consider $A^* = \mathrm{Hom}_{\mathbf{Z}_l}(T, \mu_{l^\infty})$, which is also isomorphic as an abelian group to $(\mathbf{Q}_l/\mathbf{Z}_l)^3$. Lastly, for technical reasons we will later need to consider the finite modules $T_n = T/l^n T$ and $A^*_n = A^*[l^n]$ (both of which are isomorphic to $(\mathbf{Z}/l^n\mathbf{Z})^3$ as abelian groups).

To formalize the notion of a Selmer group, we wish to define "unramified subgroups" (the usual term is *finite subgroups*) $H^1_f(\mathbf{Q}_p, A)$ of $H^1(\mathbf{Q}_p, A)$ for every prime p. We will then define the *Selmer group* $H^1_f(\mathbf{Q}, A)$ of A by

$$\begin{aligned} H^1_f(\mathbf{Q}, A) &= \ker\left(H^1(\mathbf{Q}, A) \to \prod_p H^1(\mathbf{Q}_p, A)/H^1_f(\mathbf{Q}_p, A) \right) \\ &= \{c \in H^1(\mathbf{Q}, A) \mid \mathrm{res}_p\, c \in H^1_f(\mathbf{Q}_p, A) \text{ for all } p\}. \end{aligned}$$

Here res_p is the restriction map from $H^1(\mathbf{Q}, A)$ to $H^1(\mathbf{Q}_p, A)$.

The definition of $H^1_f(\mathbf{Q}_p, A)$ is fairly straightforward for primes p which do not lie in S. Indeed, the most obvious notion of an unramified cocycle is one which becomes trivial when restricted to inertia; that is, it should lie in the kernel of the restriction map

$$H^1(\mathbf{Q}_p, A) \to H^1(I_p, A)$$

where I_p is the inertia subgroup of $G_{\mathbf{Q}_p}$. The inflation-restriction sequence (see [Was97b, Proposition 2 and the discussion following]) identifies this kernel with

$$H^1(G_{\mathbf{Q}_p}/I_p, A) = H^1(\mathbf{F}_p, A).$$

(Here we are using that I_p acts trivially on A to see that A is a $G_{\mathbf{Q}_p}/I_p$-module.) We take this as our definition of the finite subgroup, at least for $p \notin S$:

$$H^1_f(\mathbf{Q}_p, A) = H^1(\mathbf{F}_p, A),$$

or more honestly its image in $H^1(\mathbf{Q}_p, A)$ under inflation.

Note that the inflation-restriction exact sequence now takes the form

$$0 \to H^1_f(\mathbf{Q}_p, A) \to H^1(\mathbf{Q}_p, A) \to H^1(I_p, A)^{G_{\mathbf{F}_p}} \to H^2(\mathbf{F}_p, A).$$

In fact, $H^2(\mathbf{F}_p, A)$ vanishes for reasons relating to the cohomology of $G_{\mathbf{F}_p}$; see [Ser97, Chapter II.3]. We will call $H^1(I_p, A)^{G_{\mathbf{F}_p}}$ the *singular quotient* of $H^1(\mathbf{Q}_p, A)$ and write it as $H^1_s(\mathbf{Q}_p, A)$, so that we have an exact sequence

$$0 \to H^1_f(\mathbf{Q}_p, A) \to H^1(\mathbf{Q}_p, A) \to H^1_s(\mathbf{Q}_p, A) \to 0.$$

In analogy with this definition, for $p \in S$ it might seem most reasonable to define the finite part of $H^1(\mathbf{Q}_p, A)$ also as the kernel of $H^1(\mathbf{Q}_p, A) \to H^1(I_p, A)$, which equals $H^1(\mathbf{F}_p, A^{I_p})$. However, for reasons which will not become apparent in this paper this definition turns out to be inadequate. It turns out that the correct definition is as follows: first assume $p \neq l$. Let $\pi : V \to A$ be the natural quotient map. We define

$$H^1_f(\mathbf{Q}_p, V) = H^1(\mathbf{F}_p, V^{I_p})$$

and

$$H^1_f(\mathbf{Q}_p, A) = \pi_* H^1_f(\mathbf{Q}_p, V).$$

Here $\pi_* : H^1(\mathbf{Q}_p, V) \to H^1(\mathbf{Q}_p, A)$ is the induced map on cohomology. Despite appearances, $\pi_* H^1_f(\mathbf{Q}_p, V)$ need not be the same as $H^1(\mathbf{F}_p, V^{I_p})$, at least for $p \in S$. For later use, let us also set $H^1_f(\mathbf{Q}_p, V) = H^1(\mathbf{F}_p, V)$ for $p \notin S$. One checks easily that in this case $\pi_* H^1_f(\mathbf{Q}_p, V)$ does agree with our previous definition of $H^1_f(\mathbf{Q}_p, A)$.

The definition of $H^1_f(\mathbf{Q}_l, A)$ is much more subtle. The generally accepted definition (which recovers the usual definition in the case of the Tate module of an elliptic curve) is

$$H^1_f(\mathbf{Q}_p, V) = \ker\big(H^1(\mathbf{Q}_p, V) \to H^1(\mathbf{Q}_p, V \otimes B_{\mathrm{crys}})\big)$$

and $H^1_f(\mathbf{Q}_p, A) = \pi_* H^1_f(\mathbf{Q}_p, V)$. Here B_{crys} is one of Fontaine's "big rings". We will not concern ourselves very much with this definition in this paper, although in many ways it is one of the most important topics. It is possible to make this definition much more concrete, but even that does not really make this condition any easier to deal with.

In passing, we should note that $H^1(\mathbf{R}, A) = 0$ (since $l \neq 2$), so we need not concern ourselves with any definitions at infinity. We have now defined $H^1_f(\mathbf{Q}_p, A)$ for all primes p, and with it the Selmer group $H^1_f(\mathbf{Q}, A)$. Of course, we can mimic the identical construction with A^* instead of A, and thus we also have a Selmer group $H^1_f(\mathbf{Q}, A^*)$.

We can also redo the construction for the Galois module T. Note that T is fundamentally quite different from A, in that it is free over $\mathbf{Z}_l$ rather than isomorphic to several copies of $\mathbf{Q}_l/\mathbf{Z}_l$. The definitions are nevertheless quite analogous. Let $i : T \to V$ be the natural inclusion, and for all p define

$$H^1_f(\mathbf{Q}_p, T) = i_*^{-1} H^1_f(\mathbf{Q}_p, V).$$

We also define singular quotients $H^1_s(\mathbf{Q}_p, T) = H^1(\mathbf{Q}_p, T)/H^1_f(\mathbf{Q}_p, T)$. In this case, it will turn out that the singular part of the local cohomology is that which we can most easily work with. One can also define a Selmer group for T, although we will have no need to consider it.

We will also need corresponding subgroups for the finite modules T_n and $A^*[l^n]$. For any prime p, we simply take $H^1_f(\mathbf{Q}_p, A^*_n)$ to be the inverse image of $H^1_f(\mathbf{Q}_p, A^*)$ under the natural map $H^1(\mathbf{Q}_p, A^*_n) \to H^1(\mathbf{Q}_p, A^*)$. Similarly, we define $H^1_f(\mathbf{Q}_p, T_n)$ to be the image of $H^1_f(\mathbf{Q}_p, T)$ under the natural map $H^1(\mathbf{Q}_p, T) \to H^1(\mathbf{Q}_p, T_n)$. One can now define singular quotients and Selmer groups in the usual way.

It is worth noting the general philosophy: we took the natural definition of unramified cocycles in $H^1(\mathbf{Q}_p, V)$ (with the exception of the case $p = l$, which was more complicated) and we then let these choices propagate down to all of the related Galois modules.

Returning to the case of $T_l E$, recall that one defines the Shafarevich-Tate group $Ш(E/\mathbf{Q})$ as the cokernel of the Kummer map

$$E(\mathbf{Q}) \otimes_{\mathbf{Z}} \mathbf{Q}_l/\mathbf{Z}_l \to H^1_f(\mathbf{Q}, T_l E).$$

As before we have no obvious analogue of $E(\mathbf{Q})$ in our situation. The work of Bloch and Kato suggests that the correct analogue is the following: let

$$H^1_f(\mathbf{Q}, V) = \ker\left(H^1(\mathbf{Q}, V) \to \prod_p H^1(\mathbf{Q}_p, V)/H^1_f(\mathbf{Q}_p, V)\right)$$

be the Selmer group for V, and define the "rational points of A" to be

$$A(\mathbf{Q}) = \pi_* H^1_f(\mathbf{Q}, V) \subseteq H^1(\mathbf{Q}, A).$$

Note that it follows immediately from the definition of the $H^1_f(\mathbf{Q}_p, A)$ that $A(\mathbf{Q})$ actually lies in $H^1_f(\mathbf{Q}, A)$, although it could conceivably be smaller. We define the Shafarevich-Tate group $Ш(A/\mathbf{Q})$ to be the quotient $H^1_f(\mathbf{Q}, A)/A(\mathbf{Q})$, so that there is an exact sequence

$$0 \to A(\mathbf{Q}) \to H^1_f(\mathbf{Q}, A) \to Ш(A/\mathbf{Q}) \to 0.$$

$Ш(A/\mathbf{Q})$ is to be thought of as elements of the Selmer group which appear over A but not over V. Note also that despite the similar notation, $Ш(A/\mathbf{Q})$ is not the same as any of the Shafarevich-Tate groups we considered earlier.

Again, we can make analogous definitions for $A^*(\mathbf{Q})$, yielding an exact sequence

$$0 \to A^*(\mathbf{Q}) \to H^1_f(\mathbf{Q}, A^*) \to Ш(A^*/\mathbf{Q}) \to 0.$$

We are now in a position to finish our reductions of the previous section.

Lemma 7. $Ш^1(G_{\mathbf{Q},S}, \operatorname{Sym}^2 E[l])$ *injects into* $H^1_f(\mathbf{Q}, A)$.

Proof. As an abelian group A is isomorphic to $(\mathbf{Q}_l/\mathbf{Z}_l)^3$, so multiplication by l is surjective on A. Furthermore, the kernel of multiplication by l on A,

$$\operatorname{Sym}^2 T_l E \otimes \frac{1}{l}\mathbf{Z}_l/\mathbf{Z}_l,$$

naturally identifies with $\operatorname{Sym}^2 E[l]$, so there is an exact sequence

$$0 \to \operatorname{Sym}^2 E[l] \to A \xrightarrow{l} A \to 0. \tag{2}$$

The fact that $E[l] \otimes E[l]$ is assumed to have no $G_{\mathbf{Q}_p}$-invariants for any $p \in S - \{\infty\}$ insures that the direct summand $\operatorname{Sym}^2 E[l]$ has no $G_{\mathbf{Q},S}$-invariants; indeed, knowing that it had no invariants at any one place would suffice. It follows easily from this that A itself has no $G_{\mathbf{Q},S}$-invariants, as if there were any, then they could be realized in $\operatorname{Sym}^2 E[l]$ by multiplication by an appropriate power of l. Thus the long exact sequence in $G_{\mathbf{Q},S}$-cohomology associated to (2) yields an injection

$$H^1(G_{\mathbf{Q},S}, \operatorname{Sym}^2 E[l]) \hookrightarrow H^1(G_{\mathbf{Q},S}, A).$$

Furthermore, under this injection $Ш^1(G_{\mathbf{Q},S}, \mathrm{Sym}^2 E[l])$ maps into $Ш^1(G_{\mathbf{Q},S}, A)$. Indeed, there is a commutative diagram

$$\begin{array}{ccc} H^1(G_{\mathbf{Q},S}, \mathrm{Sym}^2 E[l]) & \longrightarrow & H^1(G_{\mathbf{Q},S}, A) \\ \downarrow & & \downarrow \\ \prod_{p\in S} H^1(\mathbf{Q}_p, \mathrm{Sym}^2 E[l]) & \longrightarrow & \prod_{p\in S} H^1(\mathbf{Q}_p, A) \end{array} \tag{3}$$

This shows that any element of $Ш^1(G_{\mathbf{Q},S}, \mathrm{Sym}^2 E[l])$, which is by definition trivial in each $H^1(\mathbf{Q}_p, \mathrm{Sym}^2 E[l])$, is automatically trivial in each $H^1(\mathbf{Q}_p, A)$, and thus lies in $Ш^1(G_{\mathbf{Q},S}, A)$. In other words, the induced map on the kernels of the vertical maps in (3) is the desired injection

$$Ш^1(G_{\mathbf{Q},S}, \mathrm{Sym}^2 E[l]) \hookrightarrow Ш^1(G_{\mathbf{Q},S}, A).$$

To prove the lemma it will therefore suffice to show that $Ш^1(G_{\mathbf{Q},S}, A)$ injects into $H^1_f(\mathbf{Q}, A)$.

It follows from Lemma 4 that there is an injection

$$H^1(G_{\mathbf{Q},S}, A) \hookrightarrow H^1(\mathbf{Q}, A)$$

and that the composite maps

$$H^1(G_{\mathbf{Q},S}, A) \to H^1(\mathbf{Q}, A) \to H^1(I_p, A) \cong H^1(\mathbf{Q}_p, A)/H^1_f(\mathbf{Q}_p, A) \tag{4}$$

are zero for all $p \notin S$. We must show that the image of $Ш^1(G_{\mathbf{Q},S}, A)$ in $H^1(\mathbf{Q}, A)$ lies in $H^1_f(\mathbf{Q}, A)$. By (4), this image is automatically locally unramified for all $p \notin S$. Furthermore, an argument using a diagram analogous to (3) above shows that the maps

$$Ш^1(G_{\mathbf{Q},S}, A) \to H^1(\mathbf{Q}, A) \to H^1(\mathbf{Q}_p, A)$$

are zero for $p \in S$. Thus the image of $Ш^1(G_{\mathbf{Q},S}, A)$ trivially lands in $H^1_f(\mathbf{Q}_p, A)$ for such p. Thus now $Ш^1(G_{\mathbf{Q},S}, A)$ maps to $H^1_f(\mathbf{Q}_p, A)$ for every prime p, so its image in $H^1(\mathbf{Q}, A)$ lies in $H^1_f(\mathbf{Q}, A)$. Thus $Ш^1(G_{\mathbf{Q},S}, A)$ injects into $H^1_f(\mathbf{Q}, A)$, which proves the lemma. □

At this point, we have reduced the proof of Theorem 1 to the vanishing of the Selmer group $H^1_f(\mathbf{Q}, A)$.

5. The L-function of $\mathrm{Sym}^2 T_l E$

Before we complete our final reformulation of Theorem 1, we should give the long promised explanation of the term $L(\mathrm{Sym}^2 T_l E, 0)/\Omega$. Recall that the L-function of the Tate module of an elliptic curve (also known as the L-function of the elliptic curve) is defined using the characteristic polynomials of Frobenius elements acting on $T_l E$. We use an analogous method to define $L(\mathrm{Sym}^2 T_l E, s)$. Specifically, the action of $G_{\mathbf{Q}_p}$ on T is unramified for every $p \notin S$, so it makes sense to talk about the action of a Frobenius element Fr_p on T. Let $P_p(t)$ be the characteristic polynomial of Fr_p^{-1} acting on T:

$$P_p(t) = \det(1 - \mathrm{Fr}_p^{-1}\,|_T t).$$

For $p \in S - \{l\}$, Fr_p is only well-defined acting on the inertia invariants T^{I_p}, so we define

$$P_p(t) = \det(1 - \mathrm{Fr}_p^{-1}\,|_{T^{I_p}} t|).$$

These are all initially polynomials with coefficients in $\mathbf{Z}_l$, but it turns out that $P_p(t)$ actually has coefficients in $\mathbf{Z}$ and the polynomial $P_p(t)$ does not depend on the distinguished prime l, so long as $l \neq p$. (Again, this is all completely analogous to the $T_l E$ case.)

This suggests that to define the factor $P_l(t)$ itself, we should not work directly with T, but rather switch to $\mathrm{Sym}^2 T_p E$ for some $p \neq l$. $\mathrm{Sym}^2 T_p E$ is unramified at l (since E is assumed to have good reduction at l), so Fr_l is well-defined here and we define

$$P_l(t) = \det(1 - \mathrm{Fr}_l^{-1} |_{\mathrm{Sym}^2 T_p E} t).$$

As before this is independent of the choice of auxiliary $p \neq l$.

We now define

$$L(T, s) = \prod_p P_p(p^{-s})^{-1}.$$

It is shown in [CS87] that $L(T, s)$ is an entire function of s.

Since E is modular, one can use the work of Shimura [Shi76] to compute special values of this L-function. Let N be the conductor of E and fix a modular parameterization

$$\phi : X_0(N) \to E$$

of E. We assume that ϕ is minimal in the sense that $\deg \phi$ is as small as possible for our fixed E and N. Let $f(z)$ be the newform corresponding to ϕ; this means that for all p not dividing N, the p^{th} Fourier coefficient of $f(z)$ equals $p + 1 - \#E(\mathbf{F}_p)$. Let ω be the Néron differential on E. (If E is given in the form $y^2 = x^3 + ax + b$, ω is just $dx/2y$.) Since ϕ is defined over $\mathbf{Q}$, one can show that the pullback of ω under ϕ must be a rational multiple of the differential $2\pi i f(z) dz$ on $X_0(N)$. We define the *Manin constant* $c \in \mathbf{Q}^\times$ by the equality

$$\phi^* \omega = c 2\pi i f(z) dz.$$

Work of Mazur shows that c is divisible only by 2 and primes of bad reduction for E; see [Maz78, Corollary 4.1].

We also use ω to define the period Ω by

$$\Omega = \pi i \int_{E(\mathbf{C})} \omega \wedge \bar{\omega}.$$

Shimura's formula is

$$\frac{L(T, 0)}{\Omega} = \frac{\deg \phi}{N c^2} \prod_{p \in S'} P_p(1). \tag{5}$$

Here S' is the subset of S of places where E has potentially good reduction. Note in particular that $L(T, 0)/\Omega$ is rational.

We now state the theorem which we will prove in the remainder of this paper and explain how it implies Theorem 1.

Theorem 8. *Let E be a rational elliptic curve and let $\phi : X_0(N) \to E$ be a modular parameterization. Let l be a prime such that*

- *E has good reduction at l;*
- *$l \geq 5$;*
- *The Tate module representation $\rho : G_{\mathbf{Q},S} \to \mathrm{GL}_2(\mathbf{Z}_l)$ is surjective.*

Then $\deg \phi \cdot H^1_f(\mathbf{Q}, A^*) = 0$.

To see that this implies Theorem 1, recall that we had already reduced the proof to showing that $H^1_f(\mathbf{Q}, A)$ vanishes. We had also assumed that l does not divide $L(T,0)/\Omega$. We first must show that l does not divide $\deg\phi$ either. To see this, by (5) we need to show that the rational number

$$\frac{1}{Nc^2}\prod_{p\in S'} P_p(1)$$

has no factors of l in the denominator. N and c^2 are divisible only by 2 and primes of bad reduction for E, and each $P_p(1)$ is an integer, so this is clear. Thus l does not divide $\deg\phi$.

Now, by Theorem 8, $H^1_f(\mathbf{Q}, A^*)$ is annihilated by the l-adic unit $\deg\phi$. But $H^1_f(\mathbf{Q}, A^*)$ is an l-power torsion group since A^* is, and it follows that it must be 0. This in turn implies that both $A^*(\mathbf{Q})$ and $Ш(A^*/\mathbf{Q})$ vanish, as they are a subgroup and a quotient of $H^1_f(\mathbf{Q}, A^*)$, respectively. Flach has shown (see [Fla90b]) that the vanishing of $A^*(\mathbf{Q})$ implies that of $A(\mathbf{Q})$. Furthermore, he constructs (generalizing ideas of Cassels and Tate; see [Fla90a]) a perfect pairing

$$Ш(A/\mathbf{Q}) \otimes Ш(A^*/\mathbf{Q}) \to \mathbf{Q}_l/\mathbf{Z}_l;$$

thus the vanishing of $Ш(A^*/\mathbf{Q})$ implies that of $Ш(A/\mathbf{Q})$. Since both $A(\mathbf{Q})$ and $Ш(A/\mathbf{Q})$ vanish, this implies that the Selmer group $H^1_f(\mathbf{Q}, A)$ vanishes, which completes the proof of Theorem 1.

6. Kolyvagin's theory of Euler systems

Until the mid-eighties the problem of bounding Selmer groups was nearly hopeless; there were no methods which worked in any generality. This changed dramatically with the work of Thaine and Rubin and finally Kolyvagin's theory of Euler systems. Since we only seek to annihilate $H^1_f(\mathbf{Q}, A^*)$, rather than actually bound its order, we will need only the rudiments of the theory. There are several good sources for more extensive treatments: see [Was97a, Chapter 15] for a nice introduction, [Gro91] and [Rub89] for applications to the arithmetic of elliptic curves, and [Rub99] for a general theory. In fact, all of these sources deal with a slightly different type of Euler system than we will use. We will have more to say about this later.

We only sketch the main ideas. For a proof of the result we will need, see [Fla92, Proposition 1.1] or [Wes98].

Fix a power l^n of l and set $T_n = T/l^nT$, $A^*_n = A^*[l^n]$. We must work with these finite modules for technical reasons; passing from them to the full modules will be easy. The basic idea is the following: recall that since $A^*_n = \mathrm{Hom}(T_n, \mu_{l^n})$ there is a Tate local duality

$$H^1(\mathbf{Q}_p, T_n) \otimes H^1(\mathbf{Q}_p, A^*_n) \to \mathbf{Q}_l/\mathbf{Z}_l;$$

see [Was97b, Theorem 1]. One can show easily that $H^1_f(\mathbf{Q}_p, T_n)$ and $H^1_f(\mathbf{Q}_p, A^*_n)$ are exact annihilators of each other (see [Wes98, Lectures 5 and 6]), so that restricting the right-hand factor to $H^1_f(\mathbf{Q}_p, A^*_n)$ gives a perfect pairing

$$H^1_s(\mathbf{Q}_p, T_n) \otimes H^1_f(\mathbf{Q}_p, A^*_n) \to \mathbf{Q}_l/\mathbf{Z}_l. \tag{6}$$

These local pairings sum to a global pairing

$$\left(\oplus_p H^1_s(\mathbf{Q}_p, T_n)\right) \otimes H^1_f(\mathbf{Q}, A^*_n) \to \mathbf{Q}_l/\mathbf{Z}_l; \tag{7}$$

the pairing of an element $(c_p) \in \oplus H^1_s(\mathbf{Q}_p, T_n)$ and $d \in H^1_f(\mathbf{Q}, A^*_n)$ is simply the sum of the local pairings (6) of c_p and $\mathrm{res}_p\, d$; since $c_p = 0$ for almost all p, this is well-defined. This pairing is not perfect, but it does have the following key property, which is a consequence of global class field theory: the image of $H^1(\mathbf{Q}, T_n)$ under the natural map

$$H^1(\mathbf{Q}, T_n) \to \prod_p H^1(\mathbf{Q}_p, T_n) \to \prod_p H^1_s(\mathbf{Q}_p, T_n)$$

actually lands in $\oplus_p H^1_s(\mathbf{Q}_p, T_n)$ (see [Wes98, Lecture 7, Section 2.1]; this is one place where it is critical that we dropped to a finite quotient of T) and it is orthogonal to all of $H^1_f(\mathbf{Q}, A^*_n)$ under the global pairing (7); see [Wes98, Lecture 8].

The significance of this to our problem is the following: suppose that for lots of primes r we can exhibit elements $c_r \in H^1(\mathbf{Q}, T_n)$ with the property that they restrict to 0 in $H^1_s(\mathbf{Q}_p, T_n)$ for all p *except* for r itself, where they restrict to something non-zero. Under the global pairing, the image of c_r in $\oplus H^1_s(\mathbf{Q}_p, T_n)$ is orthogonal to all of $H^1_f(\mathbf{Q}, A^*_n)$. But the definition of the global pairing together with the fact that c_r restricts to 0 in $H^1_s(\mathbf{Q}_p, T_n)$ away from r now shows that $\mathrm{res}_r\, c_r \in H^1_s(\mathbf{Q}_r, T_n)$ is orthogonal to the image of $H^1_f(\mathbf{Q}, A^*_n)$ in $H^1_f(\mathbf{Q}_r, A^*_n)$ under the Tate local pairing at r. If $\mathrm{res}_r\, c_r$ generates a submodule of $H^1_s(\mathbf{Q}_r, T_n)$ of small index, then this orthogonality and the fact that the Tate local pairing is perfect will force $H^1_f(\mathbf{Q}, A^*_n)$ to map into a small subgroup of $H^1_f(\mathbf{Q}_r, A^*_n)$. Since we can do this for lots of r, we obtain conditions on the local behavior of $H^1_f(\mathbf{Q}, A^*_n)$ at many primes r. Hopefully if we could do this for enough primes r we could somehow show that the local conditions are so stringent that the group $H^1_f(\mathbf{Q}, A^*_n)$ itself must be small.

Before we state all of this somewhat more formally, we prove the following fundamental lemma. We will call a prime p *good* if it is not in S and if a Frobenius element at p acts on $E[l]$ as complex conjugation. This is equivalent to Fr_p being a complex conjugation element on the splitting field $\mathbf{Q}(E[l])$ of $E[l]$. This field is a finite extension of $\mathbf{Q}$ since $E[l]$ is finite, so by the Tchebatorev density theorem there are infinitely many good primes.

Lemma 9. *Assume $p \notin S$. Then*

$$H^1_s(\mathbf{Q}_p, T) \cong T(-1)^{G_{\mathbf{F}_p}}.$$

If p is good, then this group is a free $\mathbf{Z}_l$-module of rank 1. In particular, each $H^1_s(\mathbf{Q}_p, T_n)$ is a free $\mathbf{Z}/l^n\mathbf{Z}$-module of rank 1.

Proof. For the first isomorphism, recall that

$$H^1_s(\mathbf{Q}_p, T) \cong H^0(\mathbf{F}_p, H^1(I_p, T)).$$

Since I_p acts trivially on T, $H^1(I_p, T)$ is nothing more than $\mathrm{Hom}(I_p, T)$. Now, T is a pro-l group, so only the pro-l part of I_p can map to it non-trivially. By Lemma 5, this quotient is isomorphic to $\mathbf{Z}_l(1)$ as a $G_{\mathbf{F}_p}$-module. We conclude that

$$H^0(\mathbf{F}_p, H^1(I_p, T)) \cong H^0(\mathbf{F}_p, \mathrm{Hom}(\mathbf{Z}_l(1), T)).$$

But $\mathrm{Hom}(\mathbf{Z}_l(1), T)$ is canonically isomorphic to $\mathrm{Hom}(\mathbf{Z}_l, T(-1))$, which in turn is just $T(-1)$. This proves the first statement.

Now assume that p is good. This means that Fr_p acts on $E[l]$ as complex conjugation. In particular, it is a non-scalar involution, which one easily shows implies that it acts diagonally on $E[l]$ with eigenvalues 1 and -1. A Nakayama's lemma argument together with Hensel's lemma and a dimension count allows one to conclude that there is a basis x, y of $T_l E$ over $\mathbf{Z}_l$ with respect to Fr_p acts diagonally; that is, $\mathrm{Fr}_p(x) = ux$ and $\mathrm{Fr}_p(y) = vy$, and we must have

$$u \equiv -v \equiv 1 \pmod{l}.$$

Note that uv is the determinant of Fr_p acting on $T_l E$, which is just $\varepsilon(\mathrm{Fr}_p) = p$ since $T_l E$ has cyclotomic determinant by the Weil pairing. In particular, $p \equiv -1 \pmod{l}$.

A basis for $T = \mathrm{Sym}^2 T_l E$ is given by $x \otimes x, x \otimes y + y \otimes x, y \otimes y$. Fr_p acts on the first by multiplication by u^2; on the second by multiplication by $uv = p$; and on the third by multiplication by v^2. Note that $u^2 \equiv v^2 \equiv 1 \pmod{l}$, which implies that neither u^2 nor v^2 equals p.

Now consider $T(-1)$. Fr_p acts on $\mathbf{Z}_l(1)$ by multiplication by $\varepsilon(\mathrm{Fr}_p) = p$, so it acts on $\mathbf{Z}_l(-1)$ by multiplication by p^{-1}. Thus Fr_p acts on our basis of $T(-1)$ by multiplication by $u^2 p^{-1}$, 1 and $v^2 p^{-1}$ respectively. As we saw above, the first and last terms are different from 1. It follows that only the rank one subspace of multiples of $x \otimes y + y \otimes x$ is invariant under the $G_{\mathbf{F}_p}$-action, so $H^1_s(\mathbf{Q}_p, T) = T(-1)^{G_{\mathbf{F}_p}}$ is free of rank one over $\mathbf{Z}_l$, as claimed.

The result for T_n follows exactly the same argument. □

We are now in a position to give a precise definition of the sort of set of cohomology classes we seek: let η be an integer. We define a *Flach system of depth η for T_n* to be a collection of cohomology classes $c_r \in H^1(\mathbf{Q}, T_n)$, one for each good prime r, such that:

- $\mathrm{res}_p c_r$ lies in $H^1_f(\mathbf{Q}_p, T_n)$ for $p \neq r$;
- $\mathbf{Z}_l \cdot \mathrm{res}_r c_r$ contains $\eta H^1_s(\mathbf{Q}_r, T_n)$.

The second condition is equivalent to the quotient $H^1_s(\mathbf{Q}_r, T_n)/\mathbf{Z}_l \cdot \mathrm{res}_r c_r$ being annihilated by η. By Lemma 9, $H^1_s(\mathbf{Q}_r, T_n)$ is a free $\mathbf{Z}/l^n\mathbf{Z}$-module of rank 1, so this condition is reasonable. Note that to check both of the conditions in the definition above, we simply need a good understanding of the singular restriction maps

$$H^1(\mathbf{Q}, T_n) \to H^1(\mathbf{Q}_p, T_n) \to H^1_s(\mathbf{Q}_p, T_n)$$

for all primes p.

Of course, it is trivial and not very useful to write down a Flach system of depth l^n for T_n; to make this a useful notion, we will want η to be independent of n.

Recall that we have assumed that the Tate module representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ is surjective. This implies immediately that $E[l]$ is an absolutely irreducible $G_{\mathbf{Q}}$-representation, which in turn one can check implies that $A^*[l] \cong (\mathrm{Sym}^2 E[l])^*$ is absolutely irreducible. Even though we are assuming all of these hypotheses, we will include the relevant ones in the hypotheses of each result below.

Given what we have said so far, the following lemma is fairly straightforward.

Lemma 10. *Assume that T_n admits a Flach system of depth η. Then for every $d \in H^1_f(\mathbf{Q}, A^*_n)$ and every good prime r, $\mathrm{res}_r d$ lies in $H^1_f(\mathbf{Q}_p, A^*_n)[\eta]$.*

Proof. See [Wes98, Lecture 15, Section 1.2]. □

More difficult is the next result, which goes from this local annihilation result to a global annihilation result. Let K be the fixed field of the kernel of $G_{\mathbf{Q},S}$ acting on $E[l^n]$; it is a finite extension of $\mathbf{Q}$ since $E[l^n]^*$ is finite. Note that this field also lies in the kernel of the $G_{\mathbf{Q},S}$ action on $A^*[l^n]$ (since its Galois action is entirely derived from $E[l^n]$ and the cyclotomic character) and that there is a natural inflation injection

$$H^1(K/\mathbf{Q}, A_n^*) \hookrightarrow H^1(\mathbf{Q}, A_n^*).$$

Lemma 11. *Assume that $l \neq 2$ and that $A^*[l]$ is absolutely irreducible as a $G_{\mathbf{Q},S}$-module. Let $d \in H^1(\mathbf{Q}, A_n^*)$ be such that $\operatorname{res}_r d = 0$ for every good prime r. Then d lies in the image of $H^1(K/\mathbf{Q}, A_n^*)$.*

Proof. See [Wes98, Lecture 15, Section 1.3]. □

Lemma 10 and Lemma 11 combine to show that

$$\eta H_f^1(\mathbf{Q}, A_n^*) \subseteq H^1(K/\mathbf{Q}, A_n^*).$$

Since the l^n-torsion representation $\rho_n : G_{\mathbf{Q},S} \to \mathrm{GL}_2(\mathbf{Z}/l^n\mathbf{Z})$ is surjective, we will have $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathrm{GL}_2(\mathbf{Z}/l^n\mathbf{Z})$. Furthermore, Lemma 2 and Lemma 3 show that $A_n^* \cong \mathrm{ad}^0(\rho_n)$. The next result, which is purely a statement about group cohomology, now finishes our proof, at least at the level of l^n-torsion.

Lemma 12. *Let $\mathrm{GL}_2(\mathbf{Z}/l^n\mathbf{Z})$ act on $\mathrm{End}^0(\mathbf{Z}/l^n\mathbf{Z})$ via the adjoint action. Then*

$$H^1(\mathrm{GL}_2(\mathbf{Z}/l^n\mathbf{Z}), \mathrm{End}^0(\mathbf{Z}/l^n\mathbf{Z})) = 0.$$

Proof. See [DDT97, Lemma 2.48] and [Fla92]. □

Combining all of this, we have the following theorem.

Theorem 13. *Let E be a rational elliptic curve and let l be a prime. Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ be the associated Tate module representation. Assume that ρ is surjective. Further assume that for every good prime r there is a class $c_r \in H^1(\mathbf{Q}, T)$ such that*

- *$\operatorname{res}_p c_r$ lies in $H_f^1(\mathbf{Q}_p, T)$ for $r \neq p$;*
- *$\mathbf{Z}_l \cdot \operatorname{res}_r c_r$ contains $\eta H_s^1(\mathbf{Q}_r, T_n)$.*

Then η annihilates $H_f^1(\mathbf{Q}, A^*)$.

Proof. The given Flach system for T induces one for each T_n. The results to this point have thus shown that $\eta H_f^1(\mathbf{Q}, A_n^*) = 0$ for each n. But any class $d \in H_f^1(\mathbf{Q}, A^*)$ must be annihilated by some power of l, so it lies in the image of some $H_f^1(\mathbf{Q}, A_n^*)$. (Note that $H_f^1(\mathbf{Q}, A_n^*)$ maps into $H_f^1(\mathbf{Q}, A^*)$ since we defined the finite subgroups for A_n^* using those for A^*.) Thus $\eta d = 0$, which completes the proof. □

The proof of Theorem 13 is purely a Galois cohomology argument, and therefore there is no actual need to assume that the representation ρ comes from an elliptic curve. For example, in [Fla95] Galois representations coming from more general modular forms are considered.

The machinery we have given is sufficient for annihilation and finiteness results. To actually obtain a bound on the order of $H_f^1(\mathbf{Q}, A^*)$, one has to exhibit classes not only for prime levels (like the c_r) but also for composite levels. Kolyvagin's derivative construction is then used to turn these classes into better and better

annihilators. We should note, however, that with most Euler systems which have been studied the classes c_n are defined over larger and larger fields, depending on n. In our case, the classes would all be defined over $\mathbf{Q}$. Such an Euler system is often called a *geometric Euler system*, and there is not yet a general theory of such objects. For one example, see [Rub91]. In fact, no one has succeeded in extending the Flach system above to a full geometric Euler system; this was the "gap" in the original proof of semistable Taniyama-Shimura by Wiles, which was eventually filled in by Taylor-Wiles using different methods.

7. The Flach map

We continue to let E be an elliptic curve over $\mathbf{Q}$ and $\phi : X_0(N) \to E$ a modular parameterization. It remains to construct a Flach system for T of depth $\deg \phi$. This construction lies at the heart of Flach's proof. These classes will come from certain well-chosen geometric objects on the surface $E \times E$, although in order to actually exhibit them we will need to work on the surface $X_0(N) \times X_0(N)$, which has a much richer intrinsic geometry. These objects are then transformed into classes in $H^1(\mathbf{Q}, T)$ via a certain Chern class map. The key to Flach's construction is that it is possible to read off local properties of these classes in $H^1_s(\mathbf{Q}_p, T)$ from corresponding local properties of the associated geometric objects. That is, we will begin with a map $\sigma : \mathcal{C}(E \times E) \to H^1(\mathbf{Q}, T)$, where $\mathcal{C}(E \times E)$ will be defined in a moment purely geometrically. We can not describe the image of σ directly (we can't even really describe $H^1(\mathbf{Q}, T)$ effectively), but there is (for p not lying in S) a commutative diagram

$$\begin{array}{ccccc} \mathcal{C}(E \times E) & \longrightarrow & \cdot & & \\ \downarrow{\scriptstyle \sigma} & & & & \downarrow \\ H^1(\mathbf{Q}, T) & \longrightarrow & H^1(\mathbf{Q}_p, T) & \longrightarrow & H^1_s(\mathbf{Q}_p, T) \end{array} \tag{8}$$

to be filled in later. Since all we care about for the production of our Flach system is the restriction of classes to $H^1_s(\mathbf{Q}_p, T)$, to check that classes c_r really form a Flach system we will be able to bypass the complicated $H^1(\mathbf{Q}, T)$ entirely and work instead with much more concrete geometric objects.

We begin by defining $\mathcal{C}(E \times E)$, which will involve working with curves lying in the surface $E \times E$. Let C be any projective algebraic curve over $\mathbf{Q}$; we do *not* assume that C is non-singular. We will be interested in rational functions on C which have trivial Weil divisor. (Recall that the *Weil divisor* of the function f on C is the formal sum of the points at which it has zeros minus the formal sum of the points at which it has poles, all counted with multiplicity. Often Weil divisors are only defined for *nonsingular* curves, but it is possible to define them more generally. One possible definition will become clear below.) If C is nonsingular, then it is a standard fact that the only such functions are constant. However, if C is singular, it is possible to exhibit non-constant rational functions with trivial Weil divisor.

For an example, consider a curve C with a nodal singularity P. Let C' be its normalization, with P_1 and P_2 the points lying above P. Let f be a rational function on C' with divisor $nP_1 - nP_2$ for some n. (Such a function may or may not exist for a general C'; it will certainly exist if C' has genus 0, for example.) C' and C are birational, so f can also be interpreted as a rational function on C, and

both P_1 and P_2 map to P. Thus f has trivial Weil divisor on C, even though it is a non-constant rational function.

Now consider the non-singular projective surface $E \times E$. We define $\mathcal{C}(E \times E)$ as follows: elements are pairs (C, f) of (possibly singular) curves C contained in $E \times E$ together with a rational function f on C with trivial Weil divisor. We also require that both C and f are defined over $\mathbf{Q}$. Flach defines a map

$$\sigma : \mathcal{C}(E \times E) \to H^1(\mathbf{Q}, T)$$

which is what we will use to generate our Flach system. For the definition of σ, which involves étale cohomology and algebraic K-theory, see Appendix B.

Let us try briefly to explain the underlying philosophy by analogy with algebraic topology. Begin with the genus one complex curve $E(\mathbf{C})$, which we can regard as $\mathbf{C}/\Lambda$ for an appropriate lattice Λ. One way to obtain Λ is as the integral homology group $H_1(E(\mathbf{C}), \mathbf{Z})$ (just thing about the standard homology generators on a torus), which is a lattice of maximal rank in $H_1(E(\mathbf{C}), \mathbf{R}) \cong \mathbf{C}$. From this point of view the l^n-torsion on E is $\frac{1}{l^n}\Lambda$, so that the l-adic Tate module of E is $\Lambda \otimes_{\mathbf{Z}} \mathbf{Z}_l$; thus we can regard the l-adic Tate module of E as $H_1(E(\mathbf{C}), \mathbf{Z}_l)$. Of course, we have lost any trace of Galois actions, but let us not concern ourselves with this at the moment.

Now consider the complex surface $E(\mathbf{C}) \times E(\mathbf{C})$ and its second homology group $H_2(E(\mathbf{C}) \times E(\mathbf{C}), \mathbf{Z})$. The Künneth theorem shows that this group surjects onto

$$H_1(E(\mathbf{C}), \mathbf{Z}) \otimes_{\mathbf{Z}} H_1(E(\mathbf{C}), \mathbf{Z}).$$

Tensoring this with $\mathbf{Z}_l$ yields

$$H_1(E(\mathbf{C}), \mathbf{Z}_l) \otimes_{\mathbf{Z}_l} H_1(E(\mathbf{C}), \mathbf{Z}_l)$$

which by the above discussion contains $\mathrm{Sym}^2 T_l E = T$ as a direct summand. Combining all of this we see that we have a map

$$H_2(E(\mathbf{C}) \times E(\mathbf{C}), \mathbf{Z}_l) \to T.$$

By Poincaré duality, we can also regard this as a map

$$H^2(E(\mathbf{C}) \times E(\mathbf{C}), \mathbf{Z}_l)^\vee \to T \tag{9}$$

where the $\vee$ denotes the Poincaré dual. We will return to this map later.

Now consider a pair (C, f). The curve C has real dimension 2, and therefore determines in a natural way an element of the homology group

$$H_2(E(\mathbf{C}) \times E(\mathbf{C}), \mathbf{Z}).$$

If f has non-trivial divisor on C, then we could also use this divisor (which has real dimension 0) to determine an element of

$$H_0(E(\mathbf{C}) \times E(\mathbf{C}), \mathbf{Z}).$$

In our case, however, f has trivial divisor. In this situation, the pair (C, f) does not determine anything of dimension 0, but still somehow contains more information than just C itself. This extra information has the effect of cutting down the relevant dimension by 1, so that (C, f) determines an element of

$$H_1(E(\mathbf{C}) \times E(\mathbf{C}), \mathbf{Z}).$$

(This is where the algebraic K-theory comes in; K-theory is very good at keeping track of dimensions like this which may not make all that much sense purely

geometrically.) Applying Poincaré duality we can regard this as an element of $H^3(E(\mathbf{C}) \times E(\mathbf{C}), \mathbf{Z})^\vee$. So far, then, we have a map

$$\mathcal{C}(E \times E) \to H^3(E(\mathbf{C}) \times E(\mathbf{C}), \mathbf{Z})^\vee. \tag{10}$$

(At this point we should confess that this map turns out to just be the zero map. It will nevertheless serve our motivational purposes.)

Étale cohomology is the algebraic analogue of singular cohomology, and the first miracle of étale cohomology is that the preceding construction can be carried out over $\bar{\mathbf{Q}}$ rather than $\mathbf{C}$, so long as we always use l-adic coefficients. Thus the pair (C, f) should give rise to an element of the dual $H^3_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l)^\vee$ of the étale cohomology group $H^3_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l)$; this last cohomology group is isomorphic to $H^3(E(\mathbf{C}) \times E(\mathbf{C}), \mathbf{Z}_l)$ as an abelian group, but has the advantage of having a Galois action.

In fact, since (C, f) is defined over $\mathbf{Q}$, this element should be Galois invariant, yielding a map

$$\mathcal{C}(E \times E) \to \left(H^3_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l)^\vee\right)^{G_{\mathbf{Q}}}$$

analogous to (10). Unfortunately, $H^3_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l)^\vee$ can be shown to have no Galois invariants, so at the moment all of this work has produced 0.

The second miracle of étale cohomology is that we can carry our construction out over $\mathbf{Q}$, rather than $\bar{\mathbf{Q}}$. Thus (C, f) yields an element of $H^3_{\text{ét}}(E \times E, \mathbf{Z}_l)^\vee$. This group is no longer isomorphic to any singular cohomology group, but rather is a complicated combination of various Galois cohomology groups of étale cohomology groups of $E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}$. It admits a natural map via a spectral sequence to

$$H^0\left(\mathbf{Q}, H^3_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l)^\vee\right).$$

However, as we said above, this group vanishes, and from this one shows that the spectral sequence yields a map

$$H^3_{\text{ét}}(E \times E, \mathbf{Z}_l)^\vee \to H^1\left(\mathbf{Q}, H^2_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l)^\vee\right).$$

Thus we finally have a map

$$\mathcal{C}(E \times E) \to H^1\left(\mathbf{Q}, H^2_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l)^\vee\right).$$

Combining this with the étale analogue of (9), we finally obtain our desired Flach map

$$\sigma : \mathcal{C}(E \times E) \to H^1(\mathbf{Q}, T).$$

We now discuss the local behavior of σ. Let p be a prime not lying in S. We will define a map

$$d_p : \mathcal{C}(E \times E) \to \mathrm{Div}(E_{\mathbf{F}_p} \times E_{\mathbf{F}_p})$$

where $\mathrm{Div}(E_{\mathbf{F}_p} \times E_{\mathbf{F}_p})$ is the group of Weil divisors (defined over $\mathbf{F}_p$) on the non-singular surface $E_{\mathbf{F}_p} \times E_{\mathbf{F}_p}$. (Recall that a Weil divisor on a surface is a formal sum of curves on the surface.) d_p is the map which will go on the top of (8) above. To define $d_p(C, f)$, first consider the reduction of C modulo p. This may well have several components $C_1, \ldots, C_n$, even if in characteristic 0 it did not. We claim that if the function f has a zero or pole at any point of a component C_i, then it has a zero or pole of the same order along the entire component C_i. (Actually, poles and zeros can combine at the points where the C_i intersect, but this doesn't matter much.) The idea is that if f had a zero or pole at an isolated point of C_i, then we could lift this to a zero or pole of f over $\mathbf{Q}$, which is not possible by the definition

of $\mathcal{C}(E \times E)$. Given this, for any component C_i we can let m_i be the order of the zero or pole of f on C_i: of course, we could have $m_i = 0$. We define

$$d_p(C, f) = \sum m_i C_i.$$

The last thing we will need to connect the geometry to the behavior of cohomology classes is a map from $\mathrm{Div}(E_{\mathbf{F}_p} \times E_{\mathbf{F}_p})$ to $H^1_s(\mathbf{Q}_p, T)$. Recall that by Lemma 9 we have $H^1_s(\mathbf{Q}_p, T) \cong T(-1)^{G_{\mathbf{F}_p}}$. This in turn is isomorphic to $\mathrm{End}^0_{G_{\mathbf{F}_p}}(T_l E)$, by Lemma 2. That is, the singular quotient at p corresponds precisely to trace zero $G_{\mathbf{F}_p}$-equivariant maps of the l-adic Tate module of E. The map we seek is a standard one in algebraic geometry, called a *cycle class map*:

$$s : \mathrm{Div}(E_{\mathbf{F}_p} \times E_{\mathbf{F}_p}) \to \mathrm{End}_{G_{\mathbf{F}_p}}(T_l E) \to \mathrm{End}^0_{G_{\mathbf{F}_p}}(T_l E)$$

(the second map is simply projection onto a direct summand). We will not give a general description of the map $\mathrm{Div}(E_{\mathbf{F}_p} \times E_{\mathbf{F}_p}) \to \mathrm{End}_{G_{\mathbf{F}_p}}(T_l E)$, except in the special case we will need. (In fact, if $\mathrm{End}_{G_{\mathbf{F}_p}}(T_l E)$ is given an appropriate cohomological interpretation, then the cycle class map is really just an algebraic version of part of the algebraic topology construction discussed above.) Let $g : E_{\mathbf{F}_p} \to E_{\mathbf{F}_p}$ be some map. Let Γ_g be the graph of g, by which we mean the image of the product map

$$\mathrm{id} \times g : E_{\mathbf{F}_p} \to E_{\mathbf{F}_p} \times E_{\mathbf{F}_p}.$$

Then Γ_g has codimension 1 in $E_{\mathbf{F}_p} \times E_{\mathbf{F}_p}$, and thus is an element of $\mathrm{Div}(E_{\mathbf{F}_p} \times E_{\mathbf{F}_p})$. The image of Γ_g under s is nothing other than the endomorphism of $T_l E$ induced by the map g (or more honestly its projection onto the trace zero direct summand). This endomorphism is $G_{\mathbf{F}_p}$-equivariant since g is defined over $\mathbf{F}_p$.

We are finally in a position to state the fundamental local description of the map σ: for every prime p not in S, there is a commutative diagram

$$\begin{array}{ccccccc} \mathcal{C}(E \times E) & & \xrightarrow{\qquad\qquad d_p \qquad\qquad} & & & & \mathrm{Div}(E_{\mathbf{F}_p} \times E_{\mathbf{F}_p}) \\ \downarrow{\scriptstyle \sigma} & & & & & & \downarrow{\scriptstyle s} \\ H^1(\mathbf{Q}, T) & \longrightarrow & H^1(\mathbf{Q}_p, T) & \longrightarrow & H^1_s(\mathbf{Q}_p, T) & \xrightarrow{\cong} & \mathrm{End}^0_{G_{\mathbf{F}_p}}(T_l E) \end{array} \tag{11}$$

"All" we have to do to generate our Flach system, then, is to exhibit appropriate elements of $\mathcal{C}(E \times E)$ and compute their image in $\mathrm{End}^0_{G_{\mathbf{F}_p}}(T_l E)$ via the clockwise maps. Unfortunately, in general this would be extremely difficult. That is, given an arbitrary surface S, it is a very difficult problem in algebraic geometry to write down many particularly useful curves on S. In order to do this in our case we will have to take full advantage of the fact that E is modular.

8. The geometry of modular curves

In this section we review the facts we will need about the geometry of modular curves. For a more thorough treatment and references to the standard sources, see [DI95, Part II].

Let N be a positive integer and let $\Gamma_0(N)$ be the usual congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$. Recall that orbits for the $\Gamma_0(N)$-action on the upper half plane $\mathfrak{H}$ correspond to isomorphism classes of pairs of complex elliptic curves E and cyclic subgroups of $E(\mathbf{C})$ of order N. Furthermore, the orbit space $\Gamma_0(N)\backslash\mathfrak{H}$ can be given the structure of a non-compact Riemann surface. We will write $Y_0(N)^{\mathrm{an}}$ for this

Riemann surface. (The "an" is for analytic.) We can also compactify $Y_0(N)^{\mathrm{an}}$ by adding a finite number of points called the *cusps*; we write $X_0(N)^{\mathrm{an}}$ for the resulting compact Riemann surface.

It is a classical fact of algebraic geometry that every compact Riemann surface can be realized as a nonsingular projective complex algebraic curve; that is, there is an algebraic curve $X_0(N)_{\mathbf{C}}$ over the complex numbers such that the $\mathbf{C}$-valued points of $X_0(N)_{\mathbf{C}}$ recover $X_0(N)^{\mathrm{an}}$. A fundamental fact in the arithmetic theory of modular curves is that this curve can actually be defined over the rational numbers $\mathbf{Q}$. That is, the polynomial equations which define $X_0(N)_{\mathbf{C}}$ can be written in such a way that all of the coefficients are rational. We will write $X_0(N)_{\mathbf{Q}}$ for this nonsingular projective rational algebraic curve. All of the cusps of $X_0(N)_{\mathbf{Q}}$ are actually defined over $\mathbf{Q}$, so $Y_0(N)^{\mathrm{an}}$ can also be realized as the complex points of a nonsingular algebraic curve $Y_0(N)_{\mathbf{Q}}$; of course, $Y_0(N)_{\mathbf{Q}}$ is only quasi-projective.

Now that we have a model for our modular curve over $\mathbf{Q}$, we can ask how the equations for $X_0(N)_{\mathbf{Q}}$ reduce modulo primes p. The fundamental result is that $X_0(N)_{\mathbf{Q}}$ reduces to a nonsingular projective algebraic curve over $\mathbf{F}_p$ for every prime p which does not divide N. (Perhaps the most compact way to say this is that $X_0(N)_{\mathbf{Q}}$ is the generic fiber of a smooth proper $\mathbf{Z}[1/N]$-scheme. This description allows one to work with $X_0(N)_{\mathbf{Q}}$ and all of its reductions simultaneously, which is often convenient; nevertheless, we will content ourselves below with working one prime at a time.) From now on we will just write $X_0(N)$ when it does not matter what field (of characteristic 0 or p not dividing N) we are working over; the behavior of the modular curves over the various fields is virtually identical.

If p is a prime which divides N, then $X_0(N)$ will pick up singularities over $\mathbf{F}_p$, but at least in the case that p divides N exactly once it is possible to very explicitly describe $X_0(N)_{\mathbf{F}_p}$: it has two irreducible components, each isomorphic to $X_0(N/p)_{\mathbf{F}_p}$ (which is nonsingular by what we said above), and they intersect transversally at a finite number of points.

The other question one might ask about our models $Y_0(N)$ is whether or not they still classify pairs of elliptic curves and cyclic subgroups of order N. Let us say that a pair of an elliptic curve E and a cyclic subgroup C of order N is *defined over a field* K (of characteristic 0 or p not dividing N) if E is defined over K and if C is mapped to itself under the action of every element of the absolute Galois group of K. (Note that we do not require that C is fixed pointwise by the Galois group, which is equivalent to C actually lying in $E(K)$.) We could hope that the K-rational points of $Y_0(N)$ correspond to the pairs (E, C) as above which are defined over K. If this were the case, we would call these modular curves *fine moduli spaces* for classifying such pairs. Unfortunately, this is simply not true. This is well-known in the case $N = 1$: $Y_0(1)_{\mathbf{Q}}$ is isomorphic to the affine line $\mathbf{A}^1_{\mathbf{Q}}$ via the j-invariant, but the j-invariant is not enough to determine the isomorphism class of elliptic curves over fields which are not algebraically closed. The problem in the general case is similar, although somewhat less severe.

However, these modular curves are at least *coarse moduli spaces*. We will not give the technical definition of this, except to say that it means that the modular curves are as close to fine moduli spaces for classifying pairs as it is possible for them to be. In particular, every pair of an elliptic curve E and a cyclic subgroup C of order N, defined over a field K, does give rise to a point of $Y_0(N)(K)$.

In passing, we should note that it is also possible to give a modular interpretation to the cusps of $X_0(N)$ in terms of *generalized elliptic curves*. We will not give a description of this here; it is, however, extremely useful for computations involving the cusps.

We can use our moduli interpretations to define various maps between modular curves. (Actually, the description we gave above is not enough to actually make rigorous the upcoming definitions. However, we assure the reader that these constructions can be made entirely rigorous with a more thorough understanding of the moduli interpretation of $X_0(N)$.) Let K be a field as above, and let r be a prime not dividing N. A pair of an elliptic curve E and a cyclic subgroup C of order Nr, defined over K, gives rise in a natural way to a corresponding pair with respect to N: take the same elliptic curve E and take the unique cyclic subgroup of C of order N; call it C_N. We define

$$j_r : X_0(Nr) \to X_0(N)$$

to be the corresponding map; that is, it sends the point corresponding to the pair (E, C) to the point corresponding to the pair (E, C_N). (As we said above, this doesn't actually make sense, but it is possible to give it a better interpretation.) The fact that we can make this definition on the level of points for any field K (of the appropriate characteristics) insures that j_r can actually be defined over any of the fields $\mathbf{Q}$ or $\mathbf{F}_p$ for p not dividing N. Note that there is a slight subtlety (which we will ignore) for the field $\mathbf{F}_r$, as there we have not said anything about the moduli interpretation of $X_0(Nr)$.

There is a second way to obtain a map between these modular curves: let C_r be the unique subgroup of C of order r, and now send the pair (E, C) to the pair $(E/C_r, C/C_r)$. This gives rise to a second map

$$j'_r : X_0(Nr) \to X_0(N).$$

We define the r^{th} *Hecke correspondence* T_r on $X_0(N)$ to be the image of the product map

$$j_r \times j'_r : X_0(Nr) \to X_0(N) \times X_0(N).$$

It can be shown that T_r is a singular curve which is birational to $X_0(Nr)$. Furthermore, it is possible to give a very precise description of T_r in characteristic r. Recall that a curve (or more generally any scheme) over $\mathbf{F}_r$ has a Frobenius endomorphism induced by the r-power map on the function field. Define $\Gamma \subseteq X_0(N)_{\mathbf{F}_r} \times X_0(N)_{\mathbf{F}_r}$ as the graph of the Frobenius map $\mathrm{Fr} : X_0(N)_{\mathbf{F}_r} \to X_0(N)_{\mathbf{F}_r}$; that is, Γ is the image of the product map

$$\mathrm{id} \times \mathrm{Fr} : X_0(N)_{\mathbf{F}_r} \to X_0(N)_{\mathbf{F}_r} \times X_0(N)_{\mathbf{F}_r}.$$

We define the *Verschiebung* $\Gamma' \subseteq X_0(N)_{\mathbf{F}_r} \times X_0(N)_{\mathbf{F}_r}$ to be the image of the transpose map

$$\mathrm{Fr} \times \mathrm{id} : X_0(N)_{\mathbf{F}_r} \to X_0(N)_{\mathbf{F}_r} \times X_0(N)_{\mathbf{F}_r}.$$

Note that $T_{r,\mathbf{F}_r}$, Γ and Γ' are all of codimension one in the surface $X_0(N)_{\mathbf{F}_r} \times X_0(N)_{\mathbf{F}_r}$, and thus are divisors. The *Eichler-Shimura relation* states that there is an equality

$$T_{r,\mathbf{F}_r} = \Gamma + \Gamma'.$$

of divisors on $X_0(N)_{\mathbf{F}_r} \times X_0(N)_{\mathbf{F}_r}$. In fact, each of Γ and Γ' is the isomorphic image of one of the irreducible components of $X_0(Nr)_{\mathbf{F}_r}$ (both isomorphic to $X_0(N)_{\mathbf{F}_r}$) which we discussed above. This relation will be the key to our computations below.

9. Some modular units

Modular curves will be of use to us since the surface $X_0(N) \times X_0(N)$ has all of the fairly explicit divisors T_r. Our basic plan at this point is to find an appropriate rational function f_r on $T_{r,\mathbf{Q}}$ (for each r not dividing N) such that $(T_{r,\mathbf{Q}}, f_r) \in \mathcal{C}(X_0(N)_{\mathbf{Q}} \times X_0(N)_{\mathbf{Q}})$. We will then map the pair $(T_{r,\mathbf{Q}}, f_r)$ via $\phi \times \phi$ into $\mathcal{C}(E_{\mathbf{Q}} \times E_{\mathbf{Q}})$, and then by σ into $H^1(\mathbf{Q}, T)$. If we can also arrange for f_r to have trivial divisor away from characteristic r, then our geometric description of the local behavior of σ will show that f_r maps to 0 in each $H^1_s(\mathbf{Q}_p, T)$ for p not dividing rlN (recall that our geometric description of the Flach map broke at the primes in S) and we will be well on our way to constructing the desired Flach system.

Since $T_{r,\mathbf{Q}}$ is birational to $X_0(Nr)_{\mathbf{Q}}$, to exhibit rational functions on $T_{r,\mathbf{Q}}$ we can work instead on $X_0(Nr)_{\mathbf{Q}}$. Recall that rational functions on $X_0(Nr)_{\mathbf{Q}}$ are precisely modular forms of level Nr and weight 0, with coefficients in $\mathbf{Q}$. We will define such a function as the ratio of two modular forms of the same weight.

We want f_r to have trivial divisor over $\mathbf{Q}$, so we should start with modular forms with especially simple divisors. Perhaps the best known is $\Delta(z)$, the unique cusp form of level 1 and weight 12. Δ is initially defined on $X_0(1)_{\mathbf{Q}}$, and has a simple zero at the unique cusp ∞ and no other zeros or poles. (Δ is a differential form, not a function, so it can have more zeros than poles.) Pulling back Δ via the natural map $\pi : X_0(N)_{\mathbf{Q}} \to X_0(1)_{\mathbf{Q}}$ yields a form $\pi^*\Delta$ on $X_0(N)_{\mathbf{Q}}$ (this is really nothing more than reinterpreting Δ as having level N) which will have zeros of various orders at the cusps and no other zeros or poles:

$$\operatorname{div}_{X_0(N)_{\mathbf{Q}}} \Delta = \sum_{\text{cusps } c_i} n_i c_i$$

for some integers n_i.

We will pull back Δ to $X_0(Nr)_{\mathbf{Q}}$ via the two maps j_r and j'_r. In order to understand the divisors of these forms, we need to know how the cusps behave under these maps. The basic fact is that the preimage of a cusp c_i of $X_0(N)_{\mathbf{Q}}$ under j_r consists of two cusps $c_{i,1}$ and $c_{i,2}$ of $X_0(Nr)_{\mathbf{Q}}$; j_r is unramified at $c_{i,1}$ and ramified of degree r at $c_{i,2}$. Under j'_r we have the opposite behavior: $c_{i,1}$ and $c_{i,2}$ are again the only two points in the preimage of c_i, but now $c_{i,2}$ is unramified and $c_{i,1}$ is ramified of degree r. Combining all of this, we find that

$$\operatorname{div}_{X_0(Nr)_{\mathbf{Q}}} j_r^*\Delta = \sum n_i c_{i,1} + r n_i c_{i,2}$$
$$\operatorname{div}_{X_0(Nr)_{\mathbf{Q}}} j_r'^*\Delta = \sum r n_i c_{i,1} + n_i c_{i,2}.$$

Both of these forms have weight 12, since Δ does, so their ratio is a rational function f_r on $X_0(Nr)_{\mathbf{Q}}$ with divisor

$$\operatorname{div}_{X_0(Nr)_{\mathbf{Q}}} f_r = \sum (1-r) n_i (c_{i,1} - c_{i,2}).$$

We now think of f_r as a rational function on the singular curve $T_{r,\mathbf{Q}}$, which is birational to $X_0(Nr)_{\mathbf{Q}}$. As we said above, both $c_{i,1}$ and $c_{i,2}$ map to c_i under j_r and j'_r. Since $T_{r,\mathbf{Q}}$ is the image of $X_0(Nr)_{\mathbf{Q}}$ under the map $j_r \times j'_r$, the divisor of f_r on $T_{r,\mathbf{Q}}$ is

$$\operatorname{div}_{T_{r,\mathbf{Q}}} f_r = \sum (1-r) n_i \big((j_r(c_{i,1}), j'_r(c_{i,1})) - (j_r(c_{i,2}), j'_r(c_{i,2})) \big) = 0.$$

Thus $(T_{r,\mathbf{Q}}, f_r) \in \mathcal{C}(X_0(N)_{\mathbf{Q}} \times X_0(N)_{\mathbf{Q}})$, as desired.

We can now define the Flach classes $c_r \in H^1(\mathbf{Q}, T)$: we first map $(T_{r,\mathbf{Q}}, f_r)$ to $\mathcal{C}(E_\mathbf{Q} \times E_\mathbf{Q})$ via $(\phi \times \phi)_*$. That is, let $T'_{r,\mathbf{Q}}$ be the image of $T_{r,\mathbf{Q}}$ under $\phi \times \phi$ and let f'_r be the rational function on $T_{r,\mathbf{Q}}$ induced by f_r. (f'_r is really the norm of f_r in the finite extension of function fields $k(X_0(N)_\mathbf{Q})/k(E_\mathbf{Q})$ induced by ϕ.) One easily checks that

$$\operatorname{div}_{T'_{r,\mathbf{Q}}} f'_r = (\phi \times \phi)_* \operatorname{div}_{T_{r,\mathbf{Q}}} f_r = 0,$$

so $(T'_{r,\mathbf{Q}}, f'_r) \in \mathcal{C}(E_\mathbf{Q} \times E_\mathbf{Q})$. We now map this pair to $H^1(\mathbf{Q}, T)$ via the Flach map σ. This is the class c_r. Note that we defined these classes for all r not dividing N, even though we only need them for good r. (In fact, one can even define classes for r dividing N with some care.)

10. Local behavior of the c_r

To complete the construction of our Flach system, we need to analyze the local behavior of the classes c_r in $H^1_s(\mathbf{Q}_p, T)$ for all p. Specifically, we need to show that they map to 0 for all $p \neq r$ and we need to compute them explicitly for $p = r$. We do this using our description in terms of divisors and cycle classes. We distinguish several cases; for simplicity, we assume that r is good, although this is not critical to these computations.

10.1. p **does not divide** Nlr**.** This is the easiest case. $d_p(T'_{r,\mathbf{Q}}, f'_r)$ is just the divisor of f'_r on $T'_{r,\mathbf{F}_p}$, and the analysis of the preceding section of the divisor of f_r over $\mathbf{Q}$ goes through in exactly the same way over $\mathbf{F}_p$. Thus

$$\operatorname{div}_{T'_{r,\mathbf{F}_p}} f'_r = (\phi \times \phi)_* \operatorname{div}_{T_{r,\mathbf{F}_p}} f_r = 0,$$

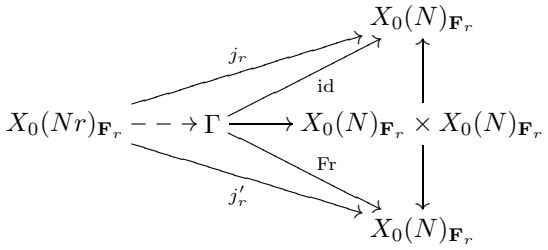
so $d_p(T'_{r,\mathbf{Q}}, f'_r) = 0$. Commutativity of the diagram (11) now shows that c_r maps to 0 in $H^1_s(\mathbf{Q}_p, T)$, since it is the image of the pair $(T'_{r,\mathbf{Q}}, f'_r)$ which already maps to 0 in $\operatorname{Div}(E_{\mathbf{F}_p} \times E_{\mathbf{F}_p})$. In particular, there is no need to know anything at all about the map s in this case.

10.2. p **divides** N**.** This is the case of bad reduction of E and the local diagram we used in the first case does not hold in this setting. Flach uses two different arguments to handle this case. If E has potentially multiplicative reduction at p, then one can give a very explicit description of the $G_{\mathbf{Q}_p}$-action on V, and one can compute that $H^1_f(\mathbf{Q}_p, V) = H^1(\mathbf{Q}_p, V)$. It follows that $H^1_s(\mathbf{Q}_p, T) = 0$, so that there is no local condition to check! If E has potentially good reduction at p, Flach mimics the argument above in the case of good reduction, using the Néron model of E; see [Fla92, pp. 324–325] and [Fla95, Section 5.5.2 and Section 6].

10.3. $p = l$**.** In this case we again do not have the local diagram to fall back on. Flach uses results of Faltings to conclude that $\operatorname{res}_l c_r$ lies in $H^1_f(\mathbf{Q}_l, T)$; see [Fla92, pp. 322-324].

10.4. $p = r$**.** This is the key computation. Recall that the Eichler-Shimura relation says that $T_{r,\mathbf{F}_r}$ can be written as a sum $\Gamma + \Gamma'$ of the graph of Frobenius and the Verschiebung. We will work with each piece separately.

We begin with Γ:



(Only one of the irreducible components of $X_0(Nr)_{\mathbf{F}_r}$ maps to Γ, which is why we have used a dotted line there.) The function on Γ corresponding to $j_r^*\Delta$ is just the pull back of Δ under the identity map; thus $\operatorname{div}_\Gamma j_r^*\Delta$ will just be the usual linear combination of points of Γ corresponding to cusps. The function on Γ corresponding to $j_r'^*\Delta$ is the pull back of Δ under Fr. Fr is purely inseparable, and purely inseparable maps are trivial on differentials; see [Sil86, Chapter 2, Proposition 4.2]. Thus $\operatorname{Fr}^*\Delta = j_r'^*\Delta$ will pick up a zero on Γ in addition to the usual cuspidal divisor. One can check that this zero has order 6 (essentially because Δ has weight $12 = 2 \cdot 6$). As always, the cuspidal parts of the divisor cancel, and we conclude that

$$\operatorname{div}_\Gamma f_r = \operatorname{div}_\Gamma j_r^*\Delta - \operatorname{div}_\Gamma j_r'\Delta = -6\Gamma.$$

The computation for Γ' is virtually identical, except that id and Fr are interchanged. Thus

$$\operatorname{div}_{\Gamma'} f_r = 6\Gamma'.$$

We conclude that

$$\operatorname{div}_{T_{r,\mathbf{F}_r}} f_r = 6(\Gamma' - \Gamma).$$

The next step is to push our whole construction forward to $E \times E$. If we let Γ_E and Γ'_E be the image of

$$\operatorname{id} \times \operatorname{Fr} : E_{\mathbf{F}_r} \to E_{\mathbf{F}_r} \times E_{\mathbf{F}_r}$$

$$\operatorname{Fr} \times \operatorname{id} : E_{\mathbf{F}_r} \to E_{\mathbf{F}_r} \times E_{\mathbf{F}_r}$$

respectively, then it is clear that $\phi \times \phi$ maps Γ onto Γ_E and Γ' onto Γ'_E. Since each point of Γ_E and Γ'_E is the image of $\deg \phi$ points of Γ and Γ', we have the equalities

$$(\phi \times \phi)_*\Gamma = (\deg \phi)\Gamma_E$$

$$(\phi \times \phi)_*\Gamma' = (\deg \phi)\Gamma'_E$$

as divisors. We conclude finally that

$$d_p(\phi \times \phi)_*(T_{r,\mathbf{Q}}, f_r) = 6(\deg \phi)(\Gamma'_E - \Gamma_E) \in \operatorname{Div}(E_{\mathbf{F}_r} \times E_{\mathbf{F}_r}).$$

We now need to compute the image of this under the cycle class map s. Our description of s shows that Γ_E, being the graph of Frobenius at r maps to precisely the endomorphism of $T_l E$ given by Fr_r. (This is well defined since $T_l E$ is unramified at r.) r is assumed to be good, so the proof of Lemma 9 shows that we can choose a basis x, y for $T_l E$ with respect to which Fr_r has matrix

$$\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}$$

with $u \equiv -v \equiv 1 \pmod{l}$ and $uv = r$. This matrix is the image of Γ_E in $\operatorname{End}_{G_{\mathbf{F}_p}}(T_l E)$.

To make the corresponding calculation for Γ'_E we will need to reinterpret it as a graph. Since Fr has degree r, there is a map $V : E_{\mathbf{F}_r} \to E_{\mathbf{F}_r}$ with the property that $V \circ \mathrm{Fr} = \mathrm{Fr} \circ V$ is the multiplication by r map on $E_{\mathbf{F}_r}$; see [Sil86, Chapter 3, Section 6]. Γ'_E is the image of the map

$$\mathrm{Fr} \times \mathrm{id} : E_{\mathbf{F}_r} \to E_{\mathbf{F}_r} \times E_{\mathbf{F}_r}.$$

If we precompose with the map $V : E_{\mathbf{F}_r} \to E_{\mathbf{F}_r}$, which is a surjective map of degree r, the literal image will not change, but each point will pick up a multiplicity of r. Thus the image of the map $\mathrm{Fr} \circ V \times V = r \times V$ is $r\Gamma'_E$. We claim that we can cancel the two r's, which leaves us with the fact that Γ'_E is the graph of V. The easiest way to do this is to pretend for the moment that multiplication by r has an inverse r^{-1} on E. (Of course, this is absurd, but it is somewhat less absurd when one does the entire computation in the range $\mathrm{End}(T_l E)$, where r is invertible.) Then an argument similar to the one above for precomposing with V shows that the image of $r \times V$ is r^2 times the image of $\mathrm{id} \times V r^{-1}$. This means that $s(r\Gamma'_E) = rs(\Gamma'_E)$ is the same as $r^2 V r^{-1}$, where now V is regarded as an endomorphism of $T_l E$. In other words, $s(\Gamma'_E)$ is just the endomorphism induced by V.

Since $V \circ \mathrm{Fr} = r$, this implies that the cycle class of Γ'_E has matrix

$$r \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}^{-1} = \begin{pmatrix} v & 0 \\ 0 & u \end{pmatrix}.$$

We conclude that $6(\deg \phi)(\Gamma'_E - \Gamma_E)$ maps to

$$6(\deg \phi) \begin{pmatrix} (v-u) & 0 \\ 0 & (u-v) \end{pmatrix}$$

in $\mathrm{End}_{G_{\mathbf{F}_r}}(T_l E)$, and even in $\mathrm{End}^0_{G_{\mathbf{F}_r}}(T_l E)$ since this matrix already has trace 0. This, then, is the image of c_r in $H^1_s(\mathbf{Q}_r, T)$.

Recall that $H^1_s(\mathbf{Q}_r, T) \cong \mathrm{End}^0_{G_{\mathbf{F}_r}}(T_l E)$ is a free $\mathbf{Z}_l$-module of rank 1. One easily checks that the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

is a generator of this module. Combined with our computation above, we find that $6(\deg \phi)(v-u)$ annihilates

$$H^1_s(\mathbf{Q}_r, T)/\mathbf{Z}_l \cdot \mathrm{res}_r\, c_r.$$

But 6 is an l-adic unit, and $v - u \equiv -2 \pmod{l}$, so it is as well. We conclude that $\deg \phi$ annihilates this module, and thus that the c_r form a Flach system of depth $\deg \phi$ for T. This concludes the proof of Theorem 13, and with it the proof of Theorem 1.

Appendix A. On the local Galois invariants of $E[l] \otimes E[l]$

The purpose of this appendix is to prove the following result.

Theorem 14. *Let E be an elliptic curve over $\mathbf{Q}$ without complex multiplication. Let $\phi : X_0(N) \to E$ be a modular parameterization of E and let S_0 be the set of places of $\mathbf{Q}$ at which E has bad reduction. Then the set of primes such that*

- *E has good reduction at l;*
- *The l-adic representation $\rho : G_{\mathbf{Q}, S_0 \cup \{l\}} \to \mathrm{GL}_2(\mathbf{Z}_l)$ is surjective;*
- *For all $p \in S_0$, $E[l] \otimes E[l]$ has no $G_{\mathbf{Q}_p}$-invariants;*

- *$E[l] \otimes E[l]$ has no $G_{\mathbf{Q}_l}$-invariants;*
- *l does not divide the degree of ϕ;*

has density 1 *in the set of all primes.*

Of course, the first and fifth conditions are obviously satisfied for almost all l. That the second condition is satisfied for almost all l is a result of Serre; see [Ser72]. The new content is in the third and fourth conditions. We will show that the third condition is also satisfied for almost all l, and that the fourth condition is satisfied for a set of primes of density 1.

Recall that by the Weil pairing we can write

$$E[l] \otimes E[l] \cong \mu_l \oplus \operatorname{Sym}^2 E[l].$$

The analysis of $\mathbf{Q}_p$-rational points on the first of these factors is immediate from the fact that (for $p \neq 2$) $\mathbf{Q}_p$ contains precisely the $(p-1)^{\text{st}}$ roots of unity: it has $\mathbf{Q}_p$-rational points if and only if $p \equiv 1 \pmod{l}$.

We begin the analysis of $\operatorname{Sym}^2 E[l]$ with a modification of the argument of [CS97, Lemma 2.3(i)].

Lemma 15. *Let E be an elliptic curve over $\mathbf{Q}_p$ and let l be any prime. Then $H^0(\mathbf{Q}_p, \operatorname{Sym}^2 E[l]) \neq 0$ if and only if $E(K)$ has non-trivial l-torsion for some quadratic extension K of $\mathbf{Q}_p$.*

Proof. We first set some notation. Let $\varepsilon : G_{\mathbf{Q}_p} \to \mathbf{Z}_l^*$ be the cyclotomic character; its image has finite index in $\mathbf{Z}_l^*$. Let $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}(E[l])$ and $\varphi : G_{\mathbf{Q}_p} \to \mathrm{GL}(\operatorname{Sym}^2 E[l])$ be the Galois representations associated to E. By the Weil pairing we have $\det \rho = \varepsilon$.

If x is a K-rational l-torsion point for some quadratic extension K of $\mathbf{Q}_p$, then one checks immediately that $x \otimes x \in E[l] \otimes E[l]$ is $G_{\mathbf{Q}_p}$-invariant, which proves one direction of the lemma.

Suppose, then, that there exists $t \in \operatorname{Sym}^2 E[l]$ such that $\varphi(\tau)t = t$ for all $\tau \in G_{\mathbf{Q}_p}$. Thus 1 is an eigenvalue of $\varphi(\tau)$ for every $\tau \in G_{\mathbf{Q}_p}$.

Now choose $\sigma_0 \in G_{\mathbf{Q}_p}$ such that $\varepsilon(\sigma_0)$ is not a root of unity; this is certainly possible since the image of ε has finite index. Let λ and μ be the eigenvalues of $\rho(\sigma_0)$. Then the eigenvalues of $\varphi(\sigma_0)$ are λ^2, $\lambda\mu = \varepsilon(\sigma_0)$ and μ^2. Since one of these is 1 and $\varepsilon(\sigma_0)$ is not a root of unity, we can assume without loss of generality that $\lambda^2 = 1$.

Set $\sigma = \sigma_0^2$. The eigenvalues of $\rho(\sigma)$ are $\lambda^2 = 1$ and μ^2. We have $\mu^2 \neq 1$ (since $\lambda^2\mu^2 = \varepsilon(\sigma_0)^2$ is not a root of unity), so we can choose a basis x, y for $E[l]$ of eigenvectors for $\rho(\sigma)$, with eigenvalues 1 and $\varepsilon(\sigma)$ respectively. $\varepsilon(\sigma)^2$ is still not 1, from which one easily computes (using the basis $x \otimes x$, $x \otimes y + y \otimes x$, $y \otimes y$ of $\operatorname{Sym}^2 E[l]$) that t is a scalar multiple of $x \otimes x$. It follows easily that x is rational over some quadratic extension of $\mathbf{Q}_p$. □

We now state the general analysis of torsion in elliptic curves over local fields, coming from an analysis of the formal group and the component group of the Néron model.

Proposition 16. *Let E be an elliptic curve over a finite extension K of $\mathbf{Q}_p$ and assume $p \neq l$. Let k be the residue field of K.*

- *If E has good reduction over K, then $E(K)$ has non-trivial l-torsion only if l divides $\#E(k)$.*

- *If E has non-split multiplicative reduction over K, then $E(K)$ has non-trivial l-torsion only if $p \equiv 1 \pmod{l}$ or $l \leq 3$.*
- *If E has split multiplicative reduction over K, then $E(K)$ has non-trivial l-torsion only if $p \equiv 1 \pmod{l}$ or $l \leq 11$.*
- *If E has additive reduction over K, then $E(K)$ has non-trivial l-torsion only if $l \leq 3$.*

Proof. By [Sil86, Proposition VII.2.1] there is an exact sequence

$$0 \to E_1(\mathfrak{m}_K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0$$

where E_1 is the formal group of E, $\mathfrak{m}_K$ is the maximal ideal of the ring of integers of K, $E_0(K)$ is the set of points of $E(K)$ with non-singular reduction and $\tilde{E}_{ns}(k)$ are the non-singular points of the reduction. By [Sil86, Proposition IV.3.2(b)], $E_1(K)$ has no non-trivial l-torsion, so any l-torsion in $E(K)$ must appear in $E(K)/E_0(K)$ or $\tilde{E}_{ns}(k)$. The proposition now follows from the determination of $\tilde{E}_{ns}(k)$ in the various cases (see [Sil86, Proposition VII.5.1]) and the analysis of the component group of the Néron model of E (see [Sil86, Theorem VII.6.1] and use that the minimal discriminant has valuation at most 11). □

An entirely similar argument yields the following result for the case $p = l$.

Proposition 17. *Let E be an elliptic curve over a quadratic extension K of $\mathbf{Q}_l$ and assume $l \geq 5$. Let k be the residue field of K.*

- *If E has good reduction over K, then $E(K)$ has non-trivial l-torsion only if l divides $\#E(k)$.*
- *If E has non-split multiplicative reduction over K, then $E(K)$ has no non-trivial l-torsion.*
- *If E has split multiplicative reduction over K, then $E(K)$ has non-trivial l-torsion only if $l \leq 11$.*

Proof. The only difference with Proposition 16 is the possibility of torsion in $E_1(K)$, but this is ruled out by [Sil86, Theorem IV.6.1] and the fact that the valuation of l in K is at most 2. We can make no statement about the case of additive reduction since then $\tilde{E}_{ns}(k)$ always has l-torsion. □

The last ingredient of the proof of Theorem 14 is some additional analysis of l-torsion in the case of good reduction in characteristic l. Note that if $K/\mathbf{Q}_l$ is a quadratic extension, then the residue field k is either $\mathbf{F}_l$ or $\mathbf{F}_{l^2}$.

Consider first the case that $k = \mathbf{F}_l$. Then by the Riemann hypothesis for elliptic curves over finite fields (see [Sil86, Theorem V.1.1]) we know that

$$-2\sqrt{l} \leq \#E(\mathbf{F}_l) - l - 1 \leq 2\sqrt{l}.$$

It follows easily that for $l \geq 7$ the only way to have l divide $\#E(\mathbf{F}_l)$ is to have $\#E(\mathbf{F}_l) = l$.

Now consider the case $k = \mathbf{F}_{l^2}$. This time the Riemann hypothesis shows that the only way to have l divide $\#E(\mathbf{F}_{l^2})$ is to have

$$\#E(\mathbf{F}_{l^2}) \in \{l^2 - l, l^2, l^2 + l, l^2 + 2l\}.$$

Let α, β be the eigenvalues of Frobenius at l acting on the p-adic Tate module of E for some $p \neq l$; we have $\alpha\beta = l$. Then by [Sil86, Section V.2],

$$\#E(\mathbf{F}_l) = 1 + l - \alpha - \beta$$
$$\#E(\mathbf{F}_{l^2}) = 1 + l^2 - \alpha^2 - \beta^2.$$

Since $\alpha\beta = l$, we have

$$\alpha^2 + 2\alpha\beta + \beta^2 = \alpha^2 + 2l + \beta^2,$$

and we conclude that

$$|l + 1 - \#E(\mathbf{F}_l)| = \sqrt{1 + 2l + l^2 - \#E(\mathbf{F}_{l^2})}.$$

This equation has several consequences. First, suppose that $\#E(\mathbf{F}_{l^2}) = l^2 - l$. Then $3l + 1$ must be a perfect square, say n^2. Thus $3l = n^2 - 1$, which implies that $l = 5$. Similarly, the case $\#E(\mathbf{F}_{l^2}) = l^2$ can not occur, and if $\#E(\mathbf{F}_{l^2}) = l^2 + l$, then $l = 3$. If $\#E(\mathbf{F}_{l^2}) = l^2 + 2l$, then we find that

$$\#E(\mathbf{F}_l) \in \{l, l + 2\}.$$

We now state and prove a more precise version of the unresolved part of Theorem 14.

Theorem 18. *Let E be an elliptic curve over $\mathbf{Q}$ and let S_0 be the set of places of $\mathbf{Q}$ at which E has bad reduction. Let l be a prime such that*

- *$l \geq 13$;*
- *l does not divide $p - 1$ for any $p \in S_0$;*
- *l does not divide $\#E(\mathbf{F}_p)$ or $\#E(\mathbf{F}_{p^2})$ for any $p \in S_0$;*
- *E has good reduction at l;*
- *$\#E(\mathbf{F}_l)$ is not l or $l + 2$.*

Then $H^0(\mathbf{Q}_p, E[l] \otimes E[l]) = 0$ for all $p \in S_0 \cup \{l\}$. In particular, the set of such l has density 1 in the set of all primes.

Proof. The second condition insures that μ_l has no $\mathbf{Q}_p$-rational points for any $p \in S_0$. To show that $\mathrm{Sym}^2 E[l]$ has no $\mathbf{Q}_p$-rational points for $p \in S_0$, we must (by Lemma 15) show that $E(K)$ has no non-trivial l-torsion for any quadratic extension of $\mathbf{Q}_r$. This possibility is ruled out by the first three conditions and Proposition 16. Note that we do need to consider the case of good reduction here, as even though E has bad reduction over $\mathbf{Q}_p$, it may attain good reduction over K.

To show that $H^0(\mathbf{Q}_l, E[l] \otimes E[l]) = 0$, note first that μ_l has no $\mathbf{Q}_l$-rational points, so we must only consider $\mathrm{Sym}^2 E[l]$. By Proposition 17 and the first and fourth hypotheses, it suffices to show that l does not divide $\#E(\mathbf{F}_l)$ or $\#E(\mathbf{F}_{l^2})$, and this follows from the preceding discussion and the fifth hypothesis.

It remains to show that the set of such l has density 1. It is clear that the first four conditions eliminate only finitely many primes l. It is shown as a very special case of [Ser81, Theorem 20] that the fifth condition is satisfied for a set of primes of density 1. This completes the proof. □

Appendix B. The definition of the Flach map

In this section we give the formal definition of the Flach map. For conceptual clarity we will work in a more general setting. Let X be a nonsingular projective variety of dimension n, defined over $\mathbf{Q}$.

Let X^p denote the set of irreducible subschemes of X of codimension p. Quillen has constructed a spectral sequence from the filtration by codimension of support:

$$E_1^{pq} = \bigoplus_{x \in X^p} K_{-p-q} k(x) \Rightarrow K_{-p-q}(X);$$

here $k(x)$ is the function field of the scheme x and the $K_i k(x)$ are Quillen's K-groups. There is an analogous spectral sequence in étale cohomology:

$$(E_1^{pq})'(\mathcal{F}) = \bigoplus_{x \in X^p} H_{\text{ét}}^{q-p}(\operatorname{Spec} k(x), \mathcal{F}(-p)) \Rightarrow H^{p+q}(X, \mathcal{F})$$

where $\mathcal{F}$ is some Tate twist of the constant étale sheaf $\mathbf{Z}_l$. For any integer i, these spectral sequence are connected by Chern class maps

$$E_r^{pq} \to (E_r^{p,q+2i})'(\mathbf{Z}_l(i))$$

constructed by Gillet.

Now fix an integer m between 0 and n and assume

- $H_{\text{ét}}^{2m+1}(X_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(m+1))$ has no $G_{\mathbf{Q}}$-invariants.

This is implied by the Weil conjectures if this cohomology group is torsion free, as is the case when X is a curve or a product of curves. We define the Flach map

$$\sigma_m : E_2^{m,-m-1} \to H^1(\mathbf{Q}, H_{\text{ét}}^{2m}(X_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(m+1)))$$

as the composition of three maps. The first is the Chern class map above with $p = m$, $q = -m-1$ and $i = m+1$:

$$E_2^{m,-m-1} \to (E_2^{m,m+1})'(\mathbf{Z}_l(m+1)).$$

The second is an edge map in the étale cohomology spectral sequence above:

$$(E_2^{m,m+1})'(\mathbf{Z}_l(m+1)) \to H_{\text{ét}}^{2m+1}(X, \mathbf{Z}_l(m+1)).$$

(To see that there really is an edge map from this term, one uses the fact that terms of this spectral sequence below the diagonal always vanish, as is clear from the expression above.) This last group appears in the Hochschild-Serre spectral sequence

$$H^p(\mathbf{Q}, H_{\text{ét}}^q(X_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(m+1))) \Rightarrow H_{\text{ét}}^{p+q}(X, \mathbf{Z}_l(m+1)).$$

Our assumption above that $H^0(\mathbf{Q}, H_{\text{ét}}^{2m+1}(X_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(m+1))) = 0$ insures that there is an edge map

$$H_{\text{ét}}^{2m+1}(X, \mathbf{Z}_l(m+1)) \to H^1(\mathbf{Q}, H^{2m}(X_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(m+1)))$$

and gives the last map in the definition of σ_m.

The map considered in the text is a slight variant of this. Take $X = E \times E$ and $m = 1$, so that we have a map

$$\sigma_1 : E_2^{1,-2} \to H^1(\mathbf{Q}, H_{\text{ét}}^2(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(2))).$$

We now show how to manipulate these terms to obtain the map

$$\sigma : \mathcal{C}(E \times E) \to H^1(\mathbf{Q}, \operatorname{Sym}^2 T_l E)$$

of the text. Working from the expression above for the Quillen spectral sequence, we see that $E_2^{1,-2}$ is the cohomology of a sequence

$$K_2 k(E \times E) \to \bigoplus_{x \in (E \times E)^1} k(x)^* \to \bigoplus_{y \in (E \times E)^2} \mathbf{Z}.$$

Quillen computes that the second map is just the divisor map sending a term $f \in k(x)^*$ to $\oplus_{y \in x} m_y$, where m_y is the order of f at y. The kernel of this map is

precisely the group $\mathcal{C}(E \times E)$; σ_1 is defined on the quotient of this group by the image of $K_2 k(E \times E)$, so we can also regard it as defined on $\mathcal{C}(E \times E)$ itself. This takes care of the domain.

Next, the Kunneth theorem implies that $H^2_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(2))$ is torsion free and that there is a projection

$$H^2_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(2)) \to H^1_{\text{ét}}(E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(1)) \otimes_{\mathbf{Z}_l} H^1_{\text{ét}}(E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(1)).$$

The Kummer sequence naturally identifies $H^1_{\text{ét}}(E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(1))$ with the l-adic Tate module $T_l E$, so projecting onto the symmetric direct summand yields a map

$$H^2_{\text{ét}}(E_{\bar{\mathbf{Q}}} \times E_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(2)) \to \operatorname{Sym}^2 T_l E$$

which is easily used to finish the definition of the map σ.

Returning to the general case, let us now investigate the local behavior of σ_m. Let p be a prime different from l at which X has good reduction (meaning that $X_{\mathbf{Q}_p}$ is the generic fiber of a proper smooth $\operatorname{Spec} \mathbf{Z}_p$-scheme $\mathfrak{X}$) and make the additional assumption:

- $H^{2m+1}_{\text{ét}}(X_{\bar{\mathbf{Q}}_p}, \mathbf{Z}_l(m+1))$ has no $G_{\mathbf{Q}_p}$-invariants;

Let $T = H^{2m}(X_{\bar{\mathbf{Q}}}, \mathbf{Z}_l(m+1))$. Then there is a commutative diagram

$$\begin{array}{ccc}
E_2^{m,-m-1} & \xrightarrow{\operatorname{div}_{\mathbf{F}_p}} & A^m \mathfrak{X}_{\mathbf{F}_p} \\
\downarrow{\scriptstyle \sigma_m} & & \downarrow{\scriptstyle s} \\
H^1(\mathbf{Q}, T) & & H^{2m}_{\text{ét}}(\mathfrak{X}_{\bar{\mathbf{F}}_p}, \mathbf{Z}_l(m))^{G_{\mathbf{F}_p}} \\
\downarrow & & \downarrow{\scriptstyle \cong} \\
H^1(\mathbf{Q}_p, T) & \longrightarrow & H^1_s(\mathbf{Q}_p, T)
\end{array}$$

Here $A^m \mathfrak{X}_{\mathbf{F}_p}$ is the codimension m Chow group of $\mathfrak{X}_{\mathbf{F}_p}$, which is just the analogue of the Picard group in higher codimension; $\operatorname{div}_{\mathbf{F}_p}$ sends a pair (x, f) of a cycle and a rational function to its divisor in characteristic p; s is the usual cycle class map in étale cohomology; and the bottom right isomorphism is the natural analogue of the isomorphism of Lemma 9, using the smooth base change theorem to identify $H^{2m}_{\text{ét}}(\mathfrak{X}_{\bar{\mathbf{F}}_p}, \mathbf{Z}_l(m))$ with $T(-1)$. The diagram of the text follows immediately from this one.

Flach defines the map σ (in the case $X = E \times E$, $m = 1$) using a related method in [Fla92]. There he proves the commutativity of the above local diagram (in a slightly different form) through explicit computations. In [Fla95] he gives the construction of σ (this time in the case $X = X_0(N) \times X_0(N)$, $m = 1$) we gave above and writes down the local diagram, although his proof of commutativity is somewhat incomplete and does not immediately generalize. The general case, which relies heavily on purity conjectures of Grothendieck (which have been proven in the relevant cases by Raskind and Thomason), is the subject of [Wes00, Chapters 6 and 7]. The construction of maps similar to σ also appear in the work of Kato; see [BK90] and [Sch98]. Mazur offers an alternative construction of the Flach map in [Maz94], without any explicit dependence on K-theory. There he also studies some algebraic properties of the map which are not immediately apparent and which permit some Euler system type conclusions even without the existence of an Euler system.

References

[BK90] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, In Cartier et al. [CIK+90], pp. 333–400.

[BL89] Wolf Barth and Herbert Lange (eds.), *Arithmetic of complex manifolds (Erlangen, 1988)*, Lecture notes in mathematics, no. 1399, Springer-Verlag, 1989.

[CF67] Ian Cassels and Jurg Fröhlich (eds.), *Algebraic number theory (Brighton, 1965)*, Academic press, 1967.

[CIK+90] Pierre Cartier, Luc Illusie, Nick Katz, Gérard Laumon, Yuri Manin, and Ken Ribet (eds.), *The Grothendieck Festschrift I*, Birkhauser, 1990.

[CS87] John Coates and Claus-Günther Schmidt, *Iwasawa theory for the symmetric square of an elliptic curve*, Journal für die Reine und Angewandte Mathematik **375/376** (1987), 104–156.

[CS97] John Coates and Andrew Sydenham, *On the symmetric square of a modular elliptic curve*, In Coates and Yau [CY97], pp. 152–171.

[CSS97] Gary Cornell, Joseph Silverman, and Glenn Stevens (eds.), *Modular forms and Fermat's last theorem*, Springer-Verlag, New York, 1997.

[CT91] John Coates and Michael Taylor (eds.), *L-functions and arithmetic (Durham, 1989)*, Cambridge University Press, 1991.

[CY97] John Coates and Shing-Tung Yau (eds.), *Elliptic curves, modular forms and Fermat's last theorem (Hong Kong, 1993)*, International Press, 1997.

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, In Coates and Yau [CY97], pp. 2–140.

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, In Murty [Mur95], pp. 39–133.

[Fla90a] Matthias Flach, *A generalisation of the Cassels-Tate pairing*, Journal für die Reine und Angewandte Mathematik **412** (1990), 113–127.

[Fla90b] Matthias Flach, *Selmer groups for the symmetric square of an elliptic curve*, Ph.D. thesis, University of Cambridge, 1990.

[Fla92] Matthias Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, Inventiones Mathematicae **109** (1992), 307–327.

[Fla95] Matthias Flach, *Annihilation of Selmer groups for the adjoint representation of a modular form*, In Murty [Mur95], pp. 249–265.

[Frö67] Jurg Fröhlich, *Local fields*, In Cassels and Fröhlich [CF67], pp. 1–41.

[Gou] Fernando Gouvea, *Deformations of Galois representations*, this volume.

[Gre] Ralph Greenberg, *Iwasawa theory for elliptic curves*, this volume.

[Gro91] Benedict Gross, *Kolyvagin's work on modular elliptic curves*, In Coates and Taylor [CT91], pp. 235–256.

[IRS90] Yasutaka Ihara, Ken Ribet, and Jean-Pierre Serre (eds.), *Galois groups over* **Q** *(Berkeley 1990)*, Mathematical Sciences Research Institute Publications, no. 16, Springer-Verlag, 1990.

[Maz78] Barry Mazur, *Rational isogenies of prime degree*, Inventiones Mathematicae **44** (1978), 129–162.

[Maz90] Barry Mazur, *Deforming Galois representations*, In Ihara et al. [IRS90], pp. 385–437.

[Maz94] Barry Mazur, *Galois deformations and Hecke curves*, Harvard University course notes, 1994.

[Maz97] Barry Mazur, *An introduction to the deformation theory of Galois representations*, In Cornell et al. [CSS97], pp. 243–311.

[Mil86] John Milne, *Arithmetic duality theorems*, Academic Press, Boston, 1986.

[Mur95] V. Kumar Murty (ed.), *Seminar on Fermat's last theorem*, Canadian Mathematical Society, Providence, Rhode Island, 1995.

[Rub89] Karl Rubin, *The work of Kolyvagin on the arithmetic of elliptic curves*, In Barth and Lange [BL89], pp. 128–136.

[Rub91] Karl Rubin, *Kolyvagin's system of Gauss sums*, In van der Geer et al. [vdGOS91], pp. 309–324.

[Rub99] Karl Rubin, *Euler systems*, Princeton University Press, Princeton, New Jersey, 1999.

[Sch98] Anthony Scholl, *An introduction to Kato's Euler system*, In Scholl and Taylor [ST98], pp. 379–460.

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae **15** (1972), 259–331.

[Ser81] Jeam-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Institut des Hautes Etudes Scientifiques, Publications Mathematiques **54** (1981), 323–401.

[Ser97] Jean-Pierre Serre, *Galois cohomology*, Springer-Verlag, New York, 1997.

[Shi76] Goro Shimura, *The special values of zeta functions associated with cusp forms*, Communications on Pure and Applied Mathematics **6** (1976), 783–804.

[Sil86] Joseph Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[ST98] Anthony Scholl and Richard Taylor (eds.), *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, Cambridge, Cambridge Universtiy Press, 1998.

[vdGOS91] Gerard van der Geer, Frans Oort, and Jan Steenbrink (eds.), *Arithmetic algebraic geometry (Texel, 1989)*, Birkhauser, 1991.

[Was97a] Lawrence Washingotn, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1997.

[Was97b] Lawrence Washington, *Galois cohomology*, In Cornell et al. [CSS97], pp. 101–120.

[Wes98] Tom Weston, *Euler systems and arithmetic geometry*, Notes from a course given by Barry Mazur at Harvard University, available at `http://www.math.harvard.edu/weston/mazur.html`, 1998.

[Wes00] Tom Weston, *On Selmer groups of geometric Galois representations*, Ph.D. thesis, Harvard University, 2000.

E-mail address: `weston@math.harvard.edu`