

Euler Systems of Heegner Points

Andrei Jorza, Stefan Patrikis

July 16, 2004

Abstract

For elliptic curves of rank 0 or 1, the theorem of Gross and Zagier relates the derivative at 1 of the L function associated with the elliptic curve to the canonical height of a Heegner point of the curve. We can construct a system of generalized Heegner points on the modular curve that correspond to pairs of elliptic curves with complex multiplication by the same order of a quadratic imaginary number field. This collection of Heegner points in fact forms an Euler system and can be used to construct certain cohomology classes that are used to bound the order of the Selmer group. This, in turn, is the key to determining the Mordell-Weil rank of a curve with analytic rank 1. In the first part of the paper, we present a brief survey of global class field theory, complex multiplication, and modular curves. The second part of the paper is an exposition of Gross's paper that treats Kolyvagin's work on the rank-one Birch Swinnerton-Dyer conjecture. This article follows closely [Gro91].

Contents

1	Introduction	2
1.1	Statement of the Main Problem	2
1.2	Primer on Elliptic Curves	3
2	The Modular Curve	5
2.1	Moduli Space	5
2.2	Operators on the Modular Space	5
3	Heegner Points	6
3.1	Class Field Theory	6
3.2	Complex Multiplication	7
3.3	Construction of Heegner Points	7
4	Euler Systems	8
4.1	Operators on Heegner Points	8
4.1.1	The Operator D_n	8
4.2	The Euler System	8
4.2.1	Action on Heegner Points	10
5	Kolyvagin's Theorem	10
5.1	Construction of the Cohomology Classes	10
5.2	The Action of $G(K/\mathbb{Q}) = \{1, \tau\}$ on the Cohomology Classes	12
5.3	Local Triviality of the Cohomology Classes	14
5.4	The Pairing from Tate Local Duality	16
5.5	Application of the Local Pairing	20
5.6	The Selmer group	22
5.6.1	Cohomology	22
5.6.2	Applications to the Selmer Group	24
5.7	The Eigenspaces of the Selmer Group	26

1 Introduction

1.1 Statement of the Main Problem

Let E be an elliptic curve of conductor N defined over \mathbb{Q} . Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field where all the prime factors of N split. For simplicity we will also assume that $D \neq 3, 4$, so $O_K^* = \{\pm 1\}$. The Birch Swinnerton-Dyer Conjecture predicts that the order of vanishing of the L-function of E at $s = 1$ (the “analytic rank”) is equal to the rank of its Mordell-Weil group. Kolyvagin has proven part of the rank 1 case, starting with the limit formula of Gross-Zagier: letting y_K be the Heegner point (to be defined later),

$$L'(E/K, 1) = \frac{\int_{E(\mathbb{C})} \omega \wedge \overline{i\omega}}{\sqrt{D}} \cdot \hat{h}(y_K).$$

Here \hat{h} represents the canonical height on the elliptic curve, which is known to vanish precisely on the torsion points of E . In particular, $L'(E/K, 1) \neq 0$ if and only if y_K has infinite order. Our main result will be

Theorem 1 *Assume that y_K has infinite order in $E(K)$. Then $E(K)$ has rank 1.*

More precisely, we will prove the following

Theorem 2 *Let E be an elliptic curve defined over \mathbb{Q} that does not have complex multiplication over \mathbb{C} . Let p be an odd prime such that the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group $GL_2(\mathbb{Z}/p\mathbb{Z})$, and assume that p does not divide y_K in $E(K)$. Then*

1. $E(K)$ has rank 1.
2. $\text{III}(E/K)[p] = 0$.

Serre has shown that $G(\mathbb{Q}(E[p])/\mathbb{Q}) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$ for all but finitely many primes p , and we are able to derive our result with the use of any one of these primes. The condition that E/\mathbb{C} not have complex multiplication is a hypothesis of Serre's result, and it only excludes thirteen j -invariants (isomorphism classes) of elliptic curves. Note that our hypothesis also implies that $E(K)$ contains no p -torsion. ¹

1.2 Primer on Elliptic Curves

On an elliptic curve E over a number field K we have the multiplication by p isogeny, which is surjective when the curve is considered over an algebraic closure \bar{K} of K . For any group G let $G[p]$ denote the kernel of multiplication by p , $G \xrightarrow{[p]} G$. Then we have the short exact sequence

$$0 \rightarrow E[p] \rightarrow E \rightarrow E \rightarrow 0.$$

Taking $G(\bar{K}/K)$ -cohomology and extracting the relevant short-exact sequence, we find

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\delta} H^1(G(\bar{K}/K), E[p]) \longrightarrow H^1(G(\bar{K}/K), E)[p] \longrightarrow 0$$

is exact, where δ denotes the boundary map in the long-exact sequence on Galois cohomology. For each place v of K , we fix an extension of v to \bar{K} , i.e. an embedding $\bar{K} \rightarrow \bar{K}_v$, and by restriction we obtain the corresponding inclusion $G(\bar{K}_v/K_v) \subset G(\bar{K}/K)$. Repeating the construction of the above short-exact sequence, and taking the natural maps on cohomology, we obtain the commutative diagram

¹The skeptical reader can just— by the Mordell-Weil Theorem— throw out the finitely many primes p for which $E(K)$ has p -torsion.

$$\begin{array}{ccccccc}
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(G(\bar{K}/K), E[p]) & \longrightarrow & H^1(G(\bar{K}/K), E)[p] \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \prod_{v \in M_K} E(K_v)/pE(K_v) & \longrightarrow & \prod_{v \in M_K} H^1(G(\bar{K}_v/K_v), E[p]) & \longrightarrow & \prod_{v \in M_K} H^1(G(\bar{K}_v/K_v), E)[p] \longrightarrow 0
\end{array}$$

We can now define the p -Selmer group and the Shafarevich-Tate group.

Definition 3 *The p -Selmer group of E/K is*

$$Sel(E/K)_p = \ker\{H^1(G(\bar{K}/K), E[p]) \rightarrow \prod_{v \in M_K} H^1(G(\bar{K}_v/K_v), E)\}.$$

The Shafarevich-Tate group of E/K is

$$\text{III}(E/K) = \ker\{H^1(G(\bar{K}/K), E) \rightarrow \prod_{v \in M_K} H^1(G(\bar{K}_v/K_v), E)\}.$$

From the above commutative diagram and the definitions of $Sel(E/K)_p$ and $\text{III}(E/K)$, we obtain the crucial short-exact sequence

Proposition 4

$$0 \rightarrow E(K)/pE(K) \xrightarrow{\delta} Sel(E/K)_p \rightarrow \text{III}(E/K)[p] \rightarrow 0 \quad (1)$$

It is known that $Sel(E/K)_p$ is finite [Sil99], and in particular we see that $\text{III}(E/K)[p]$ is finite.

We will use the existence of a distinguished point of infinite order on an elliptic curve E/K with $L'(E/K, 1) \neq 0$ to show that E/K has rank one. Under the hypotheses of Theorem 2, we will show that $Sel(E/K)_p$ is one-dimensional over $\mathbb{Z}/p\mathbb{Z}$, which, since $E(K)$ contains no p -torsion, will imply that $E(K)$ has rank 1: the above exact sequence of $\mathbb{Z}/p\mathbb{Z}$ -vector spaces implies that

$$rk_{\mathbb{Z}} E(K) = rk_{\mathbb{Z}/p\mathbb{Z}} E(K)/pE(K) \leq 1,$$

and since $E(K)$ contains a point of infinite order, we conclude that its rank is exactly one. Thus, the short-exact sequence implies that $\text{III}(E/K)[p] = 0$ for almost all p . Unfortunately, this is not enough to deduce Kolyvagin's result that $\text{III}(E/K)$ is finite (even though we know that $\text{III}(E/K)[p]$ is finite for all p because $Sel(E/K)_p$ surjects onto it). In any case, the bulk of this paper will be devoted to bounding the p -Selmer group.

2 The Modular Curve

2.1 Moduli Space

For a positive integer N we may define the group $\Gamma_0(N) \subset SL_2(\mathbb{Z})$ as

$$\Gamma_0 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \pmod{N} \right\}.$$

There is a natural action of this group on $\mathfrak{h} = \{z \in \mathbb{C} \mid \text{Im}z > 0\}$.

Definition 5 $Y_0(N) = \Gamma_0(N) \backslash \mathfrak{h}$ is the modular curve. This space has a natural structure as a Riemann surface. The projective closure is $X_0(N) = \Gamma_0(N) \backslash (\mathbb{P}\mathbb{Q} \cup \mathfrak{h})$. The points $\Gamma_0(N) \backslash \mathbb{P}\mathbb{Q}$ are called cusps.

An important characterization of the modular curve comes from the uniformization theorem ([Sil99]):

For $\tau \in \mathfrak{h}$, there is an elliptic curve E so that $E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$, and conversely any E/\mathbb{C} arises from a lattice Λ via a complex analytic isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$.

Theorem 6 $X_0(N)$ has the structure of a moduli space for pairs (E, C) , where E is an elliptic curve and C is a cyclic subgroup of order N of E .

Proof: See [Kna92]. ■

2.2 Operators on the Modular Space

Let N be a positive integer and p a prime that does not divide N . Consider the following diagram:

$$\begin{array}{ccc} & X_0(Np) & \\ i_1 \swarrow & & \searrow i_2 \\ X_0(N) & \longrightarrow & X_0(N) \end{array}$$

where $i_1(E, C) = (E/D, (C + D)/D)$ for D the unique subgroup of order p , and $i_2(E, C) = (E, C/D)$. Define $T_p : \text{Div}(X_0(N)) \rightarrow \text{Div}(X_0(N))$ by setting $T_p(E, C)$ to be the sum of $(E/D, (C + D)/D)$ where D runs through all $p + 1$ subgroups of order p of $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

On the level of the modular curve, this action can be made explicit. $T_p(\tau)$ is the set $\{\frac{\tau+i}{p} \mid i = 0, \dots, p-1\} \cup \{p\tau\}$. Via the uniformization theorem, we get a characterization of T_p on the level of lattices in \mathbb{C} . For a lattice Λ , $T_p\Lambda$ is the set of all sublattices of index p .

Definition 7 The correspondence T_p on lattices is the p -th Hecke operator. Under the relations:

1. $R_a T_m = T_m R_a$ (where $R_a \Lambda = a\Lambda$).
2. $T_m T_n = T_{mn}$, for $(m, n) = 1$.
3. $T_{p^{r+1}} = T_p T_{p^r} - p R_p T_{p^{r-1}}$.

the Hecke operators form a commutative algebra, called the Hecke algebra.

For N a positive integer which is not a prime we may write $N = mn$ for $(m, n) = 1$. Let (E, C) be a point on $X_0(N)$. There exists a unique decomposition $C = C_m + C_n$, with C_m cyclic of order m and C_n cyclic of order n . Since $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ we may define $w_m(E, C)$ to be $(E/C_m, (E[m] + C_n)/C_m)$ since $E[m]/C_m$ is cyclic of order m and $C_m \cap C_n = 1$.

Definition 8 *The operator w_m is the Atkin-Lehner involution.*

Proof: We need that $w_m^2 = 1$. To see this note that $w_m^2(E, C) = w_m(E/C_m, (E[m] + C_n)/C_m) = (E/E[m], ((E/C_m)[m] + C_n)/E[m])$. The result follows since $[m] : E/E[m] \rightarrow E$ is an isomorphism. ■

On the level of the modular curve, the Atkin-Lehner involution is given by $\tau \mapsto -\frac{1}{m\tau}$.

Definition 9 *The Frobenius operator for p coprime with N is an operator $Frob_p : X_0(N) \rightarrow X_0(N)$ so that $Frob_p(E, C) = (E^{(p)}, C^p)$.*

The following theorem due to Eichler and Shimura relates the Hecke operator and the Frobenius.

Theorem 10 *For p coprime to N we have $T_p = Frob_p + pFrob_p^{-1}$, as correspondences on $X_0(N)$.*

3 Heegner Points

3.1 Class Field Theory

Let $K = \mathbb{Q}(\sqrt{-D})$ be a quadratic imaginary number field and \mathcal{O} be an order in K , i.e., a subring of $\mathcal{O}_K = \mathbb{Z}[w_D]$ so that $\mathcal{O} \otimes \mathbb{Q} = K$. In this case there is an integer c called the conductor of \mathcal{O} so that $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}cw_D$. The conductor determines the order uniquely.

Theorem 11 *Let $\mathbb{A}_{K,f}$ be the set of finite adeles. There exists an abelian extension K_c (called the ring class field of conductor c) of K which is unramified outside of the prime factors of the conductor c . The Artin map defines an isomorphism*

$$Pic(\mathcal{O}) = \mathbb{A}_{K,f}^\times / K^\times \prod \mathcal{O}_p \xrightarrow{\cong} G(K_c/K).$$

3.2 Complex Multiplication

This exposition follows [Sil94]. The set $\mathcal{E}(\mathcal{O})$ is the set of elliptic curves that have the property that $\text{End}(E) \cong \mathcal{O}$, modulo isomorphism.

Proposition 12 *$\text{Pic}(\mathcal{O})$ acts on $\mathcal{E}(\mathcal{O})$ simply transitively via $\alpha * E = \mathbb{C}/\alpha^{-1}\Lambda$ for $E = \mathbb{C}/\Lambda$.*

Proposition 13 *$G(\bar{K}/K)$ acts on $\mathcal{E}(\mathcal{O})$ via a map $\eta : G(\bar{K}/K) \rightarrow \text{Pic}(\mathcal{O})$ (that takes the Frobenius element of \mathfrak{p} to the class of \mathfrak{p}) so that $E^\sigma = \eta(\sigma) * E$. Moreover, H_c is the fixed field of the kernel of η .*

This proposition is extremely important for the construction of Heegner points since it shows that the j -invariants of the curves in $\mathcal{E}(\mathcal{O})$ are in K_c which shows that the elliptic curves are defined over K_c . In particular, we have the proposition:

Proposition 14 *If $\tau \in \mathfrak{h} \cap K$ is quadratic over \mathbb{Q} and c is the conductor of the order defined by τ , then $j(\tau) \in K_c$. Moreover, for $\sigma \in \text{Pic}(\mathcal{O})$ we have that $j(\sigma * \tau) = \text{rec}(\sigma)^{-1}j(\tau)$.*

3.3 Construction of Heegner Points

We follow [Dar04, Gro84, Ghi]. Let E be an elliptic curve of conductor N . Wiles' theorem implies the existence of a parametrization defined over \mathbb{Q} $\Phi : X_0(N) \rightarrow E(\mathbb{C})$.

Define $\mathcal{O}_\tau^N = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c = 0 \pmod{N}, \gamma\tau = \tau \right\} \cup \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$.

Write $CM(\mathcal{O})$ to be the set of $\tau \in \mathfrak{h} \cap K$ so that $\mathcal{O}_\tau^N = \mathcal{O}$. Note that entire $\Gamma_0(N)$ orbits are included in $CM(\mathcal{O})$. We have the following proposition:

Proposition 15 *Let $\tau \in CM(\mathcal{O})$ and let c be the conductor of \mathcal{O} . Then $\Phi(\tau) \in E(K_c)$, where K_c is the ring class field. Shimura's reciprocity law states that*

$$\Phi(\sigma * \tau) = \text{rec}(\sigma)^{-1}\Phi(\tau),$$

for all $\sigma \in \text{Pic}(\mathcal{O})$.

Definition 16 *Let \mathcal{O}_n be the order of conductor n , for n square-free. A Heegner point is a point $\Phi(\tau) \in E(K_n)$ for $\tau \in CM(\mathcal{O}_n)$.*

The following proposition settles the existence of Heegner points:

Proposition 17 *$CM(\mathcal{O}_n)$ is nonempty if and only if all the prime factors of N split in K .*

Equivalently, and more intuitively, a Heegner point on $X_0(N)$ is a pair of elliptic curves with one mapped to the other by a cyclic N -isogeny. On the level of lattices, this is made explicit by $(\mathbb{C}/\mathcal{O}_n, \mathbb{C}/(\mathcal{N} \cap \mathcal{O}_n)^{-1})$, where \mathcal{N} is chosen so that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. For example, if a is any fractional ideal of K , \mathbb{C}/a has complex multiplication by \mathcal{O}_K .

We require the following hypothesis for the construction of Heegner points:

For the p defined in the first section and for any prime factor l of n , l does not divide NDp . Moreover, we require that the Frobenius elements associated to l in $G(K(E[p])/K)$ be in the same conjugacy class as complex conjugation. By the Chebotarev density theorem, there are infinitely many primes l with this property. A corollary is that $Frob_l$ is complex conjugation even in $G(K/\mathbb{Q})$. Therefore, l is inert in K .

Remark 18 *Since the j -invariant of an elliptic curve determines the curve up to isomorphism, a Heegner point is characterized by a pair $(j(E_n), j(E'_n))$. This induces a very explicit action of the Hecke operators as $T_l(j(E_n), j(E'_n)) = \sum_{i=0}^l (j(E_n/S_i), j(E'_n/\psi(S_i)))$ on the level of $Div(X_0(N))$, where ψ is the isogeny and S_i range through the $l+1$ subgroups of order l .*

4 Euler Systems

4.1 Operators on Heegner Points

4.1.1 The Operator D_n

We follow [Pop]. For l a prime as above, let $a_l = Tr Frob_l$. Since $Frob_l = \tau$ complex conjugation, it means that their respective characteristic polynomials are equal. Therefore $x^2 - a_l x + l = x^2 - 1$, all these $(\text{mod } p)$ of course. Therefore $a_l \equiv l + 1 \equiv 0 \pmod{p}$.

Since l is inert in K , it has a unique prime factor λ in K . Let $\mathbb{F}_\lambda = \mathcal{O}_K/\lambda\mathcal{O}_K$. Since $\tau \in Frob_l$ it means that for any prime q of L lying above l we have $\tilde{\tau} = Frob_l$, acting on $\tilde{E}(\mathbb{F}_\lambda)$, where $\tilde{\tau}$ is the reduction mod q of τ . Let $\tilde{E}(\mathbb{F}_\lambda)^\pm$ be the \pm eigenspaces of $\tilde{\tau} = Frob_l$. Then we have

$$|\tilde{E}(\mathbb{F}_\lambda)^+| = |\{P \in \tilde{E}(\mathbb{F}_\lambda) | P^{\sigma_l} = P\}| = |\tilde{E}(\mathbb{F}_l)| = l + 1 - a_l.$$

$$\begin{aligned} |\tilde{E}(\mathbb{F}_\lambda)^-| &= |\{P \in \tilde{E}(\mathbb{F}_\lambda) | P^{\sigma_l+1} = 0\}| = |\ker(1 + \sigma_l)| \\ &= \det(1 + \sigma_l) = \det(1 + \sigma_l) = 1 + a_l + l \pmod{p}. \end{aligned}$$

Therefore, p divides the orders of both eigenspaces. Since the reduction map $E[p] \rightarrow \tilde{E}(\mathbb{F}_\lambda)$ is injective, and the eigenspaces are nonzero, this implies that $\tilde{E}(\mathbb{F}_\lambda)^\pm \cong \mathbb{Z}/p\mathbb{Z}$.

Since n is square-free, let $n = \prod l$. Let $G_n = G(K_n/K_1)$. Then we have $G_n = \prod G_l$, where $G_l = G(K_n/K_{n/l})$. This follows from the identifications $G_n = (\mathcal{O}_K/n\mathcal{O}_K)^\times / (\mathbb{Z}/n\mathbb{Z})^\times$, etc, and the Chinese remainder theorem.

Let $Frob_l$ generate $G_l \cong \mathbb{F}_\lambda/\mathbb{F}_l$. Since this is cyclic of order $l+1$, the augmentation ideal of $\mathbb{Z}[G_l]$ is principal and generated by $\sigma_l - 1$. Therefore we may define $D_l = (l+1 - \sum_{G_l} \sigma) / (\sigma_l - 1)$, which is well-defined up to $Tr_l \mathbb{Z}$, where $Tr_l = \sum \sigma$.

4.2 The Euler System

Definition 19 *We follow [Cla]. We call a collection of points $\{y_n\}$ an Euler system if they satisfy the following two conditions:*

1. $Tr_l y_n = a_l y_{n/l}$ in $E(K_{n/l})$.
2. Each prime λ_n lying above l in K_n divides a unique $\lambda_{n/l}$ in $K_{n/l}$ and $y_n = Fro_b(\lambda_{n/l})(y_{n/l}) \pmod{\lambda_n}$.

In order to prove statements about Heegner points we generally look on the level of the modular curve and then use Φ . Let $n = ml$.

Proposition 20 $Tr_l x_n = T_l x_m \in Div(X_0(N))$.

Proof: Recall the map η so that $E^\sigma = \eta(\sigma) * E$. Write $x_n = (j(E_n), j(E'_n))$. Then we have that the first coordinate of $Tr_l(x_n)$ is

$$\sum_{G_l} j(E_n^\sigma) = \sum j(\mathbb{C}/\eta^{-1}(\sigma)).$$

Also, we have seen how the Hecke operators act on Heegner points. We have that $T_l(j(E_n), j(E'_n)) = \sum_{S_i} (j(E_n/S_i), j(E'_n/\psi(S_i)))$. Note that $[\mathcal{O}_m : \eta(\sigma)^{-1}] = [\eta(\sigma)\mathcal{O}_m : \mathcal{O}_m] = \frac{n}{m} = l$ because $\eta(\sigma)\mathcal{O}_m$ is an invertible ideal in \mathcal{O}_n . Therefore, on the level of divisors, the first coordinates of $Tr_l x_n$ is the same as the first coordinate of $T_l x_m$. The second coordinates are equal by symmetry since Heegner points are pairs of isogenous elliptic curves.

Proposition 21 For any point $x \in Div(X_0(N))$ and for any prime l we have that $\Phi(T_l x) = a_l \Phi(x)$.

Proof: If f is an eigenform for all the Hecke operators, then $T_l f = a_l f$. By the Eichler-Shimura construction (for example, pull back the Neron differential on E to get such an eigenform differential on $X_0(N)$ and then project back) this implies that on E , T_l acts as multiplication by a_l . The result follows. ■

Proposition 22 The Heegner points previously defined form an Euler system.

Proof:

1. From the previous propositions we get that $T_l(x_m) = Tr_l x_n$ and that $\Phi(T_l x_m) = a_l \Phi(x_m) = a_l y_m$. Since Φ is defined over \mathbb{Q} and Tr_l fixes \mathbb{Q} we have that $Tr_l(y_n) = a_l y_m$.
2. By class field theory we get that λ splits completely in K_m but λ_m (factors of λ in K_m) are totally ramified in K_n (the l -ray class field is totally ramified over the Hilber class field). Therefore $\lambda_m = \lambda_n^{l+1}$ and from here we get that $\mathbb{F}_{\lambda_m} = \mathbb{F}_\lambda$ (since they both have the same cardinality).

Using a previous proposition we get that $Tr_l x_n = T_l x_m$. But $Tr_l x_n = \sum \sigma x_n$. When interpreted mod λ_n , we are working in \mathbb{F}_λ . Here each σ which is a power of σ_l acts as $x \mapsto x^{l^s} = x \pmod{\lambda_n}$. Therefore $Tr_l x_n = (l+1)x_n \pmod{\lambda_n}$.

By the Eichler-Shimura relation we have that $T_l = Fro_b + lFro_b^{-1}$. In $\mathbb{F}_\lambda/\mathbb{F}_l$ (which is a quadratic extension), Fro_b acts as conjugation, and therefore it is an involution.

So Eichler-Shimura implies that $T_l = (l + 1)Frob_l$. Therefore the result would follow if we prove that $Frob_{\lambda_m} = Frob_l \pmod{\lambda_n}$ since we may cancel the $l + 1$ factor and then project via Φ . But this follows from the relation $\lambda_m = \lambda_n^{l+1}$, i.e., from total ramification. ■

4.2.1 Action on Heegner Points

Let x_n be the Heegner points on the modular curve as previously defined, and let $y_n = \Phi(x_n)$.

Set $D_n = \prod D_l \in \mathbb{Z}[G_n]$. Note that $D_n y_n \in E(K_n)$.

Proposition 23 G_n fixes $G_n y_n$ in $E(K_n)/pE(K_n)$.

Proof: Since the σ_l generate D_n it is enough to show that σ_l fixes it. Let $n = lm$.

Then $(\sigma_l - 1)D_n = (\sigma_l - 1)D_l D_m = (l + 1 - Tr_l)D_m$. Therefore we need to show that $0 = (l + 1)D_m y_n - D_m(Tr_l y_n)$.

But $p|l + 1$ and since we are working mod p it is enough to show that $Tr_l y_n \in pE(K_n)$. But this follows from the previous proposition. ■

5 Kolyvagin's Theorem

5.1 Construction of the Cohomology Classes

We follow [?]. We now begin the construction of the cohomology classes which Kolyvagin uses to bound the order of $Sel(E/K)_p$. Letting $n = \prod l$ as before, we also let $G_n = G(K_n/K_1)$ and $\mathfrak{g}_n = G(K_n/K)$. Let S be a system of coset representatives for $G_n \subset \mathfrak{g}_n$, and define

$$P_n = \sum_{\sigma \in S} \sigma(D_n y_n) \in E(K_n)$$

We have shown that the class $[D_n y_n] \in E(K_n)/pE(K_n)$ is fixed by G_n , so the class $[P_n]$ is as well. Consequently, $[P_n]$ is also independent of the choice of representatives S of \mathfrak{g}_n/G_n . For any $m|n$, we can similarly define $P_m = \sum_{\sigma \in S} \sigma(D_m y_m)$, so in particular

$$P_1 = \sum_{\sigma \in S} \sigma y_1 = Tr_{K_1/K} y_1 = y_K.$$

Our familiar exact sequence $0 \longrightarrow E[p] \longrightarrow E \xrightarrow{[p]} E \longrightarrow 0$ gives the commutative diagram

Proposition 24

$$\begin{array}{ccccccc}
& & & & & 0 & \\
& & & & & \downarrow & \\
& & & & & H^1(G(K_n/K), E)[p] & \\
& & & & & \text{Inf} \downarrow & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(G(\bar{K}/K), E[p]) & \longrightarrow & H^1(G(\bar{K}/K), E)[p] \longrightarrow 0 \\
& & \downarrow & & \text{Res} \downarrow \cong & & \text{Res} \downarrow \\
0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathfrak{g}_n} & \xrightarrow{\delta_n} & H^1(G(\bar{K}/K_n), E[p])^{\mathfrak{g}_n} & \longrightarrow & (H^1(G(K_n/K), E)[p])^{\mathfrak{g}_n}
\end{array}$$

Proof: The two rows are exact by taking Galois cohomology (with respect to $G(\bar{K}/K)$ and $G(\bar{K}/K_n)$), although in the bottom row surjectivity is lost when we take \mathfrak{g}_n -invariants. The maps in the middle and right-hand columns come from the inflation-restriction exact sequence: for a normal, closed subgroup H of a group G acting on the G -module A , there is an exact sequence

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A)^{G/H} \xrightarrow{\text{Tg}} H^2(G/H, A^H) \xrightarrow{\text{Inf}} H^2(G, A).$$

[Tg is the transgression homomorphism; see [NSW00]] The middle column is an isomorphism because the following lemma implies that $H^i(K_n/K, E(K_n)[p]) = 0$ for all i .

Lemma 25 *E has no p -torsion over K_n .*

Proof: $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, so if the lemma does not hold, we must have $E(K_n)[p] \cong \mathbb{Z}/p\mathbb{Z}$ or $E(K_n)[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Suppose $E(K_n)[p] \cong \mathbb{Z}/p\mathbb{Z}$, and let $P \in E(K_n)[p]$. Since K_n/\mathbb{Q} is Galois, any $\sigma \in G(\bar{\mathbb{Q}}/\mathbb{Q})$ maps P into $E(K_n)$; since $[p]$ commutes with any automorphism, $\sigma(P) \in E(K_n)[p]$. In particular, by restricting $G(\bar{\mathbb{Q}}/\mathbb{Q})$ to $G(\mathbb{Q}(E[p])/\mathbb{Q}) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$, we have obtained a contradiction since no one-dimensional subspace $\mathbb{Z}/p\mathbb{Z}$ is fixed by all of $GL_2(\mathbb{Z}/p\mathbb{Z})$.

Now suppose $E(K_n) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, so $\mathbb{Q}(E[p]) \subset K_n$, and we obtain the surjective homomorphism $G(K_n/\mathbb{Q}) \rightarrow G(\mathbb{Q}(E[p])/\mathbb{Q}) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$. $G(K_n/\mathbb{Q})$ is a group of ‘‘dihedral’’ type because it contains \mathfrak{g}_n as a normal, abelian subgroup of index 2. But for $p > 2$, $GL_2(\mathbb{Z}/p\mathbb{Z})$ is not the quotient of a group of dihedral type, and the lemma follows. ■

Using the diagram, we can now define Kolyvagin’s cohomology classes. Since the middle restriction map is an isomorphism, we let $c(n)$ be the unique class in $H^1(G(\bar{K}/K), E[p])$ such that

$$\text{Res}(c(n)) = \delta_n[P_n].$$

Define $d(n)$ to be the image of $c(n)$ in $H^1(G(\bar{K}/K, E)[p])$. A simple diagram chase shows that there is a unique class $\tilde{d}(n) \in H^1(G(K_n/K), E)[p]$ such that

$$\text{Inf}(\tilde{d}(n)) = d(n).$$

It will be useful later on to have an explicit description of these cohomology classes. It is immediate from the definition of the boundary map δ_n that $\delta_n P_n$ is represented by the inhomogeneous 1-cocycle $\sigma \mapsto \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n$ (here $\frac{1}{p}P_n$ is any lift of P_n under $[p]$). We claim that the cocycle f represents $c(n)$, where

$$f(\sigma) = \sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n - \frac{(\sigma - 1)P_n}{p}.$$

It is easily checked that f is a 1-cocycle ($f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$), so we need only observe that $\text{Res}(f) = \delta_n[P_n]$. This clearly holds from the above computation since $(\sigma - 1)P_n = 0$ for $\sigma \in G(\bar{K}/K_n)$ (recall that $P_n \in E(K_n)$).

Pushing f forward to $H^1(G(\bar{K}/K), E)[p]$, the term $\sigma\left(\frac{1}{p}P_n\right) - \frac{1}{p}P_n$ dies because it is a coboundary, and we are left with the representative cocycles

$$d(n) : \sigma \mapsto -\frac{(\sigma - 1)P_n}{p}, \forall \sigma \in G(\bar{K}/K)$$

and

$$\tilde{d}(n) : \sigma \mapsto -\frac{(\sigma - 1)P_n}{p}, \forall \sigma \in \mathfrak{g}_n.$$

Proposition 26 (1) *The class $c(n)$ is trivial in $H^1(G(\bar{K}/K), E[p])$ if and only if $P_n \in pE(K_n)$.*

(2) *The class $d(n)$ is trivial in $H^1(G(\bar{K}/K), E)[p]$, and the class $\tilde{d}(n)$ is trivial in $H^1(G(K_n/K), E)[p]$, if and only if $P_n \in pE(K_n) + E(K)$.*

Proof: In both cases, the proof is a simple diagram chase. (1) is obvious, so we will prove (2). Since Inf is injective, the triviality of $d(n)$ and $\tilde{d}(n)$ are equivalent. By the definition of $c(n)$, $d(n)$ is trivial if and only if $c(n) \in \text{Im}\delta$. If so, then $c(n) = \delta(P)$ for some $P \in E(K)$. Since $\text{Res}(c(n)) = \delta_n[P_n]$, the injectivity of δ_n implies that $P \equiv P_n \pmod{pE(K_n)}$. The result follows. ■

5.2 The Action of $G(K/\mathbb{Q}) = \{1, \tau\}$ on the Cohomology Classes

Complex conjugation τ acts on the $\mathbb{Z}/p\mathbb{Z}$ -vector space $H^1(G(\bar{K}/K), E[p])$, thereby decomposing it into the +1 and -1 eigenspaces

$$H^1(G(\bar{K}/K), E[p]) \cong H^1(G(\bar{K}/K), E[p])^+ \oplus H^1(G(\bar{K}/K), E[p])^-.$$

Let $\varepsilon = \pm 1$ be the eigenvalue of the Atkin-Lehner involution w_N on $f = \sum a_n q^n$ which is the modular form associated with the elliptic curve E .

Complex conjugation acts on $G(K_n/K)$ by $\sigma^\tau = \tau\sigma\tau^{-1}$, on K_n and on $y_n \in E(K_n)$.

Proposition 27 $\tau y_n = \varepsilon\sigma' y_n + \text{torsion} \in E(K_n)$, for some $\sigma' \in \mathfrak{g}_n$.

Proof: From [Gro84] we get that there is a σ' so that $\tau x_n = w_N \sigma' x_n$. Passing to divisors we get that

$$\tau(x_n - \infty) = w_n \sigma'(x_n - \infty) + (w_N \infty - \infty).$$

But $w_N \infty = 0$ and $(0 - \infty)$ is a degree 0 cusp and so it is a torsion point on the Jacobian $J(X_0(N))$. Passing down by Φ we get the statement of the proposition. \blacksquare

Proposition 28 (1) *The class $[P_n]$ lies in the $\epsilon_n = (-1)^{f_n} \epsilon$ -eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathfrak{g}_n}$, where f_n is the number of primes dividing n .*

(2) *The class $c(n)$ lies in the ϵ_n -eigenspace for τ in $H^1(G(\bar{K}/K), E[p])$, and the class $d(n)$ lies in the ϵ_n -eigenspace for τ in $H^1(G(\bar{K}/K), E)[p]$.*

Proof: τ acts on \mathfrak{g}_n by $\tau\sigma\tau^{-1} = \sigma^{-1}$, so

$$\tau P_n = \tau \sum_{\sigma \in S} \sigma D_n y_n = \sum_{\sigma \in S} \sigma^{-1} \tau D_n y_n.$$

[recall that S is a set of coset representatives for \mathfrak{g}_n/G_n]. Note that τ commutes with $l+1 - Tr_l$, and the D_l were chosen such that

$$(\sigma_l - 1)D_l = l + 1 - Tr_l,$$

so we find that

$$(\sigma_l - 1)D_l \tau = \tau(\sigma_l - 1)D_l = (\sigma_l^{-1} - 1)\tau D_l = (\sigma - 1)(-\sigma_l^{-1})\tau D_l.$$

The kernel of $(\sigma_l - 1)$ (acting on the group ring $\mathbb{Z}[G_l]$) is just $\mathbb{Z}Tr_l$, so from the above we find a $k \in \mathbb{Z}$ such that $\tau D_l = -\sigma_l D_l \tau + kTr_l$. Recall the Euler system condition satisfied by the Heegner points, that $Tr_l y_n = a_l y_n \equiv 0 \pmod{pE(K_n)}$. Thus we can compute

$$\begin{aligned} \tau P_n &= \sum_{\sigma \in S} \sigma^{-1} \tau D_n y_n = \sum_{\sigma \in S} \sigma^{-1} \prod_{l|n} (-\sigma_l D_l \tau + kTr_l) y_n \\ &\equiv (-1)^{f_n} \prod_{l|n} \sigma_l \sum_{\sigma \in S} \sigma^{-1} \cdot D_n \tau y_n \pmod{pE(K_n)} \end{aligned}$$

We have used the definition of f_n , the commutativity of \mathfrak{g}_n , the fact that $\prod_{l|n} D_l = D_n$, and the above Euler system relation. Proposition 27 showed that $\tau y_n = \epsilon \cdot \sigma' y_n + \text{torsion}$ for some $\sigma' \in \mathfrak{g}_n$, so we substitute to find

$$\begin{aligned} \tau P_n &\equiv (-1)^{f_n} \prod_{l|n} \sigma_l \sum_{\sigma \in S} \sigma^{-1} \cdot D_n (\epsilon \cdot \sigma' y_n + \text{torsion}) \\ &\equiv \epsilon_n \prod_{l|n} \sigma_l \cdot \sigma' \sum_{\sigma \in S} \sigma^{-1} D_n y_n \pmod{pE(K_n)} \end{aligned}$$

To check that the second congruence holds, let $Q \in E(K_n)$ be a torsion point of order r . We have shown (lemma 25) that $E(K_n)[p] = 0$, so $(r, p) = 1$, and there exist $a \in \mathbb{Z}$ such

that $ar \equiv 1 \pmod{p}$. Consequently, $Q \equiv 0 \pmod{pE(K_n)}$, so the torsion drops out of our equation.

Since $[D_n y_n]$ is fixed by G_n modulo p , and $\{\sigma^{-1} : \sigma \in S\}$ is another set of coset representatives for \mathfrak{g}_n/G_n , we conclude that

$$\tau P_n \equiv \epsilon_n \cdot P_n \pmod{pE(K_n)}.$$

Thus, we have shown that P_n is in the ϵ_n -eigenspace of τ in $(E(K_n)/pE(K_n))^{\mathfrak{g}_n}$.

Part (2) of the proposition is immediate, since the maps in Proposition 20 commute with τ . In particular, since $d(n) \in H^1(G(\bar{K}/K), E)[p]^{\epsilon_n}$, Proposition 22, part (2), becomes

Corollary 29 *$d(n)$ is trivial in $H^1(G(\bar{K}/K), E)[p]^{\epsilon_n}$ if and only if $P_n \in pE(K_n) + E(K)^{\epsilon_n}$.*

5.3 Local Triviality of the Cohomology Classes

We follow [And].

Proposition 30 *The class $d(n)_\mu = 0 \in H^1(K_\mu, E)[p]$ for $\mu = \infty$ and for all μ not dividing n .*

Proof: When $\mu = \infty$, \mathbb{C} is algebraically closed the the cohomology is trivial.

Assume that μ does not divide n . If μ does not divide N , then E has good reduction at μ . Recall the diagram:

$$\begin{array}{ccc} \tilde{d}(n) \in H^1(G(K_n/K), E)[p] & \longrightarrow & H^1(G(K_\mu^{un}/K_\mu), E)[p] \\ \downarrow & & \downarrow \\ d(n) \in H^1(G(\bar{K}/K), E)[p] & \longrightarrow & H^1(G(\bar{K}_\mu/K_\mu), E(K_\mu))[p] \\ \downarrow & & \downarrow \\ H^1(G(\bar{K}/K_n), E)[p]^{\mathfrak{g}_n} & \longrightarrow & H^1(G(\bar{K}_\mu/K_{n,\mu}), E)[p]^{\mathfrak{g}_n} \end{array}$$

The class $d(n)$ comes from the class $\tilde{d}(n) \in H^1(G(K_n/K), E)[p]$. Since K_n is unramified over K it means that $d(n)_\mu$ is actually in $H^1(G(K_\mu^{un}/K_\mu), E)[p]$. But $H^1(G(K_\mu^{un}/K_\mu), E) = 0$ since E has good reduction at μ ([Mil86]). Therefore the class $d(n)_\mu = 0$ because it comes from $\tilde{d}(n)_\mu = 0$.

When $\mu|N$ but μ does not divide n , the same result holds, and the proof uses properties of Neron models. For details see [Gro91]. \blacksquare

Proposition 31 *Let $n = lm$, λ be the prime of K over l . Then the class $d(n)_\lambda = 0 \in H^1(G(\bar{K}_\lambda/K_\lambda), E)[p]$ if and only if $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$ for λ_m above λ in K_m .*

Proof: Recall that λ splits completely in K_m and λ_m is totally ramified in K_n with $\lambda_m = \lambda^{l+1}$. From section 5.1 we get that $d(n)_\lambda$ is given by the cocycle $\sigma \mapsto -\frac{(\sigma-1)P_n}{p}$, defined on $G(K_{\lambda_n}/K_{\lambda_m}) \cong G_l$. Therefore $d(n)_\lambda \in H^1(G_l, E(K_\lambda))[p]$.

Since l does not divide N by assumption on n , E has good reduction at λ , so there is an exact sequence

$$0 \longrightarrow E_1(K_{\lambda_n}) \longrightarrow E(K_{\lambda_n}) \longrightarrow \tilde{E}(\mathbb{F}_{\lambda_n}) \longrightarrow 0.$$

G_l cohomology gives the long exact sequence

$$(\tilde{E}(\mathbb{F}_{\lambda_n})) [p]^{G_l} \longrightarrow H^1(G_l, E_1(K_{\lambda_n})) [p] \longrightarrow H^1(G_l, E(K_{\lambda_n})) [p] \longrightarrow H^1(G_l, \tilde{E}(\mathbb{F}_{\lambda_n})) [p]$$

From [Sil99] we get that $E_1 = \hat{E}(\mathcal{M})$ where \mathcal{M} is the maximal ideal of the local field and \hat{E} represents the formal group on the maximal ideal. Since the local field is K_{λ_n} , the uniformizer has norm an l -power and so the group E_1 is a pro- l group. Since $l \neq p$, multiplication by p is an isomorphism on E_1 . Therefore a p -torsion u in $H^1(G_l, E_1)$ such that $pu = \sigma x - x$ will give $u = \sigma \frac{x}{p} - \frac{x}{p}$ which is well-defined because of the isomorphism. Therefore $u = 0$ so $H^1(G_l, E_1(K_{\lambda_n})) [p] = 0$.

The exact sequence implies that $d(n)_\lambda$ is 0 if the image in $H^1(G_l, \tilde{E}(\mathbb{F}_{\lambda_n})) [p] = \text{Hom}(G_l, \tilde{E}(\mathbb{F}_\lambda) [p])$ is also 0. (This last equality comes from trivial action of G_l on $\tilde{E}(\mathbb{F}_{\lambda_n})$.)

But the image is represented by the cocycle $\sigma \mapsto -\frac{(\sigma-1)P_n}{p}$ reduced $(\text{mod } \lambda_n)$. But G_l is cyclic generated by σ_l and so it is enough to check that $Q_n = \frac{(\sigma_l-1)P_n}{p} = 0 \pmod{\lambda_n}$.

Note that σ_l acts trivially on $\tilde{E}(\mathbb{F}_{\lambda_n}) = \tilde{E}(\mathbb{F}_\lambda)$ and so $\bar{Q}_n \in \tilde{E}(\mathbb{F}_\lambda) [p]$.

The rest reduces to calculations, recalling that the points y_n form an Euler system.

$P_n = \sum \sigma D_m D_l y_n$ where $(\sigma_l - 1)D_l = l + 1 - \text{Tr}_l$. Therefore

$$Q_n = -(\sigma_l - 1)P_n/p = \sum_{\mathfrak{g}_n/G_n} \sigma D_m \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right),$$

because $\sigma_l - 1$ commutes with \mathfrak{g}_n and $\text{Tr}_l y_n = a_l y_m$ because the y_n form an Euler system (the first property).

The second property of Euler systems gives:

$$\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \equiv \frac{(l+1)\text{Frob}(\lambda_m) - a_l}{p} y_m \pmod{\lambda_n},$$

for any λ_n lying above λ . Therefore for $\sigma \in \mathfrak{g}_n$ ($\sigma\lambda_n$ is another prime above λ) we have

$$\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \equiv \frac{(l+1)\text{Frob}(\sigma^{-1}\lambda_m) - a_l}{p} y_m \pmod{\sigma^{-1}\lambda_n},$$

which gives

$$\sigma \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) \equiv \sigma \left(\frac{(l+1)\text{Frob}(\sigma^{-1}\lambda_m) - a_l}{p} y_m \right) \pmod{\lambda_n},$$

But $\sigma \text{Frob}(\sigma^{-1}\lambda_m) = \text{Frob}(\lambda_m)\sigma$, so we get that

$$\sigma \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) \equiv \left(\frac{(l+1)\text{Frob}(\lambda_m) - a_l}{p} \right) \sigma y_m \pmod{\lambda_n}.$$

Plugging back in the expression for Q_n , we get that

$$Q_n = \sum D_m \left(\frac{(l+1)Frob(\lambda_m) - a_l}{p} \right) \sigma y_m \pmod{\lambda_n} = \left(\frac{(l+1)Frob(\lambda_m) - a_l}{p} \right) P_m \pmod{\lambda_m}.$$

In the previous section we saw that \tilde{P}_n is in the ε_n -eigenspace of $Frob(l)$ on $\tilde{E}(\mathbb{F}_\lambda)/p\tilde{E}(\mathbb{F}_\lambda)$. But from the Eichler-Shimura theorem and the formula for the action of the Hecke operator T_l we get that $(l+1)Frob(l) - a_l$ annihilates $\tilde{E}(\mathbb{F}_\lambda)$. Also we have shown that the ε_n -eigenspace of $\tilde{E}(\mathbb{F}_\lambda)$ is cyclic. Therefore the reduction of Q_n is 0 if and only if $\tilde{P}_m \in p\tilde{E}(\mathbb{F}_\lambda)$. But then P_m is in $pE(K_\lambda)$ plus p -torsion in E_1 (from the exact sequence). But E_1 is a pro- l group and so its p -torsion is 0. So $P_m \in pE(K_\lambda)$. ■

5.4 The Pairing from Tate Local Duality

The goal of this section is to interpret Tate's local duality theorem to produce a non-degenerate pairing that we will apply in the next section to study the Selmer group. Throughout, we let K be a local field with ring of integers O and finite residue field k of characteristic l . Let E be an elliptic curve defined over K with good reduction over O . Also, let $p \neq l$ be prime. Our exposition follows [Pap].

We begin with a cohomological lemma:

Lemma 32 *Let \mathbb{F}_q be the finite field with q elements, and let $G = G(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ be its absolute Galois group, with the usual topological generator $Frob$. Let A be a continuous G -module. If A is a torsion group or a divisible group such that A^G is torsion, then*

1. $H^0(G, A) = A^G$
2. $H^1(G, A) = A/(Frob - 1)A$
3. $H^s(G, A) = 0$ for $s \geq 2$

For the proof, see [Ser79] ■

Letting $\tilde{E}(k)$ denote the reduced curve, we can form the exact sequence

$$0 \rightarrow E^1(K) \rightarrow E(K) \rightarrow \tilde{E}(k) \rightarrow 0$$

The kernel of reduction $E^1(K)$ is a formal group [Sil99]; in fact, it is pro- l , and multiplication by p is an isomorphism. We use the reduced curve to study E/K . We have the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E^1(K) & \longrightarrow & E(K) & \longrightarrow & \tilde{E}(k) \longrightarrow 0 \\ & & \downarrow p & & \downarrow p & & \downarrow p \\ 0 & \longrightarrow & E^1(K) & \longrightarrow & E(K) & \longrightarrow & \tilde{E}(k) \longrightarrow 0 \end{array}$$

Since the left-hand map is an isomorphism, the snake lemma implies that the middle and right-hand cokernels are isomorphic, i.e. $E(K)/pE(K) \cong \tilde{E}(k)/p\tilde{E}(k)$. The usual exact sequence induced from multiplication by p on \tilde{E} yields the following exact sequence:

$$0 \rightarrow \tilde{E}(k)/p\tilde{E}(k) \rightarrow H^1(G(K^{un}/K), \tilde{E}[p]) \rightarrow H^1(G(K^{un}/K), \tilde{E}).$$

By the cohomological lemma, this last group is $\tilde{E}/(\text{Frob} - 1)\tilde{E}$, where Frob is the Frobenius automorphism, the topological generator of $G(\bar{k}/k)$. $\text{Frob} - 1$ is a non-constant morphism of smooth curves, so it is surjective.

Proposition 33 $E(K)/pE(K) \cong H^1(G(K^{un}/K), E[p])$.

Proof: From the above observations, we obtain the isomorphisms

$$E(K)/pE(K) \cong \tilde{E}(k)/p\tilde{E}(k) \cong H^1(G(K^{un}/K), \tilde{E}[p]).$$

Since \tilde{E} is non-singular and $(l, p) = 1$, $E(K)[p]$ injects into $\tilde{E}(k)$. In particular, we can identify $E[p]$ with $\tilde{E}[p]$: all the p -torsion lies in some finite algebraic extension L of K (with residue field λ), and $E(L)[p] = E[p]$ injects into $\tilde{E}(\lambda)$. But we know that $E[p]$ and $\tilde{E}[p]$ are both isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$, so this injection must give an identification $E[p] = \tilde{E}[p]$. This gives $E(K)/pE(K) \cong H^1(G(K^{un}/K), E[p])$. \blacksquare

Later, we will use this proposition to reinterpret Tate local duality, which we now state. For a proof, see [Mil86].

Theorem 34 *For all i , $H^i(G(\bar{K}/K), E[p])$ is finite, and there are alternating, non-degenerate pairings*

$$\langle \cdot, \cdot \rangle : H^i(G(\bar{K}/K), E[p]) \otimes H^{2-i}(G(\bar{K}/K), E[p]) \rightarrow \mathbb{Z}/p\mathbb{Z}.$$

Remark: To construct the pairing, simply apply the cup-product and the Weil-pairing to get maps

$$H^i(G(\bar{K}/K), E[p]) \times H^{2-i}(G(\bar{K}/K), E[p]) \rightarrow H^2(G(\bar{K}/K), E[p] \otimes E[p]) \rightarrow H^2(G(\bar{K}/K), \mu_p).$$

We can easily check that the last group is just $\mathbb{Z}/p\mathbb{Z}$ since $H^2(G(\bar{K}/K), \mu_p)$ is isomorphic to the p -torsion of $H^2(G(\bar{K}/K), \bar{K}^\times)$ using the long exact sequence on Galois cohomology coming from the fundamental Kummer sequence, along with an invocation of Hilbert's Theorem 90. Finally, the invariant map of local class field theory tells us that $H^2(G(\bar{K}/K), \bar{K}^\times) \cong \mathbb{Q}/\mathbb{Z}$, so its p -torsion is clearly $\mathbb{Z}/p\mathbb{Z}$.

In particular, if we consider the Tate pairing with $i = 1$ and restrict to the Galois group of K^{un}/K , we obtain the

Proposition 35 *The subspace $H^1(G(K^{un}/K), E[p]) \cong E(K)/pE(K)$ is self-orthogonal with respect to the Tate pairing.*

Proof: $H^2(G(K^{un}/K), \mathbb{Z}/p\mathbb{Z}) = 0$ by lemma 32, so the result follows from the commutativity of the following diagram:

$$\begin{array}{ccc}
H^1(G(K^{un}/K), E[p]) \otimes H^1(G(K^{un}/K), E[p]) & \xrightarrow{Inf \otimes Inf} & H^1(G(\bar{K}/K), E[p]) \otimes H^1(G(\bar{K}/K), E[p]) \\
\downarrow & & \downarrow \\
H^2(G(K^{un}/K), E[p] \otimes E[p]) & & H^2(G(\bar{K}/K), E[p] \otimes E[p]) \\
\downarrow & \xrightarrow{Inf} & \downarrow \\
H^2(G(K^{un}/K), \mathbb{Z}/p\mathbb{Z}) & \longrightarrow & H^2(G(\bar{K}/K), \mathbb{Z}/p\mathbb{Z}) \\
& & \downarrow \\
& & \mathbb{Z}/p\mathbb{Z}
\end{array}$$

We have now come to the main theorem of this section:

Theorem 36 *The Tate pairing induces a non-degenerate pairing of $\mathbb{Z}/p\mathbb{Z}$ -vector spaces*

$$\langle \cdot, \cdot \rangle : E(K)/pE(K) \otimes H^1(G(\bar{K}/K), E)[p] \rightarrow \mathbb{Z}/p\mathbb{Z}.$$

Proof: Letting I_K denote the inertial subgroup of $G(\bar{K}/K)$, we have the exact sequence

$$0 \rightarrow I_K \rightarrow G(\bar{K}/K) \rightarrow G(K^{un}/K) \rightarrow 0$$

We have the corresponding inflation-restriction exact sequence

$$0 \rightarrow H^1(G(K^{un}/K), E[p]^{I_K}) \rightarrow H^1(G(\bar{K}/K), E[p]) \rightarrow H^1(I_K, E[p])^{G(K^{un}/K)} \rightarrow H^2(G(K^{un}/K), E[p]^{I_K})$$

Since E has good reduction over O and $(l, p) = 1$, I_K acts trivially on $E[p]$ [Sil99]; in particular, lemma 32 implies that the last cohomology group in this sequence is zero. Comparing with the parallel exact sequence in Galois cohomology

$$0 \rightarrow E(K)/pE(K) \rightarrow H^1(G(\bar{K}/K), E[p]) \rightarrow H^1(G(\bar{K}/K), E)[p] \rightarrow 0$$

we conclude that $H^1(I_K, E[p])^{G(K^{un}/K)} \cong H^1(G(\bar{K}/K), E)[p]$.

Let W be the wild group (the Galois group defined by the extensions $K - K^{un} - K_0 - \bar{K}$ so that \bar{K}/K_0 is wild and K_0/K^{un} is tame [Ser79]). It is known that W is a pro- l group and that the tame group defined by the exact sequence

$$0 \rightarrow W \rightarrow I_K \rightarrow T \rightarrow 0,$$

and $T = \prod_{q \neq l} \mathbb{Z}_q$. This exact sequence allows us to study the group $H^1(I_K, E[p])^{G(K^{un}/K)}$.

Since I_K acts trivially on $E[p]$, so do W and T . Then the inflation-restriction sequence applied to the above short-exact sequence is

$$0 \rightarrow H^1(T, E[p]) \rightarrow H^1(I_K, E[p]) \rightarrow H^1(W, E[p])^T$$

But since W acts trivially on $E[p]$, $H^1(W, E[p]) \cong \text{Hom}(W, E[p])$, which is trivial since W is a pro- l group: multiplication by p is an isomorphism, and any $\phi \in \text{Hom}(W, E[p])$ must send $W = pW \mapsto 0$. Consequently,

$$\begin{aligned} H^1(I_K, E[p])^{G(K^{un}/K)} &= H^1(T, E[p])^{G(K^{un}/K)} = \text{Hom}(T, E[p])^{G(K^{un}/K)} \\ &= \text{Hom}\left(\prod_{q \neq l} \mathbb{Z}_q, E[p]\right)^{G(K^{un}/K)} = \text{Hom}(\mathbb{Z}_p, E[p])^{G(K^{un}/K)} \end{aligned}$$

where these last equalities hold by our discussion of T and the fact that \mathbb{Z}_q is pro- q ($\neq p$), so multiplication by p is again an isomorphism.

$$\text{Hom}(\mathbb{Z}_p, E[p])^{G(K^{un}/K)} = \text{Hom}(\lim_{\leftarrow} \mathbb{Z}/p^n \mathbb{Z}, E[p])^{G(K^{un}/K)} = \text{Hom}(\mathbb{Z}/p\mathbb{Z}, E[p])^{G(K^{un}/K)}$$

where we have used the fact that Hom and projective limit commute, and that $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$. Now, we have observed that I_K fixes $E[p]$, so all of the p -torsion of E is K^{un} -rational. $\text{Hom}(\mathbb{Z}/p\mathbb{Z}, E[p]) \cong E[p]$ implies $\text{Hom}(\mathbb{Z}/p\mathbb{Z}, E[p])^{G(K^{un}/K)} = E(K)[p]$.

By the cohomological lemma, $H^1(G(K^{un}/K), E[p]) = E[p]/(\text{Frob} - 1)E[p]$, which is isomorphic to $\tilde{E}(k)[p]$ (see for example [Ser79]).

But we've already observed that $\tilde{E}(k)[p] = E(K)[p]$ and that $H^1(G(K^{un}/K), E[p]) = E(K)/pE(K)$, so we conclude that

$$E(K)/pE(K) \cong E(K)[p].$$

We have now reached the crux of the proof, the existence of a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/pE(K) & \longrightarrow & H^1(G(\bar{K}/K), E[p]) & \longrightarrow & H^1(G(\bar{K}/K), E)[p] \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & (H^1(G(\bar{K}/K), E)[p])^* & \longrightarrow & (H^1(G(\bar{K}/K), E[p]))^* & \longrightarrow & (E(K)/pE(K))^* \longrightarrow 0 \end{array}$$

Here $G^* = \text{Hom}(G, \mathbb{Z}/p\mathbb{Z})$. The middle map is that arising from Tate local duality (and is consequently an isomorphism), while the others are induced by the duality pairing. The diagram exists because $E(K)/pE(K)$ is isotropic for the Tate pairing. To be more precise, we will construct the right-hand vertical map. For $x \in H^1(G(\bar{K}/K), E)[p]$, take any lift $y \in H^1(G(\bar{K}/K), E[p])$. Map y to the homomorphism $\langle y, \cdot \rangle : H^1(G(\bar{K}/K), E[p]) \rightarrow \mathbb{Z}/p\mathbb{Z}$, and then restrict this to an element of $(E(K)/pE(K))^*$. Any other lift y' differs from y by an element of $E(K)/pE(K)$, so by linearity the resulting map in $(E(K)/pE(K))^*$ differs by $\langle \epsilon, \cdot \rangle : E(K)/pE(K) \rightarrow \mathbb{Z}/p\mathbb{Z}$ for $\epsilon \in E(K)/pE(K)$. Since $E(K)/pE(K)$ is isotropic, this map is trivial, so we have constructed a well-defined map $H^1(G(\bar{K}/K), E)[p] \rightarrow (E(K)/pE(K))^*$. We can proceed similarly to construct the left-hand vertical map, and the diagram clearly commutes.

Since the middle map is an isomorphism, the left and right-hand vertical maps are clearly injective and surjective, respectively, and a simple dimension count implies that they are in fact isomorphisms: we observed previously that $E(K)/pE(K) = E(K)[p]$ has the same

dimension (over $\mathbb{Z}/p\mathbb{Z}$) as $H^1(I_K, E[p])^{G(K^{un}/K)} = H^1(G(\bar{K}/K), E)[p]$. That the left and right-hand maps are isomorphisms is precisely the statement that

$$E(K)/pE(K) \otimes H^1(G(\bar{K}/K), E)[p] \rightarrow \mathbb{Z}/p\mathbb{Z}$$

is a non-degenerate pairing, so the proof is complete. \blacksquare

5.5 Application of the Local Pairing

We will apply the local pairing constructed above to give a condition for the local triviality of an element of the Selmer group. Let us again let K be an imaginary quadratic extension of \mathbb{Q} subject to the initial conditions of this paper, and let K_λ be the completion at an inert prime λ lying over the prime $l \in \mathbb{Z}$. We also assume that the p -torsion of E is rational over K_λ , which implies that $E(K_\lambda)/pE(K_\lambda)$ and $H^1(G(\bar{K}_\lambda/K_\lambda), E)[p]$ have dimension two as $\mathbb{Z}/p\mathbb{Z}$ -vector spaces: this is clear for the first group, and for the second it follows from our proof of Theorem 36, since we showed $H^1(G(\bar{K}_\lambda/K_\lambda), E)[p] = \text{Hom}(\mathbb{Z}/p\mathbb{Z}, E[p])^{G(K_\lambda^{un}/K_\lambda)} = E(K_\lambda)[p] = (\mathbb{Z}/p\mathbb{Z})^2$.

As before, we assume p is odd and that l has been chosen so that $l + 1 \equiv 0 \pmod{p}$. By section 4.1.1, the τ -eigenspaces $E(K_\lambda)^\pm$ are one-dimensional $\mathbb{Z}/p\mathbb{Z}$ -vector spaces.

Proposition 37 (1) *The eigenspaces $(E(K_\lambda)/pE(K_\lambda))^\pm$ and $H^1(G(\bar{K}_\lambda/K_\lambda), E)[p]^\pm$ are one-dimensional $\mathbb{Z}/p\mathbb{Z}$ -vector spaces.*

(2) *The pairing $\langle \cdot, \cdot \rangle$ of Theorem 36 induces non-degenerate pairings of $\mathbb{Z}/p\mathbb{Z}$ -vector spaces*

$$\langle \cdot, \cdot \rangle^\pm : (E(K_\lambda)/pE(K_\lambda))^\pm \times H^1(G(\bar{K}_\lambda/K), E)[p]^\pm \rightarrow \mathbb{Z}/p\mathbb{Z}.$$

In particular, if d_λ is a non-zero element of $H^1(G(\bar{K}_\lambda/K), E)[p]^\pm$ and $s_\lambda \in (E(K_\lambda)/pE(K_\lambda))^\pm$ satisfies $\langle s_\lambda, d_\lambda \rangle = 0$, then $s_\lambda \equiv 0 \pmod{pE(K_\lambda)}$.

Proof:

Recall from the proof of Theorem 36 that $E(K_\lambda)/pE(K_\lambda) = E(K_\lambda)[p]$ and $H^1(G(\bar{K}_\lambda/K_\lambda), E)[p] = \text{Hom}(\mu_p, E[p])^{G(K_\lambda^{un}/K_\lambda)}$ where $\mu_p = \mu_p(\bar{K}_\lambda) = \mathbb{Z}/p\mathbb{Z}$. But $l + 1 \equiv 0 \pmod{p}$, so $\mu_p(K_\lambda) = \mu_p(\bar{K}_\lambda)$: since $\mu_p(\bar{K}_\lambda) = \mu_p(K^{un})$, we need only check that applying Frobenius to an element $x \in \mu_p(\bar{K}_\lambda)$ is trivial. This is clear since

$$x^{l^2} = x^{(pn-1)^2} = 1,$$

where $n \in \mathbb{Z}$ such that $pn = l + 1$. Finally, since we have assumed the p -torsion is defined over K_λ , we obtain the isomorphism

$$H^1(G(\bar{K}_\lambda/K_\lambda), E)[p] = \text{Hom}(\mu_p(K_\lambda), E(K_\lambda)[p]).$$

Furthermore, $\mu_p(\mathbb{Q}_l) = \{1\}$ since the only roots of unity in \mathbb{Q}_l are the $(l - 1)^{st}$, and $l - 1 \not\equiv 0 \pmod{p}$ by assumption. Thus, $\tau \in G(K_\lambda/\mathbb{Q}_l)$ can only fix the p^{th} root of unity 1, and $\mu_p(K_\lambda) = \mu_p(K_\lambda)^-$. Consequently, the above isomorphisms of $G(K_\lambda/\mathbb{Q}_l)$ -modules imply that

$$E(K_\lambda)^\pm = (E(K_\lambda)/pE(K_\lambda))[p]^\pm = H^1(G(K_\lambda/\mathbb{Q}_l), E)[p]^\mp,$$

so all eigenspaces have dimension 1.

Now we prove (2): it suffices to show that the $+$ and $-$ eigenspaces are orthogonal under \langle, \rangle . If c_1 and c_2 are chosen to lie in opposite eigenspaces,

$$\langle c_1, c_2 \rangle = \langle \tau c_1, \tau c_2 \rangle = -\langle c_1, c_2 \rangle = 0,$$

where we have used the construction of the Tate pairing and the fact that $H^2(G(\bar{K}_\lambda/K_\lambda), \mu_p) = \mathbb{Z}/p\mathbb{Z}$ is τ -invariant.

For the final observation of (2), note that this follows from non-degeneracy of the pairing and the fact that the eigenspaces have dimension 1. \blacksquare

Before proving the next proposition, a reinterpretation of the above pairings on the eigenspaces, we recall for convenience the following commutative diagram, which contains the definition of $Sel(E/K)_p$:

$$\begin{array}{ccccccc} 0 & & & & & & \\ & \searrow & & & & & \\ & & Sel(E/K)_p^\pm & & & & \\ & & \searrow & & & & \\ 0 & \longrightarrow & (E(K)/pE(K))^\pm & \longrightarrow & H^1(G(\bar{K}/K), E[p])^\pm & \longrightarrow & H^1(G(\bar{K}/K), E)[p]^\pm \\ & & & & \downarrow \text{Res} & & \downarrow \\ & & & & H^1(G(\bar{K}_\lambda/K_\lambda), E[p])^\pm & & \prod_v H^1(G(\bar{K}_v/K_v), E)[p]^\pm \\ & & & & \downarrow \cong & & \\ & & & & (E(K_\lambda)/pE(K_\lambda))^\pm & & \end{array}$$

Proposition 38 *Assume that the class $d \in H^1(G(\bar{K}/K), E)[p]^\pm$ is locally trivial for all places $v \neq \lambda$ of K , but that $d_\lambda \neq 0$ in $H^1(G(\bar{K}_\lambda/K_\lambda), E)[p]^\pm$. Then for any class $s \in Sel(E/K)_p^\pm \subset H^1(G(\bar{K}/K), E[p])^\pm$, $s_\lambda = Res_{K_\lambda}(s) = 0$ in $H^1(G(\bar{K}_\lambda/K_\lambda), E[p])^\pm$.*

Proof: Using the above diagram as guidance, the proof will be a combination of Proposition 37 and global class field theory. From the diagram, we see that the restriction s_λ lies in $(E(K_\lambda)/pE(K_\lambda))^\pm$, so by part (2) of Proposition 37, it suffices to show that $\langle s_\lambda, d_\lambda \rangle = 0$.

Lift d to a class $c \in H^1(G(\bar{K}/K), E[p])$, defined up to an element of $E(K)/pE(K)$. The global pairing $\langle s, c \rangle_K$ induced by cup-product and the Weil pairing takes

$$H^1(G(\bar{K}/K), E[p]) \otimes H^1(G(\bar{K}/K), E[p]) \rightarrow H^2(G(\bar{K}/K), \mu_p) = Br(K)[p],$$

where $Br(K)$ denotes the Brauer group of K ; any element of $Br(K)$ is determined by its images in all of the local Brauer groups, and we recall the exact sequence from class field theory

$$0 \rightarrow Br(K) \rightarrow \bigoplus_v Br(K_v) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

Since the local Tate pairing simply applies the invariant map to our global pairing, the image of $\langle s, c \rangle_K \in \oplus_v Br(K_v)$ is $\{\langle s_v, c_v \rangle\}_v$. But $d_v = 0$ for all $v \neq \lambda$, so $\langle s_v, c_v \rangle = 0$ for all $v \neq \lambda$: localizing the sequence

$$0 \rightarrow E(K)/pE(K) \rightarrow H^1(G(\bar{K}/K), E[p]) \rightarrow H^1(G(\bar{K}/K), E)[p] \rightarrow 0$$

at v , we see that $d_v = 0$ implies $c_v \in E(K_v)/pE(K_v)$, and $s_v \in E(K_v)/pE(K_v)$, combined with the fact that $E(K_v)/pE(K_v)$ is an isotropic subgroup for the pairing \langle, \rangle_v , gives us $\langle s_v, c_v \rangle = 0$. Since the sum of local invariants (the map $\oplus_v Br(K_v) \rightarrow \mathbb{Q}/\mathbb{Z}$) is zero by exactness of the class field theory exact sequence, $0 = \sum_v \langle s_v, c_v \rangle_v = \langle s_\lambda, c_\lambda \rangle$, and the proof is complete. \blacksquare

5.6 The Selmer group

The results from the previous section can be used to understand the Selmer group. Recall that p is an odd prime so that $G(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{Aut}(E[p]) \cong (\mathbb{Z}/p\mathbb{Z})^2$. Moreover, $(D, Np) = 1$ which implies that the ramifications of $\mathbb{Q}(E[p])$ and K over \mathbb{Q} are disjoint. Therefore $\mathbb{Q}(E[p]) \cap K = \mathbb{Q}$. Let $L = K(E[p])$ and the previous observation implies that $G(L/K) \cong G(\mathbb{Q}(E[p])/\mathbb{Q})$ because the extensions are linearly disjoint. In these sections we follow [Ossa, Ossb].

5.6.1 Cohomology

The results on the Selmer group follow from general cohomology. We give a few lemmas that will be needed in the next section.

Definition 39 *A spectral sequence $E_2^{p,q} \implies E^n$ consists of objects $E_r^{p,q}, E^n$ and boundary maps $d_r^{p,q} : E_r^{p,q} \rightarrow E_r^{p+r, q-r+1}$ so that the cohomology groups $\ker d_r^{p,q} / \text{Im} d_r^{p+r, q-r+1} \cong E_{r+1}^{p,q}$ and there are isomorphisms $E_\infty^{p,q} \xrightarrow{\sim} gr_p E^{p+q}$.*

An important property of spectral sequences is that if $E_2^{p,q} = 0$ when $p \geq 1$ or $q \geq 1$ then $E_2^{p,0} \cong E^p$ for all p .

Proposition 40 (Hochschild-Serre, [NSW00]) *If G is a profinite group and H a closed normal subgroup then the Hochschild-Serre sequence $H^p(G/H, H^q(H, A)) \implies H^{p+q}(G, A)$ is a spectral sequence.*

We will use the Hochschild-Serre spectral sequence applied to the groups $\mathcal{G} = G(L/K) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$ which contains the central subgroup $Z \cong (\mathbb{Z}/p\mathbb{Z})^*$.

Lemma 41 $H^n(Z, E[p]) = 0$ for all $n \geq 0$.

Proof: $|Z| = p - 1$ while $|E[p]| = p^2$. Therefore $\frac{1}{p-1}$ is an isomorphism in $E[p]$. Pulling back to cocycles, any cocycle is $(p - 1)$ times another cocycle. Therefore it is enough to prove that $p - 1 = 0$ as maps in $H^n(Z, E[p])$. This follows from the fact that $Z \cong (\mathbb{Z}/p\mathbb{Z})^*$.

Fix an injective resolution $0 \rightarrow E[p] \rightarrow I_0 \rightarrow \dots$. Then $H^*(Z, E[p])$ is the cohomology of $0 \rightarrow I_0^Z \rightarrow \dots$. Since elements in this complex are Z -invariant, $Tr_Z = p - 1$. Since Tr_Z maps I_k to I_k^Z the result follows immediately by nonsense.

This works for $n \geq 1$. For $n = 0$ this follows easily since $p - 1 > 1$. \blacksquare

Using the spectral sequence ($H^n(Z, E[p]) = 0$) and the previous lemma we get the following proposition immediately:

Proposition 42

$$H^n(\mathcal{G}, E[p]) = H^n(\mathcal{G}/Z, H^0(Z, E[p])) = 0.$$

Proposition 43 *There is a pairing*

$$[\cdot, \cdot] : H^1(G(\bar{K}/K), E[p]) \times G(\bar{\mathbb{Q}}/L) \rightarrow E[p](L).$$

Proof: The transgression exact sequence gives ($k = G(\bar{K}/K)$, $l = G(\bar{K}/L)$, $k/l = \mathcal{G}$)

$$0 \rightarrow H^1(\mathcal{G}, E[p]^l) \xrightarrow{\text{inf}} H^1(k, E[p]) \xrightarrow{\text{res}} H^1(l, E[p])^{\mathcal{G}} \xrightarrow{\text{tg}} H^2(\mathcal{G}, E[p]^l) \xrightarrow{\text{inf}} H^2(l, E[p]).$$

Using the previous proposition we get that $H^1(k, E[p]) \xrightarrow{\sim} H^1(l, E[p])^{\mathcal{G}} = \text{Hom}_{\mathcal{G}}(G(\bar{\mathbb{Q}}/L), E[p](l))$.

The definition of $[\cdot, \cdot]$ is $[s, \rho] = \text{ress}(\rho)$. The action of $\mathcal{G} = G(L/K)$ is $[s, \rho]^{\sigma} = [s^{\sigma}, \rho^{\sigma}]$ since s is fixed by \mathcal{G} by the previous proposition.

Injectivity means that if $[s, \rho] = 0$ for all ρ then $s = 0$. \blacksquare

Let $S \subset H^1(K, E[p])$ be a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ (since H^1 is).

Definition 44 *Let $G_S(\bar{\mathbb{Q}}/L) = \{\rho \in G(\bar{\mathbb{Q}}/L) \mid [s, \rho] = 0, \forall s \in S\}$. Then $L_S = L^{G_S(\bar{\mathbb{Q}}/L)}/L$ is Galois. To see this we need that G_S is normal and closed. Closure is clear and normality follows from definition and from the fact that $[s, \rho] = 0$ for $\rho \in G_S$.*

Proposition 45 *The induced pairing*

$$[\cdot, \cdot] : S \times G(L_S/L) \rightarrow E[p],$$

is nondegenerate and induces isomorphisms (of \mathcal{G} -modules and $G(K/\mathbb{Q})$ -modules respectively)

$$\begin{aligned} G(L_S/L) &\xrightarrow{\sim} \text{Hom}(S, E[p]) \\ S &\xrightarrow{\sim} \text{Hom}_{\mathcal{G}}(G(L_S/L), E[p]). \end{aligned}$$

Proof: It is nondegenerate on the left because $[\cdot, \cdot]$ is nondegenerate on the left as originally defined. Assume that $[s, \rho] = 0$ for all $s \in S$. Then $\rho \in G_S$ and $G(L_S/L) = G(\bar{\mathbb{Q}}/L)/G(\bar{\mathbb{Q}}/L_S) = G(L_S/L)$ so $\rho = 0$ in the quotient group.

Therefore we have injections $G(L_S/L) \rightarrow \text{Hom}(S, E[p])$ and $S \rightarrow \text{Hom}_{\mathcal{G}}(G(L_S/L), E[p])$ (the last one as \mathcal{G} modules comes from the action of \mathcal{G} on $[\cdot, \cdot]$).

Let $r = \dim_{\mathbb{Z}/p\mathbb{Z}} S$. Then $\text{Hom}(S, E[p]) = E[p]^r$. Since $E[p] \subset L$, \mathcal{G} permutes all of $E[p]$ and so $E[p]$ is simple as a \mathcal{G} -module. Therefore $\text{Hom}(S, E[p])$ is semisimple. Therefore $G(L_S/L) \subset E[p]^r$ so $G(L_S/L) = E[p]^s$ for $s \leq r$.

Now $\text{Hom}_{\mathcal{G}}(E[p], E[p]) = \mathbb{Z}/p\mathbb{Z}$ because $E[p] = (\mathbb{Z}/p\mathbb{Z})^2$ and \mathcal{G} is the full group acting on it, and so only the $\mathbb{Z}/p\mathbb{Z}$ group (the scalars) commute with \mathcal{G} . This implies that $\text{Hom}_{\mathcal{G}}(G(L_S/L), E[p]) = (\mathbb{Z}/p\mathbb{Z})^s \supset S$ and a rank comparison yields $r = s$. This proves both isomorphisms. \blacksquare

5.6.2 Applications to the Selmer Group

We apply the results of the previous section to $S = Sel(E/K)_p \subset H^1(K, E[p])$.

The main goal of this section is to prove that $Sel(E/K)_p$ is generated by δy_K where δ is the connecting homomorphism in section 1. The Mordell-Weil theorem implies that there are finitely many primes p so that $y_K \in pE(K)$ so we may assume that we have chosen p such that $y_K \notin pE(K)$.

Proposition 46 *The field $L_1 = L(\frac{1}{p}y_K)$ is well defined, Galois over L and is a subfield of L_S .*

Proof: Since $E[p] \subset L$ we have that L_1/L is Galois ($\frac{1}{p}y_K$ is well-defined up to $E[p] \subset L$).

Let $\sigma \in G(\bar{\mathbb{Q}}/L_S)$, i.e., an element $\sigma \in G(\bar{\mathbb{Q}}/L)$ so that $[Sel(E/K)_p, \sigma] = 0$. So any cocycle $f \in Sel(E/K)_p \subset H^1(G(\bar{K}/K), E[p])$ sends σ to 0. Therefore δy_K (which is a cocycle $u \mapsto u(\frac{1}{p}y_K) - \frac{1}{p}y_K$) sends σ to 0. Therefore, σ fixes $\frac{1}{p}y_K$ and this means that $L_1 \subset L_S$ clearly. ■

The Galois groups of these extensions are defined in the following diagram:

$$\begin{array}{ccc}
 & L_S & \\
 & \swarrow I & \downarrow H \cong \text{Hom}(Sel(E/K)_p, E[p]) \\
 L_1 = L(\frac{1}{p}y_K) & & L = K(E[p]) \\
 & \searrow E[p] & \downarrow \mathcal{G} \\
 & & K \\
 & & \downarrow \\
 & & \mathbb{Q}
 \end{array}$$

Since $\frac{1}{p}y_K$ is defined up to $E[p]$, the Galois group $G(L_1/L) = E[p]$.

Fix complex conjugation $\tau \in G(L_S/\mathbb{Q})$. As usually \pm define the \pm eigenspaces of τ , when it acts by conjugation on $H = G(L_S/L)$ and $I = G(L_S/L_1)$.

Proposition 47 *The eigenspaces H^+ and I^+ are given by $H^+ = \{(\tau h)^2 | h \in H\}$, $I^+ = \{(\tau i)^2 | i \in I\}$, and $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$. Moreover, if $s \in Sel(E/K)_p^\pm$ then the following are equivalent:*

1. $[s, H] = 0$.
2. $[s, H^+] = 0$.
3. $[s, H^+ \setminus I^+] = 0$.
4. $s = 0$.

Proof: Note that by proposition 45 $H \cong \text{Hom}(\text{Sel}(E/K)_p, E[p])$ and so it is a $\mathbb{Z}/p\mathbb{Z}$ -vector space. Since $\tau^2 - 1 = 0$, $H^+ = H^{\tau^{-1}} \supset H^{\tau+1}$. Also $h \in H^+ \implies h^{\tau+1} = h^2$, since p is odd and H is a vector space over $\mathbb{Z}/p\mathbb{Z}$ then $h \mapsto h^2$ is an isomorphism. Then $h = (h^{1/2})^{\tau+1} \in H^{\tau+1}$ and so $H^+ = H^{\tau+1} = \{h^\tau h \mid h \in H\}$.

By the action of conjugation we get that $h^\tau = \tau h \tau^{-1} = \tau h \tau$ and the structure of H^+ (and similarly for I^+) follows. Now $H^+/I^+ = (H/I)^+ = E[p]^+ \cong \mathbb{Z}/p\mathbb{Z}$.

For the second part of the proof note that we have the implications $4 \iff 1 \implies 2 \implies 3$. We only need $3 \implies 2 \implies 1$.

Assume that $s : H^+ \rightarrow E[p]$ vanishes on $H^+ \setminus I^+$. Then s vanishes on the representatives of the nontrivial elements of $H^+/I^+ \cong \mathbb{Z}/p\mathbb{Z}$. There are such cosets since $I^+ \neq H^+$ and so s vanishes on all of H^+ clearly.

The element $s \in \text{Sel}(E/K)_p^\pm$ induces (via the pairing) a homomorphism $H \rightarrow E[p]$ so that $H^+ \rightarrow E[p]^\pm$ and $H^- \rightarrow E[p]^\mp$. These homomorphisms are \mathcal{G} -invariant by construction. Since s is 0 on H^+ , $s(H) \subset E[p]^\mp$. Since $E[p]$ is simple and $s(H)$ is a sub \mathcal{G} -module, $s(H) = 0$ since it cannot be $E[p]$. \blacksquare

Consider λ a prime in K that is unramified in L_S/K . Assume that λ splits completely in L/K and let λ_M a prime of $M = L_S$ sitting above λ . Then $\text{Frob}(\lambda_M) \in G(L_S/K)$.

Remark 48 $\text{Frob}(\lambda_M) \in H$ and $\text{Frob}(\lambda)$, the \mathcal{G} orbit of $\text{Frob}(\lambda_M)$ depends only on λ .

Proof: Localize at λ . Take a prime λ' of L above λ . Then there is an injection $E(L_{\lambda'})[p] \rightarrow \tilde{E}(\mathbb{F}_{\lambda'})$. Since λ splits completely in L , $\mathbb{F}_{\lambda'} = \mathbb{F}_\lambda$. But $\text{Frob}(\lambda_M)$ fixes \mathbb{F}_λ , so when lifted, it will fix p -torsion. Since $L = K(E[p])$, $\text{Frob}(\lambda_M)L = L$ and the first part follows since $H = G(L_S/L)$.

$$\begin{array}{ccc} \lambda_M & & L_S \\ \downarrow & & \downarrow_H \\ \lambda' & & L \\ \downarrow & & \downarrow_{\mathcal{G}} \\ \lambda & & K \end{array}$$

For the second part observe that $\text{Frob}(\lambda'_M) = \sigma \text{Frob}(\lambda_M) \sigma^{-1}$ for two choices of primes above λ . Then by restricting σ to action on L , we get that the \mathcal{G} orbits are the same. \blacksquare

Proposition 49 For $s \in \text{Sel}(E/K)_p \subset H^1(G(\bar{K}/K), E[p])$ the following are equivalent:

1. $[s, \rho] = 0$, where $\rho = \text{Frob}(\lambda_M) \in H$.
2. $[s, \text{Frob}(\lambda)] = 0$.
3. $s_\lambda = 0 \in H^1(G(\bar{K}_\lambda/K_\lambda), E[p])$.

Proof: Since the action of \mathcal{G} on the pairing is given by $[s, \sigma\rho] = \sigma[s, \rho]$ we have that the first two statements are equivalent.

We will now show that $1 \iff 3$.

$\text{III}(E/K_\lambda) = 0$ by construction since there is only one localization. Therefore the exact sequence (1) will give an isomorphism

$$E(K_\lambda)/pE(K_\lambda) \xrightarrow{\sim} \text{Sel}(E/K_\lambda)_p.$$

Moreover, in the sequence

$$0 \longrightarrow E(K_\lambda)/pE(K_\lambda) \xrightarrow{\delta} H^1(G(\bar{K}_\lambda/K_\lambda), E[p]) \longrightarrow H^1(G(\bar{K}_\lambda/K_\lambda), E)[p],$$

the element $s_\lambda \in H^1(G(\bar{K}_\lambda/K_\lambda), E[p])$ will then map to 0. Therefore $s_\lambda = \delta P_\lambda$ for some $P_\lambda \in E(K_\lambda)/pE(K_\lambda)$. By definition, s_λ takes $\sigma \in G(\bar{K}_\lambda/K_\lambda)$ to $\sigma(\frac{1}{p}P_\lambda) - \frac{1}{p}P_\lambda$.

Since $\frac{1}{p}P_\lambda \in M_{\lambda_M}$ and λ is unramified in M , the extension M_{λ_M}/K_λ is generated by $\text{Frob}(\lambda_M)$ and so the fixed field of $\text{Frob}(\lambda_M)$ is K_λ . Therefore $[s, \text{Frob}(\lambda_M)] = \text{Frob}(\lambda_M)(\frac{1}{p}P_\lambda) - \frac{1}{p}P_\lambda = 0$ if and only if $\frac{1}{p}P_\lambda$ is in the fixed field of $\text{Frob}(\lambda_M)$ when acting on $E(M_{\lambda_M})$, and this is contained in $E(K_\lambda)$ by the above. This is equivalent to the fact that $s_\lambda = 0$. \blacksquare

5.7 The Eigenspaces of the Selmer Group

In this section we complete the proof that $\text{Sel}(E/K)_p$ is dimension one by showing that one of its τ -eigenspaces is trivial, and that δy_K generates the other. Recall that $y_K = P_1$ lies in the ε -eigenspace for complex conjugation, and consequently so does δy_K .

Proposition 50 $\text{Sel}(E/K)_p^{-\varepsilon} = 0$.

Proof: Let $s \in \text{Sel}(E/K)_p^{-\varepsilon}$, so we want to show $s = 0$. It suffices to check that $[s, \rho] = 0$ for all $\rho \in H^+ \setminus I^+$. Such ρ have the form $\rho = (\tau h)^2$ for some $\rho \in H \setminus I$.

Let $l \in \mathbb{Z}$ be a prime which is unramified in L_S/\mathbb{Q} ($S = \text{Sel}(E/K)_p$, for convenience) and which has a factor λ_{L_S} with Frobenius automorphism equal to τh . The Chebotarev density theorem implies that such l exist. Since the Frobenius map in $G(\mathbb{F}_{\lambda_{L_S}}/\mathbb{F}_\lambda)$, $x \mapsto x^{l^2}$, is the square of Frobenius in $G(\mathbb{F}_{\lambda_{L_S}}/\mathbb{F}_l)$, we see that the (global) Frobenius map of $\mathbb{F}_{\lambda_{L_S}}/\mathbb{F}_\lambda$ is $(\tau h)^2$. Thus, by Proposition 49, we need only show $s_\lambda \equiv 0 \in H^1(G(\bar{K}_\lambda/K_\lambda), E[p])$.

Let $c(l)$ and $d(l)$ be the distinguished cohomology classes as previously constructed. We've shown (Proposition 28) that both lie in the $-\varepsilon$ -eigenspace for complex conjugation, and $d(l)_v = 0$ for all places $v \neq \lambda$. $d(l)_\lambda$ is trivial precisely when $y_K \in pE(K_\lambda)$, which is equivalent to λ splitting completely in $L(\frac{1}{p}y_K)$. But we have assumed that $\rho = \text{Frob}(\lambda) \notin I^+$, so λ cannot split completely in $L(\frac{1}{p}y_K)$. We have therefore produced a cohomology class that is locally trivial everywhere except at λ , where it is non-trivial, so we can conclude $s_\lambda = 0$ by Proposition 49. \blacksquare

Proposition 51 *Assume y_K is not divisible by p in $E(K)$. Let $l \in \mathbb{Z}$ be a prime satisfying the same conditions as in the previous proposition. Then the following are equivalent:*

1. $c(l) \equiv 0$ in $H^1(G(\bar{K}/K), E[p])$
2. $c(l) \in Sel(E/K)_p \subset H^1(G(\bar{K}/K), E[p])$
3. $p|P_l$ in $E(K_l)$
4. $d(l) \equiv 0$ in $H^1(G(\bar{K}/K), E[p])$
5. $d(l)_\lambda \equiv 0$ in $H^1(G(\bar{K}_\lambda/K_\lambda), E[p])$
6. $p|y_k$ in $E(K_\lambda)$
7. $h^{1+\tau} \in I^+ = H^+ \cap I$

Proof: Clearly (1) \iff (2) because $c(l)$ is in the $(-\varepsilon)$ -eigenspace and $Sel(E/K)_p^{-\varepsilon} = 0$. From the diagram in the proof of Proposition 24 (namely, injectivity of δ_l and Res), we see that (1) \iff (3). Next, $E(K)/pE(K) \subset Sel(E/K)_p$ (from the definitions and an easy diagram-chase), so $c(l) \equiv 0 \iff d(l) \equiv 0$ ((1) \iff (4)).

Recall that $Sel(E/K)_p$ surjects onto $\text{III}(E/K)[p]$, so $Sel(E/K)_p^{-\varepsilon} = 0$ implies that $\text{III}(E/K)[p]^{-\varepsilon} = 0$, and in particular, if $d(l)$ is everywhere locally trivial, then $d(l)$ is trivial. Thus, since $d(l)_v = 0$ for $v \neq \lambda$, we conclude that (4) \iff (5).

(5) \iff (6) is just a restatement of Proposition 31, and this same result implies that (5) and (7) are equivalent, also using the argument of the previous proposition. \blacksquare

Theorem 52

$$Sel(E/K)_p^\varepsilon \cong (\mathbb{Z}/p\mathbb{Z})\delta y_K.$$

Proof: Let $s \in Sel(E/K)_p^\varepsilon$. We want to show that s is a multiple of δy_K because the other inclusion is clear. It suffices to prove that $[s, \rho] = 0$ for all $\rho \in I$ because then we may quotient I out so that $\sigma \in Hom_{\mathcal{G}}(H/I, E[p]) = Hom_{\mathcal{G}}(G(L_1/L), E[p]) \cong (\mathbb{Z}/p\mathbb{Z})\delta y_K$.

It is enough to show that $[s, I^+] = 0$ because then we have that s maps I^- into a $+$ or $-$ eigenspace of $E[p]$ and so $[s, I] \subset E[p]^\pm$. This takes place as \mathcal{G} -modules and by simplicity of $E[p]$ we get that $[s, I] = 0$.

Therefore we need to show that $[s, (\tau i)^2] = 0$ for $i \in I$.

We would like to apply Proposition 38 to $d = d(l')$ for suitably chosen l and l' to get that $s_\lambda = 0$ for some λ ; we also apply Proposition 49 to $Frob(\lambda_M) = (\tau i)^2$ to get that $[s, (\tau i)^2] = 0$. This will prove the theorem.

Now we will prove the existence of l and l' that will suffice for this proof.

Choose l' so that $c(l') \neq 0 \in H^1(G(\bar{K}/K), E[p])$. By the previous proposition it is enough to require that $Frob(l') = \tau h$ for $h \in H$ so that $h^{\tau+1} \notin I^+$. In that case $c(l') \notin Sel(E/K)_p$. The extension $L' = L_{\langle c(l') \rangle}/L$ has Galois group $E[p]$ as before. Moreover, it is disjoint from L_S/L because $c(l') \notin S = Sel(E/K)_p$. If λ is a prime of K above l so that it splits completely in L , then it splits completely in L' if and only if $P_{l'} \in pE(K_{\lambda_{l'}})$ for all $\lambda_{l'}$ above λ in $K_{l'}$.

Let l be a prime so that both of the following two conditions are satisfied:

1. $Frob(l) = \tau i \in G(L_S/\mathbb{Q})$ with $i \in I$.

2. $\text{Frob}(l) = \tau j \in G(L'/\mathbb{Q})$ with $j \in G(L'/L)$ so that $j^{\tau+1} \neq 1$.

The two conditions may be simultaneously satisfied because $L' \cap L_S = \emptyset$.

The rest of the theorem will follow (as mentioned above) from the following proposition:

Proposition 53 *For l, l' chosen as above, the class $d(l') \in H^1(G(\bar{K}/K), E)[p]^\varepsilon$ is locally trivial at every $\mu \neq \lambda$ but not trivial at λ .*

Proof: Local triviality for $\mu \neq \lambda, \lambda'$ follows from proposition 30.

Since $i \in I$ the previous proposition guarantees that $c(l) = 0$ and $P_l \in pE(K_l)$. Therefore P_l will be divisible by p in $E(K_{\lambda_1})$ for a place λ_1 lying above λ' . By proposition 30 this means that $d(l')_{\lambda'} = 0$.

Finally, $d(l')_\lambda$ is trivial if and only if $P_{l'} \in pE(K_\lambda)$. From the observation made above, this is equivalent to the fact that λ splits completely in L' which means that $(\tau j)^2 = j^{\tau+1} = 1$ contradicting our choice of j .² ■

This concludes the proof that $\text{Sel}(E/K)_p \cong \mathbb{Z}/p\mathbb{Z}$. From this paper's opening discussion, it follows that $\text{III}(E/K)[p] = 0$ and that the rank of $E(K)$ is exactly one.

²We don't get this... we basically ran out of time to understand this final proposition

References

- [And] Fabrizio Andreatta, *A criterion for local triviality*, <http://www-math.mit.edu/osserman/semold/neron.ps>.
- [Cla] Peter L. Clark, *Lecture notes on eichler-shimura theory*, <http://www-math.mit.edu/osserman/semold/eichler.ps>.
- [Dar04] Henri Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, vol. 101, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004. MR 2 020 572
- [Ghi] Alexandru Ghitza, *Modular curves and heegner points*, <http://www-math.mit.edu/osserman/semold/frob.ps>.
- [Gro84] Benedict H. Gross, *Heegner points on $X_0(N)$* , Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 87–105. MR 87f:11036b
- [Gro91] ———, *Kolyvagin's work on modular elliptic curves, L -functions and arithmetic* (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256. MR 93c:11039
- [Kna92] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR 93j:11032
- [Mil86] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press Inc., Boston, MA, 1986. MR 88e:14028
- [NSW00] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2000. MR 2000j:11168
- [Ossa] Brian Osserman, *Applying the local pairing to selmer groups*, <http://www-math.mit.edu/osserman/semold/8.ps>.
- [Ossb] ———, *Concrete selmer group manipulations*, <http://www-math.mit.edu/osserman/semold/9.ps>.
- [Pap] Mihran Papikian, *On tate local duality*, <http://www-math.mit.edu/osserman/semold/duality.ps>.
- [Pop] Alexandru-Anton Popa, *Galois actions on torsion points of elliptic curves*, <http://www-math.mit.edu/osserman/semold/modular.ps>.
- [Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 82e:12016

- [Sil99] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 199?, Corrected reprint of the 1986 original. MR 95m:11054
- [Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 96b:11074