Kolyvagin's work on modular elliptic curves

BENEDICT H. GROSS

1. Let $X_0(N)$ be the modular curve over $\mathbf{Q}$ which classifies elliptic curves with a cyclic N-isogeny. Let $K = \mathbf{Q}(\sqrt{-D})$ be an imaginary quadratic field of discriminant $-D$, where all prime factors of N are split. For simplicity, we assume that $D \neq 3, 4$, so the integers $\mathcal{O}$ of K have unit group $\mathcal{O}^\times = (\pm 1)$. Choose an ideal $\mathcal{N}$ of $\mathcal{O}$ with $\mathcal{O}/\mathcal{N} \simeq \mathbf{Z}/N\mathbf{Z}$.

We consider K, and all other number fields in this paper, as subfields of $\mathbf{C}$. Then the complex tori $\mathbf{C}/\mathcal{O}$ and $\mathbf{C}/\mathcal{N}^{-1}$ define elliptic curves related by a cyclic N-isogeny, hence a complex point x_1 of $X_0(N)$. The theory of complex multiplication shows that the point x_1 is rational over K_1, the Hilbert class field of K.

Let E be a modular elliptic curve of conductor N over $\mathbf{Q}$, and fix a parametrization $\varphi : X_0(N) \longrightarrow E$ which maps the cusp ∞ of $X_0(N)$ to the origin of E. Once φ has been chosen, there is a unique invariant differential ω on E over $\mathbf{Q}$ such that $\varphi^*(\omega)$ is the differential $\Sigma a_n q^n dq/q$ associated to a normalized ($a_1 = 1$) newform on $X_0(N)$. Write $\omega_0 = c\omega$, where ω_0 is a Néron differential on E. It is known that c is an integer, and we may assume that $c \geq 1$.

Let $y_1 = \varphi(x_1)$ in $E(K_1)$, and define the point $y_K = \mathrm{Tr}_{K_1/K}(y_1)$ in $E(K)$. This point is obtained by adding y_1 to its conjugates, using the group law on E. If $\mathcal{N}'$ is another ideal with $\mathcal{O}/\mathcal{N}' \simeq \mathbf{Z}/N\mathbf{Z}$, and y'_K is the corresponding point in $E(K)$, we have $y'_K = \pm y_K +$ (torsion). Hence the canonical height $\hat{h}(y_K)$ is well-defined, independent of the choice of $\mathcal{N}$. Zagier and I proved the limit formula [GZ; Ch. I, (6.5)]:

$$L'(E/K, 1) = \frac{\iint_{E(\mathbf{C})} \omega \wedge \overline{i\omega}}{\sqrt{D}} \cdot \hat{h}(y_K). \tag{1.1}$$

In particular, the point y_K has infinite order if and only if $L'(E/K, 1) \neq 0$.

By comparing (1.1) with the conjecture of Birch and Swinnerton-Dyer for $L(E/K,s)$, Zagier and I were led to the following [GZ; Ch. V, 2.2].

Conjecture 1.2 Assume that $\hat{h}(y_K) \neq 0$, or equivalently, that the point y_K has infinite order in $E(K)$. Then

(1) the group $E(K)$ has rank 1, so the index $I_K = [E(K) : \mathbf{Z}y_K]$ is finite,
(2) the Tate–Shafarevich group $Ш(E/K)$ is finite; its order is given by

$$\#Ш(E/K) = (I_K/c \cdot \Pi_{p|N} m_p)^2$$

where $m_p = (E(\mathbf{Q}_p) : E^0(\mathbf{Q}_p))$.

In (2), note that both the index I_K and the integer c depend on the parametrization φ, but that the ratio I_K/c is independent of the parametrization chosen. Since c and the local factors m_p are integers, the formula in (2) predicts that the order of $Ш(E/K)$ should always divide $(I_K)^2$. This implies, by the existence of the Cassels pairing, that the group $Ш(E/K)$ should always be annihilated by I_K.

Kolyvagin has proved a great part of Conjecture 1.2. His main result is the following [K1, Thm. A].

Theorem 1.3 (Kolyvagin) Assume that the point y_K has infinite order in $E(K)$. Then

(1) the group $E(K)$ has rank 1,
(2) the group $Ш(E/K)$ is finite, of order dividing $t_{E/K} \cdot (I_K)^2$.

In part (2) of this theorem, $t_{E/K}$ is an integer ≥ 1, whose prime factors depend only on the curve E: they consist of 2 and the odd primes p where the Galois group of the extension $\mathbf{Q}(E_p)$ is smaller than expected.

In many cases, Theorem 1.3 reduces the conjecture of Birch and Swinnerton-Dyer to a finite amount of computation. For example, let $E = X_0(37)/w_{37}$ be the curve $y^2 + y = x^3 - x$, and let φ be the modular parametrization of degree 2. Then $c = 1$ and $m_{37} = 1$ in part (2) of Conjecture 1.2, so we expect that $\#Ш(E/K) = (I_K)^2$ when y_K has infinite order. Kolyvagin shows that $t_{E/K}$ is a power of 2 in this case, and that $t_{E/K} = 1$ when I_K is odd. To prove the full conjecture of Birch and Swinnerton-Dyer for E over K, one must construct non-trivial elements in $Ш(E/K)$ when $I_K > 1$. (Kolyvagin's method suggests such a construction - see §11). We remark that in this case the point y_K lies in $E(\mathbf{Q})$, which is infinite cyclic and generated by $P = (0,0)$.

Writing $y_K = m_K \cdot P$ we find $I_K = \pm m_K$; the integers m_K appear as Fourier coefficients of a modular form of weight 3/2 for $\Gamma_0(4 \cdot 37)$ [Z; §5].

2. We will not prove all of Theorem 1.3, but will sketch the proof of a slightly weaker result to illustrate Kolyvagin's main argument. In all that follows, we assume that the curve E does not have complex multiplication over $\mathbf{C}$. (This excludes only thirteen j-invariants.) Then Serre has shown that the extension $\mathbf{Q}(E_p)$ generated by the p-division points of E has Galois group isomorphic to $GL_2(\mathbf{Z}/p\mathbf{Z})$ over $\mathbf{Q}$ for all sufficiently large primes p [S; Thm. 2]. In fact, if E is semi-stable (i.e., if N is square-free), the Galois group of $\mathbf{Q}(E_p)/\mathbf{Q}$ is isomorphic to $GL_2(\mathbf{Z}/p\mathbf{Z})$ for all $p \geq 11$ [Ma; Thm. 4].

The first (crucial) observation is the following. If y_K has infinite order in $E(K)$, one does not know *a priori* that the index $[E(K) : \mathbf{Z}y_K]$ is finite. However, since the group $E(K)$ is finitely generated, the point y_K is not infinitely divisible in $E(K)$. In other words, there are only finitely many integers n such that $y_K = nP$ with $P \in E(K)$.

Proposition 2.1 Let p be an odd prime such that the extension $\mathbf{Q}(E_p)$ has Galois group $GL_2(\mathbf{Z}/p\mathbf{Z})$, and assume that p does not divide y_K in $E(K)$. Then

(1) the group $E(K)$ has rank 1,
(2) the p-torsion subgroup $Ш(E/K)_p$ is trivial.

When y_K has infinite order in $E(K)$, Proposition 2.1 applies for almost all primes p. Our hypotheses imply that p does not divide the index $I_K = [E(K) : \mathbf{Z}y_K]$, so the conclusion is consistent with part (2) of Conjecture 1.2. Kolyvagin obtains Theorem 1.3 by refining the argument for primes p which divide y_K, using the fact that p^n does not divide y_K for large n. The p-primary component of $Ш(E/K)$ is bounded using his techniques on ideal class groups (see [R2]). When the Galois group of $\mathbf{Q}(E_p)$ is strictly contained in $GL_2(\mathbf{Z}/p\mathbf{Z})$, he uses Serre's result that the Galois group of $\mathbf{Q}(E_{p^n})$ has bounded index in $GL_2(\mathbf{Z}/p^n\mathbf{Z})$ for $n \to \infty$.

In fact, what we will prove involves the Selmer group $\mathrm{Sel}(E/K)_p$ at p, which sits in an exact sequence of $\mathbf{Z}/p\mathbf{Z}$-vector spaces

$$(2.2) \qquad 0 \longrightarrow E(K)/pE(K) \xrightarrow{\delta} \mathrm{Sel}(E/K)_p \longrightarrow Ш(E/K)_p \longrightarrow 0.$$

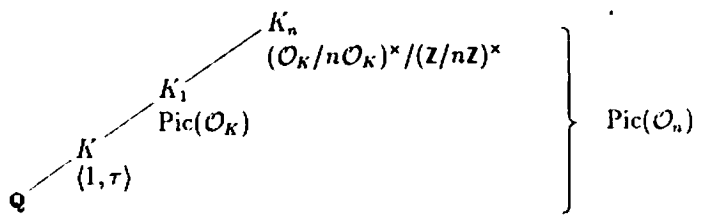
By our hypothesis on $\mathbf{Q}(E_p)$, the group $E(K)$ contains no p-torsion and the dimension of $E(K)/pE(K)$ over $\mathbf{Z}/p\mathbf{Z}$ is equal to the rank of $E(K)$.

Proposition 2.3 Let p be an odd prime such that the extension $\mathbf{Q}(E_p)$ has Galois group $GL_2(\mathbf{Z}/p\mathbf{Z})$, and assume that p does not divide y_K in $E(K)$. Then the group $\mathrm{Sel}(E/K)_p$ is cyclic, generated by δy_K.

The proof of Proposition 2.3 (following Kolyvagin) has three steps. The first is the construction of certain cohomology classes $c(n) \in H^1(K, E_p)$ from Heegner points of conductor n for K, and the study of their amazing properties. The second is the use of Tate duality to obtain information on the local components of elements in the Selmer group $\mathrm{Sel}_p(E/K)$ from the classes $c(n)$. The third is the use of the Čebotarev density theorem to convert information on the local components of the Selmer group to an upper bound on its order. Proposition 2.1 is an immediate corollary of Proposition 2.3, using (2.2).

3. We begin with a construction of the cohomology classes $c(n)$, or rather, with a description of the properties of Heegner points on which the construction depends.

Let $n \geq 1$ be an integer which is prime to N, and let $\mathcal{O}_n = \mathbf{Z} + n\mathcal{O}_K$ be the order of index n in $\mathcal{O}_K$. The ideal $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_n$ is an invertible $\mathcal{O}_n$-module with $\mathcal{O}_n/\mathcal{N}_n \simeq \mathbf{Z}/N\mathbf{Z}$. Consequently the elliptic curve $\mathbf{C}/\mathcal{O}_n$ (with its cyclic N-isogeny to $\mathbf{C}/\mathcal{N}_n^{-1}$) defines a complex point x_n on $X_0(N)$. The theory of complex multiplication shows that the point x_n is rational over K_n, the ring class field of conductor n over K. We have a field diagram with Galois groups marked:



Here τ is complex conjugation, which lifts to an involution of K_n and acts on $\mathrm{Gal}(K_n/K)$ by: $\tau\sigma\tau^{-1} = \sigma^{-1}$.

We will only consider the points x_n on $X_0(N)$, and their images $y_n = \varphi(x_n)$ in $E(K_n)$, when the integer n is square-free. We insist that every prime factor ℓ of n satisfies:

(3.1) $\qquad \ell$ does not divide $N \cdot D \cdot p$.

This hypothesis implies that the prime ℓ is unramified in the extension $K(E_p)$. We let $\mathrm{Frob}(\ell)$ be the conjugacy class in $\mathrm{Gal}(K(E_p)/\mathbf{Q})$ containing the Frobenius substitutions of the prime factors of ℓ, and further insist that

(3.2) $$\mathrm{Frob}(\ell) = \mathrm{Frob}(\infty)$$

as conjugacy classes in $\mathrm{Gal}(K(E_p)/\mathbf{Q})$. Here $\mathrm{Frob}(\infty)$ is the conjugacy class of complex conjugation τ. There are an infinite number of primes ℓ satisfying (3.2), by Čebotarev's density theorem.

A simple implication of (3.2) is that $\mathrm{Frob}(\ell) = \tau$ in $\mathrm{Gal}(K/\mathbf{Q})$. Hence the prime (ℓ) remains inert in K; we let λ denote its unique prime factor. The implication $\mathrm{Frob}(\ell) = \mathrm{Frob}(\infty)$ in $\mathrm{Gal}(\mathbf{Q}(E_p)/\mathbf{Q})$ is equivalent to the congruences:

(3.3) $$a_\ell \equiv \ell + 1 \equiv 0 \pmod{p},$$

where $\ell + 1 - a_\ell$ is the number of points on the reduction $\tilde{E}$ over the finite field $F_\ell = \mathbf{Z}/\ell\mathbf{Z}$. Indeed, the characteristic polynomial of $\mathrm{Frob}(\ell)$ acting on E_p is known to be $x^2 - a_\ell x + \ell$, whereas the characteristic polynomial of $\mathrm{Frob}(\infty) = \tau$ is known to be $x^2 - 1 = (x-1)(x+1)$.

Let F_λ denote the residue field of K at λ, which has ℓ^2 elements. By (3.2) the prime λ splits completely in the extension $K(E_p)$. Hence $\tilde{E}(F_\lambda)_p \simeq (\mathbf{Z}/p\mathbf{Z})^2$; in fact we have:

(3.4) $$\tilde{E}(F_\lambda)_p^{\pm} \simeq \mathbf{Z}/p\mathbf{Z}$$

where $\pm$ denote the eigenspaces for the automorphism group $\langle 1, \tau \rangle$. Indeed $\tilde{E}(F_\lambda)^+$ has order $\ell + 1 - a_\ell$, and $\tilde{E}(F_\lambda)^-$ has order $\ell + 1 + a_\ell$; both are divisible by p by (3.3).

We recall that n is square-free. Write $n = \prod \ell$ and let G_n be the Galois group of the extension K_n/K_1. Then $G_n \simeq \prod G_\ell$ where, for each $\ell | n$, G_ℓ is the subgroup fixing the subfield $K_{n/\ell}$. The subgroups $G_\ell \simeq F_\lambda^\times/F_\ell^\times$ are cyclic of order $\ell + 1$. Let σ_ℓ be a fixed generator of G_ℓ; the augmentation ideal of the group ring $\mathbf{Z}[G_\ell]$ is principal and generated by $(\sigma_\ell - 1)$. Let Tr_ℓ be the element $\sum_{G_\ell} \sigma$ in $\mathbf{Z}[G_\ell]$, and let D_ℓ be a solution of

(3.5) $$(\sigma_\ell - 1) \cdot D_\ell = \ell + 1 - \mathrm{Tr}_\ell$$

in $\mathbf{Z}[G_\ell]$. Then D_ℓ is well-defined up to addition of elements in the subgroup $\mathbf{Z} \cdot \mathrm{Tr}_\ell$ (Kolyvagin uses the solution $D_\ell^0 = \sum_{i=1}^{\ell} i \cdot \sigma_\ell^i = -\sum_{i=1}^{\ell+1} (\sigma_\ell^i - 1)/(\sigma_\ell - 1)$

but this has little advantage over the others). Finally, define $D_n = \prod D_\ell$ in $\mathbf{Z}[G_n]$.

Proposition 3.6 The point $D_n y_n$ in $E(K_n)$ gives a class $[D_n y_n]$ in $(E(K_n)/pE(K_n))$ which is fixed by G_n.

Proof It suffices to show that $[D_n y_n]$ is fixed by σ_ℓ, for all primes $\ell | n$, as these elements generate G_n. Hence we must prove that $(\sigma_\ell - 1)D_n y_n$ lies in $pE(K_n)$.

Write $n = \ell \cdot m$. By (3.5) we have $(\sigma_\ell - 1)D_n = (\sigma_\ell - 1)D_\ell \cdot D_m = (\ell + 1 - \mathrm{Tr}_\ell)D_m$ in $\mathbf{Z}[G_n]$. Hence

$$(\sigma_\ell - 1)D_n y_n = (\ell + 1)D_m y_n - D_m(\mathrm{Tr}_\ell y_n).$$

Since $\ell + 1 \equiv 0 \pmod p$ by (3.3), it suffices to show that $\mathrm{Tr}_\ell y_n$ lies in $pE(K_m)$. This follows from part (1) of the following proposition, and the congruence $a_\ell \equiv 0 \pmod p$ of (3.3).

Proposition 3.7 Let $n = \ell \cdot m$. Then

(1) $\mathrm{Tr}_\ell y_n = a_\ell \cdot y_m$ in $E(K_m)$.
(2) Each prime factor λ_n of ℓ in K_n divides a unique prime λ_m of K_m, and we have the congruence $y_n \equiv \mathrm{Frob}(\lambda_m)(y_m) \pmod{\lambda_n}$.

Proof This follows from the corresponding facts about the points x_n and x_m on $X_0(N)$ over K_n. If T_ℓ denotes the Hecke correspondence, which is self-dual of bidegree $\ell + 1$, we have: $\mathrm{Tr}_\ell x_n = T_\ell(x_m)$ as an equality of divisors of degree $\ell + 1$ on $X_0(N)$ over K_m [G; §6]. Since $\varphi(T_\ell d) = a_\ell \cdot \varphi(d)$ for any divisor d on $X_0(N)$, this proves (1).

To prove (2), we note that by class-field theory, the prime λ is split completely in K_m/K (as it is principal, and generated by an integer ℓ prime to m). The factors λ_m of λ in K_m are totally ramified in $K_n : \lambda_m = (\lambda_n)^{\ell+1}$. In particular, the residue field F_{λ_n} has ℓ^2 elements and is canonically isomorphic to F_λ. We have the congruence: $x_n \equiv \mathrm{Frob}(\lambda_m)(x_m)$ on $X_0(N)$ over F_{λ_n}. Indeed, the points in the divisor $T_\ell(x_m)$ are the conjugates of x_n over K_m; these are all congruent to $x_n \pmod{\lambda_n}$ as λ_m is totally ramified in K_n/K_m. The Eichler-Shimura congruence relation $T_\ell \equiv Fr_\ell + Fr'_\ell \pmod \ell$ shows that at least one point in the divisor $T_\ell x_m$ is congruent to $\mathrm{Frob}(\lambda_m)(x_m) \pmod{\lambda_n}$. Hence all points in the divisor are congruent to $\mathrm{Frob}(\lambda_m)(x_m)$; this also follows from the fact that the residue field has ℓ^2 elements, so $\alpha^\ell \equiv \alpha^{1/\ell}$.

The two properties of Heegner points in Proposition 3.7 show that the collection $\{y_n\}$ forms an 'Euler system', in the language of Kolyvagin [K1; §1]. In the next section, we show how they may be used to construct cohomology classes $c(n)$ in $H^1(K, E_p)$. We observe that since $\mathrm{Tr}_\ell y_n = a_\ell y_m$ lies in $pE(K_n)$, the class $[D_n y_n]$ in $E(K_n)/pE(K_n)$ is independent of the choice of solutions D_ℓ of (3.5). It depends on the choice of generators σ_ℓ of G_ℓ only up to scaling by $(\mathbf{Z}/p\mathbf{Z})^\times$.

4. We retain the notation $n = \prod \ell$ with ℓ satisfying (3.1) and (3.2). Let $\mathcal{G}_n$ be the Galois group of K_n over K; this sits in an exact sequence $0 \to G_n \to \mathcal{G}_n \to \mathrm{Gal}(K_1/K) \to 0$. Let S be a set of coset representatives for G_n in $\mathcal{G}_n$, and define

$$P_n = \sum_{\sigma \in S} \sigma(D_n y_n) \qquad \text{in } E(K_n). \tag{4.1}$$

By Proposition 3.6, the class $[P_n]$ in $E(K_n)/pE(K_n)$ is fixed by $\mathcal{G}_n$. We use the same set S to define P_m for any $m | n$; note that $P_1 = \sum_{\sigma \in S} \sigma y_1 = \mathrm{Tr}_{K_1/K}(y_1) = y_K$. The class $[P_n]$ is independent of the choice of S, and depends on the choice of generators σ_ℓ of G_ℓ, for $\ell | n$, only up to scaling by $(\mathbf{Z}/p\mathbf{Z})^\times$.

The exact sequence $0 \to E_p \to E \xrightarrow{p} E \to 0$ of group schemes over $\mathbf{Q}$ gives, on taking cohomology (Galois = étale) over K and K_n, a commutative diagram

(4.2)

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & H^1(K_n/K, E)_p & & \\
 & & & & & & \mathrm{Inf}\downarrow & & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta} & H^1(K, E_p) & \longrightarrow & H^1(K, E)_p & \longrightarrow & 0 \\
 & & \downarrow & & \mathrm{Res}\downarrow \ell & & \mathrm{Res}\downarrow & & \\
0 & \longrightarrow & (E(K_n)/pE(K_n))^{\mathcal{G}_n} & \xrightarrow{\delta_n} & H^1(K_n, E_p)^{\mathcal{G}_n} & \longrightarrow & H^1(K_n, E)_p^{\mathcal{G}_n}. & &
\end{array}$$

Both rows of (4.2), and the right column, are exact. The restriction from $H^1(K, E_p)$ to $H^1(K_n, E_p)^{\mathcal{G}_n}$ is an isomorphism, as its kernel is $H^1(K_n/K, E_p(K_n))$ via inflation and its cokernel injects into $H^2(K_n/K, E_p(K_n))$ via transgression in the Hochschild-Serre spectral sequence. These cohomology groups are both trivial by the following.

Lemma 4.3 The curve E has no p-torsion rational over K_n.

Proof If not, either $E_p(K_n) = \mathbf{Z}/p\mathbf{Z}$ or $E_p(K_n) = (\mathbf{Z}/p\mathbf{Z})^2$. The first implies that E_p has a cyclic subgroup scheme over $\mathbf{Q}$, as K_n is Galois over $\mathbf{Q}$. Hence the Galois group of $\mathbf{Q}(E_p)$ is contained in a Borel subgroup of $GL_2(\mathbf{Z}/p\mathbf{Z})$. If $E_p(K_n) = (\mathbf{Z}/p\mathbf{Z})^2$, then $\mathbf{Q}(E_p)$ is a subfield of K_n and we have a surjective homomorphism $\mathcal{G}_n \longrightarrow\!\!\!\!\!\rightarrow GL_2(\mathbf{Z}/p\mathbf{Z})$. This is impossible: when $p > 2$, $GL_2(\mathbf{Z}/p\mathbf{Z})$ is not a quotient of a group of 'dihedral' type.

We now define Kolyvagin's cohomology classes. Let $c(n)$ be the unique class in $H^1(K, E_p)$ such that

$$\text{Res } c(n) = \delta_n[P_n] \quad \text{in } H^1(K_n, E_p)^{\mathcal{G}_n}. \tag{4.4}$$

Let $d(n)$ be the image of $c(n)$ in $H^1(K, E)_p$. Since Res $d(n) = 0$ by the commutativity of (4.2) and the exactness of the bottom row, there is a unique class $\tilde{d}(n)$ in $H^1(K_n/K, E)_p = H^1(\mathcal{G}_n, E(K_n))_p$ such that

$$\text{Inf } \tilde{d}(n) = d(n) \quad \text{in } H^1(K, E)_p. \tag{4.5}$$

W. McCallum has observed that the class $c(n)$ is represented by the 1-cocycle

$$f(\sigma) = \sigma(\frac{1}{p} P_n) - \frac{1}{p} P_n - \frac{(\sigma - 1)P_n}{p} \tag{4.6}$$

on $\text{Gal}(\overline{K}/K)$. Here $\frac{1}{p} P_n$ is a fixed p^{th} root of P_n in $E(\overline{K})$, and $\frac{(\sigma - 1)P_n}{p}$ is the unique p^{th} root of $(\sigma - 1)P_n$ in $E(K_n)$, which exists by Lemma 4.3. The class $\tilde{d}(n)$ is represented by the 1-cocycle

$$\tilde{f}(\sigma) = -\frac{(\sigma - 1)P_n}{p}$$

on $\mathcal{G}_n$.

Proposition 4.7 (1) The class $c(n)$ is trivial in $H^1(K, E_p)$ if and only if $P_n \in pE(K_n)$.
(2) The class $d(n)$ is trivial in $H^1(K, E)_p$, and the class $\tilde{d}(n)$ is trivial in $H^1(K_n/K, E)_p$, if and only if $P_n \in pE(K_n) + E(K)$.

Proof This follows from their definitions and the diagram (4.2).

Note The class $c(1)$ is trivial if and only if $P_1 = y_K$ is divisible by p in $E(K)$, and the classes $d(1)$ and $\tilde{d}(1)$ are always globally trivial.

5. We now discuss the action of $\text{Gal}(K/\mathbf{Q}) = \langle 1, \tau \rangle$ on the cohomology classes $c(n)$ in $H^1(K, E_p)$. Since p is odd, we have a direct sum decomposition into eigenspaces for τ:

$$H^1(K, E_p) = H^1(K, E_p)^+ \oplus H^1(K, E_p)^-. \tag{5.1}$$

We will see that the class $c(n)$ lies in one of these eigenspaces, whose sign depends both on E and the number of primes ℓ dividing n.

Let $\epsilon = \pm 1$ be the eigenvalue of the Fricke involution w_N on the eigenform $f = \Sigma a_n q^n$ associated to the modular curve E:

$$f|w_N = \epsilon \cdot f. \tag{5.2}$$

Then the L-function of E over $\mathbf{Q}$ satisfies a functional equation with sign $= -\epsilon$.

Complex conjugation τ acts on the Galois extension K_n, and hence on the point y_n in $E(K_n)$.

Proposition 5.3 We have $y_n^\tau = \epsilon \cdot y_n^{\sigma'} +$ (torsion) in $E(K_n)$, for some $\sigma' \in \mathcal{G}_n$.

Proof This follows from the identity [G, §5]

$$x_n^\tau = w_N(x_n^{\sigma'})$$

for some σ' in $\mathcal{G}_n$. Hence

$$(x_n - \infty)^\tau = w_N(x_n - \infty)^{\sigma'} + (w_N\infty - \infty).$$

Since $w_N\infty$ is the cusp 0 of $X_0(N)$, and the class of $(0 - \infty)$ is torsion in the Jacobian, this gives the claim on the curve E.

Proposition 5.4 (1) The class $[P_n]$ lies in the $\epsilon_n = \epsilon \cdot (-1)^{f_n}$ eigenspace for τ in $(E(K_n)/pE(K_n))^{\mathcal{G}_n}$, where $f_n = \#\{\ell : \ell | n\}$.
(2) The class $c(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E_p)$, and the class $d(n)$ lies in the ϵ_n-eigenspace for τ in $H^1(K, E)_p$.

Proof Recall that $P_n = \sum_{\sigma \in S} \sigma D_n y_n$ in $E(K_n)$, where S is a set of coset representatives for G_n in $\mathcal{G}_n$. For any $\sigma \in \mathcal{G}_n$ we have the commutation relation $\tau\sigma = \sigma^{-1}\tau$. Hence $\tau P_n = \sum_S \sigma^{-1}\tau D_n y_n$.

But $D_n = \prod_{\ell|n} D_\ell$ in $\mathbf{Z}[G_n]$, where $D_\ell \in \mathbf{Z}[G_\ell]$ is a solution (well-defined up to $m\,\mathrm{Tr}_\ell$) of $(\sigma_\ell - 1)D_\ell = \ell + 1 - \mathrm{Tr}_\ell$. Applying τ on the right and left of this identity, we find

$$\begin{aligned}(\sigma_\ell - 1)D_\ell\tau &= \tau(\sigma_\ell - 1)D_\ell \\ &= (\sigma_\ell^{-1} - 1)\tau D_\ell \\ &= -\sigma_\ell^{-1}(\sigma_\ell - 1)\tau D_\ell.\end{aligned}$$

Hence $\tau D_\ell = -\sigma_\ell D_\ell \tau + k\mathrm{Tr}_\ell$ for some $k \in \mathbf{Z}$, as $\tau D_\ell + \sigma_\ell D_\ell \tau$ is annihilated by $(\sigma_\ell - 1)$. (For $D_\ell^0 = \sum_1^\ell i\sigma_\ell^i$, one has $k = \ell$). Since $\mathrm{Tr}_\ell y_n = a_\ell y_{n/\ell} \equiv 0$ in $pE(K_n)$, we have

$$\tau P_n \equiv (-1)^{l_n} \cdot \prod_{\ell|n} \sigma_\ell \cdot \sum_S \sigma^{-1} \cdot D_n(\tau y_n) \pmod{pE(K_n)}.$$

But $\tau y_n = \epsilon \cdot \sigma'(y_n)+$ torsion, by Proposition 5.3, for some σ' in $\mathcal{G}_n$. But Lemma 4.3 shows that $E(K_n)_p = 0$. Hence

$$\tau P_n \equiv \epsilon_n \cdot \prod_{\ell|n} \sigma_\ell \cdot \sigma' \cdot \sum_S \sigma^{-1} D_n y_n \pmod{pE(K_n)}.$$

The sum $\sum \sigma^{-1} D_n y_n$ is $\equiv P_n$, as $[D_n y_n]$ is fixed by G_n and $\{\sigma^{-1}\}$ is another set of coset representatives for G_n in $\mathcal{G}_n$. Since $[P_n]$ is fixed by $\mathcal{G}_n$, we have

$$\tau P_n \equiv \epsilon_n \cdot P_n \qquad \bmod pE(K_n)$$

which proves (1). The statements in (2) are an immediate corollary, as all the maps in the diagram (4.2) commute with the action of $\mathrm{Gal}(K/\mathbf{Q}) = \langle 1, \tau \rangle$.

Since $d(n) \in H^1(K, E)_p^{\zeta_n}$, we may refine Proposition 4.7, part (2).

Corollary 5.5 The class $d(n)$ is trivial in $H^1(K, E)_p^{\zeta_n}$ if and only if $P_n \in pE(K_n) + E(K)^{(n)}$.

6. Recall that

$$(6.1) \qquad Ш(E/K)_p = \ker(H^1(K, E)_p \longrightarrow \coprod_v H^1(K_v, E)_p)$$

where the sum is taken over all places v of K. The Selmer group $\mathrm{Sel}(E/K)_p$ is, by definition, the largest subgroup of $H^1(K, E_p)$ which maps to $Ш(E/K)_p$ in $H^1(K, E)_p$. We now wish to decide if the class $c(n)$ is in the Selmer group, i.e., if the class $d(n)$ is locally trivial at all places of K. We note that $\delta_n[P_n]$ is in the Selmer group of E over K_n, and is fixed by $\mathcal{G}_n$, but restriction does not necessarily induce an isomorphism: $\mathrm{Sel}(E/K)_p \to \mathrm{Sel}(E/K_n)_p^{\mathcal{G}_n}$.

Proposition 6.2 (1) The class $d(n)_v$ is locally trivial in $H^1(K_v, E)_p$ at the archimedean place $v = \infty$, and at all finite places v of K which do not divide n.
(2) If $n = \ell m$ and λ is the unique prime of K dividing ℓ, the class $d(n)_\lambda$ is locally trivial in $H^1(K_\lambda, E)_p$ if and only if $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$ for one (and hence all) places λ_m of K_m dividing λ.

Proof If $v = \infty, K_v = \mathbf{C}$ is algebraically closed and the Galois cohomology of E is trivial. If $v \nmid n$ then the class $d(n)$ is inflated from the class $\widetilde{d(n)}$ of an extension K_n/K which is unramified at v. Hence $d(n)_v$ lies in the subgroup $H^1(K_v^{un}/K_v, E)$, where K_v^{un} is the maximal unramified extension. This group is trivial when E has good reduction at v [M; Ch. I, §3], so $d(n)_v = 0$ for $v \nmid N$.

If $v|N$ the curve E has bad reduction: let E^0 be the connected component of the Néron model and $\phi = E/E^0$ the group of components. Then $H^1(K_v^{un}/K_v, E^0) = 0$, so $H^1(K_v^{un}/K_v, E)$ injects into $H^1(F_v, \phi)$ [M; Ch. I, Prop. 3.8]. But the class $d(n)_v$ is represented by a cocycle with values in a subgroup E' with $(E' : E^0)$ prime to p. Indeed, let J be the Jacobian of $X_0(N)$. Then for any place w dividing v in K_n, the class of the Heegner divisor $(x_n) - (\infty)$ in $J(K_{n,w})$ lies, up to translation by the rational torsion point $(0) - (\infty)$, in J^0 [GZ; III, 3.1]. Hence y_n is, up to translation by rational torsion on E, in E^0. Since $E(\mathbf{Q})_p = 0$ by assumption, the points y_n (and hence $D_n y_n$ and P_n) lie in a subgroup E' whose image in ϕ has order prime to p. Since $d(n)_v$ is killed by p, we have $d(n)_v = 0$.

(2) We recall that the prime λ splits completely in K_m, and each factor λ_m is totally ramified, of degree $\ell + 1$, in K_n. The localization $d(n)_\lambda$ is represented by the cocycle $\sigma \longmapsto \frac{(\sigma-1)P_n}{p}$ on $\mathrm{Gal}(K_{\lambda_n}/K_{\lambda_m}) \simeq G_\ell$ with values in $E(K_{\lambda_n})$. Since $\ell \nmid N$ the curve E has good reduction at λ; let E^1 denote the subgroup of points reducing to the identity. Since E^1 is a pro-ℓ-group and $\ell \neq p$, the cohomology group $H^1(G_\ell, E^1(K_{\lambda_n}))_p = 0$. Hence $d(n)_\lambda$ is trivial if and only if it has trivial image in

$$H^1(G_\ell, \tilde{E}(F_{\lambda_n}))_p = \mathrm{Hom}(G_\ell, \tilde{E}(F_\lambda)_p),$$

where $\tilde{E} = E/E^1$ is the reduced curve. The image of $d(n)_\lambda$ is represented by the cocycle $\sigma \longmapsto$ reduction of $-\frac{(\sigma-1)P_n}{p}$. Since G_ℓ is cyclic, generated by σ_ℓ, we see that the local class $d(n)_\lambda$ is trivial if and only if the point $Q_n = \frac{(\sigma_\ell - 1)P_n}{p}$ has trivial reduction (mod λ_n). Since σ_ℓ acts trivially on $\tilde{E}(F_{\lambda_n}) = \tilde{E}(F_\lambda)$, the reduction $\tilde{Q}_n$ is contained in $\tilde{E}(F_\lambda)_p$.

Since $P_n = \sum_S \sigma D_m \cdot D_\ell \cdot y_n$ and $(\sigma_\ell - 1)D_\ell = \ell + 1 - \mathrm{Tr}_\ell$, we have

$$Q_n = \sum_S \sigma D_m \left(\frac{\ell+1}{p} y_n - \frac{a_\ell}{p} y_m \right)$$

by Proposition 3.7, part (1). By part (2) of that proposition, we have the congruence:

$$\frac{\ell+1}{p} y_n - \frac{a_\ell}{p} y_m \equiv \frac{(\ell+1)\mathrm{Frob}(\lambda_m) - a_\ell}{p} y_m \pmod{\lambda_n}$$

at all places λ_n dividing λ in K_n. For any $\sigma \in \mathcal{G}_n$ we conjugate this congruence (mod $\sigma^{-1}\lambda_n$) by σ to obtain

$$\sigma\left(\frac{\ell+1}{p} y_n - \frac{a_\ell}{p} y_m\right) \equiv \sigma\left(\frac{(\ell+1)(\mathrm{Frob}\ \sigma^{-1}\lambda_m) - a_\ell}{p}\right) y_m \pmod{\lambda_n}.$$

But $\sigma \cdot \mathrm{Frob}(\sigma^{-1}\lambda_m) = \mathrm{Frob}(\lambda_m) \cdot \sigma$, so we obtain

$$\sigma\left(\frac{\ell+1}{p} y_n - \frac{a_\ell}{p} y_m\right) \equiv \left(\frac{(\ell+1)(\mathrm{Frob}\ \lambda_m) - a_\ell}{p}\right) \sigma y_m \pmod{\lambda_n}.$$

Hence

$$Q_n \equiv \frac{(\ell+1)(\mathrm{Frob}\ \lambda_m) - a_\ell}{p} P_m \pmod{\lambda_n}.$$

The reduction $\tilde{P}_m$ lies in the ϵ_m-eigenspace for $\mathrm{Frob}(\ell)$ on $\tilde{E}(F_\lambda)/p\tilde{E}(F_\lambda)$. Since $(\ell+1)\mathrm{Frob}(\ell) - a_\ell$ annihilates $\tilde{E}(F_\lambda)$, and the ϵ_m-eigenspace of p-torsion is cyclic, we see that $\tilde{Q}_n = 0$ if and only if $\tilde{P}_m \in p\tilde{E}(F_\lambda)$. Since E^1 is p-divisible, this is equivalent to the divisibility $P_m \in pE(K_{\lambda_m})$.

Note We have seen that the class $d(1)$ is always globally trivial, hence is locally trivial at all places of K. This is in accord with Proposition 6.2, part (1). For a more interesting example, assume $n = \ell$ is prime. Then, by Proposition 4.7, the class $d(\ell)$ is globally trivial if and only if $P_\ell \in pE(K_\ell) + E(K)$. By Proposition 6.2, the class $d(\ell)$ is locally trivial at all places $v \neq \lambda$ of K, and is locally trivial at λ if and only if $P_1 = y_K \in pE(K_\lambda)$.

7. We now review the relevant results of Tate local duality [T, §2], [M, Ch. I] which will be used in the proof of Proposition 2.3. In this section, we let K_λ be a local field, with ring of integers $\mathcal{O}_\lambda$ and finite residue field F_λ of characteristic ℓ. We let E be an elliptic curve over K_λ, with good reduction over $\mathcal{O}_\lambda$.

Let p be a prime, with $p \neq \ell$. Then E_p is a finite étale group scheme of rank p^2 over $\mathcal{O}_\lambda$. The Kummer sequence $0 \to E_p \to E \xrightarrow{p} E \to 0$ induces an isomorphism

$$E(K_\lambda)/pE(K_\lambda) \xrightarrow{\delta} H^1(\mathcal{O}_\lambda, E_p), \tag{7.1}$$

as $H^1(\mathcal{O}_\lambda, E) = 0$. Since the subgroup $E^1(K_\lambda)$ is ℓ-divisible, the group $E(K_\lambda)/pE(K_\lambda)$ is isomorphic to $\tilde{E}(F_\lambda)/p\tilde{E}(F_\lambda)$, so has dimension ≤ 2 over $\mathbf{Z}/p\mathbf{Z}$, with equality holding if all the p-torsion on E is rational over K_λ.

The Weil pairing $\{,\} : E_p \times E_p \longrightarrow \mu_p$ of finite group schemes over K_λ induces a cup-product pairing in Galois (= étale, or flat) cohomology:

$$H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow H^2(K_\lambda, \mu_p). \tag{7.2}$$

The invariant map of local class field theory gives a canonical isomorphism $H^2(K_\lambda, \mu_p) = \mathrm{Br}(K_\lambda)_p \xrightarrow{\sim} \frac{1}{p}\mathbf{Z}/\mathbf{Z} = \mathbf{Z}/p\mathbf{Z}$, and Tate's local duality theorem states that the resulting pairing of $\mathbf{Z}/p\mathbf{Z}$-vector spaces

$$\langle,\rangle : H^1(K_\lambda, E_p) \times H^1(K_\lambda, E_p) \longrightarrow \mathbf{Z}/p\mathbf{Z} \tag{7.3}$$

is alternating and non-degenerate (see [M, Ch. I, Corollary 2.3]).

The Kummer sequence $0 \to E_p \to E \xrightarrow{p} E \to 0$ gives a short exact sequence in cohomology:

$$0 \longrightarrow E(K_\lambda)/pE(K_\lambda) \longrightarrow H^1(K_\lambda, E_p) \longrightarrow H^1(K_\lambda, E)_p \to 0. \tag{7.4}$$

The subspace $E(K_\lambda)/pE(K_\lambda) \xrightarrow{\sim} H^1(\mathcal{O}_\lambda, E_p)$ is isotropic for the pairing $\langle,\rangle$ induced by cup-product, as $H^2(\mathcal{O}_\lambda, \mu_p) = 0$.

Proposition 7.5 The pairing $\langle,\rangle$ of (7.3) induces a non-degenerate pairing of $\mathbf{Z}/p\mathbf{Z}$-vector spaces (of dimension ≤ 2)

$$\langle,\rangle : E(K_\lambda)/pE(K_\lambda) \times H^1(K_\lambda, E)_p \longrightarrow \mathbf{Z}/p\mathbf{Z}.$$

Proof It suffices to check that the subspace $H^1(\mathcal{O}_\lambda, E_p)$ is maximal isotropic, or equivalently, that $\dim H^1(K_\lambda, E)_p = \dim E(K_\lambda)_p$. This is a general fact, due to Tate [T, §2] (see [M, Ch. I, Thm. 2.6]); we give a proof using tame local class field theory. Let K_λ^{un} be the completion of the maximal unramified extension of K_λ; since $H^1(K_\lambda^{un}/K_\lambda, E) = H^1(\mathcal{O}_\lambda, E) = 0$, restriction induces an isomorphism $H^1(K_\lambda, E)_p \xrightarrow{\sim} H^1(K_\lambda^{un}, E)_p^{\mathrm{Frob}(\lambda)}$. The latter group is isomorphic to $H^1(K_\lambda^{un}, E_p)^{\mathrm{Frob}(\lambda)}$, using the Kummer sequence and the fact that

$E(K_\lambda^{un})$ is p-divisible. Since the residue field of K_λ^{un} is algebraically closed, $H^1(K_\lambda^{un}, E_p)^{\mathrm{Frob}(\lambda)} = \mathrm{Hom}(\mathrm{Gal}(\overline{K}_\lambda/K_\lambda^{un}), E_p)^{\mathrm{Frob}(\lambda)}$. But the homomorphism of $\mathrm{Gal}(\overline{K}_\lambda/K_\lambda^{un})$ to E_p must kill the wild inertia subgroup (as $\ell \neq p$), and factor through the maximal pro-p quotient of the tame inertia group. This quotient is isomorphic to $\mathbf{Z}_p(1) = T_p\mathbf{G}_m$ as a $\mathrm{Frob}(\lambda)$-module, so $H^1(K_\lambda, E)_p$ is isomorphic to $\mathrm{Hom}(\mu_p, E_p)^{\mathrm{Frob}(\lambda)}$. The latter space has the same dimension as $\tilde{E}(F_\lambda)_p \simeq E(K_\lambda)_p$, by the Weil pairing.

We henceforth assume that the p-torsion on E is rational over K_λ, so the $\mathbf{Z}/p\mathbf{Z}$-vector spaces in Proposition 7.5 each have dimension $= 2$. In this case there is an elegant formula for the pairing $\langle , \rangle$, which is due to Kolyvagin and gives an independent proof of its non-degeneracy. To $c_1 \in E(K_\lambda)/pE(K_\lambda)$ we associate the point $e_1 = \left(\frac{1}{p}\, c_1\right)^{\mathrm{Frob}(\lambda)-1}$ in $E(K_\lambda)_p$. To $c_2 \in H^1(K_\lambda, E_p)$ we associate a homomorphism $\phi_2 : \mu_p \to E_p(K_\lambda)$ as above, using tame local class field theory. Fix a primitive p^{th} root ζ of 1 in K_λ^*, and let $\phi_2(\zeta) = e_2$ in $E(K_\lambda)_p$. Then

$$\zeta^{\langle c_1, c_2\rangle} = \{e_1, e_2\}, \tag{7.6}$$

where $\{,\}$ is the Weil pairing on E_p. A proof of (7.6) may be found in the appendix of [W].

8. We now apply Proposition 7.5 in the specific local situation which arises in the study of Heegner points: K is an imaginary quadratic extension of $\mathbf{Q}$ and K_λ is the completion of K at an inert prime $\lambda = (\ell)$. The curve E is defined over $\mathbf{Q}$, so $\mathrm{Gal}(K/\mathbf{Q}) = \mathrm{Gal}(K_\lambda/\mathbf{Q}_\ell) = \langle 1, \tau\rangle$ acts on the $\mathbf{Z}/p\mathbf{Z}$-vector spaces $E(K_\lambda)/pE(K_\lambda)$ and $H^1(K_\lambda, E)_p$.

We assume, as usual, that p is odd and that ℓ satisfies the congruences $\ell + 1 \equiv a_\ell \equiv 0 \pmod{p}$ of (3.3). Then the eigenspaces $E(K_\lambda)_p^\pm$ for τ each have dimension 1 over $\mathbf{Z}/p\mathbf{Z}$.

Proposition 8.1 (1) The eigenspaces $(E(K_\lambda)/pE(K_\lambda))^\pm$ and $H^1(K_\lambda, E)_p^\pm$ for $\mathrm{Gal}(K_\lambda/\mathbf{Q}_\ell)$ each have dimension 1 over $\mathbf{Z}/p\mathbf{Z}$.
(2) The pairing $\langle , \rangle$ of (2.3) induces non-degenerate pairings of $\mathbf{Z}/p\mathbf{Z}$-vector spaces

$$\langle , \rangle^\pm : (E(K_\lambda)/pE(K_\lambda))^\pm \times H^1(K_\lambda, E)_p^\pm \longrightarrow \mathbf{Z}/p\mathbf{Z}.$$

In particular, if $d_\lambda \neq 0$ lies in $H^1(K_\lambda, E)_p^\pm$ 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 (1) We have isomorphisms of $\mathrm{Gal}(K_\lambda/\mathbf{Q}_\ell)$-modules:

$$E(K_\lambda)/pE(K_\lambda) \xrightarrow{\sim} E(K_\lambda)_p \text{ and } H^1(K_\lambda, E)_p \xrightarrow{\sim} \mathrm{Hom}(\mu_p(K_\lambda), E(K_\lambda)_p).$$

Since $\ell + 1 \equiv 0 \pmod{p}$, $\mu_p(K_\lambda) = \mu_p(K_\lambda)^-$. Hence $E(K_\lambda)_p^\pm \simeq (E(K_\lambda)/pE(K_\lambda))_p^\pm \simeq H^1(K_\lambda, E)_p^\mp$, and all eigenspaces have dimension 1.

(2) It suffices to check that the $+$ and $-$ eigenspaces for τ are orthogonal under $\langle , \rangle$. But the Tate pairing satisfies $\langle c_1^\tau, c_2^\tau\rangle = \langle c_1, c_2\rangle$, as τ acts trivially on $H^2(K_\lambda, \mu_p) = \mathbf{Z}/p\mathbf{Z}$. Since p is odd, the result follows. (Alternately, one can use the formula for the Weil pairing: $\{e_1^\tau, e_2^\tau\} = \{e_1, e_2\}^\tau = -\{e_1, e_2\}$ and Kolyvagin's formula (7.6).)

Actually, we will use the following version of Proposition 8.1, which uses the full power of global class field theory.

Proposition 8.2 Assume that the class $d \in H^1(K, E)_p^\pm$ is locally trivial for all places $v \neq \lambda$ of K, but that $d_\lambda \neq 0$ in $H^1(K_\lambda, E)_p^\pm$. Then for any class s in the subgroup $\mathrm{Sel}(E/K)_p^\pm \subset H^1(K, E_p)^\pm$ we have $s_\lambda = \mathrm{Res}_{K_\lambda}(s) = 0$ in $H^1(K_\lambda, E_p)^\pm$.

Proof The restriction s_λ lies in $(E(K_\lambda)/pE(K_\lambda))^\pm$, by the definition of the global Selmer group. Hence it suffices, by Proposition 8.1, to show that $\langle s_\lambda, d_\lambda\rangle = 0$.

To do this, we lift d to a class c in $H^1(K, E_p)$, which is well-defined modulo the image of $E(K)/pE(K)$. The global pairing $\langle s, c\rangle_K$ induced by cup-product lies in $H^2(K, \mu_p) = \mathrm{Br}(K)_p$, and is completely determined by its local components $\langle s_v, c_v\rangle \in \mathrm{Br}(K_v)_p$ for all places v of K. But $\langle s_v, c_v\rangle = 0$ for all $v \neq \lambda$, as $d_v = 0$ in $H^1(K_v, E)_p$. Since the sum of local invariants is zero, by the reciprocity law of global class field theory, we must have $\langle s_\lambda, c_\lambda\rangle = \langle s_\lambda, d_\lambda\rangle = 0$ also.

Kolyvagin's idea is to use global classes d satisfying Proposition 8.2 to bound the order of $\mathrm{Sel}(E/K)_p$. The classes $d = d(n)$ are constructed using Heegner points of conductors $n \geq 1$ for K in §4–5, and their local behavior is analyzed in Proposition 6.2.

9. In this section we give a concrete description of the Selmer group $\mathrm{Sel}(E/K)_p$ in $H^1(K, E_p)$, under the hypothesis that p is odd and that the Galois group of $\mathbf{Q}(E_p)$ is isomorphic to $GL_2(\mathbf{Z}/p\mathbf{Z}) \simeq \mathrm{Aut}(E_p)$. Let $L = K(E_p)$; the hypothesis that D is prime to Np implies that the numberfields K and $\mathbf{Q}(E_p)$ are disjoint. Hence $\mathcal{G} = \mathrm{Gal}(L/K)$ is isomorphic to $GL_2(\mathbf{Z}/p\mathbf{Z})$ and contains the central subgroup $Z \simeq (\mathbf{Z}/p\mathbf{Z})^*$ of homotheties of E_p. Since Z has order $p - 1$, which is prime to p, $H^n(Z, E_p) = 0$ for $n \geq 1$. Since p is odd, $Z \neq 1$ and $E_p^Z = H^0(Z, E_p) = 0$.

Proposition 9.1 We have $H^n(\mathcal{G}, E_p) = 0$ for all $n \geq 0$. The restriction of classes gives an isomorphism of $\mathrm{Gal}(K/\mathbf{Q})$-modules:

$$\mathrm{Res} : H^1(K, E_p) \xrightarrow{\sim} H^1(L, E_p)^{\mathcal{G}} = \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(\overline{\mathbf{Q}}/L), E_p(L)).$$

Proof The spectral sequence $H^m(\mathcal{G}/Z, H^n(Z, E_p)) \Longrightarrow H^{m+n}(\mathcal{G}, E_p)$, and the vanishing of $H^n(Z, E_p)$ for all $n \geq 0$, gives the vanishing of the cohomology of $\mathcal{G}$ in E_p. (This elegant proof is due to Serre.) The fact that restriction is an isomorphism follows, as its kernel is $H^1(\mathcal{G}, E_p)$ and its cokernel injects into $H^2(\mathcal{G}, E_p)$.

From Proposition 9.1 we obtain a pairing:

$$[\ ,\ ] : H^1(K, E_p) \times \mathrm{Gal}(\overline{\mathbf{Q}}/L) \longrightarrow E_p(L), \tag{9.2}$$

which satisfies $[s^\sigma, \rho^\sigma] = [s, \rho^\sigma] = [s, \rho]^\sigma$ for all $s \in H^1(K, E_p)$, $\rho \in \mathrm{Gal}(\overline{\mathbf{Q}}/L)$, and $\sigma \in \mathcal{G} = \mathrm{Gal}(L/K)$. If $[s, \rho] = 0$ for all $\rho \in \mathrm{Gal}(\overline{\mathbf{Q}}/L)$, then $s \equiv 0$ by the injectivity of restriction.

Let $S \subset H^1(K, E_p)$ be a finite subgroup (= finite dimensional vector space over $\mathbf{Z}/p\mathbf{Z}$). Let $\mathrm{Gal}_S(\overline{\mathbf{Q}}/L)$ be the subgroup of $\rho \in \mathrm{Gal}(\overline{\mathbf{Q}}/L)$ such that $[s, \rho] = 0$ for all $s \in S$, and let L_S be the fixed field of $\mathrm{Gal}_S(\overline{\mathbf{Q}}/L)$. Then L_S is a finite normal extension of L.

Proposition 9.3 The induced pairing

$$[\ ,\ ] : S \times \mathrm{Gal}(L_S/L) \longrightarrow E_p(L)$$

is non-degenerate: it induces an isomorphism of $\mathcal{G}$-modules:

$$\mathrm{Gal}(L_S/L) \xrightarrow{\sim} \mathrm{Hom}(S, E_p(L)),$$

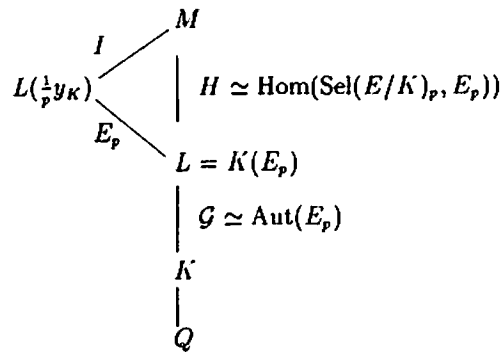
as well as an isomorphism of $\mathrm{Gal}(K/\mathbf{Q})$-modules:

$$S \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p(L)).$$

Proof From the definition of L_S, and the injectivity of restriction proved in 9.1, the pairing $[\ ,\ ] : S \times \mathrm{Gal}(L_S/L) \to E_p(L)$ induces injections $\mathrm{Gal}(L_S/L) \hookrightarrow \mathrm{Hom}(S, E_p)$ and $S \hookrightarrow \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p)$. If $r = \dim(S)$, this shows that $\mathrm{Gal}(L_S/L)$ is a $\mathcal{G}$-submodule of $\mathrm{Hom}(S, E_p) \simeq E_p^r$. Since E_p is a simple $\mathcal{G}$-module, E_p^r is semi-simple. Since any submodule of a semi-simple module is semi-simple, we have an isomorphism of $\mathcal{G}$-modules: $\mathrm{Gal}(L_S/L) \xrightarrow{\sim} E_p^s$ for $s \leq r$. Hence $\mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(L_S/L), E_p) \simeq (\mathbf{Z}/p\mathbf{Z})^s$; since this contains $S \simeq (\mathbf{Z}/p\mathbf{Z})^r$ we must have $s \geq r$. Consequently $s = r$ and the injections induced by $[\ ,\ ]$ are both isomorphisms.

We apply Proposition 9.3 to the finite subgroup $S = \mathrm{Sel}(E/K)_p$ of $H^1(K, E_p)$. For simplicity in notation, we let $M = L_S$ and $H = \mathrm{Gal}(M/L) = \mathrm{Gal}(L_S/L)$. We assume, in preparation for the proof of Proposition 2.3, that y_K is not divisible by p in $E(K)$, and let δy_K be its non-zero image in $\mathrm{Sel}(E/K)_p$. Let I be the subgroup of H which fixes the subfield $L(\frac{1}{p}y_K) = L_{(\delta y_K)}$ of M. Here is a field diagram.

(9.4)



Let τ be a fixed complex conjugation in $\mathrm{Gal}(M/\mathbf{Q})$, and let H^+ and I^+ denote the $+1$ eigenspace for τ (acting by conjugation) on H and I.

Proposition 9.5 (1) We have $H^+ = \{(\tau h)^2 : h \in H\}$, $I^+ = \{(\tau i)^2 : i \in I\}$, and $H^+/I^+ \simeq \mathbf{Z}/p\mathbf{Z}$.

(2) Let $s \in \mathrm{Sel}(E/K)_p^{\pm}$. Then the following are equivalent:

(a) $[s, \rho] = 0$ for all $\rho \in H$

(b) $[s, \rho] = 0$ for all $\rho \in H^+$

(c) $[s, \rho] = 0$ for all $\rho \in H^+ - I^+$

(d) $s = 0$.

Proof (1) Since p is odd, $H^+ = H^{\tau+1} = \{h^\tau \cdot h : h \in H\}$. But $h^\tau = \tau h \tau^{-1} = \tau h \tau$ as $\tau^2 = 1$, so $h^\tau h = (\tau h)^2$. The same works for I^+. Finally, $H^+/I^+ = (H/I)^+ = E_p^+ \simeq \mathbf{Z}/p\mathbf{Z}$.

(2) Clearly (d) $\Longleftrightarrow$ (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c), so it suffices to prove that (c) $\Longrightarrow$ (b) $\Longrightarrow$ (a). Since $s : H^+ \longrightarrow E_p$ is a group homomorphism and $I^+ \neq H^+$, the fact that s vanishes on $H^+ - I^+$ implies that it vanishes on the entire group H^+. Since $s \in \mathrm{Sel}(E/K)_p^{\pm}$, it induces a $\mathcal{G}$-homomorphism $H \longrightarrow E_p$ which maps $H^+ \longrightarrow E_p^{\pm}$ and $H^- \longrightarrow E_p^{\mp}$. If s vanishes on H^+, the image

$s(H)$ is therefore contained in $E_p^{\mp}$. But $s(H)$ is a $\mathcal{G}$-submodule of the simple module E_p, so if $s(H) \neq E_p$ we must have $s(H) = 0$.

Let λ be a prime of K which does not divide Np. Then λ is unramified in M/K; we assume further that λ splits completely in L/K and let λ_M be a prime factor of λ in M. The Frobenius substitution of λ_M in $\mathrm{Gal}(M/K)$ lies in the subgroup H, and its $\mathcal{G}$-orbit – which we denote by $\mathrm{Frob}(\lambda)$ – depends only on the place λ of K. We write $[s, \mathrm{Frob}(\lambda)] = 0$ iff $[s, \rho] = 0$ for all $\rho \in \mathrm{Frob}(\lambda)$.

Proposition 9.6 For $s \in \mathrm{Sel}(E/K)_p \subset H^1(K, E_p)$ the following are equivalent:

(a) $[s, \rho] = 0$, where ρ is the Frobenius substitution associated to the factor λ_M of λ in $\mathrm{Gal}(M/L) = H$

(b) $[s, \mathrm{Frob}(\lambda)] = 0$.

(c) $s_\lambda \equiv 0$ in $H^1(K_\lambda, E_p)$.

Proof Clearly (a) and (b) are equivalent, as for all $\sigma \in \mathcal{G}$ we have $[s, \rho^\sigma] = [s, \rho]^\sigma$. To prove the equivalence of (a) and (c) we assume $s_\lambda \equiv P_\lambda$ in $E(K_\lambda)/pE(K_\lambda) \hookrightarrow H^1(K_\lambda, E_p)$. Then $\frac{1}{p}P_\lambda$ is rational over M_{λ_M}, and $[s, \rho] = (\frac{1}{p}P_\lambda)^{\rho - 1}$ in $E(M_{\lambda_M})_p \simeq E(M)_p$. Hence $[s, \rho] = 0$ if and only if $P_\lambda \in pE(K_\lambda)$.

10. We now give the proof of Proposition 2.3, treating the eigenspaces of $\mathrm{Sel}(E/K)_p$ in turn. Recall that the Heegner point $y_K = P_1$ lies in the ϵ-eigenspace for complex conjugation on $E(K)/pE(K)$ (where ϵ is the eigenvalue of the Fricke involution on the eigenform f associated to E). Hence δy_K lies in the ϵ-eigenspace of $\mathrm{Sel}(E/K)_p$.

Claim 10.1 $\mathrm{Sel}(E/K)_p^{-\epsilon} = 0$.

Proof Assume that $s \in \mathrm{Sel}(E/K)_p^{-\epsilon}$. To show $s = 0$ it suffices, by Proposition 9.5, to show that $[s, \rho] = 0$ for all $\rho \in H^+ - I^+$. Such elements have the form $\rho = (\tau h)^2$, for some $h \in H$.

Let ℓ be a rational prime which is unramified in the extension $M/\mathbb{Q}$, and has a factor λ_M whose Frobenius substitution is equal to τh in $\mathrm{Gal}(M/\mathbb{Q})$. Such primes exist and have positive density, by Čebotarev's density theorem. Then $(\ell) = \lambda$ is inert in K and λ splits completely in L. The Frobenius substitution of F_{λ_M}/F_λ is equal to $(\tau h)^2$, so to prove that $[s, \rho] = 0$ it suffices, by Proposition 9.6, to show that $s_\lambda \equiv 0$ in $H^1(K_\lambda, E_p)$.

Let $c(\ell)$ be the global cohomology class in $H^1(K, E_p)$ constructed in §4, and let $d(\ell)$ be its image in $H^1(K, E)_p$. By Proposition 5.4, both classes lie in the $-\epsilon$-eigenspace for complex conjugation and, by Proposition 6.2, $d(\ell)$ is locally trivial except at λ. We claim that $d(\ell)_\lambda \neq 0$ in $H^1(K_\lambda, E)_p$. Indeed, by Proposition 6.2, $d(\ell)_\lambda$ is trivial if and only if $y_K = P_1 \in p\,E(K_\lambda)$, or equivalently, if the prime λ splits completely in the extension $L(\frac{1}{p}y_K)$. Since $\mathrm{Frob}(\lambda) = \rho$ is not in $I^+ = I \cap H^+$ by hypothesis, this splitting does not occur.

We therefore may apply Proposition 8.2, with $d = d(\ell)$, to conclude that $s_\lambda \equiv 0$. Since this argument works to show $[s, \rho] = 0$ for any $\rho \in H^+ - I^+$ (choosing ℓ correctly) we have shown that $s = 0$.

Proposition 10.2 Assume that y_K is not divisible by p in $E(K)$. Let ℓ be a rational prime which is unramified in $M/\mathbb{Q}$ and has a factor λ_M whose Frobenius substitution is equal to τh in $\mathrm{Gal}(M/\mathbb{Q})$, with $h \in H$. Then $(\ell) = \lambda$ is inert in K and λ splits completely in $L = K(E_p)$. The following are all equivalent:

(1) $c(\ell) \equiv 0$ in $H^1(K, E_p)$

(2) $c(\ell) \in \mathrm{Sel}(E/K)_p \subset H^1(K, E_p)$

(3) P_ℓ is divisible by p in $E(K_\ell)$

(4) $d(\ell) \equiv 0$ in $H^1(K, E_p)$

(5) $d(\ell)_\lambda \equiv 0$ in $H^1(K_\lambda, E_p)$

(6) $P_1 = y_K$ is locally divisible by p in $E(K_\lambda)$

(7) $h^{1+\tau}$ lies in the subgroup $I^+ = H^+ \cap I$ of H^+.

Proof We have (1) $\Longleftrightarrow$ (2) as $\mathrm{Sel}(E/K)_p^{-\epsilon} = 0$ by 10.1. But $c(\ell) \equiv 0$ if and only if $P_\ell \in p\,E(K_\ell)$, so (1) $\Longleftrightarrow$ (3).

Since $(E(K)/pE(K))^{-\epsilon} = 0$ by 10.1, $c(\ell) \equiv 0$ is equivalent to $d(\ell) \equiv 0$. Since $d(\ell)$ is locally trivial except perhaps at λ, and $Ш(E/K)_p^{-\epsilon} = 0$ by 10.1, we have $d(\ell) \equiv 0$ if and only if $d(\ell)_\lambda \equiv 0$. Conditions (6) and (7) are equivalent to $d(\ell)_\lambda \equiv 0$, by Proposition 6.2.

Claim 10.3 $\mathrm{Sel}(E/K)_p^{\epsilon} \simeq \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$.

Proof Let $s \in \mathrm{Sel}(E/K)_p^{\epsilon}$. To show s is a multiple of δy_K it suffices to prove that $[s, \rho] = 0$ for all $\rho \in I$. For then $s \in \mathrm{Hom}_{\mathcal{G}}(H/I, E_p) \simeq \mathbb{Z}/p\mathbb{Z} \cdot \delta y_K$. By the argument of Proposition 9.5, it suffices to show $[s, \rho] = 0$ for all $\rho \in I^+$. These elements all have the form $\rho = (\tau i)^2$, for $i \in I$.

Let ℓ' be a prime such that $c(\ell')$ is non-trivial in $H^1(K, E_p)$; by Proposition 10.2 we may obtain ℓ' by insisting that its Frobenius substitution is conjugate to τh in $\mathrm{Gal}(M/\mathbf{Q})$, where $h \in H$ and $h^{1+\tau} \notin I^+$. Then $c(\ell')$ is not in $\mathrm{Sel}(E/K)_p$, so the extension $L' = L_{\{c(\ell')\}}$ of $L = K(E_p)$ described in (9.3) has Galois group isomorphic to E_p and is disjoint from the extension M/L. A prime ideal $(\ell) = \lambda$ of K, which splits completely in L, splits completely in L' if and only if $P_{\ell'}$ is locally a p^{th} power in $E(K_{\lambda_{\ell'}}) = E(K_\lambda)$, for all factors $\lambda_{\ell'}$ of λ in $K_{\ell'}$.

Let ℓ be a prime whose Frobenius substitution is conjugate to τi in $\mathrm{Gal}(M/\mathbf{Q})$, with $i \in I$ *and* whose Frobenius substitution is conjugate to τj in $\mathrm{Gal}(L'/\mathbf{Q})$, where $j \in \mathrm{Gal}(L'/L)$ satisfies $j^{1+\tau} \neq 1$. (Since $L' \cap M = L$, these two conditions may be satisfied simultaneously.) We claim that the class $d(\ell\ell')$ in $H^1(K, E)_p^\epsilon$ is locally trivial for all places $v \neq \lambda$, but that $d(\ell\ell')_\lambda \neq 0$. The local triviality for $v \neq \lambda, \lambda'$ follows from Proposition 6.2. Since $i \in I$, the global class $c(\ell)$ is zero by Proposition 10.2, and P_ℓ is divisible by p in $E(K_\ell)$. Hence it is locally divisible by p in the completion at a place dividing λ', and $d(\ell\ell')_{\lambda'} = 0$ by Proposition 6.2. Finally $d(\ell\ell')_\lambda$ is trivial if and only if $P_{\ell'}$ is locally divisible by p in $E(K_\lambda)$. But this implies that λ splits in L', or equivalently that $(\tau j)^2 = j^{1+\tau} = 1$. This contradicts our hypothesis on j.

We may now apply Proposition 8.2, with $d = d(\ell\ell')$, to conclude that $s_\lambda = 0$. Consequently $[s, \rho] = 0$, where $\rho = (\tau i)^2$. Since this argument works for any $\rho \in I^+$ (choosing ℓ judiciously) we have shown that $s(I^+) = s(I) = 0$.

11. When the Heegner point y_K has infinite order, but is divisible by p in $E(K)$, the cohomology classes $d(n)$ constructed by Kolyvagin in §3-4 are candidates for non-trivial elements in $Ш(E/K)_p$. Indeed, the condition that $P_1 \in pE(K)$ is equivalent to $c(1) = 0$. This implies, by Proposition 6.2, that the classes $d(\ell)$ all lie in $Ш(E/K)_p$. Similarly, if $c(\ell_1) = c(\ell_2) = 0$ then the class $d(\ell_1\ell_2)$ lies in $Ш(E/K)_p$, if $c(\ell_1\ell_2) = c(\ell_1\ell_3) = c(\ell_2\ell_3) = 0$, then the class $d(\ell_1\ell_2\ell_3)$ lies in $Ш(E/K)_p$, etc. What subgroup of $Ш(E/K)_p$ can be constructed in this manner?

A related question is the following. Assume that p does not divide the integer $c \cdot \prod_{q|N} m_q$ in Conjecture 1.2. Can one show that the class $c(n)$ is non-zero in $H^1(K, E_p)$ for *some* value of $n = \ell_1\ell_2\cdots\ell_r$?

12. Let A be an abelian variety of dimension $d \geq 1$ over $\mathbf{Q}$ such that the algebra $\mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$ is isomorphic to a totally real numberfield of degree d. A generalization of the conjecture of Taniyama and Weil states that A is the quotient of the Jacobian $J_0(N)$ of some $X_0(N)$. Assume that a surjective homomorphism $\varphi : J_0(N) \to A$ exists, and define the points $y_1 = \varphi((x_1) - (\infty))$ in $A(K_1)$ and $y_K = \mathrm{Tr}_{K_1/K} y_1$ in $A(K)$ as in §1. It is easy to show that the L-function of A over K vanishes to order $\geq d$ at $s = 1$. Zagier and I proved that the order of vanishing is equal to d if and only if the Heegner point y_K has infinite order in $A(K)$ [GZ; V, 2.4]. Assuming this, Kolyvagin's method can be used to show that the finitely generated group $A(K)$ has rank d and that $Ш(A/K)$ is finite [K2].

Another generalization is the following. Let χ be a complex character of $\mathrm{Gal}(K_1/K)$, and define the point $y_\chi = \sum_\sigma \chi^{-1}(\sigma) y_1^\sigma$ in $(E(K_1) \otimes \mathbf{C})^\chi$. Following Kolyvagin, one can show [B-D] that the hypothesis $y_\chi \neq 0$ implies that the complex vector space $(E(K_1) \otimes \mathbf{C})^\chi$ has dimension one.

13. *Acknowledgements.* I would like to thank K. Rubin, J.-P. Serre, and J. Tate for their help.

BIBLIOGRAPHY

[B-D] M. Bertolini and H. Darmon, 'Kolyvagin's descent and Mordell-Weil groups over ring class fields'. To appear

[G] B. H. Gross, 'Heegner points on $X_0(N)$', in *Modular Forms* (R. A. Rankin, Ed.) Chichester, Ellis Horwood, 1984, 87-106.

[GZ] B. H. Gross and D. Zagier, 'Heegner points and derivatives of L-series'. Invent. Math., **84** (1986), 225-320.

[K1] V. A. Kolyvagin, 'Euler systems', (1988). To appear in The Grothendieck Festschrift. Prog. in Math., Boston, Birkhauser (1990).

[K2] V. A. Kolyvagin, 'Finiteness of $E(\mathbf{Q})$ and $Ш(E/\mathbf{Q})$ for a class of Weil curves'. Izv. Akad. Nauk SSSR, **52** (1988).

[K3] V. A. Kolyvagin and D.Y. Logachev, 'Finiteness of the Shafarevich-Tate group and group of rational points for some modular abelian varieties'. Algebra and analysis (USSR), No. 5. (1989).

[Ma] B. Mazur, 'Rational isogenies of prime degree'. Invent. Math., **44** (1978), 129-62.

[M] J. S. Milne, 'Arithmetic duality theorems'. Perspectives in Mathematics, Academic Press, 1986.

[R1] K. Rubin, 'The work of Kolyvagin on the arithmetic of elliptic curves'. To appear in *Arithmetic of Complex Manifolds*, Erlangen, 1988, Springer Lecture Notes.

[R2] K. Rubin, Appendix to S. Lang, *Cyclotomic Fields* I *and* II. Springer-Verlag, 1990.

[S] J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques'. Invent. Math., **15** (1972), 259–331 (= *Oe.*94)

[T] J. Tate, 'Duality theorems in Galois cohomology over number fields'. Proc. ICM Stockholm (1962), 288–95.

[W] L. C. Washington, 'Number fields and elliptic curves', in *Number Theory and Applications*, R.A. Mollin ed., Kluwer Academic Publishers, 1989, 245–78.

[Z] D. Zagier, 'Modular points, modular curves, modular surfaces, and modular forms'. Springer LNM 1111 (1985), 225–48.

Index theory, potential theory, and the Riemann hypothesis

SHAI HARAN

In this survey we would like to paint, in expressionistic brushstrokes, our hunch concerning the problem of the Riemann hypothesis. Langlands said it best [38]: '... I have exceeded my commission and been seduced into describing things as they may be and, as seems to me at present, are likely to be. They could be otherwise. Nonetheless, it is useful to have a conception of the whole to which one can refer during the daily, close work with technical difficulties, provided one does not become too attached to it ... I have simply fused my own observations and reflections with ideas of others and with commonly accepted tenets'.

Let us begin by recalling the well known analogies between number fields and function fields. For function fields the Riemann hypothesis was solved by Weil, over a finite field [49], and by Selberg, over the complex numbers [43]. Most attempts to date in solving the Riemann hypothesis for number fields follow Hilbert's old suggestion: find an operator, A, acting on a Hilbert space such that $\langle Ax, y\rangle + \langle x, Ay\rangle = \langle x, y\rangle$, and such that $i(\frac{1}{2} - A)$ is self adjoint, and identify its eigenvalues with the zeros of the zeta function. This approach received scrutiny [22; 25], especially after the success of Selberg's theory, where such an operator, the Laplacian, does in fact exists. Such an operator also exists in the context of Weil's theory, namely the Frobenius operator acting on ℓ-adic cohomology (or equivalently, the ℓth power torsion points of the Jacobian), but here such a realization exists only over $\mathbf{Q}_\ell$, $\ell \neq p$, ∞, a fact which hints of the difficulties of this approach to number fields.

Let us review the 'roundabout' proof of the Riemann hypothesis for a curve C over a finite field $\mathbf{F}_p$, as elucidated in [23; 40]. Given a function $f : p^{\mathbf{Z}} \longrightarrow \mathbf{Z}$ of finite support, we associate with it its Mellin transform $\hat{f}(s) = \sum_n f(p^n) \cdot p^{ns}, s \in \mathbf{C}$, and a divisor $\hat{f}(A) = \sum_n f(p^n) \cdot A^n$ on the surface $C \times C$, where A^n are the Frobenius correspondences given by $A^n = \{(x, x^{p^n})\}$, $A^{-n} = p^{-n} \cdot (A^n)^*$, $n \geq 0$; $*$ denoting the involution $(x, y)^* = (y, x)$. On the surface $C \times C$ we have intersection theory which is given explicitly for our divisors by: