Kolyvagin's work on Shafarevich-Tate groups

William G. McCallum
University of Arizona

January 25, 2003

1 Introduction

Let E be an elliptic modular curve defined over $\mathbf{Q}$ of conductor N, with a fixed modular parametrization $\phi : X_0(N) \to E$ mapping the cusp ∞ on $X_0(N)$ to the origin of the group law on E. Let $K = \mathbf{Q}(\sqrt{-D})$ be a quadratic imaginary field in which all the prime factors of N are split. Let $y_K \in E(K)$ be the Heegner point associated with the maximal order in K, and let $L(E/K, s)$ be the complex L-function of E/K. In [2] Gross and Zagier proved that y_K has infinite order if and only if $L'(E/K, 1) \neq 0$, and gave a formula for the value of the derivative in terms of the height of y_K. This formula and the conjecture of Birch and Swinnerton-Dyer yield the following conjectural formula for the order of the Shafarevich-Tate group of E over K.

CONJECTURE *Suppose that y_K has infinite order. Then $Ш(E/K)$ is finite of order*

$$|Ш(E/K)| = \left(\frac{[E(K) : \mathbf{Z}y_K]}{c \cdot \prod_{q|N} m_q} \right)^2 .$$

Here m_q is the number of connected components of the special fiber of the Néron model of E at q, and c is the Manin constant of the modular parametrization, i.e., if ω is a Néron differential on E then c is the unique positive integer such that $\phi^*(\omega/c)$ is the differential associated with a normalized newform on $X_0(N)$.

Let $R = \mathrm{End}(E)$, and let F be the fraction field of R. In [3] Kolyvagin proved:

THEOREM **(Kolyvagin)** *Suppose y_K has infinite order. Then $E(K)$ has rank 1 and $Ш(E/K)$ is finite. Further, if p is an odd prime which is unramified in F and such that $\mathrm{Gal}(F(E_p)/F) = \mathrm{Aut}_R(E_p)$, then*

$$\mathrm{ord}_p\,|Ш(E/K)| \le 2\,\mathrm{ord}_p[E(K) : \mathbf{Z}y_K].$$

Gross's paper [1] provides an excellent introduction to the proof of this theorem. The purpose of this paper is to given an account of more recent work of Kolyvagin in which he determines the exact group structure of the p-part of $Ш(E/K)$ in terms of his derived Heegner points P_n. (These will be defined later.) The precise result is stated in Theorem 5.4; the following is a simple consequence of it.

THEOREM **(Kolyvagin)** *Suppose y_K has infinite order, and let p be an odd prime which is unramified in F and such that $\mathrm{Gal}(F(E_p)/F) = \mathrm{Aut}_R(E_p)$. Suppose one of Kolyvagin's points P_n satisfies $P_n \notin pE(K(P_n))$. Then*

$$\mathrm{ord}_p\,|Ш(E/K)| = 2\,\mathrm{ord}_p[E(K) : \mathbf{Z}y_K].$$

In Section 2 we recall some results we need from the theory of duality of elliptic curves; in Section 3 we give an application of the Čebotarev density theorem; in Section 4 we recall the definition of Kolyvagin's cohomology classes; and in Section 5 we prove the main theorems.

Notation. If m is a positive integer and G is an abelian group object, we denote the kernel of multiplication by m on G by G_m. If G is a finite group we denote by G^* the group of characters $G \to \mathbf{Q}/\mathbf{Z}$. If L/K is a galois extension of number fields, and if λ is a prime of K, we denote by $\mathrm{Frob}(\lambda)$ the conjugacy class of Frobenius substitutions associated with λ.

Acknowledgments. I would like to thank B. Gross and K. Rubin for useful conversations, and M. Bertolini and H. Darmon for pointing out an error in an earlier version of this paper. Some of this work, including Theorem 5.8, was obtained independently by the author. H. Darmon also independently discovered a related theorem.

2 Global Duality

In this section we consider an elliptic curve E over an arbitrary number field K. If v is a valuation of K we denote the completion by K_v. If λ is a prime ideal of K we denote the associated valuation by v_λ, and write K_λ for K_{v_λ}. Recall that for a positive integer m, the cup product

$$H^1(K_v, E_m) \cup H^1(K_v, E_m) \to H^2(K_v, \mathbf{G}_\mathrm{m}) \overset{\mathrm{inv}_v}{\tilde{\to}} \mathbf{Q}/\mathbf{Z},$$

induced by the Weil pairing, is a non-degenerate pairing of finite groups, and if K is galois, this pairing is $\mathrm{Gal}(K/\mathbf{Q})$-equivariant (see [6], Chapter I, Remark 3.5). It is related to the Tate pairing

$$\langle\ ,\ \rangle_v : H^1(K_v, E) \times E(K_v) \to \mathbf{Q}/\mathbf{Z}$$

by the formula

$$\langle i_*(c), x\rangle_v = c \cup \delta(x),$$

where i is the inclusion $E_m \hookrightarrow E$ and δ is the coboundary for the Kummer sequence

$$0 \to E_m \xrightarrow{i} E \xrightarrow{m} E \to 0.$$

PROPOSITION **2.1** *Let K be a number field, and let $m > 1$ be an integer. Let w be a valuation of K such that $H^1(K_w, E_m) \neq \{0\}$, and let S be a finite set of valuations of K not containing w. For each $v \in S$, let $H_v \subset H^1(K_v, E_m)$ be a subgroup satisfying $|H_v| = (1/2)|H^1(K_v, E_m)|$. Then there exists $c \in H^1(K, E_m)$ satisfying*

1. *$c \neq 0$,*
2. *$c_v \in \delta(E(K_v))$ for all $v \notin S \cup \{w\}$, and*
3. *$c_v \in H_v$ for all $v \in S$.*

Proof. Enlarging S if necessary, and choosing $H_v = \delta(E(K_v))$ for the added valuations, we may suppose that $S \cup \{w\}$ contains the infinite primes, the primes of bad reduction of E, and the primes dividing m. Let $T = S \cup \{w\}$.

It follows from Tate global duality ([6], Chapter I, Theorem 4.10) that there is a self dual exact sequence

$$H^1(K_T/K, E_m) \to \bigoplus_{v\in T} H^1(K_v, E_m) \to H^1(K_T/K, E_m)^*,$$

where K_T is the maximal extension of K unramified outside T. Hence the image of $H^1(K_T/K, E_m)$ is a maximal isotropic subgroup of

$$\bigoplus_{v\in T} H^1(K_v, E_m).$$

Since $H^1(K_w, E_m) \neq 0$, such a subgroup is strictly of larger order than

$$\bigoplus_{v\in S} \frac{H^1(K_v, E_m)}{H_v}.$$

Thus we may choose a $c \in H^1(K_T/K, E_m)$ satsfying (1) and (3). Further, c satisfies (2) because $H^1(K_v^{\rm unr}/K_v, E_m) = \delta(E(K_v))$ if $v(m) = 0$ and E has good reduction at v. ∎

PROPOSITION **2.2** *Let c and c' be two elements of $H^1(K, E_p)$. Then*

$$\sum_v \mathrm{inv}_v(c_v \cup c'_v) = 0.$$

Proof. The sum of the invariants of a global class is zero. ∎

The group of classes $c \in H^1(K, E_m)$ satisfying

$$c_v \in \delta(E(K_v)) \quad \text{for all } v$$

is called the m-Selmer group of E over K, denoted $S_m(E/K)$. It fits into an exact sequence

$$0 \to E(K)/mE(K) \to S_m(E/K) \to Ш(E/K)_m \to 0,$$

where $Ш(E/K)$, the Shafarevich-Tate group of E over K, is defined to be the kernel of

$$H^1(K, E) \longrightarrow \sum_v H^1(K_v, E).$$

There is a skew-symmetric pairing on $Ш(E/K)$, the Cassels pairing, which is non-degenerate if $Ш(E/K)$ is finite. It is defined as follows. Suppose $d \in Ш(E/K)_m$, $d' \in Ш(E/K)_{m'}$. Choose $c' \in S_{m'}(E/K)$ so that $d' = i_*(c')$, and choose *local points* for each valuation v of K

$$y_v \in E(K_v), \quad \delta(y_v) = c'_v.$$

To pair d and d' we need

$$d_1 \in H^1(K, E)_{mm'}, \quad m'd_1 = d.$$

Note that since $d \in Ш(E/K)$, $d_{1,v} \in H^1(K_v, E)_{m'}$ for each v. Then the Cassels pairing of d and d' is

$$\langle d, d' \rangle = \sum_v \langle d_{1,v}, y_v \rangle_v. \tag{1}$$

It is not known in general that d_1 exists, and Tate has a rather clever trick for dealing with this (see [6], Chapter I, Proposition 6.9), but in our case it always exists.

3 An application of the Čebotarev density theorem.

Suppose now that E is defined over $\mathbf{Q}$. For the rest of the paper we will assume that E does not have complex multiplication, in order to simplify the exposition. The general case is not significantly more difficult. Let K be an imaginary quadratic field, and let p be an odd prime such that $\mathrm{Gal}(\mathbf{Q}(E_p)/\mathbf{Q}) = Gl_2(\mathbf{Z}/p\mathbf{Z})$. Let $L = K(E_{p^M})$. Then for $M > 0$, the restriction map

$$H^1(K, E_{p^M}) \to H^1(L, E_{p^M}) = \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbf{Q}}/L), E_{p^M})$$

is an injection of $\mathrm{Gal}(L/\mathbf{Q})$-modules (see [1], Proposition 9.1). Hence, if C is any finite subgroup of $H^1(K, E_{p^M})$ there is a finite Galois extension L_C of L and an isomorphism of $\mathrm{Gal}(L/\mathbf{Q})$-modules

$$\begin{array}{ccc} \mathrm{Gal}(L_C/L) & \simeq & \mathrm{Hom}(C, E_{p^M}), \\ \sigma & \mapsto & \phi_\sigma. \end{array} \tag{2}$$

Further,

$$c_\lambda = 0 \iff \phi_\sigma(c) = 0 \quad \text{for all} \quad \sigma \in G_{\lambda_L}, \tag{3}$$

where λ_L is a prime of L above λ, and G_{λ_L} is the decomposition group of a prime of L_C above λ_L.

Let $\tau \in \mathrm{Frob}(\infty) \subset \mathrm{Gal}(L/\mathbf{Q})$. Since τ acts as -1 on p^∞-th roots of unity and preserves the Weil pairing on E_{p^M}, it has both a plus and a minus eigenspace on E_{p^M}. Hence we may choose an isomorphism of $\langle\tau\rangle$-modules

$$p^{-M}\mathbf{Z}/\mathbf{Z} \oplus (p^{-M}\mathbf{Z}/\mathbf{Z})\tau \simeq E_{p^M}.$$

Using this, we may and do identify

$$\mathrm{Hom}(H^1(K, E_{p^M}), E_{p^M})^{\langle\tau\rangle}$$

with

$$\mathrm{Hom}(H^1(K, E_{p^M}), \mathbf{Q}/\mathbf{Z}) = H^1(K, E_{p^M})^*.$$

PROPOSITION **3.1** *Let $M > 1$ be an integer. Let C be a finite subgroup of $H^1(K, E_{p^M})$, and let $\phi \in C^* = \mathrm{Hom}(C, E_{p^M})^{\langle\tau\rangle}$. There exist infinitely many primes l satisfying the following.*

1. $\mathrm{Frob}(l) = \mathrm{Frob}(\infty)$ *in* $\mathrm{Gal}(\mathbf{Q}(E_{p^M})/\mathbf{Q})$.
2. $\phi = \phi_{\mathrm{Frob}(\lambda')}$ *for some prime λ' of $\mathbf{Q}(E_{p^M})$ lying above λ.*

Proof. By (2), there is some $\sigma \in \mathrm{Gal}(L_C/L)$ such that

$$\phi = \phi_\sigma.$$

Further, since $\phi_\sigma^\tau = \phi_\sigma$, and the order of $\mathrm{Gal}(L_C/L)$ is odd, $\sigma = \rho^\tau \cdot \rho$ for some $\rho \in \mathrm{Gal}(L_C/L)$. By the Čebotarev density theorem, there are infinitely many primes l such that $\mathrm{Frob}(l)$ contains $\tau\rho$. Since the restriction of $\tau\rho$ to L is τ, condition 1 is clearly satisfied. In particular, l has residue class degree 2 in $L/\mathbf{Q}$, so, for a suitable choice of λ',

$$\mathrm{Frob}(\lambda') = (\tau\rho)^2 = \rho^\tau \cdot \rho = \sigma.$$

This concludes the proof. ∎

We say a set of non-zero classes $c_1, \ldots, c_r \in H^1(K, E_{p^M})$ is *independent* if any relation

$$a_1 c_1 + \cdots + a_r c_r = 0, \quad a_i \in \mathbf{Z},$$

implies that $\mathrm{ord}\, c_i$ divides a_i, $1 \le i \le r$.

COROLLARY **3.2** *Let $c_1, \ldots, c_r \in H^1(K, E_{p^M})$ be independent and let $p^{M_i} = \mathrm{ord}(c_i)$, $1 \leq i \leq r$. Let $N_1, \ldots, N_r$ be integers such that $0 \leq N_i \leq M_i$, $1 \leq i \leq r$. Then there are infinitely many primes l satisfying the following.*

1. $\mathrm{Frob}(l) = \mathrm{Frob}(\infty)$ *in* $\mathrm{Gal}(\mathbf{Q}(E_{p^M})/\mathbf{Q})$.
2. *For the prime λ of K lying above l,*

$$\mathrm{ord}\, c_{i,\lambda} = p^{N_i}, \quad 1 \leq i \leq r.$$

Proof. Let $C = \langle c_1, \ldots, c_r \rangle$, and choose $\phi \in C^*$ such that $\mathrm{ord}\, \phi(c_i) = p^{N_i}$, $1 \leq i \leq r$. Choose l as in Proposition 3.1, and different from the finitely many primes where the classes c_i ramify. Then the decomposition group of λ_L is generated by $\mathrm{Frob}(\lambda_L)$, so by (3), $p^M c_{i,\lambda} = 0 \iff \phi(p^M c_i) = 0$. ∎

4 Kolyvagin's classes

We briefly review the definition of these. Since the proofs of [1] generalize easily to our situation, we won't repeat most of them.

For a positive integer n let $\mathcal{O}_n$ be the order of conductor n in K. Choose an ideal $\mathcal{N}$ in $\mathcal{O}_n$ of norm N. The isogeny of complex tori $\mathbf{C}/\mathcal{O}_n \to \mathbf{C}/\mathcal{N}^{-1}$ gives a point x_n on $X_0(N)$, defined over K_n, the ray class field over K of conductor n. The Heegner point referred to in the introduction is $y_K = \mathrm{Tr}_{K_1/K} \phi(x_1)$.

Let p be an odd prime such that $\mathrm{Gal}(\mathbf{Q}(E_p)/\mathbf{Q}) = Gl_2(\mathbf{Z}/p\mathbf{Z})$. Let r and M be integers, $r \geq 0$, $M \geq 1$, and consider the set $S_r(M)$ of positive, square-free integers with exactly r prime factors l, each of which satisfies the following conditions:

$$\begin{aligned} &l \quad \text{does not divide} \quad N \cdot D \cdot p \\ &l \quad \text{is inert in} \quad K \\ &a_l \equiv l + 1 \equiv 0 \pmod{p^M}, \end{aligned}$$

where a_l is the trace of $\mathrm{Frob}(l)$ on E_p. The last two conditions are equivalent to

$$\mathrm{Frob}(l) = \mathrm{Frob}(\infty) \quad \text{on} \quad \mathbf{Q}(E_{p^M}).$$

In particular, λ, the prime of K above l, splits completely in $K(E_{p^M})$. Let

$$S(M) = \bigcup_{r \geq 0} S_r(M).$$

Let $n \in S(M)$, and let $y_n = \phi(x_n) \in E(K_n)$. Let K_1 be the Hilbert class field of K, and let $G_n = \mathrm{Gal}(K_n/K_1)$. Then $G_n \simeq \prod G_l$, where $G_l = \mathrm{Gal}(K_n/K_{n/l})$ is cyclic of order $l+1$, with generator σ_l, say.

Define $D_n \in \mathbf{Z}[G_n]$ by $D_n = \prod D_l$, where

$$D_l = \sum_{i=1}^{l} i \cdot \sigma_l^i.$$

Let $\mathcal{G}_n = \mathrm{Gal}(K_n/K)$, let S be a set of coset representatives for G_n in $\mathcal{G}_n$, and define a point $P_n \in E(K_n)$,

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

Then

$$P_n \in (E(K_n)/p^M E(K_n))^{\mathcal{G}_n}. \tag{4}$$

From P_n we construct cohomology classes as follows. Consider the commutative diagram of cohomology sequences:

$$\begin{array}{ccccccccc}
0 & \to & E(K)/p^M E(K) & \stackrel{\delta}{\to} & H^1(K, E_{p^M}) & \to & H^1(K,E)_{p^M} & \to & 0 \\
 & & \downarrow & & \wr \downarrow \mathrm{res} & & \downarrow \mathrm{res} & & \\
0 & \to & (E(K_n)/p^M E(K_n))^{\mathcal{G}_n} & \stackrel{\delta'}{\to} & H^1(K_n, E_{p^M})^{\mathcal{G}_n} & \to & H^1(K_n,E)_{p^M}^{\mathcal{G}_n} & &
\end{array}$$

The middle vertical map is an isomorphism because

$$E \text{ has no } K_n\text{-rational } p\text{-torsion} \tag{5}$$

(see [1], Lemma 4.3). The class $c_M(n)$ is defined to be the unique class in $H^1(K, E_{p^M})$ such that

$$\mathrm{res}(c_M(n)) = \delta'(P_n). \tag{6}$$

LEMMA **4.1** *The class $c_M(n)$ is represented by the cocycle*

$$\sigma \longmapsto -\frac{(\sigma-1)P_n}{p^M} + \sigma\frac{P_n}{p^M} - \frac{P_n}{p^M}$$

where $\frac{(\sigma-1)P_n}{p^M}$ is the unique p^M-division point of $(\sigma-1)P_n$ in $E(K_n)$.

Proof. The existence of the p^M-division point follows from (4), the uniqueness from (5). Uniqueness implies that

$$\sigma \mapsto -\frac{(\sigma-1)P_n}{p^M}$$

is a cocycle, hence the expression given in the statement of the lemma is a cocycle. Clearly it takes values in E_{p^M}, and the first term disappears when we restrict to K_n, hence it satisfies (6), the defining property of $c_M(n)$. ∎

Let $d_M(n)$ denote the image of $c_M(n)$ in $H^1(K,E)$.

COROLLARY **4.2** *The class $d_M(n)$ is represented by the cocycle*

$$\sigma \longmapsto -\frac{(\sigma-1)P_n}{p^M}.$$

Proof. Regarded as a cocycle with values in E,

$$\sigma \longmapsto \sigma\frac{P_n}{p^M} - \frac{P_n}{p^M}$$

is a coboundary. ∎

Let λ be the unique prime of K above l and let λ_n represent a prime of K_n above λ. We denote the completion of K_n at λ_n by K_{λ_n}. Suppose that $n = l \cdot m$. The prime ideal λ is principle, generated by the number l prime to m, and hence splits completely in K_m by class field theory, and each prime factor of l in K_m ramifies totally in K_n. In particular, there is an embedding $K_m \hookrightarrow K_\lambda$, and by (4) the resulting image of P_m in $E(K_\lambda)/p^M E(K_\lambda)$ is independent of the choice of embedding.

LEMMA **4.3** *Let $n \in S(M)$, and let v be a valuation of K prime to n. Then $c_M(n)_v \in \delta(E(K_v))$. If in addition $v = v_\lambda$, where l is inert in K, then $c_M(n)_\lambda = \delta(P_n)$.*

Proof. The first statement is proved in [1], Proposition 6.2. By Lemma 4.1,

$$c_M(n) = -\frac{(\sigma-1)P_n}{p^M} + \sigma\frac{P_n}{p^M} - \frac{P_n}{p^M}.$$

If l is inert in K, then, as we saw above, λ splits in K_n, by class field theory. Thus, when we restrict this cocycle to the decomposition group at λ, the first term goes away. Thus the cocycle is $\delta(P_n)$ locally at λ. ∎

For primes dividing n we have the following proposition.

PROPOSITION **4.4 (Kolyvagin, [3] Theorem 3)** *Let $l \in S_1(M)$. There is a homomorphism*

$$\chi_l : E(K_\lambda) \to H^1(K_\lambda, E_{p^M})$$

such that

1. *for all $m \in S(M)$, $(m, l) = 1$,*

$$c_M(ml)_\lambda = \chi_l(P_m),$$

2. $\ker \chi_l = p^M E(K_\lambda)$ *and*

$$\chi_l(E(K_\lambda)/p^M E(K_\lambda)^{\pm}) \subset H^1(K_\lambda, E_{p^M})^{\mp},$$

   and

3. *the composition of χ_l with $H^1(K_\lambda, E_{p^M}) \to H^1(K_\lambda, E)_{p^M}$ induces an isomorphism*

$$E(K_\lambda)/p^M E(K_\lambda) \simeq H^1(K_\lambda, E)_{p^M}.$$

In particular,

$$\operatorname{ord} d_M(ml)_\lambda = \operatorname{ord} c_M(ml)_\lambda = \operatorname{ord} c_M(m)_\lambda.$$

Proof. Let $n = ml$. Let $P \in E(K_\lambda)$. Let $\mathbf{F}_\lambda$ denote the residue field of λ, and let $\tilde{P}$ be the image of P in $E(\mathbf{F}_\lambda)$. Since $\mathrm{Frob}(l)^2 = 1$ onh $\mathbf{F}_\lambda$,

$$(a_l - (l+1)\mathrm{Frob}(l))\tilde{P} = -\mathrm{Frob}(l)(\mathrm{Frob}(l)^2 - a_l \mathrm{Frob}(l) + 1)\tilde{P} = 0.$$

Since λ splits completely in $K(E_{p^M})$, $E_{p^M}(\overline{K}_\lambda) = E_{p^M}(K_\lambda)$. Since l is prime to p and E has good reduction at λ, the reduction map is injective on E_{p^M}. Hence there is a unique $T \in E_{p^M}$ such that

$$\frac{a_l - (l+1)\mathrm{Frob}(l)}{p^M} P \equiv T \pmod{\lambda}.$$

Define $\chi_l(P)$ to be the cocycle for $\mathrm{Gal}(K_{\lambda_l}/K_\lambda)$ which takes σ_l to T. To see that this satisfies the statement of the proposition, recall from Lemma 4.1 that $c_M(n)$ is represented by the cocycle

$$\sigma \mapsto -\frac{(\sigma-1)P_n}{p^M} + \sigma\frac{P_n}{p^M} - \frac{P_n}{p^M}.$$

Let $\overline{\lambda}$ be any prime of $\overline{K}$ above λ, and restrict this cocycle to the decomposition group of $\overline{\lambda}$. Let λ_n be the prime of K_n below $\overline{\lambda}$. Since $D_l = l(l+1)/2$ on the residue field of λ_n, and p^M divides $l+1$, $P_n \in p^M E(K_{\lambda_n})$. Hence the cocycle vanishes when restricted to K_{λ_n}, and factors through $\mathrm{Gal}(K_{\lambda_n}/K_\lambda) = \langle\sigma_l\rangle$. Furthermore, since σ_l is in the inertia group of λ, $\sigma_l(P_n/p^M) - (P_n/p^M)$ reduces to zero modulo λ_n. Hence

$$-\frac{(\sigma_l-1)P_n}{p^M} + \sigma_l\frac{P_n}{p^M} - \frac{P_n}{p^M}$$

is the unique torsion point congruent to $-((\sigma_l-1)P_n)/p^M$ modulo λ_n. But, as in [1], Proposition 6.2, we have

$$-\frac{(\sigma_l-1)P_n}{p^M} \equiv \frac{a_l - (l+1)\mathrm{Frob}(l)}{p^M}P_m \pmod{\lambda_n}.$$

This proves property (1). Property (2) follows from the fact that the $\mathrm{Gal}(K/\mathbf{Q})$-eigenspaces of $E(\mathbf{F}_\lambda)$ are cyclic of order $l+1-\mathrm{Frob}(l)a_l$, and that σ_l is in the minus eigenspace. Property (3) is clear since all the non-zero cocycles in $\mathrm{im}\,\chi_l$ are ramified, and thus $\mathrm{im}\,\chi_l \cap \delta(E(K_\lambda)) = 0$.

Finally, it follows from properties (1) and (3) that

$$\mathrm{ord}\, d_M(ml)_\lambda = \mathrm{ord}\, c_M(ml)_\lambda,$$

and that $\mathrm{ord}\, c_M(ml)$ equals the order of P_m in $E(K_\lambda)/p^M E(K_\lambda)$. By Lemma 4.3, this equals $\mathrm{ord}\, c_M(m)_\lambda$. ∎

COROLLARY **4.5** *Suppose $n \in S(M)$, let l be a prime divisor of n, and let $m = n/l$. If $P_m \notin p^M E(K_\lambda)$ then $P_n \notin p^M E(K_n)$.*

Proof. If $P_m \notin p^M E(K_\lambda)$, then by Proposition 4.4 $c_M(n)_\lambda \neq 0$, hence $c_M(n) \neq 0$. But it is easy to see from the definition that $c_M(n) = 0$ if and only if $P_n \in p^M E(K_n)$. ∎

Finally, we show how to compute the Cassels pairing of Kolyvagin's classes.

LEMMA **4.6** *Let $M \geq M'$ be positive integers and let $n \in S(M)$. Then*

$$p^{M'} d_M(n) = d_{M-M'}(n).$$

Proof. Clear from the definition. ∎

PROPOSITION **4.7** *Let M and M' be integers ≥ 1, and let $n \in S(M+M')$, $n' \in S(M')$. Suppose that $d_M(n), d_{M'}(n') \in Ш(E/K)$. Then the Cassels pairing is*

$$\langle d_M(n), d_{M'}(n') \rangle = \sum_{\substack{l|n \\ (l,n')=1}} \langle d_{M+M'}(n), P_{n'} \rangle_\lambda$$

Proof. We refer to the description of the Cassels pairing given in Section 2. By Lemma 4.6, $p^{M'} d_{M+M'}(n) = d_M(n)$; hence $d_{M+M'}(n)$ plays the role of d_1. Also, $c_{M'}(n')$ plays the role of c'.

First, suppose $v \not| n$. Then $d_{M+M'}(n)_v$ is unramified at v, since by Corollary 4.2 it splits over K_n. From [6], Chapter I, Proposition 3.8, it follows that $d_{M+M'}(n)_v$ is killed by m_v. We claim that $d_{M+M'}(n)_v = 0$; this is clear if v is a prime of good reduction, and follows from Gross's argument in [1], Proposition 6.2 otherwise. Hence there is no contribution to the Cassels pairing from v.

Now suppose that $v = \lambda$, for some $l|n$. If $l|n'$, then by Proposition 4.4, $c_{M'}(n')_\lambda = 0$, since $d_{M'}(n') \in Ш(E/K)$. If $l \not| n'$, then by Lemma 4.3, $P_{n'}$ plays the role of y_λ. The proposition now follows from (1). ∎

5 Structure of the Shafarevich-Tate group.

From now on we will assume that y_K has infinite order and that p is an odd prime such that $\mathrm{Gal}(\mathbf{Q}(E_p)/\mathbf{Q}) = Gl_2(\mathbf{Z}/p\mathbf{Z})$. We choose a fixed complex conjugation

$$\tau \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}),$$

and if M is a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module, denote by M^+ (resp. M^-) the part of M on which τ acts by $+1$ (resp. -1). The image of the Heegner point y_K in

$E(K)$/torsion is an eigenvector for τ ([1], Proposition 5.3); let $\epsilon = \pm 1$ be its eigenvalue. (It is the negative of the sign of the functional equation of $L(E/\mathbf{Q}, s)$.) By Kolyvagin's theorem [3], $Ш(E/K)$ is finite, and hence the Cassels pairing is non-degenerate. Since the pairing is skew-symmetric, the elementary divisors of $Ш(E/K)$ come in pairs. Let

$$N_1 \geq N_3 \geq N_5 \geq \cdots$$

be integers such that

$$Ш(E/K)_{p^\infty}^{-\epsilon} \simeq (\mathbf{Z}/p^{N_1}\mathbf{Z})^2 \times (\mathbf{Z}/p^{N_3}\mathbf{Z})^2 \times \cdots,$$

and let

$$N_2 \geq N_4 \geq N_6 \geq \cdots$$

be integers such that

$$Ш(E/K)_{p^\infty}^{\epsilon} \simeq (\mathbf{Z}/p^{N_2}\mathbf{Z})^2 \times (\mathbf{Z}/p^{N_4}\mathbf{Z})^2 \times \cdots.$$

We write $p^M | P_n$ if $P_n \in p^M E(K_n)$, and $p^M \| P_n$ if $P_n \in p^M E(K_n) - p^{M+1}E(K_n)$. Let

$$\mathrm{ord}_p(P_n) = \max\{M : p^M | P_n\},$$

and let

$$M_r = \min\{\mathrm{ord}_p(P_n) : n \in S_r(\mathrm{ord}_p(P_n) + 1)\}.$$

LEMMA **5.1** *We have* $M_0 = \mathrm{ord}_p[E(K) : \mathbf{Z}y_K]$ *and* $M_r \geq M_{r+1}$ *for all* $r \geq 0$.

Proof. We have $P_1 = y_K$, and

$$M_0 = \mathrm{ord}_p\, y_K = \max\{M : y_K \in p^M E(K_1)\},$$

and

$$\mathrm{ord}_p[E(K) : \mathbf{Z}y_K] = \max\{M : y_K \in p^M E(K)\}.$$

Since $E(K_1)$ has no p-torsion, $E(K)/p^M E(K)$ injects into $E(K_1)/p^M E(K_1)$; hence these two numbers are the same.

In particular, M_0 is finite. Now suppose that M_r is finite, and let $n \in S_r(M_r + 1)$ satisfy $p^{M_r} \| P_n$. By Corollary 3.2, we may choose $l \in S(M_r + 1)$, prime to n, so that $c_{M_r+1}(n)_\lambda \neq 0$. Then by Lemma 4.3, $P_n \notin p^{M_r+1}E(K_\lambda)$,

so by Corollary 4.5, $P_{nl} \notin p^{M_r+1}E(K_{nl})$. Hence M_{r+1} is finite and no greater than M_r. ∎

The goal of this section is to prove that $N_i = M_{i-1} - M_i$ for all i (Theorem 5.4). We will construct elements in $Ш(E/K)$ as follows. Suppose $M_{r-1} > M_r$ and let $n \in S_r(M_{r-1})$. Then it follows from the definition of the M_i that $p^{M_r}|P_n$ and $p^{M_{r-1}}|P_{n/l}$ for all l dividing n. It follows from Lemma 4.3 and Proposition 4.4 that $d_{M_{r-1}}(n) \in Ш(E/K)$. The order of this element is at most $p^{M_{r-1}-M_r}$. By careful choice of n we will construct such elements achieving this order and independent of each other. By (5) the natural map

$$H^1(K, E_{p^M}) \to H^1(K, E_{p^{M'}}), \quad M' \geq M$$

is an injection. We let

$$H^1(K, E_\infty) = \lim_{\to} H^1(K, E_{p^M}), \quad S_\infty(E/K) = \lim_{\to} S_{p^M}(E/K).$$

If $n \in S_r(M)$, then $c_M(n) \in H^1(K, E_{p^M})^{\epsilon_r}$, where $\epsilon_r = (-1)^r\epsilon$ ([1], Proposition 5.4).

PROPOSITION **5.2** *Let r be a positive integer, and let C be a subgroup of $S_\infty(E/K)^{\epsilon_r}$ of rank r. Let $M > M_r$. There exists $n \in S_r(M)$ such that $c_M(n)$ had order p^{M-M_r} and $\langle c_M(n)\rangle \cap C = \{0\}$.*

For the proof we will need the following variant of Proposition 2.1.

LEMMA **5.3** *Let $l \in S_1(M)$. The Tate pairing induces a non-degenerate pairing*

$$(E(K_\lambda)/p^M E(K_\lambda))^{\pm} \times H^1(K_\lambda, E_{p^M})^{\pm} \to \mathbf{Q}/\mathbf{Z}$$

which is a duality of cyclic groups of order p^M. Further, if S is a finite subset of $S_1(M)$ not containing l, then there exists $c \in H^1(K, E_{p^M})^{\pm}$ satisfying

1. *$c \neq 0$,*
2. *$c_v \in \delta(E(K_v))$ for all v prime to $S \cup \{l\}$, and*
3. *$c_{v_\lambda} \in \operatorname{im}\chi_l$ for all $l \in S$.*

Finally, $\operatorname{im}\chi_l$ is an isotropic subgroup of $H^1(K_\lambda, E_{p^M})$.

Proof. The first statement is proved as in [1], Proposition 8.1. It implies that

$$|\operatorname{im}(\chi_l)^+| = \frac{1}{2}|H^1(K_\lambda, E_{p^M})^+|$$

and implies that

$$|\operatorname{im}(\chi_l)^-| = \frac{1}{2}|H^1(K_\lambda, E_{p^M})^-|.$$

Hence, in the proof of Proposition 2.1, we can add the further stipulation that $c \in H^1(K, E_{p^M})^\pm$. Finally, it follows from Proposition 4.4 that $\operatorname{im}(\chi_l)^+ \simeq \operatorname{im}(\chi_l)^- \simeq \mathbf{Z}/p^M\mathbf{Z}$. Since the cup product is skew symmetric and $\operatorname{Gal}(K/\mathbf{Q})$-equivariant, it must vanish on $\operatorname{im}(\chi_l)$. ∎

Proof of Proposition 5.2. By Lemma 4.6, it suffices to prove the proposition for large enough $M > M_r$. Let

$$p^M \geq \max\{\text{exponent of } C, p^{M_{r-1}}\},$$

and let $L = K(E_{p^M})$. For $n \in S_r(M)$, the class $c_M(n)$ has order p^{M-M_r} if and only if $p^{M_r} \| P_n$. By definition of M_r, there exists

$$n \in S_r(M_r + 1)$$

such that

$$p^{M_r} \| P_n.$$

Choose such an n. Let S be the set of prime factors of n, and for each $l \in S$, choose a prime factor λ_L of l in L. Let $X \subset C^*$ be the group of characters generated by

$$\phi_{\operatorname{Frob}(\lambda_L)}, \quad l \in S \cap S(M).$$

Let k be the rank of the image of X in C^*/pC^*. Suppose that $k < r$. Then there is a redundant $l_0 \in S$ such that the characters

$$\phi_{\operatorname{Frob}(\lambda_L)}, \quad l \in S \cap S(M) - \{l_0\}$$

generate X modulo pC^*. Choose $\psi \in C^*$ such that

$$\psi \notin X + pC^*;$$

and if $c_{M_r+1}(n) \in C$ choose $\psi \in C^*$ such that

$$\psi \notin X + pC^* \quad \text{and} \quad \psi \notin \langle c_{M_r+1}(n) \rangle^\perp$$

(this is possible since a finite group cannot be the union of two proper subgroups). Using Lemma 5.3, choose

$$c \in H^1(K, E_p)^{-\epsilon_r}$$

satisfying

$$\begin{aligned} c &\neq 0, && (7)\\ c_v &\in \delta(E(K_v)), \quad v \notin S. && (8)\\ c_{v_\lambda} &\in \mathrm{im}(\chi_l) \quad \text{for all} \quad l \in S - \{l_0\}, && (9) \end{aligned}$$

Since c is in a different eigenspace,

$$C \times \langle c_{M_r+1}(n) \rangle \cap \langle c \rangle = \{0\}.$$

So we can choose

$$\phi : C \times \langle c_{M_r+1}(n) \rangle \times \langle c \rangle \to \mathbf{Q}/\mathbf{Z}$$

such that

$$\begin{aligned} \phi|_C &= \psi, && (10)\\ \phi(c_{M_r+1}(n)) &\neq 0, && (11)\\ \phi(c) &\neq 0. && (12) \end{aligned}$$

By Proposition 3.1, there exists $l' \in S_1(M)$ such that

$$\phi = \phi_{\mathrm{Frob}(\lambda'_L)}.$$

Consider

$$\sum_v c_{M_r+1}(nl')_v \cup c_v. \tag{13}$$

If $v \notin S \cup \lambda'$, then $c_{M_r+1}(nl')_v \in \delta(E(K_v))$ by Lemma 4.3 and and $c_v \in \delta(E(K_v))$ by (8), so $c_{M_r+1}(nl')_v \cup c_v = 0$. If $v = v_\lambda \in S - \{\lambda_0\}$, then $c_v \in \mathrm{im}(\chi_l)$ by (9), so again $c_{M_r+1}(nl')_v \cup c_v = 0$. So the only possible nonzero terms in the sum (13) are at $v = \lambda_0, \lambda'$. Suppose $v = \lambda'$. From (11) and (3), $c_{M_r+1}(n)_{\lambda'} \neq 0$, hence by Proposition 4.4 $d_{M_r+1}(nl')_{\lambda'} \in H^1(K_{\lambda'}, E)_p^{-\epsilon_r}$ is not zero. Further, $c_{\lambda'} \in \delta(E(K_{\lambda'}))^{-\epsilon_r}$ by (8), and it is not zero by (12). Hence

$$c_{M_r+1}(nl')_{\lambda'} \cup c_{\lambda'} \neq 0.$$

Since the sum (13) is zero by Proposition 2.2, this implies

$$c_{M_r+1}(nl')_{\lambda_0} \cup c_{\lambda_0} \neq 0.$$

Hence $c_{M_r+1}(nl')_{\lambda_0} \neq 0$, and so by Proposition 4.4, $P_{nl'/l_0} \notin p^{M_r+1}E(K_{\lambda_0})$, hence $p^{M_r} \| P_{nl'/l_0}$. Replacing n by nl'/l_0, we add ψ to X and increase k to $k+1$, and hence eventually to r. But if $k = r$, then $S \subset S(M)$ and $X = C^*$, so $c_M(n)$ is defined and

$$\begin{aligned} \{c \in C : c_\lambda = 0 \quad \text{for all} \quad l \in S\} &= \\ \{c \in C : \phi_{\mathrm{Frob}(\lambda_L)}(c) = 0 \quad \text{for all} \quad l \in S\} &= \{0\}. \end{aligned}$$

Since, by Proposition 4.4, $c_{M_{r-1}}(n)_\lambda = 0$ for all $l \in S$, we deduce

$$C \cap \langle c_{M_{r-1}}(n) \rangle = \{0\}.$$

Also, since $p^{M_r} \| P_n$, $c_M(n)$ has order p^{M-M_r} for any $M > M_r$. So the proposition is proved if $M_{r-1} > M_r$ or if $C = \{0\}$.

So suppose that $M_r = M_{r-1}$. Apply the proposition with $C = \{0\}$ to find $m \in S_{r-1}(M)$ such that $p^{M_r} \| P_m$, then use Proposition 3.1 to find $l \in S(M)$ such that $c_{M_r+1}(m)_\lambda \neq 0$ and set $n = lm$. By Proposition 4.4, $d_{M_r+1}(n)_\lambda \neq 0$, and hence $c_{M_r+1}(n) \notin S_\infty(E/K)$. Since $C \subset S_\infty(E/K)$, this implies that

$$C \cap \langle c_{M_r+1}(n) \rangle = \{0\}.$$

This proves the proposition in this case also. ∎

Using the Cassels pairing and a simple induction argument one can immediately deduce from Proposition 5.2 that Ш(E/K) contains a subgroup isomorphic to

$$(\mathbf{Z}/p^{M_0-M_1}\mathbf{Z})^2 \times (\mathbf{Z}/p^{M_1-M_2}\mathbf{Z})^2 \times \cdots.$$

Further, by using a slightly refined version of Kolyvagin's upper bound on the order of Ш(E/K), or by adding the hypothesis that $p \not| P_n$ for some $n \in S(1)$, one can show that this subgroup is the full group. Thus the N_i are the $M_{i-1} - M_i$ in some order. To prove that $N_i = M_{i-1} - M_i$ requires more work. To give the basic idea, we sketch the case $i = 1$ first.

Applying Proposition 5.2 with $C = \{0\}$, we find $l \in S(M_0)$ such that $c_{M_0}(l)$ has order $p^{M_0-M_1}$ in $S_\infty(E/K)^{-\epsilon} = Ш(E/K)^{-\epsilon}$. From the definition of N_1, we see

$$M_0 - M_1 \leq N_1.$$

Now let $d \in Ш(E/K)^{-\epsilon}$ have order p^{N_1}. Lift d to c in the Selmer group. Using Corollary 3.2, choose a prime l such that

$$\begin{aligned} \operatorname{ord} c_{M_0+N_1}(1)_\lambda &= \operatorname{ord} c_{M_0+N_1}(1), & (14) \\ \operatorname{ord} c_\lambda &= \operatorname{ord} c. & (15) \end{aligned}$$

(These two elements are in different eigenspaces.) Then the Cassels pairing

$$\langle d_{M_0}(l), p^M d\rangle = \langle d_{M_0+N_1-M}(l)_\lambda, y_\lambda\rangle_\lambda,$$

where $c_\lambda = \delta(y_\lambda)$. By (14) and Proposition 4.4, $d_{M_0+N_1-M}(l)_\lambda$ has order p^{N_1-M} in $H^1(K_\lambda, E)^{-\epsilon}_{p^{N_1}}$, which is cyclic of order p^{N_1}, and by (15), y_λ has order p^{N_1} in $E(K_\lambda)/p^{N_1}E(K_\lambda)^{-\epsilon}$, which is also cyclic of order p^{N_1}. Thus the pairing is non-zero for $1 \le M \le N_1 - 1$, and hence $d_{M_0}(l)$ has order at least p^{N_1}. Since the greatest order it can have is $M_0 - M_1$, we deduce

$$N_1 \le M_0 - M_1,$$

and hence

$$N_1 = M_0 - M_1.$$

Now we give the theorem in general. If

$$G = G_1 \times \cdots \times G_r$$

is a product of cyclic groups, we say that a set $\{\chi_1, \ldots, \chi_r\}$ of characters of G is a triangular basis for G^* if

$$\chi_i(G_j) = 0, \quad j > i,$$

and

$$\langle \chi_1, \ldots, \chi_i\rangle = G_1^* \times \cdots \times G_i^*, \quad 1 \le i \le r.$$

THEOREM **5.4** *Let $p > 2$ be such that* $\mathrm{Gal}(\mathbf{Q}(E_p)/\mathbf{Q}) = Gl_2(\mathbf{Z}/p\mathbf{Z})$. *We have $N_i = M_{i-1} - M_i$ for $i \ge 1$.*

Proof. First, observe that by Lemma 5.3, if $l \in S_1(M)$, then two elements

$$y \in E(K_\lambda)/p^M E(K_\lambda), \quad d \in H^1(K_\lambda, E)_{p^M},$$

pair nontrivially if they are in the same $\mathrm{Gal}(K/\mathbf{Q})$-eigenspace and their orders multiply to more than p^M.

By definition of the N_i, there exists a maximal isotropic subgroup

$$D = D_1 \times D_2 \times \cdots$$

of $Ш(E/K)$ such that each D_i is cyclic of order p^{N_i}, $D^{-\epsilon} = D_1 \times D_3 \times \cdots$, and $D^{\epsilon} = D_2 \times D_4 \times \cdots$.

Let d_i be a generator of D_i and let c_i be a lifting of d_i to $S_\infty(E/K)$. For each valuation v of K and each i, choose $y_{i,v} \in E(K_v)$ such that $c_{i,v} = \delta(y_{i,v})$. By Corollary 3.2, we can choose $l_1 \in S_1(M_0 + N_1)$ so that

$$\begin{aligned} \operatorname{ord} c_{M_0+N_1}(1)_{\lambda_1} &= p^{N_1}, && (16)\\ \operatorname{ord} c_{1,\lambda_1} &= p^{N_1}, && (17)\\ c_{i,\lambda_1} &= 0, \quad i \geq 2. && (18) \end{aligned}$$

Let $n_1 = l_1$. By Proposition 4.7, for $0 \leq M \leq N_i - 1$,

$$\langle d_{M_0}(n_1), p^M d_i \rangle = \langle d_{M_0-M}(n_1), d_i \rangle = \langle d_{M_0-M+N_i}(n_1), y_{i,\lambda_1} \rangle_{\lambda_1}.$$

This is zero if $i \geq 2$, by (18). Let $i = 1$. By (17), y_{1,λ_1} has order p^{N_1} in $E(K_{\lambda_1})/p^{N_1}E(K_{\lambda_1})^{-\epsilon}$, and by (16) and Proposition 4.4, $d_{M_0+N_1-M}(n_1)_{\lambda_1}$ has order p^{N_1-M} in $H^1(K_{\lambda_1}, E)^{-\epsilon}$. Hence the pairing is non-trivial for $0 \leq M \leq N_1 - 1$. Thus we have proved that the character

$$d \mapsto \langle d_{M_0}(n_1), d \rangle$$

vanishes on $D_2 \times D_3 \cdots$, and its restriction to D_1 generates D_1^*. Hence $d_{M_0}(n_1)$ has order at least p^{N_1}. Since it has order at most $p^{M_0-M_1}$, we conclude

$$N_1 \leq M_0 - M_1.$$

On the other hand, p^{N_1} is the maximum order an element of $Ш(E/K)^{-\epsilon}$ can have, and by Proposition 5.2, there is an element in $S_\infty(E/K)^{-\epsilon} = Ш(E/K)^{-\epsilon}_{p^\infty}$ of order $p^{M_0-M_1}$, which implies

$$M_0 - M_1 \leq N_1.$$

Hence

$$N_1 = M_0 - M_1.$$

In particular, p^{M_1+1} does not divide P_{n_1}, and hence

$$p^{M_1} \| P_{n_1}.$$

Now suppose we have found primes $\{l_1, l_2, \ldots, l_k\} \in S_1(M)$ such that

$$c_{i,\lambda_j} = 0, \quad i > j, \quad 1 \leq j \leq k, \tag{19}$$

and if

$$n_j = l_1 \cdots l_j,$$

then

$$p^{M_j} \| P_{n_j}, \quad 1 \leq j \leq k, \tag{20}$$

and the characters

$$d \mapsto \langle d_{M_{j-1}}(n_j), d \rangle, \quad 1 \leq j \leq k,$$

vanish on $D_{k+1} \times \cdots$, and form a diagonal basis of $(D_1 \times \cdots \times D_k)^*$. Suppose further that we have shown that $M_{j-1} - M_j = N_j$ for $1 \leq j \leq k$. (We have just done all this for $k = 1$.) In particular, the order of $d_{M_{k-1}}(n_k)$ in $Ш(E/K)$ is the same as its order as a character on D. Since D is isotropic, it follows that

$$\langle d_{M_{k-1}}(n_k) \rangle \cap D = \{0\}.$$

So by Corollary 3.2, we may choose $l_{k+1} \in S_1(M_k + N_{k+1})$ satisfying

$$\begin{aligned} \operatorname{ord} c_{M_k+N_{k+1}}(n_k)_{\lambda_{k+1}} &= p^{N_{k+1}}, & (21) \\ \operatorname{ord} c_{k+1,\lambda_{k+1}} &= p^{N_{k+1}}, & (22) \\ c_{i,\lambda_{k+1}} &= 0, \quad i > k+1. & (23) \end{aligned}$$

Let $n_{k+1} = n_k l_{k+1}$. Then for $0 \leq M \leq N_i - 1$,

$$\begin{aligned} \langle d_{M_k}(n_{k+1}), p^M d_i \rangle &= \\ \langle d_{M_k - M}(n_{k+1}), d_i \rangle &= \sum_{j=1}^{k+1} \langle d_{M_k - M + N_i}(n_{k+1})_{\lambda_j}, y_{i,\lambda_j} \rangle_{\lambda_j}. \end{aligned}$$

All terms but the last are zero for $i > k$ by (19), and the last term is zero for $i > k+1$ by (23). Let $i = k+1$. By (22), $y_{k+1,\lambda_{k+1}}$ has order $p^{N_{k+1}}$ in $E(K_{\lambda_{k+1}})/p^{N_1}E(K_{\lambda_{k+1}})^{\epsilon_{k+1}}$, and by (21) and Proposition 4.4,

$d_{M_k+N_{k+1}-M}(n_{k+1})_{\lambda_{k+1}}$ has order $p^{N_{k+1}-M}$ in $H^1(K_{\lambda_{k+1}}, E)^{\epsilon_{k+1}}$. Hence the pairing is non-trivial for $0 \leq M \leq N_{k+1} - 1$.

Thus the character

$$d \mapsto \langle d_{M_k}(n_{k+1}), d \rangle$$

vanishes on $D_{k+2} \times \cdots$, and its restriction to D_{k+1} generates D_{k+1}^*, and hence extends the triangular basis to generate $(D_1 \times \ldots \times D_{k+1})^*$. Thus $d_{M_k}(n_{k+1})$ has order at least $p^{N_{k+1}}$. Since it has order at most $p^{M_k - M_{k+1}}$, we conclude

$$N_{k+1} \leq M_k - M_{k+1}.$$

Let

$$C = \langle c_{M_0+N_1}(1), c_1, \ldots, c_k, c_{M_0}(n_1), \ldots, c_{M_{k-1}}(n_k) \rangle^{\epsilon_{k+1}}.$$

Then $p^{N_{k+1}}$ is the maximum order an element $c \in S_\infty(E/K)^{\epsilon_{k+1}}$ can have if

$$\langle c \rangle \cap C = \{0\}.$$

On the other hand, by Proposition 5.2 applied to C, there is an element in $S_\infty(E/K)^{\epsilon_{k+1}}$ of order $p^{M_k - M_{k+1}}$ satisfying this condition. Hence

$$M_k - M_{k+1} \leq N_{k+1},$$

and so

$$N_{k+1} = M_k - M_{k+1}.$$

By induction, this proves the theorem. ∎

COROLLARY **5.5** *The numbers M_i satisfy*

$$M_i - M_{i+1} \geq M_{i+2} - M_{i+3}, \quad i \geq 0,$$

and if i_0 is the first positive integer such that $M_{i_0} = M_{i_0+1} = M_{i_0+2}$, then $M_i = M_{i_0}$ for all $i \geq i_0$. We have

$$Ш(E/K)_{p^\infty} \simeq \prod_{i \geq 0} (\mathbf{Z}/p^{M_i - M_{i+1}}\mathbf{Z})^2.$$

COROLLARY **5.6** *Let $m = \min\{M_i : i \geq 0\}$. Then*

$$\operatorname{ord}_p |Ш(E/K)| = 2(M_0 - m).$$

In the course of proving Theorem 5.4, we actually proved the following more precise statement.

PROPOSITION **5.7** *If*

$$D = D_1 \times D_2 \times \cdots$$

is a maximal isotropic subgroup of $Ш(E/K)$ *such that* D_i *is cyclic of order* p^{N_i}, $D^{-\epsilon} = D_1 \times D_3 \times \cdots$, *and* $D^{\epsilon} = D_2 \times D_4 \times \cdots$, *then there exist integers* $n_1 | n_2 | \cdots$ *such that* $n_i \in S_i(M_{i-1})$ *and the characters*

$$d \mapsto \langle d, d_{M_{i-1}}(n_i) \rangle$$

form a triangular basis of characters of D.

In particular, $Ш(E/K)$ can be generated from Kolyvagin's classes constructed from $n \in S_k$ with k less than or equal to half the rank of $Ш(E/K)$. (This fact was independently discovered by H. Darmon.) On the other hand, the following theorem shows that simply to generate $Ш(E/K)$, $k \leq 2$ will suffice.

THEOREM **5.8** *Let* $p > 2$ *be such that* $\mathrm{Gal}(\mathbf{Q}(E_p)/\mathbf{Q}) = Gl_2(\mathbf{Z}/p\mathbf{Z})$. *Let* $M \geq 2M_0$. *Then the classes* $\{d_{M_0}(l) : l \in S_1(M)\}$ *generate* $Ш(E/K)^{-\epsilon}_{p^\infty}$ *and the classes in* $\{d_{M_1}(l_1 l_2) : l_1 l_2 \in S_2(M)\}$ *generate* $Ш(E/K)^{\epsilon}_{p^\infty}$.

Proof. We will show that the dual of $Ш(E/K)$ under the Cassels pairing is generated by these classes, using the same technique as in Theorem 5.4. Since the Cassels pairing is non-degenerate, this will prove the theorem. First suppose that $d \in Ш(E/K)^{-\epsilon}$ has order exactly p^M for some $M > 0$. By Kolyvagin's upper bound [3], $M \leq M_0$. Lift d to $c \in H^1(K, E_{p^M})$. As in the proof of Theorem 5.4, choose l such that

$$\mathrm{ord}\, c_{M_0+M}(1)_\lambda = p^M \tag{24}$$

and

$$\mathrm{ord}\, c_\lambda = p^M, \tag{25}$$

and deduce that the Cassels pairing

$$\langle d_{M_0}(l), p^{M-1} d \rangle \neq 0.$$

Hence the character on $Ш(E/K)$ defined by $\{d_{M_0}(l) : l \in S(M)\}$ generates $\langle d \rangle^*$. In particular, the character group of $Ш(E/K)^{-\epsilon}$ generated by the classes $d_{M_0}(l)$ does not vanish at d. Since d was arbitrary, this proves the first part of the theorem.

Now suppose that $d' \in Ш(E/K)^{\epsilon}$ has order exactly $p^{M'}$. Lift d' to $c' \in H^1(K, E_{p^{M'}})$. By Theorem 5.4 (in fact Proposition 5.2 suffices) there exists $d \in Ш(E/K)^{-\epsilon}$ of order exactly $p^{M_0 - M_1}$. Choose $l_1 \in S_1(M_0)$ satisfying (24) and (25) with respect to such a d and in addition

$$c'_{\lambda_1} = 0. \tag{26}$$

Then $\operatorname{ord} c_{M_0}(l_1) = p^{M_0 - M_1}$, hence $p^{M_1} \| P_{l_1}$. So we may choose l_2 satisfying

$$\operatorname{ord} c_{M_1 + M'}(l_1)_{\lambda_2} = p^{M'}$$

and

$$\operatorname{ord} c'_{\lambda_2} = p^{M'}.$$

Then

$$\langle d_{M_1}(l_1 l_2), d' \rangle = \langle d_{M_1 + M'}(l_1 l_2), y'_{\lambda_1} \rangle_{\lambda_1} + \langle d_{M_1 + M'}(l_1 l_2), y'_{\lambda_2} \rangle_{\lambda_2}.$$

The first term is zero by (26), and the second term is non-zero by the same argument as in the proof of Theorem 5.4. Hence the classes $d_{M_1}(l_1 l_2)$ generate the dual of $Ш(E/K)^{\epsilon}$, which proves the second part of the theorem. ∎

COROLLARY **5.9** *$Ш(E/K)_{p^\infty}$ is divisible in $H^1(K, E)_{p^\infty}$.*

Proof. Since we can choose M arbitrarily large in Theorem 5.8, this follows from Lemma 4.6. ∎

COROLLARY **5.10** *Every element of $Ш(E/K)_{p^\infty}$ splits over a field ramified at at most two primes of K.*

Proof. By Corollary 4.2, $d_M(n)$ splits over K_n. ∎

References

[1] B.H. Gross, *Kolyvagin's work on modular elliptic curves.* This volume.

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

[3] V.A. Kolyvagin, *Euler Systems.* To appear in a Birkhäuser volume in honor of Grothendieck.

[4] 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).

[5] V. A. Kolyvagin. *On the structure of Shafarevich-Tate groups.* To appear in the proceedings of USA-USSR Symposium on Algebraic Geometry, Chicago, 1989, published in the Springer Lecture Notes series.

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

W. G. McCallum
Mathematics Department
University of Arizona
Tucson AZ 85721
USA