The work of Kolyvagin on the arithmetic of elliptic curves

Karl Rubin*
Department of Mathematics, Columbia University
New York, NY 10027 USA

This paper gives a complete proof of a recent theorem of Kolyvagin [3, 4] on Mordell-Weil groups and Tate-Shafarevich groups of elliptic curves. Let E be an elliptic curve defined over $\mathbf{Q}$, and assume that E is modular: for some integer N there is a nonconstant map defined over $\mathbf{Q}$

$$\pi : X_0(N) \rightarrow E$$

which we may assume sends the cusp ∞ to 0. Here $X_0(N)$ is the usual modular curve over $\mathbf{Q}$ (see for example [8]) which over $\mathbf{C}$ is obtained by compactifying the quotient $\mathfrak{H}/\Gamma_0(N)$ of the complex upper half-plane $\mathfrak{H}$ by the group

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbf{Z}) \ : \ c \equiv 0 \ (\text{modulo } N) \right\}.$$

The points of $X_0(N)$ correspond to pairs (A, C) where A is a (generalized) elliptic curve and C is a cyclic subgroup of A of order N. Fix an imaginary quadratic field K in which all primes dividing N split, and an ideal $\mathfrak{n}$ of K such that $\mathcal{O}_K/\mathfrak{n} \cong \mathbf{Z}/N\mathbf{Z}$. Write H for the Hilbert class field of K and x_H for the point in $X_0(N)(\mathbf{C})$ corresponding to the pair

$$(\mathbf{C}/\mathcal{O}_K, \ \mathfrak{n}^{-1}/\mathcal{O}_K).$$

Fix an embedding of $\overline{\mathbf{Q}}$ into $\mathbf{C}$; then the theory of complex multiplication shows that $x_H \in X_0(N)(H)$. Define $y_H = \pi(x_H) \in E(H)$, $y_K = \mathrm{Tr}_{H/K}(y_H) \in E(K)$, and $y = y_K - y_K^{\tau} \in E(K)$, where τ denotes complex conjugation on K.

Let $Ш_{E/\mathbf{Q}}$ denote the Tate-Shafarevich group of E over $\mathbf{Q}$.

Theorem. (Kolyvagin [3, 4]) *Suppose* E *and* y *are as above. If* y *has infinite order in* $E(K)$ *then* $E(\mathbf{Q})$ *and* $Ш_{E/\mathbf{Q}}$ *are finite.*

---

*supported by grants from the NSF, the DFG, the SERC, the Max-Planck-Institut für Mathematik and the Ohio State University

Remarks. 1. The proof of this theorem given below is organized differently from Kolyvagin's proof, and somewhat simplified, but the important ideas are all due to Kolyvagin and contained in [3, 4].

2. It is not difficult to show, using the Hecke operator w_N, that y has infinite order if and only if both y_K has infinite order and the sign in the functional equation of the L-function $L(E, s)$ is $+1$.

3. The proof will give an annihilator of $Ш_{E/Q}$ which, via the theorem of Gross and Zagier [2], gives evidence for the Birch and Swinnerton-Dyer conjecture.

4. Observe that Kolyvagin's theorem makes no mention of the L-function of E. To relate his result to the Birch and Swinnerton-Dyer conjecture one needs the following:

Theorem. (Gross and Zagier [2]) *With* E *and* y *as above,* y *has infinite order in* $E(K)$ *if and only if* $L(E, 1) \neq 0$ *and* $L'(E, \chi_K, 1) \neq 0$, *where* χ_K *is the quadratic character attached to* K.

Analytic Conjecture. *If* E *is a modular elliptic curve and the sign in the functional equation of* $L(E, s)$ *is* $+1$, *then there exists at least one imaginary quadratic field* K, *in which all primes dividing* N *split, such that* $L'(E, \chi_K, 1) \neq 0$.

This analytic conjecture, as yet unproved, together with the theorems of Kolyvagin and Gross and Zagier, would imply:

(*) *For any modular elliptic curve* E, *if* $L(E, 1) \neq 0$ *then* $E(\mathbf{Q})$ *and* $Ш_{E/Q}$ *are finite.*

Assertion (*) is known for elliptic curves with complex multiplication, by theorems of Coates and Wiles [1] (for $E(\mathbf{Q})$) and Rubin [6] (for $Ш_{E/Q}$).

Acknowledgements. I would like to thank John Coates and Bryan Birch for helpful discussions, and the Mathematisches Institut (Erlangen), the Department of Pure Mathematics and Mathematical Statistics (Cambridge) and the Max-Planck-Institut für Mathematik (Bonn) for their hospitality.

Notation. For any abelian group A, A_n will denote the n-torsion in A and $A_{n^\infty} = \bigcup_i A_{n^i}$. If A is a module for the appropriate Galois group, we will write $H^i(L/F, A)$ for $H^i(\mathrm{Gal}(L/F), A)$, $H^i(F, A)$ for $H^i(\bar{F}/F, A)$, and $H^i(F, E)$ for $H^i(F, E(\bar{F}))$.

Tools of the proof.

Fix a prime number p and a positive integer n. For any completion $\mathbf{Q}_v$ of $\mathbf{Q}$ we have the diagram

$$\begin{array}{ccccccccc} 0 & \to & E(\mathbf{Q})/p^nE(\mathbf{Q}) & \to & H^1(\mathbf{Q}, E_{p^n}) & \to & H^1(\mathbf{Q}, E)_{p^n} & \to & 0 \\ & & \downarrow & & \downarrow \text{res}_v & & \downarrow \text{res}_v & & \\ 0 & \to & E(\mathbf{Q}_v)/p^nE(\mathbf{Q}_v) & \to & H^1(\mathbf{Q}_v, E_{p^n}) & \to & H^1(\mathbf{Q}_v, E)_{p^n} & \to & 0 \end{array} \tag{1}$$

and we define the Selmer group $S^{(p^n)}$ and the p^n-torsion in the Tate-Shafarevich group, $Ш_{p^n}$, by

$$S^{(p^n)} = \bigcap_v \text{res}_v^{-1}(\text{image } E(\mathbf{Q}_v)),$$

$$0 \to E(\mathbf{Q})/p^nE(\mathbf{Q}) \to S^{(p^n)} \to Ш_{p^n} \to 0.$$

To prove Kolyvagin's theorem it will suffice to show that $S^{(p)} = 0$ for almost all p, and that for other p the order of $S^{(p^n)}$ is annihilated by a power of p which is independent of n.

For $s \in S^{(p^n)}$ write s_v for the inverse image of $\text{res}_v(s)$ in $E(\mathbf{Q}_v)/p^nE(\mathbf{Q}_v)$. Our main tool for bounding $S^{(p^n)}$ is the following, which is proved using the local Tate pairings.

Proposition 1. *Suppose* ℓ *is a prime such that* $E(\mathbf{Q}_\ell)_{p^n} \cong \mathbf{Z}/p^n\mathbf{Z}$, $k \geq 0$ *is an integer, and* $c_\ell \in H^1(\mathbf{Q}, E)_{p^n}$ *satisfies*

(i) *for all* $v \neq \ell$, $\text{res}_v(c_\ell) = 0$,

(ii) $\text{res}_\ell(c_\ell)$ *has order* p^{n-k}.

Then for every $s \in S^{(p^n)}$, $p^k s_\ell = 0$.

Proof. For any place v of $\mathbf{Q}$ let $\langle\ ,\ \rangle_v$ denote the local Tate pairing

$$\langle\ ,\ \rangle_v : E(\mathbf{Q}_v)/p^nE(\mathbf{Q}_v) \times H^1(\mathbf{Q}_v, E)_{p^n} \to \mathbf{Z}/p^n\mathbf{Z}.$$

For any $s \in S^{(p^n)}$ and $c \in H^1(\mathbf{Q}, E)_{p^n}$, let c' be any lift of c to $H^1(\mathbf{Q}, E_{p^n})$ in (1) and define an element b(s, c) in the Brauer group of $\mathbf{Q}$ by the cup product

$$b(s, c) = s \cup c' \in H^2(\mathbf{Q}, E_{p^n} \otimes E_{p^n}) \cong H^2(\mathbf{Q}, \boldsymbol{\mu}_{p^n}) = \text{Br}(\mathbf{Q})_{p^n}.$$

Here the map $E_{p^n} \otimes E_{p^n} \to \boldsymbol{\mu}_{p^n}$ is given by the Weil pairing. By the definition of the Tate pairing ([5] §I.3, especially remark 3.5) we have

$$\langle s_v, \mathrm{res}_v(c)\rangle_v = \mathrm{inv}_v(b(s, c)).$$

Thus

$$\sum_v \langle s_v, \mathrm{res}_v(c)\rangle_v = \sum_v \mathrm{inv}_v(b(s, c)) = 0.$$

Applying this reciprocity law with a class c_ℓ as in the statement of the proposition we conclude that $\langle s_\ell, \mathrm{res}_\ell(c_\ell)\rangle_\ell = 0$. But

$$E(\mathbf{Q}_\ell)/p^n E(\mathbf{Q}_\ell) \cong E(\mathbf{Q}_\ell)_{p^\infty}/p^n E(\mathbf{Q}_\ell)_{p^\infty} \cong \mathbf{Z}/p^n\mathbf{Z},$$

so if $\mathrm{res}_\ell(c_\ell)$ has order p^{n-k} the nondegeneracy of the Tate pairing shows that $p^k s_\ell = 0$. //

It remains now to construct such a cohomology class c_ℓ for sufficiently many ℓ, with k bounded and usually 0. Kolyvagin constructs such a c_ℓ using Heegner points. Write τ for the complex conjugation on $\overline{\mathbf{Q}}$ induced by our embedding of $\overline{\mathbf{Q}}$ into $\mathbf{C}$, and $[\tau]$ for its conjugacy class in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. If A is a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module with $A_2 = A/2A = 0$, the action of τ gives a decomposition $A = A^+ \oplus A^-$. From now on, for simplicity we will assume that $p \neq 2$, and if $K = \mathbf{Q}(\sqrt{-3})$ we also assume $p \neq 3$. Write D_K for the discriminant of K.

Lemma 2. *Suppose* ℓ *is a prime not dividing* pD_KN, $r > 0$, *and* $\mathrm{Frob}_\ell(K(E_{p^r})/\mathbf{Q}) = [\tau]$. *Then if* $\tilde{E}$ *denotes the reduction of* E *modulo* ℓ *and* $a_\ell = \ell + 1 - \#[\tilde{E}(\mathbf{F}_\ell)]$,

(i) $p^r \mid a_\ell$ *and* $p^r \mid \ell+1$,

(ii) ℓ *remains prime in* K,

(iii) $E(\mathbf{Q}_\ell)_{p^r} \cong \tilde{E}(\mathbf{F}_\ell)_{p^r} \cong \mathbf{Z}/p^r\mathbf{Z}$, $(E(K_\ell)_{p^r})^- \cong (\tilde{E}(\mathbf{F}_{\ell^2})_{p^r})^- \cong \mathbf{Z}/p^r\mathbf{Z}$.

Proof. The characteristic polynomial of Frobenius acting on E_{p^r} is $T^2 - a_\ell T + \ell$, and the characteristic polynomial of τ acting on $E_{p^r} = E(\mathbf{C})_{p^r}$ is $T^2 - 1$. Comparing these polynomials modulo p^r proves (i). The second assertion holds because $\mathrm{Frob}_\ell(K/\mathbf{Q}) \neq 1$, and the third because $E(\mathbf{Q}_\ell)_{p^r} \cong (E_{p^r})^+ \cong E(\mathbf{R})_{p^r}$ and $E(K_\ell)_{p^r} \cong (E_{p^r})^+ \oplus (E_{p^r})^-$. //

Suppose ℓ is a rational prime which remains prime in K and $\ell \nmid N$. Let $\mathcal{O}_\ell$ be the order of conductor ℓ in $\mathcal{O}_K$, and x_ℓ the point in $X_0(N)(\mathbf{C})$ corresponding to the pair

$$(\mathbf{C}/\mathcal{O}_\ell,\ (\mathfrak{n} \cap \mathcal{O}_\ell)^{-1}/\mathcal{O}_\ell).$$

The theory of complex multiplication shows that $x_\ell \in X_0(N)(K[\ell])$ where $K[\ell]$ denotes the ring class field of K modulo ℓ, the abelian extension of K corresponding to the subgroup $K^\times C^\times \prod_q (\mathcal{O}_\ell \otimes \mathbf{Z}_q)^\times$ of the ideles of K. It follows easily that $K[\ell]$ is a cyclic extension of H of degree $(\ell+1)/u_K$ where $u_K = \#(\mathcal{O}_K^\times)/2$, $K[\ell]/H$ is totally ramified at ℓ and unramified everywhere else, and τ acts on $\mathrm{Gal}(K[\ell]/K)$ by -1. Define $y_\ell = \pi(x_\ell) \in E(K[\ell])$. The only facts about Heegner points which we will need (other than their natural fields of definition) are contained in the following proposition.

Proposition 3. i) $u_K \mathrm{Tr}_{K[\ell]/H}(y_\ell) = a_\ell y_H$.
ii) *For any prime* λ *of* $K[\ell]$ *above* ℓ, $\tilde{y}_\ell = \tilde{y}_H^{\mathrm{Frob}} \in \tilde{E}(\mathbf{F}_{\ell^2})$, *where* ~ *denotes reduction modulo* λ.

Proof. Fix an elliptic curve A defined over H, with complex multiplication by $\mathcal{O}_K$, so that $(A, A_{\mathfrak{n}})$ represents x_H. Without loss of generality we may assume that A has good reduction at all primes above ℓ. The point x_ℓ can be represented by $(A', A'_{\mathfrak{n}})$ where $A' = A/C_\ell$ is the quotient of A by a subgroup of order ℓ. Let $\mathcal{C}$ denote the collection of the $\ell+1$ subgroups of A of order ℓ. The Galois group $\mathrm{Gal}(K[\ell]/H)$ acts transitively on $\mathcal{C}/\mathrm{Aut}(E)$, which has order $(p+1)/u_K = [K[\ell]:H]$. Thus, writing T_ℓ for the Hecke correspondence on $X_0(N)$,

$(\ell+1)/u_K$

$$T_\ell(x_H) = \sum_{C \in \mathcal{C}} (A/C, (A/C)_{\mathfrak{n}}) = u_K \sum_{\sigma \in \mathrm{Gal}(K[\ell]/H)} (x_\ell)^\sigma .$$

Projecting to E via π proves the first assertion, since $\pi \circ T_\ell = a_\ell \pi$. For the second, consider the isogeny

$$\varphi : (A, A_{\mathfrak{n}}) \to (A', A'_{\mathfrak{n}})$$

of degree ℓ. Since ℓ remains prime in K, both A and A′ have supersingular reduction at λ, so the reduced isogeny

$$\tilde{\varphi} : (\tilde{A}, \tilde{A}_{\mathfrak{n}}) \to (\tilde{A}', \tilde{A}'_{\mathfrak{n}})$$

must be, up to an automorphism, Frobenius ([9] II.2.12). This proves that $\tilde{x}_p = \tilde{x}_H^{\mathrm{Frob}}$ in $\tilde{X}_0(N)(\mathbf{F}_{\ell^2})$. By the universal property of the Néron model, π reduces to a morphism $\tilde{\pi}$ from $\tilde{X}_0(N)$ to $\tilde{E}$, and applying $\tilde{\pi}$ completes the proof. //

Remark. One can avoid using the universal property of the Néron model by requiring instead that ℓ not belong to a certain finite set of primes. This restriction does not interfere with the proof of Kolyvagin's theorem.

Suppose ℓ is a prime not dividing $pD_K N$, $r > 0$, and $\mathrm{Frob}_\ell(K(E_{p^r})/\mathbf{Q}) = [\tau]$. By Lemma 2, $p^r \mid a_\ell$ and $p^r \mid u_K[K[\ell]:H]$, so there is a (unique) extension H′ of H of degree p^r in $K[\ell]$. Let ϕ denote any lift of any $\mathrm{Frob}_\ell(H/Q)$ to $\mathrm{Gal}(H'/Q)$ and define

$$z_1 = u_K \mathrm{Tr}_{K[\ell]/H}(y_\ell - y_\ell^\phi) - (a_\ell/p^r)(y_H - y_H^\phi) \in E(H').$$

Corollary 4. *Suppose* $\ell \nmid pD_K N$ *and* $\mathrm{Frob}_\ell(K(E_{p^r})/Q) = [\tau]$, *and let* z_1 *be as above.*

(i) $\mathrm{Tr}_{H'/H}(z_1) = 0$.

(ii) *For any* $\sigma \in \mathrm{Gal}(H/K)$, *let* $\bar{\sigma}$ *denote any lift of* σ *to* $\mathrm{Gal}(H'/K)$. *Then modulo any* λ *of* H' *above* ℓ,

$$\sum_{\sigma \in \mathrm{Gal}(H/K)} \widetilde{z_1^{\bar{\sigma}}} = -((\ell+1+a_\ell)/p^r)\tilde{y}.$$

Proof. This follows without difficulty from Proposition 3. //

For each place v of $\mathbf{Q}$ let $m_v = \#[H^1(\mathbf{Q}_v^{unr}/\mathbf{Q}_v, E(\mathbf{Q}_v^{unr}))]$. By [5] Proposition I.3.8, each m_v is finite and all but finitely many are zero, so $m(p) = \sup\{\mathrm{ord}_p(m_v) : \text{all } v \text{ of } \mathbf{Q}\}$ is a well-defined integer, equal to zero for almost all p.

Proposition 5. *Suppose* $\ell \nmid pD_K N$ *and* $\mathrm{Frob}_\ell(K(E_{p^r})/Q) = [\tau]$, *where* $r = n + m(p)$. *Then there is an element* $c_\ell \in H^1(\mathbf{Q}, E)_{p^n}$ *such that*

i) $\mathrm{res}_v(c_\ell) = 0$ *for all* $v \neq \ell$,

ii) *the order of* $\mathrm{res}_\ell(c_\ell)$ *in* $H^1(\mathbf{Q}_\ell, E)_{p^n}$ *is equal to the order of* y *in* $E(K_\ell)/p^n E(K_\ell)$.

Proof. First suppose $p \nmid [H:K]$. Then there is a (unique) extension K' of K of degree p^r in $K[\ell]$, totally ramified at ℓ and unramified at all other primes, and $H' = HK'$. Define

$$z = \mathrm{Tr}_{H'/K}(z_1) \in E(K').$$

By Corollary 4, $\mathrm{Tr}_{K'/K}(z) = 0$. Fixing a generator σ of $\mathrm{Gal}(K'/K)$ gives rise to a group isomorphism (which is *not* τ-equivariant, see below)

$$\{\alpha \in E(K') : \mathrm{Tr}_{K'/K}(\alpha) = 0\}/(\sigma-1)E(K') \cong H^1(K'/K, E(K')).$$

Define

$$c'_\ell \in H^1(K'/K, E(K')) \subset H^1(K, E)_{p^r}$$

to be the image of z under this isomorphism.

Since τ commutes with $\mathrm{Tr}_{K[\ell]/K'}$, $z^\tau = -z$. Since τ also acts by -1 on $\mathrm{Gal}(K'/K)$, we conclude that $c_\ell'^\tau = c'_\ell$. Thus $c'_\ell \in (H^1(K, E)_{p^r})^+$. But for $p > 2$ the restriction map gives an isomorphism $H^1(Q, E)_{p^r} \cong (H^1(K, E)_{p^r})^+$, so $c'_\ell \in H^1(Q, E)_{p^r}$. Finally, define $c_\ell = p^{m(p)} c'_\ell \in H^1(Q, E)_{p^n}$.

For $v \neq \ell$, since K'/K is unramified at v,

$$\mathrm{res}_v(c_\ell) = p^{m(p)}\mathrm{res}_v(c'_\ell) \in p^{m(p)} H^1(Q_v^{unr}/Q_v, E(Q_v^{unr}))_{p^r} = 0$$

by definition of $m(p)$.

To complete the proof of the proposition we must determine the order of $\mathrm{res}_\ell(c_\ell)$ in $H^1(Q_\ell, E)_{p^n}$. Write I_ℓ for the inertia subgroup of $\mathrm{Gal}(\overline{Q}_\ell/Q_\ell)$, and consider the maps

$$H^1(Q_\ell, E)_{p^n} \to H^1(I_\ell, E(\overline{Q}_\ell))_{p^n} \to H^1(I_\ell, \tilde{E}(\overline{F}_\ell))_{p^n} \to \mathrm{Hom}(\mathrm{Gal}(K'/K), \tilde{E}_{p^n}).$$

The first map is injective because its kernel, $H^1(Q_\ell^{unr}/Q_\ell, E(Q_\ell^{unr}))_{p^n}$, is 0 since E has good reduction at ℓ. The second map is an isomorphism because the kernel of reduction modulo ℓ is a pro-ℓ group. The third map is an isomorphism because I_ℓ acts trivially on $\tilde{E}(\overline{F}_\ell)$ and $K'Q_\ell^{unr}$ is the unique abelian extension of Q_ℓ^{unr} of exponent p^r. It is easy to see that the image of c_ℓ under this sequence of injections is the homomorphism which sends the chosen generator σ of $\mathrm{Gal}(K'/K)$ to $p^{m(p)}\tilde{z}$. Thus the order of $\mathrm{res}_\ell(c_\ell)$ in $H^1(Q_\ell, E)_{p^n}$ is the same as the order of $p^{m(p)}\tilde{z}$ in $\tilde{E}(F_{\ell^2})$.

Corollary 4 shows that

$$p^{m(p)}\tilde{z} = -((\ell+1+a_\ell)/p^n)\tilde{y}.$$

Up to a factor of 2, $\#[\tilde{E}(F_{\ell^2})^-] = \#[\tilde{E}(F_{\ell^2})]/\#[\tilde{E}(F_\ell)] = \ell+1+a_\ell$. By Lemma 2, $(\tilde{E}(F_{\ell^2})_{p^\infty})^-$ is cyclic, so we conclude that $(\ell+1+a_\ell)/p^n$ maps $\tilde{E}(F_{\ell^2})^-/p^n\tilde{E}(F_{\ell^2})^-$ isomorphically to $(\tilde{E}(F_{\ell^2})_{p^n})^-$. Therefore the order of $p^{m(p)}\tilde{z}$ in $\tilde{E}(F_{\ell^2})$ is the same as the order of y in $E(K_\ell)/p^nE(K_\ell) \cong \tilde{E}(F_{\ell^2})/p^n\tilde{E}(F_{\ell^2})$. This completes the proof when $p \nmid [H:K]$.

If $p \mid [H:K]$, there may not exist a field K' as above. In that case, use the point z_1 to define $c'_{1,\ell} \in H^1(H, E)_{p^r}$. Then define c'_ℓ to be the corestriction of $c'_{1,\ell}$ to $H^1(K, E)$ and proceed as above. //

Corollary 6. *Suppose* $\ell \nmid pD_KN$, *and* $\mathrm{Frob}_\ell(K(E_{p^{n+m(p)}})/Q) = [\tau]$. *If* $k \geq 0$ *and* $p^{n-k-1}y \notin p^nE(K_\ell)$, *then for all* $s \in S^{(p^n)}$, $p^k s_\ell = 0$.

Proof. This follows immediately from Propositions 1 and 4. //

For any $t \in H^1(K, E_{p^n})$, write $\hat{t}$ for the image of t under the restriction map

(2) $$H^1(K, E_{p^n}) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K(E_{p^{n+m(p)}})), E_{p^n})^{\mathrm{Gal}(K(E_{p^{n+m(p)}})/K)}.$$

Lemma 7. *Suppose* $t \in H^1(K, E_{p^n})^{\pm}$ *and the image of* $\hat{t}$ *is cyclic. Then the order of* t *is at most* p^{a+b}, *where* p^a *is the order of the largest* **Q**-*rational cyclic subgroup of* E_{p^∞} *and* p^b *is the exponent of* $H^1(K(E_{p^{n+m(p)}})/K, E_{p^n})$.

Proof. Since $\hat{t}$ is $Gal(K(E_{p^{n+m(p)}})/K)$-equivariant, its image is $Gal(\overline{K}/K)$-invariant. Since τ acts on $\hat{t}$ by ± 1, the image is in fact rational over **Q**. Thus if the image is cyclic, the order of $\hat{t}$ is at most p^a. The kernel of the restriction map (2) is $H^1(K(E_{p^{n+m(p)}})/K, E_{p^n})$, so t has order at most p^{a+b}. //

Proof of Kolyvagin's theorem.

As above, we fix a prime p not dividing $\#[\mathcal{O}_K^\times]$. Suppose y has infinite order in $E(K)$, and let $k = k(p)$ be the largest integer such that $y \in p^k E(K) + E(K)_{tors}$. Fix any integer $n \geq k+1$. First assume that

(3) $$E \text{ has no } p\text{-isogeny defined over } \mathbf{Q},$$

(4) $$H^1(K(E_{p^{n+m(p)}})/K, E_{p^n}) = 0,$$

both of which hold for all but a finite number of p by Serre's theorem [7] or the theory of complex multiplication. Under these assumptions we will show that $p^k S^{(p^n)} = 0$.

Write $r = n + m(p)$. Fix $s \in S^{(p^n)}$, and as in Lemma 7 write $\hat{s}$ for the restriction of s to $Gal(\overline{\mathbf{Q}}/K(E_{p^r}))$ and write $\hat{y}$ for the restriction of the image of y under the injection

$$E(K)^-/p^n E(K)^- \to H^1(K, E_{p^n})^-.$$

Fix a finite extension F of $K(E_{p^r})$, Galois over **Q**, so that both $\hat{s}$ and $\hat{y}$ factor through $G = Gal(F/K(E_{p^r}))$.

Choose any $\gamma \in G$, and choose any prime ℓ, not dividing $pD_K N$, such that $Frob_\ell(F/\mathbf{Q}) = [\gamma\tau]$. Then $Frob_\ell(K(E_{p^r})/\mathbf{Q}) = [\tau]$, and $Frob_\ell(F/K(E_{p^r})) \in [(\gamma\tau)^2]$ so

$$p^k s_\ell = 0 \Leftrightarrow p^k \hat{s}((\gamma\tau)^2) = 0, \text{ and } p^{n-k-1} y \in p^n E(K_\ell) \Leftrightarrow p^{n-k-1} \hat{y}((\gamma\tau)^2) = 0.$$

Since $\hat{s}^\tau = \hat{s}$, and $\hat{y}^\tau = -\hat{y}$,

$$\hat{s}((\gamma\tau)^2) = \hat{s}(\gamma) + \hat{s}(\tau\gamma\tau) = (1+\tau)\hat{s}(\gamma)$$

$$\hat{y}((\gamma\tau)^2) = \hat{y}(\gamma) + \hat{y}(\tau\gamma\tau) = (1-\tau)\hat{y}(\gamma)$$

By Corollary 6, we conclude that for every $\gamma \in G$, either $p^k \hat{s}(\gamma) \in (E_{p^n})^-$ or

$p^{n-k-1}\hat{y}(\gamma) \in (E_{p^n})^+$. Therefore $G = (p^k\hat{s})^{-1}((E_{p^n})^-) \cup (p^{n-k-1}\hat{y})^{-1}((E_{p^n})^+)$. But a group cannot be the union of two proper subgroups, so either $p^k\hat{s}(G) \subset (E_{p^n})^-$ or $p^{n-k-1}\hat{y}(G) \subset (E_{p^n})^+$. By Lemma 7 (using assumptions (3) and (4)) we conclude that either $p^k s = 0$ in $S^{(p^n)}$ or $p^{n-k-1}y = 0$ in $E(K)/p^nE(K)$. Since the latter is impossible by our definition of k, we have shown that $p^kS^{(p^n)} = 0$.

Since $k = 0$ for almost all p, this proves Kolyvagin's theorem except for the finite number of p-parts which we have ruled out above. Without assumptions (3) and (4), using Lemma 7 the proof above gives a somewhat weaker annihilator of $S^{(p^n)}$, but still one which is independent of n (again using [7] or the theory of complex multiplication to show that the exponent of $H^1(K(E_{p^{n+m(p)}})/K, E_{p^n})$ is bounded independent of n). Also, with a little more care, one obtains a suitable annihilator when $p \mid \#[\mathcal{O}_K^\times]$. This completes the proof. //

References.

1. Coates. J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* **39**, 223-251 (1977)

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

3. Kolyvagin, V.A.: Finiteness of E(**Q**) and Ш(E, **Q**) for a class of Weil curves. (Russian) To appear in *Izv. Akad. Nauk SSSR Ser. Mat.*

4. Kolyvagin, V.A.: On Mordell-Weil and Shafarevich-Tate groups of elliptic Weil curves. (Russian) preprint

5. Milne, J.S.: Arithmetic duality theorems. *Persp. in Math.* **1**, Orlando: Academic Press (1986)

6. Rubin, K.: Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. *Invent. Math.* **89**, 527-560 (1987)

7. Serre. J-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inv. Math.* **15**, 259-331 (1972)

8. Shimura, G.: Introduction to the arithmetic theory of automorphic forms. *Pub. Math. Soc. Japan* **11**, Princeton: Princeton University Press (1971)

9. Silverman, J.: The arithmetic of elliptic curves. *Grad. Texts in Math.* **106**, New York: Springer (1986)