There are genus one curves over $\mathbf{Q}$ of every odd index

William A. Stein*
email: was@math.harvard.edu

April 21, 2003

Abstract

The index of a genus one curve X over a field K is the smallest degree of an extension L of K such that $X(L)$ is nonempty. Let K be a number field. We prove that for every integer r not divisible by 8, there is a genus one curve X over K of index r. Our proof involves an analysis of Kolyvagin's Euler system of Heegner points combined with explicit computations on the modular curve $X_0(17)$.

1 Introduction

How complicated are curves of genus one? One possible measure of the complexity of a curve is the smallest degree of an extension of the base field in which the curve has a point. Consider a curve X of positive genus g over a number field K. The canonical divisor class on X contains a K-rational effective divisor of degree $2g-2$, so the greatest common divisor of the degrees of the extension fields in which X has a rational point divides $2g-2$. When $g=1$ this is no condition at all!

In the 1950s, S. Lang and J. Tate asked in [11] whether, given a positive integer r, there exists a genus one curve X such that r is the smallest of all degrees of extensions of K over which X has a point. Using Kolyvagin's Euler system of Heegner points, we answer their question in the affirmative, under the hypothesis that r is odd. The curves we produce are torsors for the elliptic curve $X_0(17)$, though our methods apply to a more general class of genus one curves. The following theorem is proved in Section 5.4.

Theorem 1.1. *Let K be a number field and let r be an integer not divisible by* 8*. Then there are infinitely many genus one curves over K of index r.*

In Section 2 we recall standard facts about indexes of genus one curves. Section 3 contains a brief discussion of Heegner points, and summarizes the relevant results about Kolyvagin's Euler system from [18]. In Section 4, which forms the heart of our paper, we prove a nonvanishing result for Kolyvagin's cohomology classes. Finally, in Section 5, we prove Theorem 1.1 by combining a general result about Galois representations with explicit computations on $X_0(17)$.

Acknowledgement: The author would like to thank H. Lenstra for introducing him to this problem, K. Buzzard for teaching him about Kolyvagin's Euler system, K. Rubin and M. Flach for extensive comments, D. Y. Logachev, C. O'Neil, and K. Ribet for inspiring conversations, and N. Elkies and G. Grigorov for useful comments.

*Supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship.

2 Indexes of genus one curves

Let E be an elliptic curve over an arbitrary field k. The Galois cohomology group $H^1(k,E) = H^1(\mathrm{Gal}(k^{\mathrm{sep}}/k), E(k^{\mathrm{sep}}))$ classifies the isomorphism classes of torsors (principal homogeneous spaces) for E over k.

Definition 2.1 (Index of cohomology class). The *index* of $c \in H^1(k,E)$, denoted $\mathrm{ind}(c)$, is the greatest common divisor of the degrees of the separable extensions K of k for which $\mathrm{res}_K(c) = 0$.

The torsor X corresponding to c is a genus one curve over k equipped with an action of E. Furthermore, $X(K) \neq \emptyset$ exactly when $\mathrm{res}_K(c) = 0$, so

$$\mathrm{ind}(c) = \gcd\{[K : k] : X(K) \neq \emptyset\}.$$

Thus $\mathrm{ind}(c)$ generates the image of the degree map $\deg : \mathrm{Div}_k(X) \to \mathbf{Z}$. We now define $\mathrm{ind}(X)$ so that $\mathrm{ind}(X) = \mathrm{ind}(c)$.

Definition 2.2 (Index of curve). The *index* of an algebraic curve over k is the cardinality of the cokernel of the degree map.

Any canonical divisor is an element of $\mathrm{Div}_k(X)$ of degree $2g-2$, where g is the genus of X, so $\mathrm{ind}(X)$ divides $2g-2$. As mentioned in the introduction, when $g = 1$ this is no condition; in fact, E. Artin conjectured, and Lang and Tate proved in [11, pg. 670], that for every integer r there is some genus one curve X over some field L such that $\mathrm{ind}(X) = r$. The construction of [11] requires the existence of an L-rational point of order r on the elliptic curve $E = \mathrm{Jac}(X)$. The torsion subgroups of elliptic curves are "uniformly bounded", so for K a fixed number field and for almost all r, the results of [11] do not imply the existence of genus one curves over K of index r.

Let E be an elliptic curve over a number field K, and let r be a positive integer. Is there an element of $H^1(K,E)$ of index r? In [21], Shafarevich proved that $H^1(K,E)$ contains infinitely many elements of every *order* (see also [5, §27] where Cassels sketches an alternative approach to proving Shafarevich's theorem). However, this does not answer the question of Artin, because the order need not equal the index as Cassels remarked in [4], where he found an elliptic curve E and a class $c \in H^1(\mathbf{Q},E)$ such that c has order 2 and index 4.

2.1 Elementary facts about the index

We pause to state some basic facts about the order and index, which we will use later. Fix an elliptic curve E over a number field K, and let c and c' be elements of $H^1(K,E)$.

Proposition 2.3. $\mathrm{ord}(c) \mid \mathrm{ind}(c)$*, and they have the same prime factors.*

Proof. See [11, §2, Prop. 5]. □

Lemma 2.4. *There is an extension L of K such that $[L : K] = \mathrm{ind}(c)$ and $\mathrm{res}_L(c) = 0$.*

Proof. See the paragraph before the corollary in [11, §2]. □

Proposition 2.5. *Suppose c' has order coprime to c. Then* $\mathrm{ind}(c+c') = \mathrm{ind}(c)\cdot\mathrm{ind}(c')$.

Proof. If M is a field that splits $c+c'$, then M also splits $\mathrm{ord}(c')(c+c') = \mathrm{ord}(c')c$, so M splits c. Likewise, M splits c', so $\mathrm{ind}(c)\cdot\mathrm{ind}(c') \mid \mathrm{ind}(c+c')$. For the other divisibility, note that by Lemma 2.4, there are extensions L and L' such that $[L : K] = \mathrm{ind}(c)$, $[L' : K] = \mathrm{ind}(c')$, and $\mathrm{res}_L(c) = \mathrm{res}_{L'}(c') = 0$. Then the compositum $L.L'$ splits $c + c'$ and $[L.L' : K] = \mathrm{ind}(c)\cdot\mathrm{ind}(c')$. Thus $\mathrm{ind}(c+c')$ divides $\mathrm{ind}(c)\cdot\mathrm{ind}(c')$. □

Remark 2.6. In [12], Lichtenbaum proved that $\mathrm{ind}(c) \mid \mathrm{ord}(c)^2$ for any $c \in H^1(K, E)$, and Cassels proved in [3] that if $c \in Ш(E/K)$, then $\mathrm{ord}(c) = \mathrm{ind}(c)$.

If E is an elliptic curve over $\mathbf{Q}$ such that $\#Ш(E/\mathbf{Q}) = \#E(\mathbf{Q})_{\mathrm{tor}} = 1$, then the results mentioned above do not rule out the possibility that every element of $H^1(\mathbf{Q}, E)$ has index a perfect square. We prove, under the assumption that $L(E, 1) \neq 0$, that there is an integer B such that $H^1(\mathbf{Q}, E)$ contains infinitely many elements of index n, for every integer n that is prime to B (see Theorem 3.1). For example, in Section 5 we prove that one can take $B = 2$ for the elliptic curve $X_0(17)$.

3 Kolyvagin's Euler system

In this section, we recall the definition of Heegner points and several basic results about the system of cohomology classes Kolyvagin attaches to these points. We also state the main theorem of this paper.

3.1 Kolyvagin classes

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N, and denote by $X_0(N)$ the modular curve that classifies cyclic isogenies of degree N. By [1], there is a surjective map $\pi : X_0(N) \to E$. (Note that for the proof of Theorem 1.1 we do not need any modularity theorems, because we take $E = X_0(17)$.) Let K be a quadratic imaginary extension of $\mathbf{Q}$ in which all primes dividing N split, and let D_K be the discriminant and $\mathcal{O}$ the ring of integers of K. Since all primes dividing N split, there is an ideal $\mathfrak{a} \subset \mathcal{O}$ such that $\mathcal{O}/\mathfrak{a}$ is cyclic of order N. Let H be the Hilbert class field of K, and $x_H \in X_0(N)(H)$ be the Heegner points corresponding to $(\mathbf{C}/\mathcal{O}, \mathfrak{a}^{-1}/\mathcal{O})$. Set $y_H = \pi(x_H) \in E(H)$, $y_K = \mathrm{tr}_{H/K}(y_H) \in E(K)$, and $y = y_K - y_K^\tau \in E(K)^-$, where τ denotes complex conjugation. Assume that $L(E, 1) \neq 0$, so by [2, 15] there are infinitely many ways in which to choose K as above so that y has infinite order. Under this nonvanishing hypothesis on $L(E, 1)$, Kolyvagin proves in [10] that the groups $E(\mathbf{Q})$ and $Ш(E/\mathbf{Q})$ are both finite.

In the course of his proof, Kolyvagin considers more general Heegner points $y_\ell \in E(\overline{\mathbf{Q}})$, for appropriate primes ℓ, and from these constructs cohomology classes $c_{\ell,p^n} \in H^1(\mathbf{Q}, E)[p^n]$ that are used to bound the orders of certain Selmer groups associated to E. We will study Kolyvagin's classes further and prove that for each prime p not in an explicit finite set and each positive integer n, there are infinitely many primes ℓ such that

$$\mathrm{ord}(c_{\ell,p^n}) = \mathrm{ind}(c_{\ell,p^n}) = p^n.$$

We thus obtain the following theorem, which will be proved in Section 4.2.

Theorem 3.1. *Let E be an elliptic curve over $\mathbf{Q}$ such that $L(E, 1) \neq 0$. Then there is an integer B such that, for all integers r coprime to B, there are infinitely many $c \in H^1(\mathbf{Q}, E)$ such that* $\mathrm{ord}(c) = \mathrm{ind}(c) = r$.

Remark 3.2. Cathy O'Neil [16] has investigated the obstruction to $\mathrm{ord}(c) = \mathrm{ind}(c)$. We show that when E has analytic rank 0, this obstruction vanishes for infinitely many c.

3.2 Basic properties of Kolyvagin's Euler system

In [18], Rubin gives a concise account of Kolyvagin's proof of finiteness of $Ш(E/\mathbf{Q})[p^\infty]$, under the simplifying assumption that p is odd. Though Kolyvagin's argument works even when $p = 2$, for simplicity, we rely exclusively on Rubin's paper.

Let K be a quadratic imaginary field as above, chosen in such a way that the associated Heegner point y_K has infinite order. Fix embeddings of $\overline{\mathbf{Q}}$ into $\mathbf{C}$ and into each p-adic field $\overline{\mathbf{Q}}_p$. Let τ denote complex conjugation, and for any $\mathbf{Z}[\tau]$-module A, let A^+ and A^- denote the kernel of $\tau - 1$ and $\tau + 1$, respectively. For the remainder of this section, we assume that p is an odd prime, and if $K = \mathbf{Q}(\sqrt{-3})$ that $p \geq 5$. If ℓ is a prime that is inert in K, let K_ℓ denote the completion of K at the unique prime lying over ℓ. If L is a finite Galois extension of $\mathbf{Q}$, let $\mathrm{Frob}_\ell(L/\mathbf{Q})$ denote the conjugacy class of some Frobenius element of a prime lying over ℓ. For each prime $\ell \nmid N$, let $a_\ell = \ell + 1 - \#E(\mathbf{F}_\ell)$ be the ℓth Fourier coefficient of the newform attached to E.

Definition 3.3. For each place v of $\mathbf{Q}$, let

$$m_v = \#H^1(\mathbf{Q}_v^{\mathrm{unr}}/\mathbf{Q}_v, E(\mathbf{Q}_v^{\mathrm{unr}})).$$

By [14, I.3.8], each m_v is finite and $m_v = 1$ for all but finitely many v, so

$$m(p) = \sup\{\mathrm{ord}_p(m_v) : \text{all places } v \text{ of } \mathbf{Q}\}$$

is well defined, and $m(p) = 0$ for almost all p.

Let n be a positive integer.

Proposition 3.4. *Let p be a prime that does not divide the class number of K and for which $m(p) = 0$. Suppose $\ell \nmid pD_KN$ and $\mathrm{Frob}_\ell(K(E[p^n])/\mathbf{Q}) = [\tau]$. Then there is an element $c_{\ell,p^n} \in H^1(\mathbf{Q}, E)[p^n]$ such that the order of $\mathrm{res}_\ell(c_{\ell,p^n})$ in $H^1(\mathbf{Q}_\ell, E)[p^n]$ is equal to the order of the image of y in $E(K_\ell)/p^nE(K_\ell)$, and the index of c_{ℓ,p^n} divides p^n.*

Proof. The existence of c_{ℓ,p^n} and statement about its order is proved in [18, Prop. 5], where c_{ℓ,p^n} is constructed from Heegner points on $X_0(N)$. For the index bound, note that in the proof of [18, Prop. 5], when $p \nmid [H : K]$, Rubin constructs a class $c' \in H^1(K'/K, E(K'))[p^r]^+$, where $r = n + m(p)$ and K' is the unique extension of K of degree p^r in a certain class field of K. Since p is odd, the restriction map $\mathrm{res} : H^1(\mathbf{Q}, E)[p^r] \to H^1(K, E)[p^r]^+$ is an isomorphism. Rubin takes $c_{\ell,p^n} = \mathrm{res}^{-1}(c')$. Since c_{ℓ,p^n} splits over the degree $2p^r$ extension K' of $\mathbf{Q}$, the index of c_{ℓ,p^n} divides $2p^r$. But c_{ℓ,p^n} has odd order and, by Proposition 2.3, $\mathrm{ind}(c_{\ell,p^n})$ has the same prime factors as $\mathrm{ord}(c_{\ell,p^n})$, so $\mathrm{ind}(c_{\ell,p^n})$ divides p^r. □

Remark 3.5. The author does not know whether or not the proposition is true if p is allowed to divide the class number of K.

4 Nonvanishing of cohomology classes

In this section, we prove a nonvanishing result about the cohomology classes c_{ℓ,p^n} of Proposition 3.4, then use it to deduce Theorem 3.1.

4.1 Local nonvanishing

Let E be as above. For any point $x \in E(K)$, let $K([p^n]^{-1}x)$ denote the field obtained by adjoining the coordinates of all p^nth roots of x to K. Without imposing further hypothesis, this field need not be Galois over $\mathbf{Q}$.

Lemma 4.1. *If $x \in E(K)^+ \cup E(K)^-$, then $K([p^n]^{-1}x)$ is Galois over $\mathbf{Q}$.*

Proof. Since $G_{\mathbf{Q}}$ acts on x by ± 1, the subgroup $\mathbf{Z}x$ is $G_{\mathbf{Q}}$-invariant. Since $[p^n] \colon E \to E$ is a $\mathbf{Q}$-rational isogeny the inverse image $[p^n]^{-1}\mathbf{Z}x$ is also $G_{\mathbf{Q}}$-invariant, so $K([p^n]^{-1}x) = K([p^n]^{-1}\mathbf{Z}x)$ is Galois over $\mathbf{Q}$. □

Definition 4.2. An odd prime p is *firm* for E if $m(p) = 0$, there are no nontrivial $\mathbf{Q}$-rational cyclic subgroups of $E[p^\infty]$, and $H^1(K(E[p^n])/K, E[p^n]) = 0$ for all $n \geq 1$.

Remark 4.3. The set of primes that are not firm is finite, by Serre's theorem [19] and the theory of complex multiplication.

Let p be an odd prime that is firm for E. The following proposition produces infinitely many primes ℓ such that we have control over the orders of the image in $E(K_\ell)/p^n E(K_\ell)$ of a global point. It will be used as input to Proposition 3.4 to produce cohomology classes of known index. The proof, which involves an application of the Chebotarëv density theorem, follows a strategy similar to that used in the proof of Kolyvagin's theorem on page 135 of [18].

Proposition 4.4. *Let p be a prime that is firm for E, and let $x \in E(K)^\pm$. Then there is a set of primes ℓ of positive Dirichlet density such that $\mathrm{Frob}_\ell(K(E[p^n])/\mathbf{Q}) = [\tau]$ and the orders of the images of x in $E(K)/p^n E(K)$ and in $E(K_\ell)/p^n E(K_\ell)$ are the same.*

Proof. Let p^a be the order of the image of x in $E(K)/p^n E(K)$. If $a = 0$, then there is nothing to prove, so assume that $a > 0$. If ℓ is a prime such that the orders of the images of $p^{a-1}x$ in $E(K)/p^n E(K)$ and $E(K_\ell)/p^n E(K_\ell)$ both equal p, then the images of x in $E(K)/p^n E(K)$ and $E(K_\ell)/p^n E(K_\ell)$ both have order p^a. It thus suffices to prove the proposition in the case when the order of the image of x in $E(K)/p^n E(K)$ is p.

Let $L = K(E[p^n])$, suppose ℓ is a prime such that $\mathrm{Frob}_\ell(L/\mathbf{Q}) = [\tau]$, and let λ be one of the prime ideals of L that lies over ℓ. We have a diagram

$$\begin{tikzcd}
E(K)/p^n E(K) \arrow[r, hook] \arrow[d] & H^1(K, E[p^n]) \arrow[r, hook] \arrow[d] & \mathrm{Hom}(G_L, E[p^n]) \arrow[d] \\
E(K_\ell)/p^n E(K_\ell) \arrow[r] & H^1(K_\ell, E[p^n]) \arrow[r] & \mathrm{Hom}(G_{L_\lambda}, E[p^n]),
\end{tikzcd}$$

Let $\varphi : G_L \to E[p^n]$ be the element of $\mathrm{Hom}(G_L, E[p^n])$ that x maps to. The top row is injective, because p is firm, so it suffices to show that the image φ_ℓ of φ in $\mathrm{Hom}(G_{L_\lambda}, E[p^n])$ is nonzero.

Let M be the fixed field of the kernel of φ. Since M is the compositum of the two Galois extensions $K([p^n]^{-1}x)$ and $\mathbf{Q}(E[p^n])$ of $\mathbf{Q}$, it is also Galois (see Lemma 4.1). Because $\mathrm{Frob}_\ell(M/\mathbf{Q})|_L = [\tau]$, there is an element $\sigma \in \mathrm{Gal}(M/L)$ such that $\mathrm{Frob}_\ell(M/\mathbf{Q}) = [\sigma\tau]$. The order of $\sigma\tau$ equals the degree of $M_{\lambda'}$ over $\mathbf{Q}_\ell$, where λ' is a prime of M lying over ℓ. If $\varphi_\ell = 0$, then $M_{\lambda'} = L_\lambda = K_\ell$, so $\sigma\tau$ would have order 2.

The image of φ is a nonzero subgroup H of $E[p^n]$, which is defined over $\mathbf{Q}$ since $x \in E(K)^\pm$. If every $\sigma \in \mathrm{Gal}(M/L)$ has the property that $\sigma\tau$ has order 2, then $H \subset E[p^n]^-$. This contradicts our assumption that p is firm, since H is a nontrivial cyclic subgroup of $E[p^\infty]$. Thus there exists $\sigma \in \mathrm{Gal}(M/L)$ such that $\sigma\tau$ has order different than 2. For this σ and for any prime ℓ such that $\mathrm{Frob}_\ell(M/\mathbf{Q}) = [\sigma\tau]$, we see that $\varphi_\ell \neq 0$. The Chebotarëv density theorem provides a positive density of such ℓ. $\square$

4.2 Proof of Theorem 3.1

Proof of Theorem 3.1. Let E be an elliptic curve over $\mathbf{Q}$ such that $L(E,1) \neq 0$. Let K be one of the infinitely many imaginary quadratic fields such that the associated Heegner point y has infinite order. Let B_K be an integer that is divisible by 2 and

— the primes p such that $y \in pE(K)$,
— the primes p that are not firm,
— the order $\#E(K)_{\mathrm{tor}}$, and
— the class number of K.

If $K = \mathbf{Q}(\sqrt{-3})$, assume in addition that 3 divides B_K.

Fix a prime $p \nmid B_K$. Since $E(K)$ has rank 1 (see, e.g., [9, Thm 1.3]) and $p \nmid \#E(K)_{\mathrm{tor}}$, the image of y in $E(K)/p^n E(K)$ has order p^n. By Proposition 4.4 there are infinitely many primes ℓ such that $\mathrm{Frob}_\ell(K(E[p^n])/\mathbf{Q}) = [\tau]$ and the image of y in $E(K_\ell)/p^n E(K_\ell)$ has order p^n. For these ℓ, Proposition 4.4 produces infinitely many cohomology classes c_{ℓ,p^n} having order and index both equal to p^n. (Note that if $\ell \neq \ell'$ then $c_{\ell,p^n} \neq c_{\ell',p^n}$.)

Let B be the greatest common divisor of the set of integers B_K, as K varies over all quadratic imaginary extensions such that the associated Heegner point has infinite order. For each prime power p^n that does not divide B, we have produced infinitely many $c \in H^1(\mathbf{Q}, E)$ having order and index both equal to p^n. If the orders of c and c' are coprime, then $\mathrm{ord}(c + c') = \mathrm{ord}(c) \cdot \mathrm{ord}(c')$ and, by Proposition 2.5, $\mathrm{ind}(c + c') = \mathrm{ind}(c) \cdot \mathrm{ind}(c')$. This proves the theorem. $\square$

5 Computing the bound B_K

In this section we compute, in some cases, the the bound B_K that appears in Section 4.2. First we prove a general theorem about semistable elliptic curves. Next we compute the index of a Heegner point, and finally in Section 5.4 we prove Theorem 1.1.

5.1 Galois representations attached to isolated curves

The following proposition sometimes permits us to compute the integer B_K, which appears in Section 4.2.

Proposition 5.1. *Let E be a semistable elliptic curve over $\mathbf{Q}$ of conductor N, let p be an odd prime, and let K be a quadratic imaginary field such that $\gcd(D_K, pN) = 1$. Assume that $p \nmid \mathrm{ord}_\ell(j(E))$, for each prime ℓ, and that E admits no isogenies of degree p. Then $p \nmid \#E(K)_{\mathrm{tor}}$ and p is firm for E.*

Before giving the proof, we summarize its main ingredients. First, we observe that the assertion that $m(p) = 0$ (see Definition 3.3) uses a standard result that relates unramified Galois cohomology to component groups. Next, we use the semistability and isogeny hypotheses to deduce that $\rho_{E,p}$ is surjective. Then we use standard group cohomology to deduce that p is firm.

Proof. Let ℓ be a prime. By [14, I.3.8], $H^1(\mathbf{Q}_\ell^{\mathrm{unr}}/\mathbf{Q}_\ell, E(\mathbf{Q}_\ell^{\mathrm{unr}})) \cong H^1(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell, \Phi_{E,\ell}(\overline{\mathbf{F}}_\ell))$, where $\Phi_{E,\ell}$ is the component group of E at ℓ. If $\ell \nmid N$, there is nothing further to prove, so assume $\ell \mid N$. Since E is semistable, $\#\Phi_{E,\ell}(\overline{\mathbf{F}}_\ell) = -\mathrm{ord}_\ell(j)$. By hypothesis, $p \nmid \mathrm{ord}_\ell(j)$. Thus $m(p) = 0$.

Since E admits no isogenies of degree p, the Galois representation $\rho_{E,p} : G_{\mathbf{Q}} \to \mathrm{GL}(2, E[p])$ is irreducible, and there are no nontrivial $\mathbf{Q}$-rational cyclic subgroups of $E[p^\infty]$. Since E is semistable, work of Serre [19, Prop. 21] and [20, §3.1] implies that $\rho_{E,p}$ is surjective. Thus $p \nmid \#E(K)_{\mathrm{tor}}$ because a point in $E(\overline{\mathbf{Q}})$ of order p must generate an extension of $\mathbf{Q}$ of degree at least $p^2 - 1 \geq 3$.

The field K and $\mathbf{Q}(E[p])$ are linearly disjoint, since $\gcd(D_K, pN) = 1$, so

$$H^1(K(E[p])/K, E[p]) \cong H^1(\mathbf{Q}(E[p])/\mathbf{Q}, E[p]) \approx H^1(\mathrm{GL}(2, \mathbf{F}_p), \mathbf{F}_p^2).$$

The group $H = H^1(K(E[p^n])/K, E[p^n])$ has exponent a power of p. If an element α in $\mathrm{Gal}(K(E[p^n])/K) \subset \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$ is scalar, then every element of H has order dividing $\alpha - 1$. This is because the scalar is central, so the morphism of pairs it induces is both the identity and multiplication by α. It is necessary only to choose α such that $\gcd(\alpha - 1, p) = 1$. Since p is odd, -1 is a nonidentity element of $\mathrm{Aut}(E[p]) = \mathrm{Gal}(K(E[p])/K)$. Every automorphism lifts, so -1 lifts to some g in $\mathrm{Gal}(K(E[p^n])/K) \subset \mathrm{Aut}(E[p^n])$. Then $g^{p^{n-1}} = -1$ in $\mathrm{Aut}(E[p^n])$, so $-1 \in \mathrm{Gal}(K(E[p^n])/K)$ and every element of H has order dividing 2. (To show that $g^{p^{n-1}} = -1$, we use that $\mathrm{ord}_p \binom{p^n}{k} = n + \mathrm{ord}_p\left(\frac{1}{k}\right)$.) $\square$

5.2 The number B_K for $X_0(17)$

In this section, we show that for $E = X_0(17)$ and $K = \mathbf{Q}(\sqrt{-2})$, we have $B_K = 2$. This is accomplished by showing that the index $[E(K) : \mathbf{Z}y]$ is a power of 2. The elliptic curve $E = X_0(17)$ given by the Weierstrass equation

$$y^2 + xy + y = x^3 - x^2 - x - 14$$

satisfies the hypothesis of Proposition 5.1 for each odd prime p. Since the j-invariant of E is $3^3 \cdot 11^3/17^4$, every odd prime p is firm for E and $\#E(K)_{\mathrm{tor}}$ is a power of 2.

The conductor 17 of E splits in K, and the quadratic twist E' of E by K is the curve $y^2 = x^3 - 44x + 7120$, which is labeled **1088K4** in [7]. Using MAGMA (or `mwrank`), one finds that $E'(\mathbf{Q}) \cong \mathbf{Z}P \times \mathbf{Z}/2$, where $P = (-3, 85) \in E'(\mathbf{Q})$ has infinite order. Since the rank of E' is 1, we set $K = \mathbf{Q}(\sqrt{-2})$ in Section 4.2. Then B_K is divisible only by 2 and the index $[E(K) : \mathbf{Z}y]$. This index can only change by a power of 2 if y is replaced by y_K, so we instead consider the index $[E(K) : \mathbf{Z}y_K]$. The cokernel of the natural map $E(\mathbf{Q}) \oplus E'(\mathbf{Q}) \to E(K)$ is a 2-group and $E(\mathbf{Q}) \cong \mathbf{Z}/4\mathbf{Z}$, so $[E(K) : \mathbf{Z}y_K]$ is a power of 2 times $h(y_K)/h(P)$, where h is the Néron-Tate canonical height on E_K. By the Gross-Zagier formula (see [8, Thm. 6.3]),

$$h(y_K) = \frac{u^2|D|^{\frac{1}{2}}}{||\omega_f||} L'_{E'}(1) L_E(1), \tag{1}$$

where $D = -8$ is the discriminant of K, $u = 1$ is half the number of units, and $||\omega_f||$ is the Peterson norm of the newform f corresponding to E. Generators for the period lattice of E are $\omega_1 \sim 1.547079$ and $\omega_2 \sim 0.773539 + 1.372869i$; taking the determinant gives $||\omega_f|| \sim 2.123938$. Furthermore, again from [7], we find that $L_E(1) \sim 0.386769$ and $L'_{E'}(1) \sim 2.525026$, so $h(y_K) \sim 1.300533$. Using a computer, we find that $h(P) \sim 1.300533$ as well, so $[E(K) : \mathbf{Z}y_K]$ is a power of two.

5.3 Elements of index 2 and 4

The torsion subgroup of $E = X_0(17)$ is isomorphic to $\mathbf{Z}/4\mathbf{Z}$, so [11, pg. 670] implies that there are infinitely many elements of $H^1(\mathbf{Q}, E)$ having order and index equal to 2, and also infinitely many having order and index equal to 4.

5.4 Proof of Theorem 1.1

To prove Theorem 1.1, we combine the above computations with Theorem 3.1, and an observation about the local properties of Kolyvagin's classes c_{ℓ,p^n}.

Proof of Theorem 1.1. Let $E = X_0(17)$ as above, and let K be an arbitrary number field. Let p^n be either an odd prime power, or 2, or 4. The computations of the previous section combined with Theorem 3.1 prove that there are infinitely many elements c_{ℓ,p^n} of $H^1(\mathbf{Q}, E)$ whose index and order both equal p^n. Let A be the subgroup of $H^1(\mathbf{Q}, E)$ generated by these classes. The kernel B of $\mathrm{res}_K : A \to H^1(K, E)$ is finite, so the set $\mathcal{S}$ of primes ℓ such that $\mathrm{res}_\ell(c) \neq 0$ for some $c \in B$ is finite. By Proposition 3.4, we have $\mathrm{res}_v(c_{\ell,p^n}) = 0$ for all places $v \neq \ell$, so the subgroup A' of A generated by all c_{ℓ,p^n} with $\ell \notin \mathcal{S}$ has trivial intersection with B. Thus $\mathrm{res}_K(A')$ consists of infinitely many classes in $H^1(K, E)$ having order and index both equal to p^n, and the theorem now follows from Proposition 2.3. $\square$

References

[1] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: Wild* 3*-adic exercises*, (2001), to appear in J. Amer. Math. Soc., see also http://www.math.harvard.edu/∼ rtaylor/.

[2] D. Bump, S. Friedberg, and J. Hoffstein, *Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic* L*-functions and their derivatives*, Ann. of Math. (2) **131** (1990), no. 1, 53–127.

[3] J. W. S. Cassels, *Arithmetic on curves of genus* 1*. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.

[4] ______, *Arithmetic on curves of genus 1. V. Two counterexamples*, J. London Math. Soc. **38** (1963), 244–248.

[5] ______, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[6] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[7] J. E. Cremona, *Elliptic curves of conductor* ≤ 10000*,* `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

[8] B. Gross and D. Zagier, *Heegner points and derivatives of* L*-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[9] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[10] V. A. Kolyvagin, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Springer, Berlin, 1991, pp. 94–121.

[11] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684.

[12] S. Lichtenbaum, *Duality theorems for curves over* p*-adic fields*, Invent. Math. **7** (1969), 120–136.

[13] W. G. McCallum, *Kolyvagin's work on Shafarevich-Tate groups*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 295–316.

[14] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[15] M. R. Murty and V. K. Murty, *Non-vanishing of* L*-functions and applications*, Birkhäuser Verlag, Basel, 1997.

[16] C. O'Neil, *The Period-Index Obstruction for Elliptic Curves*, submitted, 2001.

[17] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, IAS/Park City Mathematics Institute 1999.

[18] K. Rubin, *The work of Kolyvagin on the arithmetic of elliptic curves*, Arithmetic of complex manifolds (Erlangen, 1988), Springer, Berlin, 1989, pp. 128–136.

[19] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[20] ———, *Travaux de Wiles (et Taylor, ...). I*, Astérisque (1996), no. 237, Exp. No. 803, 5, 319–332, Séminaire Bourbaki, Vol. 1994/95.

[21] I. R. Shafarevich, *Exponents of elliptic curves*, Dokl. Akad. Nauk SSSR (N.S.) **114** (1957), 714–716.