THERE ARE GENUS ONE CURVES OF EVERY INDEX OVER EVERY NUMBER FIELD

PETE L. CLARK

Abstract. We show that there exist genus one curves of every index over the rational numbers, answering affirmatively a question of Lang and Tate. The proof is "elementary" in the sense that it does not assume the finiteness of any Shafarevich-Tate group. On the other hand, using Kolyvagin's construction of a rational elliptic curve whose Mordell-Weil and Shafarevich-Tate groups are both trivial, we show that there are infinitely many genus one curves of every index over every number field.

1. Introduction

Let $C_{/K}$ be a genus one curve over a field K. There are two numerical invariants which quantify, in different ways, the extent to which C fails to have a K-rational point. The *index* of C is the least degree of a field extension L/K such that C has an L-rational point; equivalently, it is the least positive degree of a K-rational divisor on C. The *period* of C is the order of the cohomology class corresponding to C in the Weil-Châtelet group $H^1(K, \mathrm{Jac}(C))$; equivalently, it is the least positive degree of a K-rational divisor class on C. It is well known (e.g. [6]) that the period divides the index and that the two quantities have the same prime divisors.

When K is a number field, the index can strictly exceed the period [2], [4]. This is in a sense unfortunate, because while the index is of more geometric interest, it is the period which is directly addressed by the machinery of Galois cohomology. For example, it is an old theorem of Shafarevich-Cassels [3, § 27] that for any elliptic curve E over a number field K and any integer $n > 1$, there are infinitely many classes in the Weil-Châtelet group $H^1(K, E)$ of period n.

With regard to the index, almost fifty years ago Lang and Tate [6] asked the much more modest question of whether there are genus one curves of every index over $\mathbb{Q}$. They were able to show that if $E_{/K}$ is an elliptic curve over a number field with a K-rational torsion point of order n, then $H^1(K, E)$ contains infinitely many classes of index n. In view of the uniform boundedness of torsion on elliptic curves, this does not get us very far. Only recently has substantial progress been made: in [10], Stein showed that for any number field K there are infinitely many genus one curves over K of index equal to any number *not divisible by* 8.

The following theorem and its corollary give a complete answer to the question of Lang and Tate.

Theorem 1. *Let $E_{/K}$ be an elliptic curve over a number field with $E(K) = 0$. For every positive integer n, there exists an element $\eta \in H^1(K, E)$ of index n.*

It is known (e.g. [8]) that there are infinitely many rational elliptic curves with trivial Mordell-Weil group. Thus:

Corollary 2. *For every positive integer n there are infinitely many genus one curves $C_{/\mathbb{Q}}$ of index n.*

We want to emphasize that Theorem 1 does not require the finiteness of any Shafarevich-Tate group. This is to be contrasted with the following results:

Theorem 3. *Let $E_{/K}$ be an elliptic curve with $E(K) = 0$ and $Ш(K, E) = 0$. Then for every number field L/K and every positive integer n, there are infinitely many elements of $H^1(L, E)$ of index n.*

Luckily for us, some examples of elliptic curves $E_{/\mathbb{Q}}$ satisfying the hypotheses of Theorem 3 can be found in a paper of Kolyvagin [5, Theorem H]: taking in his notation $D = -7$, we get an elliptic curve $E_{/\mathbb{Q}}$ with minimal Weierstrass equation $y^2 + y = x^3 - 49x - 86$ ($1813B1$ in Cremona's tables) with $E(\mathbb{Q}) = Ш(\mathbb{Q}, E) = 0$. Thus we get the following, our main result:

Corollary 4. *There are innfinitely many genus one curves of every index over every number field.*

In Section 2 we set the stage with some preliminary results on a subset of $H^1(K, E)$ on which the equality of period and index is guaranteed. Readers familiar with the Heegner point Euler system will recognize these classes as the (vastly simpler) analogue of classes constructed by Kolyvagin. In Section 3 we give the proofs of Theorems 1 and 3, and in Section 4 we make some brief final remarks on generalizations and comparisons with Stein's work.

2. The Kolyvagin set

For a number field K, we denote by Σ_K the set of all places of K.

Let $E_{/K}$ be an elliptic curve over a number field and $v \in \Sigma_K$. We define $\mathcal{K}_v(K, E)$ to be the subset of $H^1(K, E)$ consisting of classes η whose local restriction to each $v' \neq v$ is zero. We define the *Kolyvagin set*

$$\mathcal{K}(K, E) = \bigcup_{v \in \Sigma_K} \mathcal{K}_v(K, E) \subset H^1(K, E).$$

The following proposition merely records for future reference some elementary properties of the Kolyvagin set. The reader will have no difficulty supplying the proof.

Proposition 5. *Let $E_{/K}$ be an elliptic curve over a number field.*
a) $Ш(K, E) \subset \mathcal{K}(K, E)$.
b) For any v and any positive integer n, $\mathcal{K}_v(K, E)[n]$ is a finite group.
c) If $\eta \in \mathcal{K}(K, E)$ and $c \in \mathbb{Z}$, then $c\eta \in \mathcal{K}(K, E)$.

The next result is the key observation about Kolyvagin classes that we will use to prove the main results of the paper.

Proposition 6. *Let $C_{/K}$ be a genus one curve over a number field whose corresponding class η lies in $\mathcal{K}(K, \mathrm{Jac}(C))$. Then every rational divisor class on C admits a rational divisor. In particular, the period and index of η are equal.*

First proof: This follows rather formally from the existence of O'Neil's period-index obstruction map [9]. Namely, for any elliptic curve $E_{/K}$ defined over a field of characteristic zero and positive integer n, there exists a map

$$\Delta : H^1(K, E[n]) \rightarrow \mathrm{Br}(K)[n],$$

functorial in K, and satisfying the following properties: a) a class $\eta \in H^1(K,E)[n]$ has index dividing n if and only if there exists some Kummer lift of η to $\xi \in H^1(K,E[n])$ such that $\Delta(\xi) = 0$; b) if $\eta = 0$ then every Kummer lift ξ of η has $\Delta(\xi) = 0$. So let $\eta \in \mathcal{K}(K,E)$ have period n, let ξ be any lift of η to $H^1(K,E[n])$ and consider $\Delta(\xi) \in \mathrm{Br}(K)[n]$. Since for all $v' \neq v$, $\eta|_{v'} = 0$, by b) above we have that $\Delta(\xi)|_{v'} = 0$ in $\mathrm{Br}(K_{v'})$. By virtue of the reciprocity law in the Brauer group of a number field, we have that $\Delta(\xi) = 0$, so η has index dividing n, hence index n.

Second proof: Let $V_{/K}$ be any (smooth, projective geometrically irreducible) variety over any field K. Taking low-degree terms in the Leray spectral sequence associated to the étale sheaf $\mathbb{G}_m$ on $\operatorname{Spec} K$ we get [1, Ch. IX] an exact sequence

$$0 \rightarrow \mathrm{Pic}(V_{/K}) \rightarrow \mathrm{Pic}(V_{/\overline{K}})^{\mathfrak{g}_K} \xrightarrow{\delta} \mathrm{Br}(K) \xrightarrow{\gamma} \mathrm{Br}(V)$$

which is functorial in K. Thus the obstruction δ to a rational divisor class being represented by a rational divisor is an element of the Brauer group of the base field K. Moreover, a K-rational point $P : \operatorname{Spec} K \rightarrow V$ would induce a map $\mathrm{Br}(P) : \mathrm{Br}(V) \rightarrow \mathrm{Br}(K)$ such that $\gamma \circ \mathrm{Br}(P) = 1_{\mathrm{Br}(V)}$, and it follows that $V(K) \neq \emptyset$ implies $\delta \equiv 0$. If now K is a number field and V is any variety which has rational points at every completion except possibly one, then the above reciprocity law argument gives us that $\delta \equiv 0$ on V.

3. The proofs of Theorem 1 and Theorem 3

We begin with the following routine result, whose proof we include for completeness.

Lemma 7. *Let $E_{/K}$ be an elliptic curve over a number field and n be any positive integer. If $v \in \Sigma_K$ is any finite place splitting completely in $K(E[n])$, then $H^1(K_v, E)$ has an element of exact order n.*

Proof: By a seminal theorem of Tate [7, Cor. I.3.4], the finite abelian groups $H^1(K_v,E)[n]$ and $E(K_v)/nE(K_v)$ are in duality, so it suffices to see that the latter group contains an element of exact order n when E has full n-torsion over K_v. By the structure theory for compact v-adic Lie groups,

$$E(K_v) \cong \mathbb{Z}_\ell^N \oplus \mathbb{Z}/(d_1) \oplus \mathbb{Z}/(d_1 d_2)$$

for some positive integers $N,\ d_1,\ d_2$; here ℓ is the residue characteristic of K_v. If E has full n-torsion over K_v, then $n \mid d_1 d_2$, so that any generator of $\mathbb{Z}/(d_1 d_2)$ has exact order n in $E(K)/nE(K)$.

We now give the proof of Theorem 1, so let $E_{/K}$ be an elliptic curve with $E(K) = 0$. By primary decomposition for period and index of a cohomology class (e.g. [10, Prop. 2.5]), it suffices to find classes of period and index equal to any prime power, say $n = p^a$. There are two cases to consider.

Case 1: $Ш(K,E)$ contains an element η of exact order p^a. Then by Propositions 5 and 6, η has index p^a.

Case 2: $Ш(K,E)[p^\infty] = Ш(K,E)[p^{a-1}]$ is a finite group. By [7, I.6.26(b)], whenever the p-primary torsion of the Shafarevich-Tate group of an abelian variety A defined over a number field K is a finite group (i.e., conjecturally always!) there is an exact sequence

$$0 \to Ш(K,A)[p^\infty] \to H^1(K,A)[p^\infty] \to \bigoplus_{v \in \Sigma_K} H^1(K_v,A)[p^\infty] \to (A^\vee(K)^\wedge)^* \to 0,$$

where the three operations on the last term are, respectively, abelian variety dual, pro$-p$ completion, and Pontrjagin dual. But since we've assumed $E(K) = 0$, this gives a surjection

$$H^1(K,E)[p^\infty] \to \bigoplus_v H^1(K_v,E)[p^\infty] \to 0. \tag{1}$$

Invoking Lemma 7, let $v \in \Sigma_K$ be such that $H^1(K_v,E)$ contains an element η_v of exact order p^a. By (1), there exists a global class η which is locally trivial at every $v' \neq v$ and is locally equal to η_ℓ, so that $\eta \in \mathcal{K}(K,E)$. By Proposition 6, any such η has index equal to its period.

The only remaining question is what the period of η is. However, certainly the period of η is of the form $c \cdot p^a$ for some positive integer c; then the class $c\eta$ has exact period p^a. By Proposition 5c), $c\eta$ is still a Kolyvagin class, so also has index p^a, as desired. This completes the proof of Theorem 1.

We turn now the setting of Theorem 3, which is a sort of degenerate case of Theorem 1. Indeed, under the hypothesis that $Ш(K,E) = 0$, the global duality relation becomes:

$$H^1(K,E) \xrightarrow{\sim} \bigoplus_{v \in \Sigma_K} H^1(K_v,E).$$

It follows that the order of a Kolyvagin class is always equal to the order of its nontrivial local restriction. We finish, appropriately enough, by recalling a result of Lang and Tate [6, Cor. 1, p. 676]: if $E_{/K_v}$ is an elliptic curve over a v-adic field with good reduction and p^a is prime to the order of the residue field, then an element of $H^1(K_v,E)$ of period p^a also has index p^a and moreover is split by a local extension field L_w/K_v if and only if p^a divides the ramification index $e(L_w/K_v)$. Thus if in Lemma 7 we choose our place v to be of good reduction for E, unramified in L and prime to p (which excludes only finitely many places), we find that the class $\eta|_L$ has the property that η_{L_w} has index at least p^a. On the other hand since η has index p^a, certainly $\eta|_L$ has index at most p^a, so $\eta|_L$ has period and index both equal to p^a. Since we can perform this construction for each v in a set of positive density, we get infinitely many such classes, completing the proof of Theorem 3.

4. Some final thoughts

There is work in progress of Stein and his students [11] whose goal is to verify the full conjecture of Birch and Swinnerton-Dyer for all rational elliptic curves of conductor at most 1000 and analytic rank at most one. This work in particular gives many other examples of rational elliptic curves satisfying the hypotheses of Theorem 3. In fact there are close relations between [10], [11] and the present paper.

In order see the connection, we first note that the argument used to establish Theorem 3 readily gives the following variant:

Theorem 8. *Let $E_{/K}$ be an elliptic curve over a number field whose Mordell-Weil group has rank zero. Suppose moreover that $Ш(K, E)$ is finite. Then, for any n prime to $N = \#E(K) \cdot \#Ш(K, E)$ and any number field L/K, there exist infinitely many genus one curves $C_{/L}$ of index n.*

Theorem 8 should be compared with Theorem 3.1 and §4.1 in Stein's paper [10], wherein attention is focused on the the rational elliptic curve $E = X_0(17)$. The calculations of [10, §5.1] showing that (in his notation) $B_K = 2$ give a good example of the techniques systemically employed in [11]: namely, they show that $Ш(\mathbb{Q}, X_0(17))[p] = 0$ for all odd primes p. By a routine computation with the 2-Selmer group, one finds that $Ш(\mathbb{Q}, X_0(17))[2] = 0$. Thus $Ш(\mathbb{Q}, X_0(17)) = 0$, as predicted by the conjecture of Birch and Swinnerton-Dyer. However the Mordell-Weil group of E is not trivial – rather, $X_0(17)(\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$ – so by Theorem 8, for all number fields K there are elements of $H^1(K, X_0(17))$ of every *odd* index.

Much more remains to be done on the index problem for genus one curves over number fields. The obvious analogue for the index of the Shafarevich-Cassels theorem is the assertion that for any positive integer $n > 1$ and any elliptic curve E over a number field K, there exist infinitely many classes in $H^1(K, E)$ with index n. The case of $n = 2$ ("biconic curves") and arbitrary E and K can be handled using the methods of [4] together with the theory of explicit 2-descent; this is the subject of work in progress of the present author. The general case may well require a deeper understanding of n-descent than we currently possess.

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud. *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete 21, Springer-Verlag, 1990.

[2] J.W.S. Cassels. *Arithmetic on a curve of genus one. (V) Two counterexamples*, J. London Math. Soc. 36 (1961), 177-184.

[3] J.W.S. Cassels. *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. 41 (1966), 193-291.

[4] P.L. Clark. *Period-index problems in WC-groups I: elliptic curves*, to appear in J. Number Theory.

[5] V. Kolyvagin. *On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Math. USSR-Izv. 33 (1989), 473-499.

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

[7] J. Milne. *Arithmetic Duality Theorems*, Perspectives in Mathematics, 1. Academic Press Inc., 1986.

[8] J. Nakagawa and K. Horie. *Elliptic curves with no rational points*, Proc. Amer. Math. Soc. 104 (1988), 20-24.

[9] C.H. O'Neil. *The period-index obstruction for elliptic curves*, J. Number Theory 95 (2002), 329-339.

[10] W. Stein. *There are genus one curves over $\mathbb{Q}$ of every odd index*, J. Reine Agnew. Math. 547 (2002), 139-147.

[11] W. Stein et al. *Verifying the Birch and Swinnerton-Dyer Conjecture for Certain Elliptic Curves*, preliminary report of work in progress.

1126 Burnside Hall, Department of Mathematics and Statistics, McGill University, 805 Sherbrooke West, Montreal, QC, Canada H3A 2K6

E-mail address: clark@math.mcgill.ca