



Weak approximation for 0-cycles on a product of elliptic curves

Evangelia Gazaki¹ · Angelos Koutsianas²

Received: 24 January 2022 / Revised: 16 December 2022 / Accepted: 17 December 2022

© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2022

Abstract

In the 1980's Colliot-Thélène, Sansuc, Kato and S. Saito proposed conjectures related to local-to-global principles for 0-cycles on arbitrary smooth projective varieties over a number field. We give some evidence for these conjectures for a product $X = E_1 \times E_2$ of two elliptic curves. In the special case when $X = E \times E$ is the self-product of an elliptic curve E over \mathbb{Q} with potential complex multiplication, we show that the places of good ordinary reduction are often involved in a Brauer–Manin obstruction for 0-cycles over a finite base change. We give many examples when these 0-cycles can be lifted to global ones.

1 Introduction

Let X be a smooth projective geometrically connected variety over a number field F . We denote by Ω the set of all places v of F and by F_v the completion of F at a place v . The classical local-to-global principles for X refer to the image of the diagonal embedding

$$X(F) \hookrightarrow X(\mathbb{A}_F) := \prod_{v \in \Omega} X(F_v)$$

Appendix by Angelos Koutsianas.

✉ Evangelia Gazaki
eg4va@virginia.edu

Angelos Koutsianas
akoutsianas@math.auth.gr

¹ Department of Mathematics, University of Virginia, 221 Kerchof Hall, 141 Cabell Dr., Charlottesville, VA 22904, USA

² Department of Mathematics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece

to the set $X(\mathbf{A}_F)$ of adelic points of X . The cohomological Brauer group $\text{Br}(X) := H^2(X_{\text{ét}}, \mathbb{G}_m)$ is known to often obstruct either the existence of an F -rational point or the density of $X(F)$ in $X(\mathbf{A}_F)$. Namely, by the foundational work of Manin [25], the Brauer group gives rise to an intermediate closed subset $X(F) \subseteq X(\mathbf{A}_F)^{\text{Br}(X)} \subseteq X(\mathbf{A}_F)$, which is often empty or properly contained in $X(\mathbf{A}_F)$. Unfortunately, the Brauer–Manin obstruction cannot always explain the failure of the Hasse principle and weak approximation for points (cf. [1, 27]). However, this happens to be the case for abelian varieties, assuming finiteness of their Tate-Shafarevich groups, and it is conjectured to be the case for geometrically rationally connected varieties [4, p. 174]. The answer is likely to be yes also for $K3$ -surfaces (cf. [36, p. 4]).

In this article we are interested in an analog of this study for 0-cycles, namely for the group $\text{CH}_0(X)$.

Denote by $\Omega_f(F)$ (resp. $\Omega_{\infty}(F)$) the set of all finite (resp. infinite) places of F . For a place $v \in \Omega$ denote by X_v the base change to F_v . We have the following conjecture.

Conjecture 1.1 ([6, Sect. 4], [18, Sect. 7], see also [5, Conjecture 1.5 (c)]) *Let X be a smooth projective geometrically connected variety over a number field F . The following complex is exact,*

$$\varprojlim_n \text{CH}_0(X)/n \rightarrow \varprojlim_n \text{CH}_{0,\mathbf{A}}(X)/n \rightarrow \text{Hom}(\text{Br}(X), \mathbb{Q}/\mathbb{Z}).$$

The above formulation is due to van Hamel [40], see also [41, Conjecture (E_0)]. The adelic Chow group $\text{CH}_{0,\mathbf{A}}(X)$ is equal to $\prod_{v \in \Omega_f(F)} \text{CH}_0(X_v)$ when F is totally imaginary, and it has a small contribution from the infinite real places otherwise.

When X is a smooth projective curve, Conjecture 1.1 has been proved by Colliot-Thélène [3, paragraph 3] assuming the finiteness of the Tate-Shafarevich group of its Jacobian. In higher dimensions, the main evidence for Conjecture 1.1 is for rationally connected varieties starting with the work of Colliot-Thélène, Sansuc and Swinnerton-Dyer [7, 8] and continued by the work of Liang [24, Theorem B]. The latter proved this conjecture assuming that the Brauer–Manin obstruction is the only obstruction to Weak Approximation for points on X_L where L is any finite extension of F . There is some recent partial evidence of Ieronymou of similar flavor for $K3$ -surfaces (cf. [16, Theorem 1.2]). Moreover, Harpaz and Wittenberg [13, Theorem 1.3] proved that the conjecture is compatible with fibrations over curves.

The purpose of this article is to give some evidence for this conjecture for a product $X = E_1 \times E_2$ of elliptic curves. We focus on the following weaker question.

Question 1.2 *Let p be a prime number and $\text{Br}(X)\{p\}$ be the p -primary torsion subgroup of $\text{Br}(X)$. Is the following complex exact*

$$\varprojlim_n \text{CH}_0(X)/p^n \rightarrow \varprojlim_n \text{CH}_{0,\mathbf{A}}(X)/p^n \rightarrow \text{Hom}(\text{Br}(X)\{p\}, \mathbb{Q}/\mathbb{Z})? \quad (1.3)$$

Assuming the finiteness of the Tate-Shafarevich group of X , and that the action of the absolute Galois group G_F on the Néron-Severi group $\text{NS}(X \otimes_F \overline{F})$ is trivial, the exactness of (1.3) can be reduced (cf. Proposition 2.16, Corollary 2.19) to the exactness of the complex,

$$\varprojlim_n F^2(X)/p^n \rightarrow \varprojlim_n F_A^2(X)/p^n \rightarrow \text{Hom} \left(\frac{\text{Br}(X)\{p\}}{\text{Br}_1(X)\{p\}}, \mathbb{Q}/\mathbb{Z} \right), \quad (1.4)$$

where $F^2(X)$ is the kernel of the Albanese map of X and $\text{Br}_1(X)$ is the algebraic Brauer group of X . From now make the above assumptions. Our first result is the following theorem.

Theorem 1.5 (Theorem 3.1) *Let $X = E_1 \times E_2$ be a product of elliptic curves over a number field F . There is an infinite set T of primes p for which the middle term in (1.4) vanishes, making the complex exact. If we further assume that at least one of the curves does not have potential complex multiplication, then the complement S of T is a set of primes of density zero (in the sense of [33]).*

When both E_1, E_2 have potentially good reduction, this result was already obtained in [12, Corollary 1.8].

It follows by [29, Theorem 3.5] that the only places that might contribute a nontrivial factor in $\varprojlim_n F_A^2(X)/p^n$ are the places of bad reduction and the places above p . The key to prove Theorem 1.5 is that under some assumptions on the prime p , the group $F^2(X_v)$ is p -divisible for every unramified place v above p of good reduction (cf. [12, Theorem 1.1]). One can think of this result as a weaker analog of the vanishing $F^2(X_v) = 0$ for X a rationally connected variety and v a place of good reduction [20, Theorem 5].

A natural follow-up question is whether the places of good reduction are ever involved in a Brauer–Manin obstruction for 0-cycles. Our second theorem gives an affirmative answer for places of good ordinary reduction that are ramified enough.

Theorem 1.6 (cf. Theorem 4.2) *Let $X = E \times E$ be the self product of an elliptic curve E over \mathbb{Q} . Suppose that $E \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ has complex multiplication by the full ring of integers of a quadratic imaginary field K . Let $p \geq 5$ be a prime which is coprime to the conductor \mathfrak{n} of E and suppose that p splits completely in K , $p = \pi\bar{\pi}$ for some prime element π of \mathcal{O}_K . Let \overline{E}_p be the reduction of E modulo p . Suppose there exists a finite Galois extension F_0/K of degree $n < p - 1$ such that there is a unique unramified place w of F_0 above π with the property that p divides $|E_p(\mathbb{F}_w)|$, where \mathbb{F}_w is the residue field of F_0 at w . Then there exists a finite Galois extension L/F_0 of degree $p - 1$, totally ramified at w such that the following are true for the group $\varprojlim_n F_A^2(X_L)/p^n$.*

- (1) *It is equal to $\prod_{v|p} \varprojlim_n F^2(X_{L_v})/p^n$, and isomorphic to $\mathbb{Z}/p \oplus \mathbb{Z}/p$.*
- (2) *It is orthogonal to the transcendental Brauer group $\text{Br}(X_L)/\text{Br}_1(X_L)$.*

The same result holds if the elliptic curve E is defined over K .

The primes p of good reduction that split completely in K are precisely the primes of good **ordinary reduction**. The involvement of the ordinary reduction places in a Brauer–Manin obstruction after suitable base change is not surprising. An analogous result for rational points was recently obtained in [2], which in particular applies to weak approximation for points on abelian varieties and $K3$ surfaces. See also [26] for an explicit example.

Global approximation

We next pass to the main question of this article namely, whether in the situation considered in Theorem 1.6, one can lift the group $\varprojlim_n F_{\mathbf{A}}^2(X_L)/p^n$ to global elements.

An important observation is that $\varprojlim_n F_{\mathbf{A}}^2(X_L)/p^n$ coincides with $\prod_{v|p} F^2(X_{L_v})/p$ (cf. Sect. 3.2). Thus, one is looking for genuine 0-cycles and the question is reduced to showing that the diagonal map $F^2(X_L)/p \xrightarrow{\Delta} \prod_{v|p} F^2(X_{L_v})/p$ is surjective.

We focus mainly on the simplest case considered in Theorem 1.6, namely when $F_0 = \mathbb{Q}$; that is, when the reduction of the elliptic curve E satisfies $|\overline{E}_p(\mathbb{F}_p)| = p$. One can find infinite families with this property. For example, consider the family of elliptic curves with Weierstrass equation $\{y^2 = x^3 + c; c \in \mathbb{Z}, c \neq 0\}$ having potential CM by the ring of integers of $\mathbb{Q}(\zeta_3)$. Let p be a prime of the form $4p = 1 + 3v^2$. Then, there exist exactly $\frac{p-1}{6}$ congruence classes $c \pmod{p}$ that give elliptic curves that satisfy $|\overline{E}_p(\mathbb{F}_p)| = p$.

In Sect. 4.2 we give various sufficient conditions that guarantee the ability to lift. The conditions are supported by explicit examples, giving therefore some evidence for Conjecture 1.1. The following Theorem 1.7 is indicative of the computations we do in Sect. 4. Before stating the result, we need to refer to some notation.

Suppose the pair E, p satisfies the assumptions of Theorem 1.6. Let $P \in E(\mathbb{Q})$. We will denote by $P_{\mathbb{Q}_p}$ the image of P under the restriction map $E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}_p)$. We abuse notation and denote by $P_{\mathbb{Q}_p}$ also its image modulo $pE(\mathbb{Q}_p)$. In Sect. 3.2.1 we construct a decomposition $P_{\mathbb{Q}_p} = \widehat{P}_{\mathbb{Q}_p} \oplus \overline{P}_{\mathbb{Q}_p}$, with $\widehat{P}_{\mathbb{Q}_p} \in \widehat{E}(p\mathbb{Z}_p)/[p]$, and $\overline{P}_{\mathbb{Q}_p} \in \overline{E}_p(\mathbb{F}_p)/p$ (cf. Notation 3.5).

We can now state our next theorem.

Theorem 1.7 *Let $p \geq 5$ be a prime and E an elliptic curve over \mathbb{Q} satisfying the assumptions of Theorem 1.6. Assume further that $|\overline{E}_p(\mathbb{F}_p)| = p$. Let L/K be the extension constructed in Theorem 1.6. Suppose that the Mordell-Weil group $E(\mathbb{Q})$ has positive rank and there exists a point $P \in E(\mathbb{Q})$ of infinite order such that the image $P_{\mathbb{Q}_p}$ of P under the restriction map $\text{res}_{\mathbb{Q}_p/\mathbb{Q}} : E(\mathbb{Q})/p \rightarrow E(\mathbb{Q}_p)/p$, has the property*

that $\widehat{P}_{\mathbb{Q}_p} \neq 0 \in \frac{\widehat{E}(p\mathbb{Z}_p)}{[p]\widehat{E}(p\mathbb{Z}_p)}$. Then we have a surjection

$$F^2(X_L)/p \rightarrow \prod_{v|p} F^2(X_{L_v})/p \rightarrow 0.$$

In particular, the complex (1.4) is exact.

We expect that Theorem 1.7 is satisfied by infinite families of elliptic curves. The criterion given in Theorem 1.7 can be checked computationally in SAGE for small values of the prime p . In the appendix Appendix A we study the family of elliptic curves $\{y^2 = x^3 - 2 + 7n, n \in \mathbb{Z}\}$ and the prime $p = 7$. When n lies in the interval $[-5000, 5000]$, we show that about 86.68% of elliptic curves with rank one over \mathbb{Q} have such a “good point” $P \in E(\mathbb{Q})$.

The method used to prove Theorem 1.7 can be generalized to more situations (cf. Corollary 4.10 for when F_0/K is a quadratic extension). In Sect. 4.2 we give criteria of similar flavor for elliptic curves that do not possess a suitable rational point of infinite order. For the purposes of the introduction, we chose to state our theorem in its simplest form.

Remark 1.8 In a recent article Liang [23] showed some compatibility of weak approximation for 0-cycles with certain products using the fibration method. The same method has been used in most known results [13, 16, 24]. Unfortunately, this breakthrough method does not seem to generalize to abelian varieties. For, the key cohomological properties $H^i(X, \mathcal{O}_X) = 0$, for $i = 1, 2$, and finiteness of $\mathrm{Br}(X)/\mathrm{Br}_0(X)$ (used for rationally connected varieties and $K3$ surfaces respectively) are no longer true. Our approach is different in the sense that it does not use the assumption that the weak approximation is the only one for rational points. The downside is that we cannot find a uniform treatment that guarantees lifting, but we instead present many different sufficient conditions. The advantages on the other hand are first that our results are unconditional and second that we construct global 0-cycles on the nose. In fact, if one only focuses on proving exactness of (1.4), then the finiteness of the Tate-Shafarevich group is no longer needed.

1.1 Notation

Throughout this note unless otherwise mentioned we will be using the following notation.

- For a number field F , \mathcal{O}_F , $\Omega(F)$, $\Omega_f(F)$, $\Omega_\infty(F)$ will be respectively its ring of integers, the set of all places, all finite and all infinite places of F .
- For a finite extension k/\mathbb{Q}_p , \mathcal{O}_k will be its ring of integers, \mathfrak{m}_k its maximal ideal and \mathbb{F}_k its residue field.
- For a place $v \in \Omega(F)$, F_v will be the completion of F at v .
- For an abelian group M and a positive integer n , M_n and M/n will be the n -torsion and n -cotorsion of M respectively. Moreover, \widehat{M} will be the completion, $\widehat{M} = \varprojlim_n M/n$.
- For an elliptic curve E and an integer n we will instead write $E[n]$ for the n -torsion.
- For a field extension L/K , and a variety X over K , X_L will be the base change to L .
- For a field k and a continuous $\mathrm{Gal}(\bar{k}/k)$ -module M we will denote by $\{H^i(k, M)\}_{i \geq 0}$ the Galois cohomology groups of M .

2 Background

2.1 Elliptic curves with complex multiplication

In this subsection we recall some necessary facts about elliptic curves with complex multiplication. Let E be an elliptic curve over \mathbb{Q} with potential complex multiplication

by the full ring of integers \mathcal{O}_K of K . It follows by [30, Corollary 5.12] that K has class number one. Note that there exactly 9 such fields $K = \mathbb{Q}(\sqrt{D})$. Namely, $D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. The same result holds if E is defined over K .

Notation 2.1 For an element $a \in \mathcal{O}_K$ we will denote by $E[a]$ the kernel of the isogeny $a : E_K \rightarrow E_K$. Similarly, if \mathfrak{a} is an ideal of \mathcal{O}_K , then $\mathfrak{a} = (a)$ for some element $a \in \mathcal{O}_K$ which is uniquely defined up to units. We will also write $E[\mathfrak{a}]$ for the kernel of $a : E_K \rightarrow E_K$ (which is independent of the choice of generator).

Let \mathfrak{a} be a nonzero proper ideal of \mathcal{O}_K which is prime to the conductor \mathfrak{n}_K of E_K . It follows by [30, Corollary 5.20 (ii)] that there is an isomorphism:

$$\mathrm{Gal}(K(E[\mathfrak{a}])/K) \xrightarrow{\sim} (\mathcal{O}_K/\mathfrak{a})^\times.$$

In particular, if \mathfrak{p} is a prime of \mathcal{O}_K not dividing the conductor, then the Galois group $\mathrm{Gal}(K(E[\mathfrak{p}])/K)$ is cyclic of order $N_{K/\mathbb{Q}}(\mathfrak{p}) - 1$, where $N_{K/\mathbb{Q}} : K^\times \rightarrow \mathbb{Q}^\times$ is the norm map. Next suppose that p is a rational prime coprime to \mathfrak{n} . We distinguish the following two cases:

- p is a prime element of \mathcal{O}_K , so $k = K_{(p)}$ is a quadratic unramified extension of \mathbb{Q}_p . Then $\mathrm{Gal}(K(E[p])/K) \xrightarrow{\sim} \mathbb{F}_{p^2}^\times$. In this case the elliptic curve E_k has good supersingular reduction.
- p splits completely in K , that is, $p = \pi\bar{\pi}$, where π is a prime element of \mathcal{O}_K . Then we have an isomorphism, $\mathrm{Gal}(K(E[p])/K) \xrightarrow{\sim} \mathbb{F}_p^\times \oplus \mathbb{F}_p^\times$, and hence $K(E[p])/K$ is an extension of degree $(p - 1)^2$. In this case the elliptic curve $E_{\mathbb{Q}_p}$ has good ordinary reduction.

The case of interest to us in this note is the latter. From now on we will refer to such primes as *ordinary primes*. We fix such an ordinary prime p and a factorization $p = \pi\bar{\pi}$ into prime elements of \mathcal{O}_K . We will denote by $\mathfrak{p}, \bar{\mathfrak{p}}$ the prime ideals $(\pi), (\bar{\pi})$ of \mathcal{O}_K respectively. Notice that the two completions $K_{\mathfrak{p}}, K_{\bar{\mathfrak{p}}}$ of K are both equal to \mathbb{Q}_p . Let $\overline{E_p}$ be the reduction of E modulo p and $r : E(\mathbb{Q}_p) \rightarrow \overline{E_p}(\mathbb{F}_p)$ be the reduction map. We will use same notation for the reduction $E(k) \xrightarrow{r} \overline{E_p}(\mathbb{F}_k)$ where k/\mathbb{Q}_p is any finite extension. Moreover, we will denote by $\widehat{E_{\mathbb{Q}_p}}$ the formal group of $E_{\mathbb{Q}_p}$.

It follows by [9] (see also [22, 13.4, Theorem 12]) that we can choose π so that the endomorphism $\pi : E_{\mathbb{Q}_p} \rightarrow E_{\mathbb{Q}_p}$ when reduced modulo p coincides with the Frobenius endomorphism $\phi_p : \overline{E_p} \rightarrow \overline{E_p}$. In particular, the reduction of π is an automorphism of $\overline{E_p}$, and hence has trivial kernel. This implies that for every $n \geq 1$ the subgroup $E[\pi^n]$ of $E[p^n]$ coincides with the p^n -torsion of the formal group, $\widehat{E_{\mathbb{Q}_p}}[p^n]$. Moreover, the relation $p = \pi\bar{\pi}$ implies that $\bar{\pi}$ induces a height zero isogeny $[\bar{\pi}] : \widehat{E_{\mathbb{Q}_p}} \rightarrow \widehat{E_{\mathbb{Q}_p}}$, and hence for every $n \geq 1$ the reduction induces an isomorphism of abelian groups $E[\bar{\pi}^n] \xrightarrow{\sim} \overline{E_p}[p^n]$.

Let k/\mathbb{Q}_p be a finite extension. Since $E_{\mathbb{Q}_p}$ has good ordinary reduction, for every $n \geq 1$ there is a short exact sequence of $\text{Gal}(\bar{k}/k)$ -modules,

$$0 \rightarrow \widehat{E_{\mathbb{Q}_p}}[p^n] \rightarrow E[p^n] \rightarrow \overline{E_p}[p^n] \rightarrow 0. \quad (2.2)$$

The above discussion shows that (2.2) splits, since the subgroup $E[\pi^n]$ of $E[p^n]$ maps isomorphically to $\overline{E_p}[p^n]$ (see also [31, A.2.4] for more general results).

Special fiber

We next recall formulas for $|\overline{E_p}(\mathbb{F}_p)|$ for the various choices of the quadratic imaginary field K . We are particularly interested in finding examples of curves that satisfy $|\overline{E_p}(\mathbb{F}_p)| = p$. That is, curves for which the extension F_0 of Theorem 1.6 can be taken to be \mathbb{Q} . In all cases we have a formula,

$$|\overline{E_p}(\mathbb{F}_p)| = p + 1 - (\pi + \bar{\pi}), \quad (2.3)$$

where $\pi\bar{\pi} = p$ and π reduces mod p to the Frobenius (cf. [17, p. 1]). For the various choices of quadratic imaginary field K , the correct choice of prime element π can be computed. We list a few examples.

Example 2.4 Suppose $D = -3$, that is, $K = \mathbb{Q}(\zeta_3)$, and E is given by the Weierstrass equation $y^2 = x^3 + c$ with $c \in \mathbb{Z}$. It follows by [28, Theorem 1] that

$$|\overline{E_p}(\mathbb{F}_p)| = p + 1 - \left(\frac{4c}{\pi_0} \right)_6 \cdot \bar{\pi}_0 - \left(\frac{4c}{\bar{\pi}_0} \right)_6 \cdot \pi_0, \quad (2.5)$$

where π_0 is a prime element of K such that $\pi_0\bar{\pi}_0 = p$ and $\pi_0, \bar{\pi}_0$ are normalized, that is, they are congruent to 1 mod 3. Here $\left(\frac{a}{\pi_0} \right)_6 = a^{\frac{p-1}{6}} \pmod{\pi_0}$ is the sixth power residue symbol. The symbol $\left(\frac{4c}{\pi_0} \right)_6$ can take any value within the set of units $\{\pm 1, \pm \zeta_3, \pm \zeta_3^2\}$ of $\mathbb{Z}[\zeta_3]$. In particular, when p is of the form $4p = 1 + 3v^2$ for some $v \in \mathbb{Z}$, there are exactly $\frac{p-1}{6}$ different reductions $\overline{E_p}$ which satisfy $|\overline{E_p}(\mathbb{F}_p)| = p$. Primes of this form include $p = 7, 37, 61, \dots$. For example, when $p = 7$, the family of elliptic curves $\{E_n : y^2 = x^3 - 2 + 7n, n \in \mathbb{Z}\}$ satisfies the desired equality. Later in this article we will make this family a case study to construct examples that satisfy Theorem 1.7. A second example is given for $p = 61$ and the family $\{E_t : y^2 = x^3 + 2 + 61t, t \in \mathbb{Z}\}$.

Example 2.6 Suppose $D = -11$. A sage computation shows that for $p = 223$ the family $\{E_s : y^2 = x^3 - 1056x + 13552 + 223s, s \in \mathbb{Z}\}$ satisfies the desired equality. Another class of examples is given for $D = -19$, $p = 43$ and $\{E_l : y^2 = x^3 - 152x + 722 + 43l, l \in \mathbb{Z}\}$.

Example 2.7 When $D = -43, -67, -163$, and E is given by a CM Weierstrass equation with parameter c (cf. [17, Tableau 1]) it follows by [17, Théorème 1] that

$$|\overline{E_p}(\mathbb{F}_p)| = p + 1 - \left(\frac{2}{p}\right) \left(\frac{u}{p}\right) \left(\frac{c}{p}\right) u, \quad (2.8)$$

where $\left(\frac{a}{b}\right)$ is the Legendre symbol, and the integer u is such that $4p = u^2 - Dv^2$. In this case it is easy to see that if $u = 1$, then every integer c such that $\left(\frac{2}{p}\right) \left(\frac{c}{p}\right) = -1$ gives $|\overline{E_p}(\mathbb{F}_p)| = p$. For example for $D = -43$ the following primes are of the form $1 + 43v^2$: $p = 11, 97, 269, 1301, \dots$

Example 2.9 When $D = -1$ or -2 , it follows that $\pi + \bar{\pi}$ is always an even integer, and hence the equality $|\overline{E_p}(\mathbb{F}_p)| = p$ never happens. That is, any extension F_0 satisfying the assumptions of Theorem 1.6 has positive degree. For example, consider the family of elliptic curves given by the Weierstrass equation $y^2 = x^3 + (3 + 5n)x$, with $n \in \mathbb{Z}$, which has potential complex multiplication by $\mathbb{Z}[i]$. Consider the prime $p = 5$, which splits completely in $\mathbb{Q}(i)$. A SAGE computation shows that if E is any elliptic curve in the family, then $p \mid |\overline{E_p}(\mathbb{F}_{p^2})|$.

2.2 0-cycles and Somekawa K -groups

Let X be a smooth projective variety over a perfect field k . We consider the Chow group of 0-cycles, $\text{CH}_0(X)$. We recall that this group has a filtration

$$\text{CH}_0(X) \supset F^1(X) \supset F^2(X) \supset 0,$$

where $F^1(X) := \ker(\deg : \text{CH}_0(X) \rightarrow \mathbb{Z})$ is the kernel of the degree map, and $F^2(X) := \ker(\text{alb}_X : F^1(X) \rightarrow \text{Alb}_X(k))$ is the kernel of the Albanese map. When $X = C_1 \times C_2$ is a product of two smooth projective, geometrically connected curves over k such that $X(k) \neq \emptyset$, Raskind and Spiess [29, Theorem 2.2, Corollary 2.4.1] showed an isomorphism

$$F^2(X) \simeq K(k; J_1, J_2), \quad (2.10)$$

where $K(k; J_1, J_2)$ is the Somekawa K -group attached to the Jacobian varieties J_1, J_2 of C_1, C_2 . The group $K(k; J_1, J_2)$, defined by Kato and Somekawa in [38], is a quotient of $\bigoplus_{L/k \text{ finite}} J_1(L) \otimes J_2(L)$ by two relations. The first relation is known as *projection formula* and the second as *Weil reciprocity*. In this article we won't make explicit use of these relations, and hence we omit the precise definition (see [29, Definition 2.1.1] and the footnote on p. 10 for a correction to Somekawa's original definition).

Example 2.11 Suppose that $X = E \times E$ is the self-product of an elliptic curve E over k . We denote by $K_2(k; E)$ the group $K(k; E, E)$. Moreover we will denote by O the zero element of E . The Albanese kernel $F^2(X)$ is generated by 0-cycles of the form

$$w_{P, Q} := f_{L/k\star}([P, Q] - [P, O] - [Q, O] + [O, O]),$$

where L/k runs through all finite extensions of k , $P, Q \in E(L)$, and $f_{L/k}$ is the proper push-forward $\text{CH}_0(X_L) \xrightarrow{f_{L/k}} \text{CH}_0(X)$. The isomorphism (2.10) sends the 0-cycle $w_{P,Q}$ to the symbol $\{P, Q\}_{L/k}$. From now on we identify these two objects.

2.3 Weak approximation for 0-cycles

Let X be a smooth projective geometrically connected variety over a number field F . Let $v \in \Omega_f(F)$. There is a local pairing,

$$\langle \cdot, \cdot \rangle_v : \text{CH}_0(X_v) \times \text{Br}(X_v) \rightarrow \text{Br}(F_v) \simeq \mathbb{Q}/\mathbb{Z}$$

called the *Brauer–Manin pairing* defined as follows. For a closed point $P \in X_v$ and a Brauer class $\alpha \in \text{Br}(X_v)$, the pull-back of α along P is denoted by $\alpha(P) \in \text{Br}(F_v(P))$, where $F_v(P)$ is the residue field of P . The pairing $\langle \cdot, \cdot \rangle_v$ is defined on points by $\langle P, \alpha \rangle_v := \text{Cor}_{F_v(P)/F_v}(\alpha(P))$ and it factors through rational equivalence (cf. [5, p. 4]). Here $\text{Cor}_{F_v(P)/F_v}$ is the Corestriction map of Galois cohomology (cf. [32, VIII.2]).

Definition 2.12 Suppose that F is totally imaginary. The adelic Chow group $\text{CH}_{0,\mathbf{A}}(X)$ is defined to be the product $\text{CH}_{0,\mathbf{A}}(X) := \prod_{v \in \Omega_f(F)} \text{CH}_0(X_v)$. Similarly, we define $F_{\mathbf{A}}^1(X) = \prod_{v \in \Omega_f(F)} F^1(X_v)$ and $F_{\mathbf{A}}^2(X) = \prod_{v \in \Omega_f(F)} F^2(X_v)$.

When F is not totally imaginary, it follows by [5, Théorème 1.3] that the group $\text{CH}_{0,\mathbf{A}}(X)$ has a small (2-torsion) contribution from the infinite real places. In this article we will mainly be working over totally imaginary number fields, and hence we omit the more general definition. For more details see [12, Definition 5.2].

The local pairings induce a global pairing,

$$\langle \cdot, \cdot \rangle : \text{CH}_{0,\mathbf{A}}(X) \times \text{Br}(X) \rightarrow \mathbb{Q}/\mathbb{Z},$$

defined by $\langle (z_v)_v, \alpha \rangle = \sum_v \text{inv}_v(\langle z_v, \iota_v^*(\alpha) \rangle_v)$, where ι_v^* is the pullback of $\iota_v : X_v \rightarrow X$. The short exact sequence of global class field theory,

$$0 \rightarrow \text{Br}(F) \rightarrow \bigoplus_{v \in \Omega} \text{Br}(F_v) \xrightarrow{\sum \text{inv}_v} \mathbb{Q}/\mathbb{Z} \rightarrow 0,$$

implies that the group $\text{CH}_0(X)$ lies in the left kernel of $\langle \cdot, \cdot \rangle$. Thus, we obtain a complex,

$$\text{CH}_0(X) \xrightarrow{\Delta} \text{CH}_{0,\mathbf{A}}(X) \rightarrow \text{Hom}(\text{Br}(X), \mathbb{Q}/\mathbb{Z}), \quad (2.13)$$

where Δ is the diagonal map. Conjecture 1.1 then predicts that the complex (2.13) becomes exact after passing to the completions; namely that the induced complex

$$\widehat{\text{CH}_0(X)} \xrightarrow{\Delta} \widehat{\text{CH}_{0,\mathbf{A}}(X)} \rightarrow \text{Hom}(\text{Br}(X), \mathbb{Q}/\mathbb{Z}) \quad (2.14)$$

is exact.

Next we consider the filtration $\mathrm{Br}(X) \supset \mathrm{Br}_1(X) \supset \mathrm{Br}_0(X)$ induced by the Hochschild-Serre spectral sequence, where $\mathrm{Br}_1(X) := \ker(\mathrm{Br}(X) \rightarrow \mathrm{Br}(X_{\overline{F}}))$ is the *algebraic Brauer group* of X , and $\mathrm{Br}_0(X) = \mathrm{Im}(\mathrm{Br}(F) \rightarrow \mathrm{Br}(X))$ are the constants. When X has a F -rational point, the exactness of (2.14) is reduced to the exactness of the induced complex,

$$\widehat{F^1(X)} \xrightarrow{\Delta} \widehat{F_A^1(X)} \xrightarrow{\varepsilon} \mathrm{Hom}(\mathrm{Br}(X)/\mathrm{Br}_0(X), \mathbb{Q}/\mathbb{Z}). \quad (2.15)$$

When X is a product of elliptic curves more can be said.

Proposition 2.16 *Let $X = E_1 \times \cdots \times E_d$ be a product of elliptic curves over a number field F . Let G_F be the absolute Galois group of F . Suppose that the Néron-Severi group $\mathrm{NS}(X_{\overline{F}})$ of the base change to the algebraic closure of F has trivial G_F -action. Then the restriction of the map $\varepsilon : F^1(X) \rightarrow \mathrm{Hom}(\mathrm{Br}(X)/\mathrm{Br}_0(X), \mathbb{Q}/\mathbb{Z})$ to the Albanese kernel $F^2(X)$ factors through the group $\mathrm{Hom}(\mathrm{Br}(X)/\mathrm{Br}_1(X), \mathbb{Q}/\mathbb{Z})$.*

Proof We need to show that for every $z \in F^2(X)$ and every $\alpha \in \mathrm{Br}_1(X)/\mathrm{Br}_0(X)$, it follows $\langle z, \alpha \rangle = 0$. A direct computation of the Hochschild-Serre spectral sequence gives an isomorphism $\mathrm{Br}_1(X)/\mathrm{Br}_0(X) \simeq H^1(F, \mathrm{Pic}(X_{\overline{F}}))$. The G_F -module $\mathrm{Pic}(X_{\overline{F}})$ fits into a (splitting) short exact sequence

$$0 \rightarrow \mathrm{Pic}^0(X_{\overline{F}}) \rightarrow \mathrm{Pic}(X_{\overline{F}}) \rightarrow \mathrm{NS}(X_{\overline{F}}) \rightarrow 0.$$

Since X is an abelian variety, the group $\mathrm{NS}(X_{\overline{F}})$ is torsion free, and hence a finitely generated free abelian group. Since we assumed that G_F acts trivially on it, it follows that $H^1(F, \mathrm{NS}(X_{\overline{F}})) = 0$. Thus, we obtain an isomorphism

$$H^1(F, \mathrm{Pic}(X_{\overline{F}})) \simeq H^1(F, X_{\overline{F}}) \simeq \bigoplus_{i=1}^d H^1(k, E_i).$$

For $i = 1, \dots, d$, let $\mathrm{pr}_i : X \rightarrow E_i$ be the projection. The map pr_i is proper and it induces a pushforward $\mathrm{pr}_{i*} : \mathrm{CH}_0(X) \rightarrow \mathrm{CH}_0(E_i)$ on Chow groups and a pullback $\mathrm{pr}_i^* : \mathrm{Br}(E_i) \rightarrow \mathrm{Br}(X)$ on Brauer groups. Since the Brauer-Manin pairing is defined just by evaluation, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{CH}_{0,A}(X) & \longrightarrow & \mathrm{Hom}(\mathrm{Br}(X), \mathbb{Q}/\mathbb{Z}) \\ \downarrow \mathrm{pr}_{i*} & & \downarrow \mathrm{Hom}(\mathrm{pr}_i^*, \mathbb{Q}/\mathbb{Z}) \\ \mathrm{CH}_{0,A}(E_i) & \longrightarrow & \mathrm{Hom}(\mathrm{Br}(E_i), \mathbb{Q}/\mathbb{Z}). \end{array}$$

That is, for $z \in \mathrm{CH}_0(X)$ and $\beta \in \mathrm{Br}(E_i)$ we have an equality $\langle z, \mathrm{pr}_i^*(\alpha) \rangle = \langle \mathrm{pr}_{i*}(z), \alpha \rangle$. Moreover, both homomorphisms preserve the two piece filtrations of CH_0 and Br . The pullbacks p_i^* induce a homomorphism

$$\bigoplus_{i=1}^d \mathrm{Br}_1(E_i)/\mathrm{Br}_0(E_i) \xrightarrow{\oplus \mathrm{pr}_i^*} \mathrm{Br}_1(X)/\mathrm{Br}_0(X).$$

Our previous analysis shows that this is in fact an isomorphism. We compute

$$\langle z, \text{pr}_i^*(\alpha) \rangle = \langle \text{pr}_{i\star}(z), \alpha \rangle = 0.$$

The vanishing follows, because $\text{pr}_{i\star}(z) \in F^2(E_i) = 0$, since E_i is a curve. \square

Corollary 2.17 *Let $X = E \times E$ be the self-product of an elliptic curve over a number field F . Suppose that E has complex multiplication defined over F by the full ring of integers of a quadratic imaginary field K . Then the assumption of Proposition 2.16 is satisfied.*

Proof Because we assumed that F contains the quadratic imaginary field K , it follows by [37, p. (120), Eq. (10)] that $\text{NS}(X_{\overline{F}})$ is a trivial G_F -module. \square

Proposition 2.16 shows that the complex (2.15) induces a complex

$$\widehat{F^2(X)} \xrightarrow{\Delta} \widehat{F_A^2(X)} \xrightarrow{\varepsilon} \text{Hom}(\text{Br}(X)/\text{Br}_1(X), \mathbb{Q}/\mathbb{Z}). \quad (2.18)$$

Combining Proposition 2.16 with [12, Proposition 5.6] yields the following corollary.

Corollary 2.19 *The exactness of (2.15) can be reduced to the exactness of (2.18).*

We note that this corollary was claimed by the main author and T. Hiranouchi in [12, Proposition 5.6]. It was brought to our attention however that the argument there was not enough. Proposition 2.16 was a key missing ingredient. We note that such a reduction cannot be made in general for other classes of varieties, for example del Pezzo surfaces, or $K3$ surfaces.

3 Local results

In this section we are going to prove Theorem 1.5 and also obtain some necessary local information in order to prove Theorems 1.6 and 1.7 in the next section.

3.1 Proof of Theorem 1.5

In this subsection k will denote a finite extension of \mathbb{Q}_p . We will often assume that p is odd. Let X be a smooth projective geometrically connected variety over k . We will denote by $F^2(X)_{\text{div}}$ the maximal divisible subgroup of the Albanese kernel $F^2(X)$ and by $F^2(X)_{\text{nd}}$ the quotient $F^2(X)/F^2(X)_{\text{div}}$. We have a decomposition,

$$F^2(X) = F^2(X)_{\text{div}} \oplus F^2(X)_{\text{nd}}.$$

The subgroup $F^2(X)_{\text{nd}}$ is expected to be finite (cf. [29, Conjecture 3.5.4], see also [5, 1.4(g)]). When $X = E_1 \times E_2$ is the product of two elliptic curves, this conjecture has been established in a large number of cases. In particular, the following are true.

- (1) When X has good reduction, the group $F^2(X)$ is m -divisible for every integer m coprime to p ([29, Theorem 3.5]).
- (2) Suppose $p \geq 3$, X has split semistable reduction and at most one of the curves has good supersingular reduction. Then the group $F^2(X)_{\text{nd}}$ is finite ([29, Theorem 1.1], [10, Theorem 1.2]).
- (3) Suppose $p \geq 3$, k is unramified over \mathbb{Q}_p , X has good reduction and at most one of the curves has good supersingular reduction. Then $F^2(X)_{\text{nd}} = 0$ ([12, Theorem 1.4]).

The finiteness of $F^2(X)_{\text{nd}}$ yields an equality $F^2(X)_{\text{nd}} = \widehat{F^2(X)}$. In the special case when X has good reduction, it follows that the group $F^2(X)_{\text{nd}}$ has p -power order. Suppose $F^2(X)_{\text{nd}} = p^N$ for some $N \geq 0$. Then $F^2(X)_{\text{nd}} \simeq F^2(X)/p^N$.

We are now ready to prove Theorem 1.5, which we restate here.

Theorem 3.1 *Let $X = E_1 \times E_2$ be a product of elliptic curves over a number field F . Suppose that the action of the absolute Galois group G_F on the Néron-Severi group $\text{NS}(X_{\overline{F}})$ is trivial. Then, there is an infinite set T of rational primes p for which the group $\varprojlim_n F_{\mathbf{A}}^2(X)/p^n$ vanishes. In particular, the complex (1.4) is exact for every $p \in T$. If we further assume that at least one of the curves does not have potential complex multiplication, then the complement S of T is a thin set of primes.*

Proof The proof will be along the lines of [12, Lemma 5.9]. Let p be an odd prime and suppose that for every place v above p the surface X_v has good reduction. It follows by Sect. 3.1 (1) that the only factors of $F_{\mathbf{A}}^2(X)$ that might not be p -divisible correspond to those places v above p and to the places of bad reduction. Let $\Lambda = \{v \text{ place of bad reduction}\}$. Then for every $n \geq 1$ we have,

$$F_{\mathbf{A}}^2(X)/p^n = \prod_{v|p} F^2(X)/p^n \times \prod_{v \in \Lambda} F^2(X)/p^n.$$

Let $v \in \Lambda$ be a place of bad reduction. Then there exists a finite extension L_v/F_v such that the base change X_{L_v} has split semistable reduction. This means that either both elliptic curves $E_i|_{L_v}$ have good reduction, or if any of them has bad reduction, then it has split multiplicative reduction. In the former case, since $v \nmid p$, it follows by [29, Theorem 3.5] that the group $F^2(X_{L_v})$ is p -divisible. In the latter case, it follows by [10, Theorem 1.2]) that the group $F^2(X_{L_v})_{\text{nd}}$ is finite. Write N_v for its order. To unify notation, we set $N_v = 1$ for the case of potentially good reduction. Consider the following positive integer,

$$M = \prod_{v \in \Lambda} [L_v : F_v] \prod_{v \in \Lambda} N_v.$$

We claim that for every prime p which is coprime to M and for every $v \in \Lambda$ the group $F^2(X_v)$ is p -divisible. Consider the projection $X_{L_v} \xrightarrow{\pi_{L_v/F_v}} X_v$, and let $\text{CH}_0(X_{L_v}) \xrightarrow{\pi_{L_v/F_v}^*} \text{CH}_0(X_v)$, and $\text{CH}_0(X_v) \xrightarrow{\pi_{L_v/F_v}^*} \text{CH}_0(X_{L_v})$ be the induced push-forward and pull back maps respectively. Then we have an equality $\pi_{L_v/F_v}^* \circ \pi_{L_v/F_v}^* =$

$[L_v : F_v]$. Since p is coprime to $[L_v : F_v]$, it follows that the pull back map induces an injective map of \mathbb{F}_p -vector spaces

$$F^2(X_v)/p \xrightarrow{\pi_{L_v/F_v}^*} F^2(X_{L_v})/p.$$

By our choice of p , it follows that the group $F^2(X_{L_v})$ is p -divisible, and hence so is $F^2(X_v)$.

As a conclusion, for every prime $p \nmid M$ such that for every place v above p the surface X_v has good reduction, we have an isomorphism

$$\varprojlim_n F_A^2(X)/p^n \simeq \prod_{v|p} \varprojlim_n F^2(X_v)/p^n.$$

Let T_0 be the set of odd primes p such that for every place v above p the abelian surface X_v has good reduction, at most one of the curves E_{1v}, E_{2v} has good supersingular reduction and $p \nmid M$. Then it follows by Sect. 3.1 (2) that for every $p \in T_0$ and for every place $v|p$ the group $F^2(X)_{\text{nd}}$ is finite of p -power order. Thus, we have an isomorphism

$$\varprojlim_n F_A^2(X)/p^n = \prod_{v|p} F^2(X_v)_{\text{nd}}. \quad (3.2)$$

If we further assume that for each place $v|p$ the extension F_v/\mathbb{Q}_p is unramified, then it follows by [12, Theorem 1.4] that the group $F^2(X_v)_{\text{nd}}$ vanishes. Consider the set

$$T = T_0 \setminus \{p : \text{ramified prime}\}.$$

Then for every $p \in T$, $\varprojlim_n F_A^2(X)/p^n = 0$ and the complex (1.4) is exact.

Note that the set T_0 is infinite, since it contains all primes p such that for every place v above p both elliptic curves have good ordinary reduction. Since the set of ramified primes is finite, it follows that T is an infinite set of primes.

Next suppose that one of the curves does not have potential complex multiplication; without loss of generality, assume $\text{End}(E_{1\bar{\mathbb{Q}}}) = \mathbb{Z}$. Then the set of primes p which are such that the curve E_{1v} has good supersingular reduction for every place v above p is a set of primes of density zero (cf. [21, 33]). We conclude that the complement S of T is a set of primes of density zero. \square

3.2 Computing the local Albanese kernel over ramified base fields

Throughout this subsection E will be an elliptic curve defined over a finite extension k of \mathbb{Q}_p . We assume that E has **good ordinary reduction**. We will denote by \widehat{E} the formal group of E and by \overline{E} the reduction of E , which is an ordinary elliptic curve over the finite field \mathbb{F}_k . Moreover, we will denote by e the absolute ramification index

of k . The purpose of this subsection is to obtain some explicit information on the group $F^2(X)_{\text{nd}} = \widehat{F^2(X)}$.

3.2.1 Decomposition of local points

We first obtain some information on points $P \in E(k)$, which will be of use in Sect. 4.2. Since the elliptic curve E has good ordinary reduction, for every integer $n \geq 1$ we have a short exact sequence of $\text{Gal}(\bar{k}/k)$ -modules.

$$0 \rightarrow \widehat{E}[p^n] \rightarrow E[p^n] \rightarrow \overline{E}[p^n] \rightarrow 0, \quad (3.3)$$

where as \mathbb{Z} -modules both $\widehat{E}[p^n]$ and $\overline{E}[p^n]$ are isomorphic to \mathbb{Z}/p^n . The sequence 3.3 is also known as the *connected-étale* exact sequence. In general this sequence does not split, but it does when $E[p^n] \subset E(k)$, and unconditionally on k if E has complex multiplication ([31, A.2.4]). In particular it splits when E satisfies the assumptions of Sect. 2.1. We assume we are in the CM situation. We additionally suppose that k is an unramified extension of \mathbb{Q}_p and $\overline{E}[p] \subset \overline{E}(\mathbb{F}_k)$. We consider the exact sequence

$$0 \rightarrow \widehat{E}(\mathfrak{m}_k) \rightarrow E(k) \xrightarrow{r} \overline{E}(\mathbb{F}_k) \rightarrow 0, \quad (3.4)$$

where $E(k) \xrightarrow{r} \overline{E}(\mathbb{F}_k)$ is the reduction map. The group $\overline{E}(\mathbb{F}_k)$ is finite, thus it decomposes as $\overline{E}(\mathbb{F}_k) \simeq \overline{E}(\mathbb{F}_k)\{p\} \oplus \overline{E}(\mathbb{F}_k)\{m\}$, for some large enough integer $m \geq 1$ coprime to p . Because E has good reduction, it follows by the criterion of Néron-Ogg-Shafarevich [35, Theorem 7.1] that the coprime-to- p torsion subgroup of $E(k)$ is isomorphic to $\overline{E}(\mathbb{F}_k)\{m\}$. Moreover, since \overline{E} is an ordinary elliptic curve and we assumed $\overline{E}[p] \subset \overline{E}(\mathbb{F}_k)$, it follows that $\overline{E}(\mathbb{F}_k)\{p\} \simeq \overline{E}[p^{N_0}]$ for some integer $N_0 \geq 1$. In particular, the group $\overline{E}(\mathbb{F}_k)\{p\}$ is cyclic of order p^{N_0} . The splitting of (3.3) implies that the map $E[p^{N_0}](k) \xrightarrow{r} \overline{E}[p^{N_0}](\mathbb{F}_k)$ is surjective. Since we assumed that k/\mathbb{Q}_p is unramified, it follows by [35, Theorem 6.1] that $\widehat{E}[p] = 0$, and hence this map is an isomorphism. We conclude that the reduction map r induces an isomorphism on torsion subgroups

$$E(k)_{\text{tor}} \simeq \overline{E}(\mathbb{F}_k)_{\text{tor}},$$

and hence the short exact sequence (3.4) has a natural splitting. Moreover, if L/k is any finite extension, this splitting commutes with the restriction map $E(k) \xrightarrow{\text{res}_{L/k}} E(L)$. It also induces a split short exact sequence

$$0 \rightarrow \widehat{E}(\mathfrak{m}_k)/p \rightarrow E(k)/p \xrightarrow{r} \overline{E}(\mathbb{F}_k)/p \rightarrow 0.$$

This splitting can be made more explicit as follows. We have an isomorphism,

$$\overline{E}(\mathbb{F}_k)/p \simeq \overline{E}[p^{N_0}]/\overline{E}[p^{N_0-1}] \simeq \overline{E}[p].$$

We fix a generator \overline{P}_0 of $\overline{E}[p^{N_0}](\mathbb{F}_k)$ and its unique lift $P_0 \in E[p^{N_0}](k)$. Let $P \in E(k)$. There exists an integer $c \in \{0, 1, \dots, p^{N_0} - 1\}$ such that $r(P \bmod p) - r(cP_0 \bmod p) = 0$. This implies that P has an expression as $P = \widehat{P} + cP_0 + pQ$ for some points $Q \in E(k)$, $\widehat{P} \in \widehat{E}(\mathfrak{m}_k)$.

Notation 3.5 From now we will abuse notation and for a point $P \in E(k)$ we will denote also by P its image in $E(k)/p$. The above discussion shows that P has a unique decomposition as $P = (\widehat{P}, \overline{P})$ where $\widehat{P} \in \widehat{E}(\mathfrak{m}_k)/p$ and $\overline{P} := r(cP_0 \bmod p) \in \overline{E}(\mathbb{F}_k)/p$. It is clear by the construction that this decomposition is compatible with the restriction map $\text{res}_{L/k}$ for finite extensions L/k . Namely, $\text{res}_{L/k}(P) = (\text{res}_{L/k}(\widehat{P}), \text{res}_{\mathbb{F}_L/\mathbb{F}_k}(\overline{P}))$.

3.2.2 Explicit isomorphism

In this subsection we consider a finite extension L/k such that $E[p^n] \subset E(L)$ for some $n \geq 1$. It follows by [29, Sect. 4] (see also [14, Theorem 4.2], [15, Theorem 3.4]) that we have an isomorphism

$$F^2(X_L)_{\text{nd}}/p^n = F^2(X_L)/p^n \simeq K_2(L; E)/p^n \simeq \mathbb{Z}/p^n\mathbb{Z}. \quad (3.6)$$

Let $N = \max\{n \geq 1 : E[p^n] \subset E(L)\}$. If we further assume that the extension L ($E[p^{N+1}])/L$ has wild ramification, it follows by [10, Theorem 3.14] that we have an isomorphism

$$\widehat{F^2(X_L)} = F^2(X_L)_{\text{nd}} = F^2(X_L)/p^N \simeq \mathbb{Z}/p^N. \quad (3.7)$$

The case of interest to us is when $N = 1$. To prove Theorem 1.6, the above information is enough. However, in order to construct global 0-cycles and prove Theorem 1.7, we need to recall the explicit construction of the isomorphism $K_2(L; E_L)/p \simeq \mathbb{Z}/p\mathbb{Z}$. We are particularly interested in describing necessary and sufficient conditions for a symbol $\{P, Q\}_{L/L} \in K_2(L; E_L)/p$ to be nontrivial.

The group $K_2(L; E_L)$ is defined to be the quotient of the Mackey product $(E_L \otimes^M E_L)(L)$ (cf. [12, Sect. 2.1]) modulo Weil reciprocity. It follows by [29] (see also [14, Theorem 4.2]) that when $E[p] \subset E(L)$ we have an isomorphism

$$K_2(L; E_L) \simeq (E_L \otimes^M E_L)(L)/p.$$

The Mackey functor E_L/p has a direct decomposition $E_L/p \simeq \widehat{E_L}/p \oplus [E_L/\widehat{E_L}]/p$, induced by the splitting short exact sequences

$$0 \rightarrow \widehat{E_L}(m_{L'})/p \rightarrow E_L(L')/p \rightarrow E_L(\mathbb{F}_{L'}/p) \rightarrow 0,$$

where L'/L is any finite extension. For the definition of the Mackey functor $[E_L/\widehat{E_L}]$ we refer to [10, Proof of Theorem 3.14]. It follows by [29, Lemma 3.4.2] and [10, Proof of Theorem 3.1.4] respectively that the Mackey products $([E_L/\widehat{E_L}] \otimes^M [E_L/\widehat{E_L}])(k)$,

$(\widehat{E}_L \otimes^M [E_L/\widehat{E}_L])(L)/p$, and $([E_L/\widehat{E}_L] \otimes^M E_L)(k)/p$ all vanish. Thus we have an isomorphism

$$K_2(L; E_L)/p \simeq (\widehat{E}_L \otimes^M \widehat{E}_L)(k)/p = (\widehat{E}_L/p \otimes^M \widehat{E}_L/p)(k).$$

The upshot is the following, which will be used in Sect. 4.2. Let k/\mathbb{Q}_p be a finite unramified extension like in the previous subsection and let $P \in E(k)/p$. Consider the restriction of P in $E(L)/p$, which for simplicity we will denote again by P . Consider the decomposition $P = (\widehat{P}, \overline{P})$ as in notation (3.5). Let $\widehat{Q} \in \widehat{E}_L(\mathfrak{m}_L)/p$. Then we have,

$$\{P, \widehat{Q}\}_{L/L} = \{\widehat{P}, \widehat{Q}\}_{L/L} \in K_2(L; E_L)/p. \quad (3.8)$$

Next we analyze the Mackey functor \widehat{E}_L/p . The inclusion $E[p] \subset E(L)$ implies $\mu_p \subset L^\times$, and $\widehat{E}[p] \subset \widehat{E}_L(\mathfrak{m}_L)$. We fix a primitive p -th root of unity $\zeta_p \in L^\times$ and a non-canonical isomorphism of $\text{Gal}(\overline{L}/L)$ -modules $\widehat{E}[p] \simeq \mathbb{Z}/p \simeq \mu_p$. This induces an isomorphism

$$H^1(L, \widehat{E}_L[p]) \simeq H^1(L, \mu_p) = L^\times/L^{\times p}.$$

We consider the connecting homomorphism of the Kummer sequence for \widehat{E}_L (cf. [12, Lemma 3.5])

$$\delta_L : \widehat{E}_L(L)/p \hookrightarrow H^1(L, \widehat{E}_L[p]).$$

Let U_L^1 be the group of 1-units of L^\times with its natural filtration $\{U_L^i = 1 + \mathfrak{m}_L^i\}_{i \geq 1}$ and define

$$\overline{U}_L^i = \text{Im}(U_L^i \rightarrow L^\times/L^{\times p}), \quad i \geq 1.$$

It then follows by [19, Theorem 2.1.6], (see also [12, Proposition 3.13]) that the homomorphism δ_L induces an isomorphism

$$\delta_L : \widehat{E}_L(L)/p \xrightarrow{\sim} \overline{U}_L^1, \quad (3.9)$$

and the same holds over any finite extension L'/L . In fact we have an isomorphism as Mackey functors $\widehat{E}_L/p \simeq \overline{U}_L^1$.

Additionally, δ_L is a filtered isomorphism in the following sense. The formal group $\widehat{E}_L(\mathfrak{m}_L)$ has a natural filtration $\widehat{E}_L^i(L) := \widehat{E}_L(\mathfrak{m}_L^i)$, for $i \geq 1$. This induces a filtration on the group $\widehat{E}_L(\mathfrak{m}_L)/[p] = \widehat{E}_L^1(L)/p$ by defining (cf. [12, Definition 3.10]),

$$\mathcal{D}^i := \frac{\widehat{E}_L^i(L)}{[p]\widehat{E}_L(L) \cap \widehat{E}_L^i(L)}, \quad i \geq 1.$$

Then the isomorphism (3.9) has the property that $\delta_L(\mathcal{D}^i) \subset \overline{U}_L^i$, for all $i \geq 1$. Moreover, it is functorial with respect to norm maps associated with finite extensions L'/L .

Since $\mu_p \subset L^\times$, we have isomorphisms $H^2(L, \mu_p \otimes \mu_p) \simeq H^2(L, \mu_p) \simeq \text{Br}(L)_p \simeq \mathbb{Z}/p$. For $a, b \in L^\times/L^{\times p}$ write $(a, b)_p \in \text{Br}(L)_p$ for the cyclic symbol algebra generated by a, b . Then we have an isomorphism

$$s_p : (\widehat{E}_L/p \otimes^M \widehat{E}_L/p)(k) \rightarrow H^2(L, \mu_p) = \text{Br}(L)_p \\ \{\widehat{P}, \widehat{Q}\}_{L/L} \mapsto (\delta(\widehat{P}), \delta(\widehat{Q}))_p, \quad (3.10)$$

known as *the generalized Galois symbol*. For a proof of the injectivity of s_p see for example [14, Theorem 4.2].

3.2.3 Criterion for nontriviality

It follows that a symbol $\{\widehat{P}, \widehat{Q}\}_{L/L}$ is nonzero in $K_2(L; E_L)/p$ if and only if $\delta_L(\widehat{P})$ is not in the image of the norm map

$$N : L\left(\delta_L(\widehat{Q})^{1/p}\right)^\times \rightarrow L^\times,$$

or equivalently if and only if \widehat{P} is not in the image of the norm map

$$N : \widehat{E}_L\left(L\left(\frac{1}{p}\widehat{Q}\right)\right)/p \rightarrow \widehat{E}_L(L)/p.$$

Here we denoted by $L\left(\frac{1}{p}\widehat{Q}\right)$ the smallest Galois extension of L over which there exists a point \widehat{Q}' such that $p\widehat{Q}' = \widehat{Q}$. The same equivalence holds with the roles of \widehat{P}, \widehat{Q} interchanged.

4 Self-product of an elliptic curve with complex multiplication

In this subsection we are going to prove Theorems 1.6 and 1.7. Throughout this section we are making the following assumption.

Assumption 4.1 K will be a quadratic imaginary field of class number one. E will be an elliptic curve over \mathbb{Q} or K with CM by \mathcal{O}_K and $p \geq 5$ will be an ordinary prime for E . Moreover, we fix a factoring $p = \pi\bar{\pi}$ into prime elements of \mathcal{O}_K such that the endomorphism $\pi : E_K \rightarrow E_K$ reduces to the Frobenius automorphism $\phi_p : \overline{E}_p \rightarrow \overline{E}_p$.

4.1 Local 0-cycles orthogonal to the Brauer group

We are now ready to prove Theorem 1.6, which we restate here.

Theorem 4.2 *Let $X = E \times E$. Suppose there exists a finite Galois extension F_0/K of degree $n < p-1$ such that there is a unique inert place w of F_0 above π with the property that p divides $|\overline{E_p}(\mathbb{F}_w)|$, where \mathbb{F}_w is the residue field of F_0 at w . Consider the extension $L := F_0 \cdot K(E[\pi])$. Then the group $\varprojlim_n F_A^2(X_L)/p^n$ has the following properties.*

- (1) *It is equal to $\prod_{v|p} F^2(X_{L_v})_{\text{nd}}$ and isomorphic to $\mathbb{Z}/p \oplus \mathbb{Z}/p$.*
- (2) *It is orthogonal to the transcendental Brauer group $\frac{\text{Br}(X_L)\{p\}}{\text{Br}_1(X_L)\{p\}}$.*

Proof The proof involves three main steps.

Claim 1: There is an isomorphism $\prod_{v|p} F^2(X_{L_v})_{\text{nd}} \simeq \mathbb{Z}/p \oplus \mathbb{Z}/p$.

It follows by [30, Corollary 5.20 (ii), (iii)] that $K(E[\pi])/K$ is a Galois extension of degree $p-1$ and it is totally ramified above $\mathfrak{p} = (\pi)$. Since F_0/K is unramified above π , the extensions $F_0, K(E[\pi])$ are totally disjoint and hence $\text{Gal}(L/K) \simeq \text{Gal}(F_0/K) \times \text{Gal}(K(E[\pi])/K)$. In particular, L/K is a Galois extension of degree $n(p-1) < (p-1)^2$, and there exists a unique place v of L above π with ramification index $p-1$ and residue field \mathbb{F}_{w_0} of degree n over \mathbb{F}_p . Moreover, the extension L/\mathbb{Q} is Galois, and hence there exists a unique place \bar{v} above $\bar{\pi}$ with the same properties and these are precisely the places of L that lie above p . The extensions L_v and $L_{\bar{v}}$ are the same. It is enough therefore to prove an isomorphism $\widehat{F^2(X_{L_v})} \simeq \mathbb{Z}/p\mathbb{Z}$.

We will simply denote by E_v (resp. $E_{\bar{v}}$) the base change E_{L_v} (resp. $E_{L_{\bar{v}}}$) which is an elliptic curve with good ordinary reduction over the p -adic field L_v/\mathbb{Q}_p . We will denote by \mathfrak{m}_v the maximal ideal of \mathcal{O}_{L_v} , $\widehat{E_v}$ will be the formal group of E_v and $\overline{E_v}$ the reduction. We claim that $E_v[p] \subset E_v(L_v)$. As noted in Sect. 2.1, the subgroup $E_{\mathbb{Q}_p}[\pi]$ of $E_{\mathbb{Q}_p}[p]$ coincides with the p -torsion of the formal group $\widehat{E_{\mathbb{Q}_p}}[p]$. It follows that $E_v[\pi]$ coincides with $\widehat{E_v}[p]$, and hence it is L_v -rational. Since the residue field of L_v/\mathbb{Q}_p is \mathbb{F}_{w_0} , the assumption that p divides $|\overline{E_p}(\mathbb{F}_{w_0})|$ implies that $\overline{E_p}[p] \subseteq \overline{E_p}(\mathbb{F}_{w_0})$. The inclusion $E_v[p] \subset E_v(L_v)$ then follows by the splitting short exact sequence

$$0 \rightarrow \widehat{E_v}[p] \rightarrow E_v[p] \rightarrow \overline{E_p}[p] \rightarrow 0.$$

The desired isomorphism $\widehat{F^2(X_{L_v})} \simeq \mathbb{Z}/p\mathbb{Z}$ follows by (3.7). More precisely, the above argument shows that we have an inequality $N \geq 1$. We claim that $N = 1$. It is enough to show that the extension $L_v(E[p^2])/L_v(E[p])$ has wild ramification. But this is clear, since $L_v(E[p^2])$ contains $L_v(\mu_{p^2})$, which has absolute ramification index dividing $p(p-1)$, while $L_v = L_v(E[p])$ has absolute ramification index $p-1$.

Claim 2: There is an isomorphism $\varprojlim_n F_{\mathbf{A}}^2(X_L)/p^n \simeq \prod_{v|p} F^2(X_{L_v})_{\text{nd}}$.

We use the notation introduced in the proof of Theorem 3.1. Namely, let

$$M = \prod_{v_0 \in \Lambda} n_{v_0} \prod_{v_0 \in \Lambda} N_{v_0},$$

where Λ is the set of all bad reduction places of E_L , n_{v_0} is the degree of an extension L'_{v_0}/L_{v_0} over which the elliptic curve $E_{L'_{v_0}}$ attains split semistable reduction and $N_{v_0} = 1$ in the potentially good reduction case, $N_{v_0} = |F^2(X_{L'_{v_0}})_{\text{nd}}|$ otherwise. To prove the claim, it is enough to show that p is coprime to M , because then the proof of Theorem 3.1 gives us the desired isomorphism (cf. 3.2). Since the elliptic curve E has complex multiplication, it follows by [34, Theorem 7] that the set Λ only contains places of potentially good reduction. Thus, $N_{v_0} = 1$ for every $v_0 \in \Lambda$.

It remains to show that for each $v_0 \in \Lambda$ there exists a finite extension L'_{v_0}/L_{v_0} of degree coprime to p over which E attains good reduction. Let $v_0 \in \Lambda$ and l be the rational prime lying below v_0 . It follows by [30, Corollary 5.22] that there exists an elliptic curve E' defined over \mathbb{Q} such that E' has good reduction at l and $E_{\overline{\mathbb{Q}}} \simeq E'_{\overline{\mathbb{Q}}}$. But any two elliptic curves over \mathbb{Q} become isomorphic over a degree 6 extension. Since we assumed that $p \geq 5$, the claim follows.

Claim 3: The group $\frac{\text{Br}(X_L)\{p\}}{\text{Br}_1(X_L)\{p\}}$ is trivial.

The group $\text{Br}(X_L)/\text{Br}_1(X_L)$ is finite by [36, Theorem 1.1]. More precisely, if $G_L = \text{Gal}(\overline{L}/L)$, then Skorobogatov and Zarhin [37, Proposition 3.3] showed an isomorphism,

$$\frac{\text{Br}(X_L)_p}{\text{Br}_1(X_L)_p} \simeq \frac{\text{Hom}_{G_L}(E_L[p], E_L[p])}{(\text{Hom}(E_L, E_L)/p)^{G_L}}.$$

Since E_L has CM defined over L , $(\text{Hom}(E_L, E_L)/p)^{G_L} \simeq (\mathbb{Z}/p\mathbb{Z})^2$. We claim that this is equal to the numerator $\text{Hom}_{G_L}(E_L[p], E_L[p])$. Since by assumption $n < p - 1$, we have proper field extensions $K \subsetneq L \subsetneq K(E[p])$. It follows that $E_L[\pi]$ is the unique nonzero submodule of $E_L[p]$ with a trivial G_L -action. Hence, any G_L -equivariant homomorphism $f : E_L[p] \rightarrow E_L[p]$ must send $E_L[\pi]$ to itself. This is precisely a subgroup of rank 2 of $\text{Hom}(E_L[p], E_L[p]) \simeq (\mathbb{Z}/p\mathbb{Z})^4$ containing $(\text{Hom}(E_L, E_L)/p)^{G_L}$, and hence it must be equal to it. \square

Definition 4.3 Let F_0/K be an extension satisfying the assumptions of Theorem 4.2. Then $\mathbb{F}_{w_0} \simeq \mathbb{F}_{p^n}$. We will say that F_0 is *minimal* if it has the minimum possible degree. That is, if $p||\overline{E_p}(\mathbb{F}_{p^n})|$ and $n \geq 1$ is the smallest possible with this property.

When we construct global 0-cycles in the next subsection, we will often start with a minimal totally real extension F_0/\mathbb{Q} and apply Theorem 4.2 for $F_0 \cdot K$. When $p||\overline{E_p}(\mathbb{F}_p)|$, $F_0 = \mathbb{Q}$. In all other cases a minimal F_0 is not uniquely determined. The following proposition shows that the extension $L = F_0 \cdot K(E[\pi])$ constructed

in Theorem 1.6 is in some sense minimal over which interesting things happen at the places above the ordinary prime p .

Proposition 4.4 *Let (E, p) be a pair satisfying the assumptions of Theorem 4.2. Let F_0/\mathbb{Q} be an extension as in Theorem 4.2 of minimal degree. Let $\mathbb{Q} \subset F \subsetneq L = F_0 \cdot K(E[\pi])$ be any intermediate extension. Then $\prod_{w \in \Omega_f(F), w|p} F^2(X_{F_w})_{\text{nd}} = 0$.*

Proof Since $F \subsetneq L = F_0 \cdot K(E[\pi])$, any such field F has at most two places w above p of ramification index dividing $p - 1$. Moreover, since F is properly contained in L , and the fields F_0 and $K(E[\pi])$ are minimal with respect to their defining properties, it follows that for every place w of F above p , $E[p] \not\subset E(F_w)$. This observation reduces the proposition to the following local claim.

Claim: Let k/\mathbb{Q}_p be a finite extension such that $E[p] \not\subset E(k)$. Then we have an equality $K_2(k; E_k)/p = 0$.

Consider the finite extension $k_1 = k(E[p])$ and notice that k_1/k is a nontrivial extension of degree coprime to p . We have a commutative diagram

$$\begin{array}{ccc} K_2(k; E_k)/p & \xrightarrow{s_p} & H^2(k, E_k[p]^{\otimes 2}) \\ \downarrow \text{res}_{k_1/k} & & \downarrow \text{res}_{k_1/k} \\ K_2(k_1; E_{k_1})/p & \xrightarrow{s_p} & H^2(k_1, E_{k_1}[p]^{\otimes 2}) \end{array},$$

where s_p is the *Galois symbol* map (cf. [12, Definition 2.13]) and $\text{res}_{k_1/k}$ are the restriction maps (cf. [12, p. 7]). The bottom horizontal map is injective (cf. [14, Theorem 4.2]). Moreover, $N_{k_1/k} \circ \text{res}_{k_1/k} = [k_1 : k]$, and hence the restriction maps are also injective. This forces the top horizontal map to be injective, and hence it is enough to show that the image of the Galois symbol $K_2(k; E_k)/p \xrightarrow{s_p} H^2(k, E_k[p]^{\otimes 2})$ is zero.

The image of s_p can be computed by [11, Theorem 1.1]. Namely, under the Tate duality perfect pairing

$$H^2(k, E_k[p]^{\otimes 2}) \times \text{Hom}_{\text{Gal}(\bar{k}/k)}(E_k[p], E_k[p]) \rightarrow \mathbb{Z}/p,$$

the orthogonal complement of $\text{Im}(s_p)$ consists precisely of those $\text{Gal}(\bar{k}/k)$ -homomorphisms $E_k[p] \xrightarrow{f} E_k[p]$ that lift to a homomorphism of finite flat group schemes $\mathcal{E}_k[p] \xrightarrow{\tilde{f}} \mathcal{E}_k[p]$, where \mathcal{E}_k is the Néron model of E_k over $\text{Spec}(\mathcal{O}_k)$. Since E_k has good ordinary reduction, it follows by [11, Proposition 8.8] that these are exactly the homomorphisms $E_k[p] \xrightarrow{f} E_k[p]$ that satisfy $f(\widehat{E}_k[p]) \subset \widehat{E}_k[p]$. Thus, to show $\text{Im}(s_p) = 0$, it is enough to show that every $\text{Gal}(\bar{k}/k)$ -equivariant homomorphism $E_k[p] \xrightarrow{f} E_k[p]$ satisfies this property. Since E_k has complex multiplication defined over k , it follows that $E_k[p] \simeq \widehat{E}_k[p] \oplus \widehat{E}_k[p]$ as $\text{Gal}(\bar{k}/k)$ -modules. Since at least one of the cyclic submodules is nontrivial, the claim follows. \square

In Sect. 2.1 we saw many examples when F_0 can be taken to be \mathbb{Q} . We will focus more on this case in the next subsection.

4.2 Constructing global 0-cycles

In this last subsection we investigate the exactness of the complex (1.4) in the situation considered in Theorem 4.2. That is, we are looking for criteria that allow us to lift the group $\prod_{v|p} F^2(X_{L_v})_{\text{nd}} \simeq (\mathbb{Z}/p)^2$ to global 0-cycles in $F^2(X)$.

Lemma 4.5 *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. Let E be an elliptic curve over \mathbb{Q} such that E_K has complex multiplication by \mathcal{O}_K . Let F/\mathbb{Q} be a totally real extension and suppose that the Mordell-Weil group $E(F)$ has positive rank. Let $P \in E(F)$ be a point of infinite order. Write $\mathcal{O}_K = \mathbb{Z}[\omega_D]$. Then the points $P, \omega_D(P) \in E(K \cdot F)$ are \mathbb{Z} -linearly independent.*

Proof We will simply write ω instead of ω_D . Note that $\omega(P) \in E(K \cdot F) \setminus E(F)$. Let $\mu(x) = x^2 - bx + c \in \mathbb{Z}[x]$ be the minimal polynomial of ω . Let $\bar{\omega}$ be the conjugate of ω , so the equalities $\omega + \bar{\omega} = b$ and $\omega\bar{\omega} = c$ hold. Suppose for contradiction that $P, \omega(P)$ are \mathbb{Z} -linearly dependent. Then we can find $n, m \in \mathbb{Z}$ such that $nP + m\omega(P) = 0$. We may assume that n, m are relatively prime, and hence we can find $x, y \in \mathbb{Z}$ such that $nx + my = 1$. The relation $nP + m\omega(P) = 0$ implies that $nxP + mx\omega(P) = 0 = nyP + my\omega(P)$. Applying the endomorphism $\bar{\omega}$ to the first equality yields $nx\bar{\omega}(P) + mx\bar{\omega}(P) = 0$, and hence $nx\omega(P) - (mx + nb)P = 0$. Adding the latter to the equation $nyP + my\omega(P) = 0$ gives

$$\omega(P) = (nxb - ny + mx)cP \in E(F),$$

which is a contradiction. \square

Remark 4.6 Suppose $D \in \{-3, -7, -11, -19, -43, -67, -163\}$. Then $\mathcal{O}_K = \mathbb{Z}[\omega_D]$, where $\omega_D = -\frac{1}{2} + \frac{\sqrt{-D}}{2}$. The minimal polynomial of ω_D is $x^2 + x + \frac{1+D}{4}$ so that in the notation of Lemma 4.5 we have $b = -1$, $c = \frac{1}{4} + \frac{D}{4}$. Let p be an odd prime, $p \neq -D$. Then the system of equations $\begin{cases} x^2 = c \\ 2x = -1 \end{cases}$ has no solution over \mathbb{F}_p . For, if x were a solution, then the solution would be $x = -1/2 \in \mathbb{F}_p$, giving $4c \equiv 1 \pmod{p} \Leftrightarrow D \equiv 0 \pmod{p}$. This simple observation will be used in the proof of the following Theorem 4.7.

Proof of lifting when a “good” rational point exists

In this section we give a first criterion to lift the local 0-cycles to global. Our criterion relies only on the existence of a “good” rational point P . Before proving our main results, we briefly describe our methodology.

From now on we assume we are in the set-up of Theorem 4.2 with the extension F_0 minimal. The base change X_L , where $L = F_0 \cdot K(E[\pi])$, contains a nontrivial L -rational π -torsion point $A \in E[\pi](L)$. Our strategy is to examine when this torsion point can be used to construct global 0-cycles.

We say that a point $P \in E(F_0)$ is good if the 0-cycle $z_1 = [A, P] - [A, O] - [O, P] + [O, O] \in F^2(X_L)$ induces a nontrivial element $(z_{1v}, z_{1\bar{v}}) \in F^2(X_{L_v})_{\text{nd}} \oplus F^2(X_{L_{\bar{v}}})_{\text{nd}}$. When this happens, we show that the 0-cycle $z_2 = [A, \omega(P)] - [A, O] - [O, \omega(P)] + [O, O]$ induces a second \mathbb{F}_p -linearly independent element of $F^2(X_{L_v})_{\text{nd}} \oplus F^2(X_{L_{\bar{v}}})_{\text{nd}}$. To find an explicit condition that guarantees $(z_{1v}, z_{1\bar{v}}) \neq (0, 0)$, we will use the nonvanishing criterion from Sect. 3.2.3. From now on we identify the 0-cycle z_1 with the symbol $\{A, P\}_{L/L} \in K_2(L; E)$ and we denote by $\{A_v, P_v\}_{L_v/L_v}$ the corresponding element of $K_2(L_v; E_v)$. We will abuse notation and write $\{A_v, P_v\}_{L_v/L_v}$ for the class of this symbol modulo $pK_2(L_v; E_v)$. We recall from (3.8) that we have an equality

$$\{A_v, P_v\}_{L_v/L_v} = \{\widehat{A}_v, \widehat{P}_v\}_{L_v/L_v} = \{A_v, \widehat{P}_v\}_{L_v/L_v},$$

where $P_v = (\widehat{P}_v, \overline{P}_v)$ is the decomposition of P modulo $pE(L_v)$ as in (3.5). Here we used the fact that $A_v \in \widehat{E}_v[p]$.

The following Theorem 4.7 develops the above idea when $F_0 = \mathbb{Q}$. In this case we are looking for a point $P \in E(\mathbb{Q})$ inducing the desired symbol $\{A, P\}_{L/L}$. For such a point we will denote by $P_{\mathbb{Q}_p} = (\widehat{P}_{\mathbb{Q}_p}, \overline{P}_{\mathbb{Q}_p}) \in \widehat{E}(\mathbb{Q}_p)/p \oplus \overline{E}_p(\mathbb{F}_p)$ the corresponding local point.

Theorem 4.7 *Suppose p is a prime and E an elliptic curve over \mathbb{Q} satisfying the assumptions of Theorem 4.2. Assume further that $|\overline{E}_p(\mathbb{F}_p)| = p$, and consider the extension $L = K(E[\pi])$ constructed in Theorem 4.2. Suppose that the Mordell-Weil group $E(\mathbb{Q})$ has positive rank and there exists a global point $P \in E(\mathbb{Q})$ of infinite order such that the induced local point $P_{\mathbb{Q}_p} \in E_{\mathbb{Q}_p}(\mathbb{Q}_p)$ has the property that $\widehat{P}_{\mathbb{Q}_p} \in \widehat{E}_{\mathbb{Q}_p}(\mathbb{Q}_p)/p$ is nontrivial. Then the global p -torsion 0-cycles $z_1, z_2 \in F^2(X_L)$ induced by A, P and $A, \omega(P)$ respectively lift the group $\prod_{v|p} F^2(X_{L_v})_{\text{nd}} \simeq \mathbb{Z}/p \oplus \mathbb{Z}/p$.*

Proof The assumption $|\overline{E}_p(\mathbb{F}_p)| = p$ implies that $K = \mathbb{Q}(\sqrt{D})$ with $D \equiv 1 \pmod{4}$. Let $\mu(x) = x^2 + x + c \in \mathbb{Z}[x]$ be the minimal polynomial of $\omega = \omega_D$ over \mathbb{Q} .

Claim 1: The symbol $\{A_v, \widehat{P}_v\}_{L_v/L_v} \in K_2(L_v; E_v)/p$ is nontrivial.

To prove the claim, we consider the Kummer extension $k_0 = L_v(\delta(A_v)^{1/p}) = L_v\left(\frac{1}{p}A_v\right)$. Recall from Sect. 3.2.3 that the symbol $\{A_v, \widehat{P}_v\}_{L_v/L_v}$ is nontrivial if and only if $\delta(\widehat{P}_v)$ is not in the image of the norm map

$$N_{k_0/L_v} : k_0^\times \rightarrow L_v^\times.$$

We consider the filtration $\{\widehat{E}_v^i(L_v)\}_{i \geq 1}$ of $\widehat{E}_v(L_v)$ and the induced filtration $\{\mathcal{D}^i\}_{i \geq 1}$ of $\widehat{E}_v(L_v)/p$ (cf. Sect. 3.2.2). We claim that $A_v \in \widehat{E}_v^1 \setminus \widehat{E}_v^2$ and it therefore induces a nontrivial element of $\mathcal{D}^1/\mathcal{D}^2$. For, let $v(A_v)$ be the valuation of A_v . Since A_v is an element of $\widehat{E}(L_v)$ of exact order p , it follows by [35, IV.6, Theorem 6.1] that

$$1 \leq v(A_v) \leq \frac{v(p)}{p-1}.$$

The extension L_v/\mathbb{Q}_p is totally ramified of degree $p-1$, and hence it follows that $\frac{v(p)}{p-1} = 1$ yielding the desired equality $v(A_v) = 1$.

We note that the integer $\frac{v(p)}{p-1} = 1$ is precisely the integer $t_0(\phi)$ defined in [12, page 11, Lemma 3.5] where $\phi = [p]$ is the p -isogeny on \widehat{E}_v , which is of height one. Using the filtered isomorphism (3.9), we deduce that $\delta(A_v) \in \overline{U}_{L_v}^1 \setminus \overline{U}_{L_v}^2$. It follows by [19, Lemma 2.1.5] (see also [12, Lemma 3.5]) that the extension k_0/L_v is totally ramified of degree p with the jump in the ramification filtration of $\text{Gal}(k_0/L_v)$ happening at $s = p-1$. It then follows by [32, V.3, Corollary 7] that there exists a unit $u \in \overline{U}_{L_v}^{p-1}$ such that the symbol algebra $(\delta(A_v), u)_p$ is nontrivial in $\text{Br}(L_v)_p$. In fact, we can conclude that $u \in \overline{U}_{L_v}^{p-1} \setminus \overline{U}_{L_v}^p$. For, it follows by [32, V.3, Corollaries 2 & 3] that $(\delta(A_v), u')_p = 0$ for every $u' \in \overline{U}_{L_v}^p$. The next key observation is that

$$(\delta(A_v), u)_p \neq 0, \text{ for every unit } u \in \overline{U}_{L_v}^{p-1} \setminus \overline{U}_{L_v}^p.$$

This is because the residue field of L_v is \mathbb{F}_p , and therefore we have an isomorphism (cf. [12, Lemma 3.4]) $\overline{U}_{L_v}^{p-1}/\overline{U}_{L_v}^p \simeq \mathbb{F}_p$. Thus, in order to prove the claim, it is enough to show $\delta(\widehat{P}_v) \in \overline{U}_{L_v}^{p-1} \setminus \overline{U}_{L_v}^p$, or equivalently that $v(\widehat{P}_v) = p-1$. Consider the inclusion

$$\text{res}_{L_v/\mathbb{Q}_p} : \widehat{E}_{\mathbb{Q}_p}^{p-1}(\mathbb{Q}_p)/p \hookrightarrow \widehat{E}_v^{p-1}(L_v)/p,$$

sending $\widehat{P}_{\mathbb{Q}_p}$ to \widehat{P}_v . This map is injective, because we have an equality $N_{L_v/\mathbb{Q}_p} \circ \text{res}_{L_v/\mathbb{Q}_p} = [L_v : \mathbb{Q}_p] = p-1$, which is coprime to p . Our last claim will then follow once we show that $\widehat{P}_{\mathbb{Q}_p} \in \widehat{E}_{\mathbb{Q}_p}^{p-1}(\mathbb{Q}_p) \setminus \widehat{E}_{\mathbb{Q}_p}^{p-2}(\mathbb{Q}_p)$. Let us assume otherwise that $\widehat{P}_{\mathbb{Q}_p} \in \widehat{E}_{\mathbb{Q}_p}^{p-2}(\mathbb{Q}_p)$, and hence $\widehat{P}_v \in \widehat{E}_v^{2(p-1)}$. Because $2(p-1) > p$, it follows by the filtered isomorphism (3.9) and [12, Lemma 3.4] that \widehat{P}_v (and hence also $\widehat{P}_{\mathbb{Q}_p}$) is a multiple of p , which contradicts our assumption that $\widehat{P}_{\mathbb{Q}_p} \in \widehat{E}_{\mathbb{Q}_p}^{p-1}(\mathbb{Q}_p)/p$ is nontrivial. This completes the proof of the Claim. The above computation shows that the global 0-cycle $z_1 = [A, P] - [A, O] - [O, P] + [O, O] \in F^2(X_L)$ has a nontrivial image $(z_{1v}, z_{1\bar{v}})$ under the diagonal map $F^2(X_L)/p \xrightarrow{\Delta} \prod_{v|p} F^2(X_{L_v})_{\text{nd}}$.

A byproduct of the proof of Claim 1 is that the following two maps are isomorphisms,

$$\begin{aligned} f : \mathcal{D}^1/\mathcal{D}^2 &\rightarrow \mathbb{Z}/p, \quad g : \mathcal{D}^{p-1}/\mathcal{D}^p \rightarrow \mathbb{Z}/p \\ x &\mapsto \{x, \widehat{P}_v\}_{L_v/L_v}, \quad y \mapsto \{A_v, y\}_{L_v/L_v}. \end{aligned}$$

The extensions L_v and $L_{\bar{v}}$ are isomorphic as abstract fields. Therefore Claim 1 holds true also for the symbol $\{A_{\bar{v}}, P_{\bar{v}}\}_{L_{\bar{v}}/L_{\bar{v}}} \in K_2(L_{\bar{v}}, E_{\bar{v}})/p$ corresponding to the 0-cycle $z_{1\bar{v}}$. Since P is defined over \mathbb{Q} , it follows that $P_{\bar{v}} = P_v$. Moreover, the map f being an isomorphism implies that there exists some $a \in \mathbb{F}_p^\times$ such that

$$f(A_{\bar{v}}) = \{A_{\bar{v}}, \widehat{P}_v\}_{L_v/L_v} = a\{A_v, \widehat{P}_v\}_{L_{\bar{v}}/L_{\bar{v}}}.$$

In other words, if we fix an isomorphism $F^2(X_{L_v})_{\text{nd}} \xrightarrow{\cong} \mathbb{Z}/p$ sending z_{1v} to 1, then the diagonal map $\Delta : F^2(X_L)/p \rightarrow F^2(X_{L_v})_{\text{nd}} \oplus F^2(X_{L_{\bar{v}}})_{\text{nd}} \xrightarrow{\cong} \mathbb{Z}/p \oplus \mathbb{Z}/p$, $z \mapsto (z_v, z_{\bar{v}})$ maps z_1 to the tuple $(1, a)$.

Claim 2: The element $\Delta(z_2)$ is \mathbb{F}_p -linearly independent from $\Delta(z_1) = (1, a)$, where z_2 is the 0-cycle $z_2 = [A, \omega(P)] - [A, O] - [O, \omega(P)] + [O, O] \in F^2(X_L)$.

The 0-cycles $z_{2v}, z_{2\bar{v}}$ correspond to the symbols $\{A_v, \widehat{\omega(P)}_v\}_{L_v/L_v}, \{A_{\bar{v}}, \widehat{\omega(P)}_{\bar{v}}\}_{L_{\bar{v}}/L_{\bar{v}}}$. Since $P \in E(K) \subset E(L)$, the point $\omega(P)_{\bar{v}}$ is the restriction of $\omega(P)_{\bar{p}}$, and hence it is none other than the complex conjugate, $\bar{\omega}(P)_v$. The points $\omega(P), \bar{\omega}(P)$ induce elements $\widehat{\omega(P)}_v, \widehat{\bar{\omega}(P)}_v \in \mathcal{D}^{p-1}/\mathcal{D}^p$. Since $\omega(P) + \bar{\omega}(P) = -P$, and $\widehat{P}_v \in \mathcal{D}^{p-1}/\mathcal{D}^p$ is nontrivial, at least one of these points induces a nontrivial element of $\mathcal{D}^{p-1}/\mathcal{D}^p$. Without loss of generality, assume there exists $m \in \mathbb{F}_p^\times$ such that $\widehat{\omega(P)}_v \equiv m \widehat{P}_v \pmod{\mathcal{D}^p}$.

The isomorphism g then yields an equality

$$g(\omega(P)_v) = \{A_v, \omega(P)_v\}_{L_v/L_v} = m \{A_v, P_v\}_{L_v/L_v}.$$

To prove linear independence, it is enough to show

$$\{A_{\bar{v}}, \bar{\omega}(P)_v\}_{L_{\bar{v}}/L_{\bar{v}}} \neq m a \{A_v, P_v\}_{L_v/L_v}.$$

Notice that we have $\{A_{\bar{v}}, \bar{\omega}(P)_v\}_{L_v/L_v} = a \{A_v, \bar{\omega}(P)_v\}_{L_v/L_v}$. Thus, it suffices to prove that the elements $\widehat{\omega(P)}_v, \widehat{\bar{\omega}(P)}_v$ induce distinct elements of $\mathcal{D}^{p-1}/\mathcal{D}^p$. Suppose for contradiction that they are the same. That is, $\widehat{\omega(P)}_v \equiv \widehat{\bar{\omega}(P)}_v \equiv m \widehat{P}_v \pmod{\mathcal{D}^p}$. We have $\widehat{\omega(P)}_v + \widehat{\bar{\omega}(P)}_v = -\widehat{P}_v$, giving $2m = -1$ in \mathbb{F}_p . Moreover, $\widehat{\omega(\omega(P))}_v = m^2 \widehat{P}_v = c \widehat{P}_v$, where $c = (D+1)/4$. That is, $m \in \mathbb{F}_p^\times$ is a solution to the system

$$\begin{cases} x^2 = c \\ 2x = -1 \end{cases},$$

which is a contradiction by Remark 4.6. \square

Remark 4.8 We believe that the condition of having a “good” rational point $P \in E(\mathbb{Q})$ is satisfied by a positive proportion of elliptic curves with positive rank over \mathbb{Q} . As we saw in the proof of Theorem 4.7, all we need is a point P such that $\widehat{P}_{\mathbb{Q}_p} \in \widehat{E}^1(\mathbb{Q}_p) \setminus \widehat{E}^2(\mathbb{Q}_p)$. The latter can be checked computationally as follows.

- (1) Compute the coordinates of a point $P \in E(\mathbb{Q})$ of infinite order.
- (2) Compute the coordinates of the induced local point $\widehat{P}_{\mathbb{Q}_p} \in E(\mathbb{Q}_p)$.
- (3) Compute the coordinates of a local nonzero p -torsion point $P_0 \in E[p](\mathbb{Q}_p)$.
- (4) Find a scalar $\lambda \in \mathbb{F}_p$ such that the x -coordinate of $P_{\mathbb{Q}_p} - \lambda P_0$ has negative valuation.
- (5) If the above valuation is exactly -2 , then P is a point that satisfies the condition of Theorem 4.7.

When the ordinary prime p is small enough, this is a computation that can be carried out in SAGE. As a case study, in the appendix [Appendix A](#) we carry out this computation for the family of elliptic curves $\{y^2 = x^3 - 2 + 7n : n \in \mathbb{Z}\}$, and the prime $p = 7$.

Remark 4.9 An interesting case to consider next is the following. Start with a pair (E, p) that satisfies the assumptions of Theorem 4.2 with $F_0 = \mathbb{Q}$ and consider extensions M/\mathbb{Q} of degree $g < p - 1$ such that p splits completely in M . Then we still have a vanishing $\text{Br}(X_{L,M})\{p\}/\text{Br}_1(X_{L,M})\{p\} = 0$, where $L = K(E[\pi])$. An analog of Theorem 4.2 gives

$$\prod_{v|p} F^2(X_{(LM)_v})_{\text{nd}} \simeq (\mathbb{Z}/p)^{2g}.$$

We see that as g gets larger, it becomes increasingly harder to find concrete criteria that guarantee the lifting of this group to global 0-cycles. For example, consider the curve E given by the Weierstrass equation $y^2 = x^3 + 2$ and the prime $p = 61$. Then p splits completely over the degree six extension $\mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^6 - x^4 + x^2 - 3x + 3$.

The key ingredient in the proof of Theorem 4.7 was that the two homomorphisms

$$\begin{aligned} f : \mathcal{D}^1/\mathcal{D}^2 &\rightarrow \mathbb{Z}/p, \quad g : \mathcal{D}^{p-1}/\mathcal{D}^p \rightarrow \mathbb{Z}/p \\ x &\mapsto \{x, \widehat{P}_v\}_{L_v/L_v}, \quad y \mapsto \{A_v, y\}_{L_v/L_v} \end{aligned}$$

are isomorphisms and this was because the residue field of $K(E[\pi])$ is only \mathbb{F}_p . A similar method can be extended to many more situations. For example the following corollary describes a generalization to when $L = F_0(E[\pi])$ with F_0/\mathbb{Q} a quadratic extension.

Corollary 4.10 *Let (E, p) be a pair that satisfies the assumptions of Theorem 4.2. Suppose that $p \nmid |\overline{E_p}(\mathbb{F}_p)|$, but $p \mid |\overline{E_p}(\mathbb{F}_{p^2})|$. Let F_0/\mathbb{Q} be a quadratic extension having a unique inert place w_0 above p . Set $k = F_0 \cdot \mathbb{Q}_p$. Suppose there exists a point $P \in E(F_0) \setminus E(\mathbb{Q})$ of infinite order such that the induced local point $P_k \in E(k)$ has the property $\widehat{P}_k \in \widehat{E}_k(k)/p$ is nontrivial. Then the global p -torsion 0-cycles $z_1, z_2 \in F^2(X_L)$ induced by A, P and $A, \omega(P)$ respectively lift the group $\prod_{v|p} F^2(X_{L_v})_{\text{nd}} \simeq \mathbb{Z}/p \oplus \mathbb{Z}/p$.*

Proof The proof is essentially the same as in Theorem 4.7.

In this case we have an isomorphism of \mathbb{F}_p -vector spaces (cf. [19, Lemma 2.1.4])

$$\overline{U}_{L_v}^{p-1}/\overline{U}_{L_v}^p \simeq \mathcal{D}_{L_v}^{p-1}/\mathcal{D}_{L_v}^p \xrightarrow{\sim} \mathbb{F}_{p^2} \simeq \mathbb{Z}/p \oplus \mathbb{Z}/p.$$

It follows by [32, V.3, Corollary 7] that there exists some $B \in \mathcal{D}_{L_v}^{p-1}/\mathcal{D}_{L_v}^p$ such that $(\delta(A_v), \delta(B))_p \neq 0$. We will show that we can take $B = (P_k)_v$. Consider the extension $F = K(E[\pi])$ and denote by v_0 the unique place of F below v . Since $p \nmid |\overline{E_p}(\mathbb{F}_p)|$, we have a proper inclusion $F \subsetneq L$. It follows by Proposition 4.4 that

$K_2(F \cdot \mathbb{Q}_p; E_{F\mathbb{Q}_p})/p = 0$. This implies that for every $C \in \mathcal{D}_{L_v}^{p-1}/\mathcal{D}_{L_v}^p$ which is the restriction of some element defined over F_{v_0} , it follows $(\delta(A_v), \delta(C))_p = 0$. Since $\overline{U}_{L_v}^{p-1}/\overline{U}_{L_v}^p$ is two dimensional over \mathbb{F}_p , every element B that is not in the image of the restriction map $\text{res}_{L_v/F_{v_0}}$ gives rise to a nontrivial symbol. The assumption $P \in E(F_0) \setminus E(\mathbb{Q})$ implies that we can take $B = (P_k)_v$, which yields the desired nonvanishing $(\delta(A_v), (P_k)_v)_p \neq 0$.

The rest of the proof of Theorem 4.7 carries through to show that the 0-cycles $z_1 = [A, P_k] - [A, O] - [O, P_k] + [O, O]$ and $z_2 = [A, \omega(P_k)] - [A, O] - [O, \omega(P_k)] + [O, O]$ are \mathbb{F}_p -linearly independent. The only difference is that we have to consider also the case when $K = \mathbb{Q}(\sqrt{D})$ with $D \not\equiv 1 \pmod{4}$ (see 2.9 for examples of elliptic curves with potential CM by $\mathbb{Z}[i]$ which satisfy the assumptions of the corollary). The computation of linear independence is in fact simpler in this case. The minimal polynomial of ω is $\mu(x) = x^2 - D$, giving $\omega(P) = -\bar{\omega}(P)$. Since $p > 2$, it is clear that the elements $\widehat{\omega(P)}_v, \widehat{\bar{\omega}(P)}_v$ induce distinct elements of $\mathcal{D}^{p-1}/\mathcal{D}^p$.

□

Extensions

We close this article by discussing alternative criteria of lifting when a “good” rational point does not exist. We focus on the simplest case considered in Theorem 4.7, namely when $|\overline{E_p}(\mathbb{F}_p)| = p$. In this case the point $A \in E[\pi]$ can no longer be used to produce global 0-cycles. One needs to find instead two “good” points $P, Q \in E(L)$ such that the induced symbol $\{\widehat{P}_v, \widehat{Q}_v\}_{L_v/L_v} \neq 0$. To look for such points we need to start with points of infinite order living in intermediate extensions $\mathbb{Q} \subsetneq F \subseteq L = K(E[\pi])$. In the following paragraphs we develop this idea.

Suppose we have a local point $B_v \in \widehat{E}(L_v)$ such that $B_v \in \widehat{E}^l(L_v) \setminus \widehat{E}^{l+1}(L_v)$ for some integer $0 < l < p$. Then it follows by [32, V.3, Corollaries 2 and 3] that the map

$$\mathcal{D}^{p-l}/\mathcal{D}^{p-l+1} \rightarrow \mathbb{Z}/p, \quad x \mapsto \{x, B_v\}_{L_v/L_v}$$

is an isomorphism. Thus, if we can find intermediate extensions $K \subset M, F \subset L$ and points $P \in E(M), Q \in E(F)$ of infinite order such that the induced local formal points $\widehat{P}_v, \widehat{Q}_v$ lie in $\widehat{E}^l(L_v) \setminus \widehat{E}^{l+1}(L_v)$, and $\widehat{E}^{p-l}(L_v) \setminus \widehat{E}^{p-l+1}(L_v)$ respectively, then the symbol $\{\widehat{P}_v, \widehat{Q}_v\}_{L_v/L_v}$ is nonvanishing in $K_2(L_v; E_v)/p$. Then we can produce a second \mathbb{F}_p -linearly independent symbol using the complex multiplication, as we did in the proof of Theorem 4.7. We next describe a potential algorithm to compute such “good points” P, Q in a particular example. A similar method can be used more generally, but the algorithm will require more steps.

An extended example

To illustrate our method, we consider the case when the quadratic imaginary field $K = \mathbb{Q}(\zeta_3)$, and $p = 7$. We consider the family of elliptic curves

$$\{E_n : y^2 = x^3 - 2 + 7n, n \in \mathbb{Z}\},$$

so that the pair $(7, E_n)$ satisfies the assumptions of Theorem 4.2, for all $n \in \mathbb{Z}$. Suppose that for a certain value of n the condition of Theorem 4.7 is not satisfied. That is, there is no good point $P \in E_n(\mathbb{Q})$. For simplicity we will write $E = E_n$.

The Galois group $G = \text{Gal}(L/K)$ is cyclic of order 6, and hence there exist unique intermediate subfields $K \subset M, F \subset L$ such that $[M : K] = 2$ and $[F : K] = 3$. Moreover, the extension L/K is totally ramified at $\mathfrak{p}, \bar{\mathfrak{p}}$. This implies that there exist unique places s, \bar{s} of M lying over $\mathfrak{p}, \bar{\mathfrak{p}}$ respectively and the extension M_s/\mathbb{Q}_p is totally ramified of degree 2. Similarly there exist unique places t, \bar{t} of F over $\mathfrak{p}, \bar{\mathfrak{p}}$ with F_t/\mathbb{Q}_p totally ramified of degree 3.

Suppose we can find global points $B \in E(M), C \in E(F)$ such that $\widehat{B}_s \in \widehat{E}^1(M_s) \setminus \widehat{E}^2(M_s)$, and $\widehat{C}_t \in \widehat{E}^1(F_t) \setminus \widehat{E}^2(F_t)$. Their restrictions $\widehat{B}_v, \widehat{C}_v$ in $\widehat{E}(L_v)$ lie in $\widehat{E}^3(L_v) \setminus \widehat{E}^4(L_v)$ and $\widehat{E}^2(L_v) \setminus \widehat{E}^3(L_v)$ respectively.

Next consider the points $\omega(C), \omega^2(C) \in E(F)$. Similarly to the proof of Theorem 4.7, at least one of these points induces a formal point in $\widehat{E}^2(L_v) \setminus \widehat{E}^3(L_v)$. Call this point C' . Then there exists some scalar $m \in \mathbb{F}_7^\times$ such that $\widehat{C}'_v \equiv m\widehat{C}_v \pmod{\mathcal{D}^3}$. This is equivalent to saying that the x -coordinate of the formal point $\widehat{C}'_t - m\widehat{C}_t$ has strictly smaller valuation than the one of \widehat{C}_t . If it happens that $\widehat{C}'_t - m\widehat{C}_t \in \widehat{E}^2(F_t) \setminus \widehat{E}^3(F_t)$, then the point $Q = C' - mC$ is a “good” point. That is, $\widehat{Q}_v \in \widehat{E}^4(L_v) \setminus \widehat{E}^5(L_v)$, and since $3+4 = 7$, our earlier discussion shows that $\{B_v, Q_v\}_{L_v/L_v} \neq 0 \in K_2(L_v; E)/p$.

Acknowledgements We are truly grateful to Professor Andrew Sutherland for computing for us many examples that satisfy the assumptions of Theorem 1.6. We heartily thank Professors Toshiro Hiranouchi, and Olivier Wittenberg for useful discussions. Additionally, we would like to express our deep gratitude to Professor Evis Ieronymou, who found a mistake in an earlier version of this paper. Finally, we would like to thank the referee for correcting our mistakes and suggesting many useful comments. The first author was partially supported by the NSF grant DMS-2001605.

Appendix A Computations with local points by Angelos Koutsianas

In this appendix we give more details about the computations we have done in order to verify the existence of a “good” rational point P that Theorem 4.7 requires for the family of elliptic curves

$$\{E_n : y^2 = x^3 - 2 + 7n, n \in \mathbb{Z}\}.$$

Our computations are based on Remark 4.8. We consider the cases $n \in [-5000, 5000]$ with $p = 7$ and $\text{rank}(E_n(\mathbb{Q})) = 1$.

For a fixed value of n we define $a = -2 + 7n$. We recall that E_n has complex multiplication by the ring of integers \mathcal{O}_K of $K = \mathbb{Q}(\sqrt{-3})$. It follows that $p = 7$

splits in \mathcal{O}_K with $7 = \pi\bar{\pi}$ where $\pi = \frac{1+3\sqrt{-3}}{2}$ and $\bar{\pi}$ is the complex conjugate of π . For the computations we need an explicit description of $E_n[p](\mathbb{Q}_p)$.

Lemma A.1 *With the above notation, it holds*

$$E_n[7](\mathbb{Q}_7) = \{(\sqrt[3]{\theta}\zeta_3^i, \pm\sqrt{\theta+a}) : \text{for } i = 0, 1, 2\},$$

where θ is the root of $f(x) = 7x^2 - 4ax + 16a^2$ such that $\theta \equiv 6 \pmod{7}$ and $i = 0, 1, 2$.

Proof A symbolic computation shows that the 7th torsion polynomial of E_n is given by

$$\begin{aligned} f_7(x) = & (7x^6 - 4ax^3 + 16a^2)(x^{18} + 564ax^{15} - 5808a^2x^{12} \\ & - 123136a^3x^9 - 189696a^4x^6 - 49152a^5x^3 + 4096a^6). \end{aligned}$$

It follows by Example 2.4 that $|\overline{E_{n,p}}(\mathbb{F}_7)| = 7$. Moreover, the leading coefficient of f_7 is divisible by 7 and thus by [35, Theorem VII.3.4] we conclude that $\#E_n[7](\mathbb{Q}_7) = 7$. Therefore, it is enough to show that the above points have order 7 and coordinates in \mathbb{Q}_7 .

Let $g(x) = 7x^2 - 4ax + 16a^2$, then we can easily prove that the roots of g are

$$\theta_{1,2} = 2a \frac{1 \pm 3\sqrt{-3}}{7}.$$

Suppose we embed $\sqrt{-3}$ into \mathbb{Q}_7 such that $\sqrt{-3} \equiv 2 + 5 \cdot 7 + 6 \cdot 7^3 + O(7^4)$. As a result, we get $\theta_1 = 2a(2 + 2 \cdot 7 + 4 \cdot 7^2 + O(7^3))$ and $\theta_2 = 2a(\frac{2}{7} + 5 + 4 \cdot 7 + 2 \cdot 7^2 + O(7^3))$. Because $v_7(\theta_2) = -1$ we understand that $\sqrt[3]{\theta_2} \notin \mathbb{Q}_7$.

Let $\theta = \theta_1$. Because $\theta \equiv 6 \pmod{7}$ by Hensel's lemma we get that the polynomial $x^3 - \theta$ has a root in \mathbb{Q}_7 . Furthermore, because $\zeta_3 \in \mathbb{Q}_7$ we conclude that $\sqrt[3]{\theta}\zeta_3^i \in \mathbb{Q}_7$ for all $i = 0, 1, 2$.

Let $x_i = \sqrt[3]{\theta}\zeta_3^i$ for $i = 0, 1, 2$. In order to finish the proof, suffices to show that the polynomial

$$x^2 - (x_i^3 + a) = x^2 - (\theta + a),$$

has both of its roots in \mathbb{Q}_7 . Because $\theta + a \equiv 4 \pmod{7}$ Hensel's lemma yields the conclusion. \square

Having determined the set $E_n[7](\mathbb{Q}_7)$, we follow the steps in Remark 4.8. We focus on the curves E_n with rank 1. The most computationally expensive part is the determination of the generator P of the free part of $E_n(\mathbb{Q})$. In order to speed up the computations we assume the finiteness of Tate-Shafarevich group.

Theorem A.2 *Let $n \in [-5000, 5000]$. Under the assumption of the finiteness of the Tate-Shafarevich group of E , the 86,68% of the rank one elliptic curves E_n satisfy the hypothesis of Theorem 4.7, in other words there exists a “good” rational point P .*

Proof We have written a Sage [39] script¹ that does all the computations we have described in Remark 4.8 and Lemma A.1.

It is important to mention that there are 176 values of n for which we are not able to compute the generator of the free part of $E_n(\mathbb{Q})$. For the calculation of the above percent we do not consider these 176 curves. The total amount of time for the computations was 31 minutes in a regular personal computer. \square

The code can be found in https://github.com/akoutsianas/local_global_0_cycles.

References

1. Alexei, N.: Skorobogatov, Beyond the Manin obstruction. *Invent. Math.* **135**(2), 399–424 (1999)
2. Bright, M., Newton, R.: Evaluating the wild brauer group (2020)
3. Colliot-Thélène, J.-L.: Conjectures de type local-global sur l'image des groupes de Chow dans la cohomologie étale, Algebraic K -theory (Seattle, WA, Proc. Sympos. Pure Math., vol. 67, Amer. Math. Soc. Providence, RI **1999**, 1–12 (1997)
4. Colliot-Thélène, J.-L.: Points rationnels sur les fibrations, Higher dimensional varieties and rational points (Budapest, Bolyai Soc. Math. Stud., vol. 12. Springer, Berlin **2003**, 171–221 (2001)
5. Colliot-Thélène, J.-L.: L'arithmétique du groupe de Chow des zéro-cycles. *J. Théor. Nombres Bordeaux* **7**(1), 51–73 (1995). (**Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993)**)
6. Colliot-Thélène, J.-L., Sansuc, J.-J.: On the Chow groups of certain rational surfaces: a sequel to a paper of S. Bloch. *Duke Math. J.* **48**(2), 421–447 (1981)
7. Colliot-Thélène, J.-L., Sansuc, J.-J., Swinnerton-Dyer, P.: Intersections of two quadrics and Châtelet surfaces. I. *J. Reine Angew. Math.* **373**, 37–107 (1987)
8. Colliot-Thélène, J.-L., Sansuc, J.-J., Swinnerton-Dyer, P.: Intersections of two quadrics and Châtelet surfaces. II. *J. Reine Angew. Math.* **374**, 72–168 (1987)
9. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* **14**, 197–272 (1941)
10. Gazaki, E., Leal, I.: Zero Cycles on a Product of Elliptic Curves Over a p -adic Field. *Int. Math. Res. Not. IMRN* **14**, 10586–10625 (2022)
11. Gazaki, E.: A finer Tate duality theorem for local Galois symbols. *J. Algebra* **509**, 337–385 (2018)
12. Gazaki, E., Hiranouchi, T.: Divisibility results for zero-cycles. *Eur. J. Math.* **7**(4), 1458–1501 (2021)
13. Harpaz, Y., Wittenberg, O.: On the fibration method for zero-cycles and rational points. *Ann. Math.* (2) **183**(1), 229–295 (2016)
14. Hiranouchi, T.: Milnor K -groups attached to elliptic curves over a p -adic field. *Funct. Approx. Comment. Math.* **54**(1), 39–55 (2016)
15. Hiranouchi, T., Hirayama, S.: On the cycle map for products of elliptic curves over a p -adic field. *Acta Arith.* **157**(2), 101–118 (2013)
16. Ieronymou, E.: The Brauer–Manin obstruction for zero-cycles on $K3$ surfaces. *Int. Math. Res. Not. IMRN* **3**, 2250–2260 (2021)
17. Joux, A., Morain, F.: Sur les sommes de caractères liées aux courbes elliptiques à multiplication complexe. *J. Number Theory* **55**(1), 108–128 (1995)
18. Kato, K., Saito, S.: Global class field theory of arithmetic schemes, Applications of algebraic K -theory to algebraic geometry and number theory, Part I, II (Boulder, Colo., Contemp. Math., vol. 55, Amer. Math. Soc. Providence, RI **1986**, 255–331 (1983)
19. Kawachi, M.: Isogenies of degree p of elliptic curves over local fields and kummer theory. *Tokyo J. Math.* **25**(2), 247–259 (2002)
20. Kollar, J., Szabó, E.: Rationally connected varieties over finite fields. *Duke Math. J.* **120**(2), 251–267 (2003)
21. Lang, S., Trotter, H.: Frobenius distributions in GL_2 -extensions. *Lect. Notes Math.* 504. Springer-Verlag, Berlin-New York (1976)
22. Lang, S.: Elliptic functions, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, (1987), With an appendix by J. Tate

¹ See function *rank_one_elliptic_curves*.

23. Liang, Y.: Compatibility of weak approximation for zero-cycles on products of varieties, (2020)
24. Liang, Y.: Arithmetic of 0-cycles on varieties defined over number fields. *Ann. Sci. Éc. Norm. Supér. (4)* **46**(1), 35–56 (2013)
25. Manin, Y.I.: Le groupe de Brauer–Grothendieck en géométrie diophantienne, *Actes du Congrès International des Mathématiciens* (Nice, 1970). Tome 1, 401–411 (1971)
26. Pagano, M.: An example of a Brauer–Manin obstruction to weak approximation at a prime with good reduction, (2021)
27. Poonen, B.: Insufficiency of the Brauer–Manin obstruction applied to étale covers. *Ann. Math. (2)* **171**(3), 2157–2169 (2010)
28. Rajwade, A.R.: Arithmetic on curves with complex multiplication by the Eisenstein integers. *Proc. Cambridge Philos. Soc.* **65**, 59–73 (1969)
29. Raskind, W., Spiess, M.: Milnor K -groups and zero-cycles on products of curves over p -adic fields. *Compos. Math.* **121**(1), 1–33 (2000)
30. Rubin, K.: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, *Arithmetic theory of elliptic curves* (Cetraro, Lecture Notes in Math., vol. 1716. Springer, Berlin **1999**, 167–234 (1997)
31. Serre, J.-P.: Abelian l -adic representations and elliptic curves, second ed., Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, (1989), With the collaboration of Willem Kuyk and John Labute
32. Serre, J.-P.: Local fields, volume 67 of Graduate Texts in Mathematics (1979)
33. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.* **54**, 323–401 (1981)
34. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. *Ann. Math. (2)* **88**, 492–517 (1968)
35. Silverman, J. H.: The arithmetic of elliptic curves, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht (2009)
36. Skorobogatov, A.N., Zarhin, Y.G.: A finiteness theorem for the Brauer group of abelian varieties and $K3$ surfaces. *J. Algebraic Geom.* **17**(3), 481–502 (2008)
37. Skorobogatov, A.N., Zarhin, Y.G.: The Brauer group of Kummer surfaces and torsion of elliptic curves. *J. Reine Angew. Math.* **666**, 115–140 (2012)
38. Somekawa, M.: On Milnor K -groups attached to semi-abelian varieties. *K-Theory* **4**(2), 105–119 (1990)
39. The Sage Developers, *Sagemath*, the Sage Mathematics Software System (Version 9.1), 2020. <https://www.sagemath.org>
40. van Hamel, J.: The Brauer–Manin obstruction for zero-cycles on Severi–Brauer fibrations over curves. *J. Lond. Math. Soc. (2)* **68**(2), 317–337 (2003)
41. Wittenberg, O.: Zéro-cycles sur les fibrations au-dessus d’une courbe de genre quelconque. *Duke Math. J.* **161**(11), 2113–2166 (2012)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH (“Springer Nature”).

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users (“Users”), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use (“Terms”). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval, sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com