RATIONAL POINTS ON CONIC BUNDLES OVER ELLIPTIC CURVES

JENNIFER BERG AND MASAHIRO NAKAHARA

ABSTRACT. We study rational points on conic bundles over elliptic curves with positive rank over a number field. We show that the étale Brauer–Manin obstruction is insufficient to explain failures of the Hasse principle for such varieties. We then further consider properties of the distribution of the set of rational points with respect to its image in the rational points of the elliptic curve. In the process, we prove results on a local-to-global principle for torsion points on elliptic curves over \( \mathbb{Q} \).

1. Introduction

The purpose of this paper is to examine the arithmetic of varieties fibered over elliptic curves of positive Mordell–Weil rank over a number field \( k \). The first portion of this paper is based on results of \([\text{CTPS16}, \S5]\), in which they consider obstructions to rational points on quadric bundles fibered over a curve with a single rational point. We show that the pathologies of the Brauer–Manin and étale–Brauer obstructions persist, even for conic bundle surfaces \( X \) fibered over positive rank elliptic curves. When \( X(k) \) is nonempty, however, the distribution of the \( k \)-rational points remains largely unexplored. In this context, it is natural to consider properties of the image of \( X(k) \) inside of the set of rational points of the base elliptic curve \( E \). We prove that there exist families of conic bundles over elliptic curves defined over \( \mathbb{Q} \) such that the image of \( X(\mathbb{Q}) \) does not contain the translate of any finite index subgroup in \( E(\mathbb{Q}) \). Along the way, we prove a local-to-global principle for torsion on elliptic curves over \( \mathbb{Q} \).

Insufficiency of obstructions. Over the last two decades, several examples of varieties \( X \) over a number field \( k \) were constructed without \( k \)-rational points, but with non-empty Brauer-Manin set \( X(\mathbb{A}_k)^\text{Br} \). The insufficiency of the Brauer-Manin obstruction was first proved in 1999, when Skorobogatov constructed a bielliptic surface over \( \mathbb{Q} \) for which the the set \( X(\mathbb{A})^\text{et,Br} \), obtained by applying the Brauer-Manin obstruction to finite étale covers, was empty even though \( X(\mathbb{A})^\text{Br} \) was not \([\text{Sko99}]\). Moreover, it is reasonable to expect that there are many varieties \( X \) lacking \( k \)-points but for which even the étale Brauer-Manin set is non-empty. The first such examples were given in \([\text{Poo10, HS14}]\).

In 2016, Colliot-Thélène, Pál, and Skorobogatov \([\text{CTPS16}]\) unified many of the previously known results which each used the trick of a fibration over a curve with a single rational point. Furthermore, they provided methods for constructing new examples of \( k \)-varieties \( X \) fibered over a curve \( C \) with a single \( k \)-rational point, such that \( X(k) = \emptyset \), but \( X(\mathbb{A}_k)^\text{et,Br} \neq \emptyset \).
(For a detailed description of the obstruction sets $X(\mathbb{A})^{Br}$, $X(\mathbb{A})^{et,Br}$ and the Brauer-Manin pairing, see [Poo10].) Their work in particular demonstrated the disparity between the arithmetic of geometrically rational surfaces, for which the Brauer-Manin obstruction is conjectured to explain all failures of the Hasse principle [CTS87], and that of conic bundle surfaces over curves of genus at least 1. We prove that the aforementioned obstructions to the Hasse principle are insufficient even when the base curve is allowed to have infinitely many $k$-rational points.

**Theorem 1.1.** There exists an elliptic curve $E$ over a number field $k$ with positive rank over $k$ and a conic bundle $X \to E$ such that $X(\mathbb{A})^{et,Br} \neq \emptyset$ but $X(k) = \emptyset$.

**Distribution of rational points on conic bundles over elliptic curves.** The latter portion of this paper is devoted to studying the distribution of $\mathbb{Q}$-rational points on conic bundle surfaces $\phi: X \to E$. Our study of the image of rational points $\phi(X(\mathbb{Q})) \subset E(\mathbb{Q})$ was motivated by the following question asked by Viray at the AIM workshop "Rational and integral points on higher-dimensional varieties" in 2014 [AIM14].

**Question 1.2 (Viray).** Let $\phi: X \to E$ be a fibration onto an elliptic curve of positive rank over $\mathbb{Q}$ with geometrically integral generic fiber. Let

$$Z = \{ P \in E(\mathbb{Q}) \mid \phi^{-1}(P) \text{ is everywhere locally soluble} \}.$$ 

What can be said about $Z$? Is $|Z| < \infty$ and nonempty possible?

It follows from [CTSSD97, LM19] that $Z$ can in fact be finite; see §3.1 for details. We also provide new examples illustrating this property. In particular, we show that it is possible for $Z$ to be finite even when $\phi: X \to E$ is a conic bundle. The main objective of §3 is to focus on the case of a Châtelet conic bundle over an elliptic curve (see §2.2 for the definition) of positive rank over $\mathbb{Q}$. We show that $Z$, considered as a subset of $E(\mathbb{Q}) \simeq \mathbb{Z}^r$, does not contain a translate of a finite index subgroup.

**Theorem 1.3.** Let $E$ be an elliptic curve over $\mathbb{Q}$ with $E(\mathbb{Q}) \simeq \mathbb{Z}^r$ for some $r > 0$, satisfying some mild conditions on the Galois representation for torsion points. Then for any Châtelet conic bundle $X$ over $E$ with a singular fiber over a point $P \neq \mathcal{O} \in E(\mathbb{Q})$, the image of $X(\mathbb{Q})$ in $E(\mathbb{Q})$ does not contain a translate of a finite index subgroup inside $E(\mathbb{Q})$.

See Theorem 3.6 for the precise conditions on the Galois representations of $E$. In particular, any elliptic curve with no exceptional primes satisfy these conditions. We prove Theorem 1.3 by first establishing results of independent interest on a local-to-global principle for torsion points on elliptic curves over $\mathbb{Q}$. If an elliptic curve $E$ over $\mathbb{Q}$ admits level structure such as a rational $n$-torsion point for some integer $n > 1$, then for almost all primes $p$ of good reduction, the reduction $E_p$ does as well. One can then ask for a converse; if $E$ has some structure locally for almost all primes $p$, must $E$ possess the same such structure over $\mathbb{Q}$? Katz first considered this question for the property that $n \mid \#E(\mathbb{Q})_{\text{tors}}$ [Kat81]. In particular, when $n$ is a prime, this reduces to a local-to-global principle for rational $n$-torsion (For other
results concerning local-to-global principles for elliptic curves, see: [Vog18], [Sut12]). We consider the related property that \( E(\mathbb{Q})[n] \neq 0 \). More precisely, we ask the following:

**Question 1.4.** Let \( E/\mathbb{Q} \) be an elliptic curve and \( n > 1 \) an integer. If \( E_p(\mathbb{F}_p)[n] \neq 0 \) for all but finitely many primes \( p \), then does there exist a curve \( E' \mathbb{Q} \)-isogenous to \( E \) such that \( E'(\mathbb{Q})[n] \neq 0 \)?

We answer Question 1.4 under some mild assumptions on the curve \( E \). We also strengthen the statement from almost all primes \( p \) to almost all primes \( p \) that do not split completely in some fixed abelian extension \( K/\mathbb{Q} \), which is needed in the proof of Theorem 1.3.

**Theorem 1.5.** Let \( K/\mathbb{Q} \) be a nontrivial abelian extension not contained in \( \mathbb{Q}(E[2]) \) or \( \mathbb{Q}(\zeta_3) \). Let \( n > 1 \) be an integer and suppose that for all except possibly one odd prime \( \ell | n \), the Galois representation on \( E[\ell] \) is surjective. If it is not surjective at \( \ell \) and \( 2\ell | n \), assume further that \( \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[\ell]) = \mathbb{Q} \). Then the following are equivalent:

1. \( E_p(\mathbb{F}_p)[n] \neq 0 \) for all but finitely many primes \( p \) that do not split completely in \( K \).
2. There exists a curve \( E' \mathbb{Q} \)-isogenous to \( E \) such that \( E'(\mathbb{Q})[n] \neq 0 \).

This paper is organized as follows. In §2, we first prove that the Brauer-Manin obstruction is insufficient to explain all failures of the Hasse principle for conic bundles over many varieties whose rational points fail to be dense in the product of the real topologies. We then prove Theorem 1.1. In §3, we turn our attention to the distribution of rational points on conic bundles over elliptic curves. We answer Question 1.2 in certain cases and prove Theorem 1.3 using Theorem 1.5. In §4, we study properties of torsion points on elliptic curves and prove Theorem 1.5.

**Acknowledgements.** We thank Dan Loughran and Tony Várilly-Alvarado for fruitful discussions and their comments on a preliminary draft of this paper. Part of the work was done at the Institut Henri Poincaré, we thank the IHP for their hospitality.

2. Insufficiency of the Brauer–Manin obstructions

A recurring technique in showing failures of the Brauer–Manin obstruction is to use the real places of the number field \( k \) (e.g., [CTPS16]). More precisely, given an adelic point \( \{P_v\} \in X(\mathbb{A}) \), we can modify the point \( P_{\infty} \) by some other point \( Q_{\infty} \) on the same real component of \( X_{\mathbb{R}} \), without changing the Brauer–Manin pairing. One can then construct a fibration \( Y \to X \) such that for each \( v \), the fiber above \( P_v \) has \( k_v \)-points, but no rational point on \( X \) can approximate \( \{P_v\} \). Conic bundles are often used in this setting since their Brauer groups are well understood and can often be expressed in terms of the Brauer group of the base.

Recall from [Sko96, Definition 0.1] that a scheme of finite type over a perfect field \( k \) is called **split** if it contains a geometrically irreducible component of multiplicity one.
2.1. Example over a general base using real places.

Theorem 2.1. Let $X$ be a geometrically irreducible projective variety of dimension $\geq 2$ over a number field $k$ such that $X(k) \neq \emptyset$. Assume further that $X(\mathbb{R})$ is connected for all real embeddings of $k$. Let $d = [k : \mathbb{Q}]$ and write $d = r + 2s$, where $r$ is the number of real embeddings and $s$ is the number of complex embeddings.

(1) If $r$ is even, suppose that $X(k) \to \prod_{v \text{ real}} X(k_v)$ is not dense.

(2) If $r$ is odd, suppose that there is a real place $v_0$ such that $X(k) \to \prod_{v \neq v_0} X(k_v)$ is not dense.

Then there is a conic bundle $Y \to X$ such that $Y(\mathbb{A})^{B_k} \neq \emptyset$ but $Y(k) = \emptyset$.

Proof. If $r$ is even, let $U = \prod_{v \text{ real}} U_v$ where $U_v \subseteq X(k_v)$ is an analytic open set such that $U$ does not intersect $X(k)$. If $r$ is odd, let $U = \prod_{v \neq v_0} U_v$ where $U_v \subseteq X(k_v)$ is an open set such that $U$ does not intersect $X(k)$.

Consider the conic

$$z_0^2 + a z_1^2 = b z_2^2$$

with $a, b \in k$ and $a$ is totally positive (positive under all real embeddings of $k$). If $r$ is even, assume that this conic has local points everywhere except at the real places. If $r$ is odd, then suppose this conic has local points everywhere except at real places other than $v_0$. We build a conic bundle $Y$ over $X$ such that one of the fibers will be isomorphic to this conic.

Let $\phi : X \to \mathbb{P}^n$ be an embedding into projective space. Let $(u_v) \in U$. Pick projective coordinates $x_0, \ldots, x_n$ for $\mathbb{P}^n$ such that the affine patch $U \subset \mathbb{P}^n$ defined by $x_n \neq 0$ contains $t_v = \phi(u_v)$ for each real place $v$ and a rational point in $\phi(X(k))$. There exists an open set $W_v \subset \mathbb{P}^n(k_v)$ containing $\phi(u_v)$ such that $W_v \cap \phi(X(k_v)) \subseteq \phi(U_v)$. Let $y = [y_0, \ldots, y_n] \in \mathbb{P}^n(k)$ be a point which approximates $u_v$ for each $v$ arbitrarily closely. Define a section $g \in \mathcal{O}_{\mathbb{P}^n}(2)$ whose restriction to $U$ is given by

$$g|_U = -\sum_{i=0}^{n-1} (x_i/x_n - y_i/y_n)^2 + \epsilon$$

where $\epsilon$ is a small enough positive rational number such that $g$ is negative on $\mathbb{P}^n(k_v) \setminus W_v$ but $g(u_v)$ is positive. Also assume there exists a point $z \in X(k)$ such that $\phi(z) \in U$ and $g(\phi(z))$ is totally negative. Thus $g$ is negative on $\phi(X)(k_v) \setminus \phi(U_v)$.

Write $g|_U = g_1/g_2$ where $g_1, g_2$ are homogeneous quadratic polynomials in the coordinate ring $k[x_0, \ldots, x_n]$. By the Bertini irreducibility theorem, since $\dim X \geq 2$, there is a dense open set of quadric hypersurfaces $H$ in $\mathbb{P}^n$ such that $H \cap X$ is irreducible. Hence we deform the coefficients of $g_1$ slightly, so that $g$ is still negative on $\phi(X)(k_v) \setminus \phi(U_v)$ and positive at $u_v$, while making the intersection of $V := \{g_1 = 0\}$ and $X$ irreducible. Define $L = \phi^*\mathcal{O}(1)$.
and $f = \phi^*g \in L^{\otimes 2}$. Let $\mathcal{E}$ be the vector bundle $\mathcal{O}_X \oplus \mathcal{O}_X \oplus L$. Define the section

$$s := 1 \oplus a \oplus \frac{b}{f|_U(z)} f \in \Gamma(X, \mathcal{O}_X \oplus \mathcal{O}_X \oplus L^{\otimes 2}) \subset \Gamma(X, \Sym^2 \mathcal{E}).$$

Then the vanishing of $s$ defines a conic bundle $\pi: Y \to X$ with a dense open affine subset given by

$$z_0^2 + az_1^2 = \frac{b}{f|_U(z)} f|_U.$$

For any real place $v$, $Y$ has $v$-adic points over $u_v$. For any finite place $v$, the fiber above $z$ has $v$-adic points by hypothesis. Thus $Y$ is everywhere locally soluble. Since for each $U_v$, there are no $v$-adic points above $X(k_v) \setminus U_v$, and $X(k) \cap U = \emptyset$, so $Y$ has no rational points.

Let $(y_v) \in Y(\mathbb{A})$ be an adelic point of $Y$ which maps to $z$ for each finite place $v$. Since $X(\mathbb{R})$ has only one connected component and the evaluation map is constant on connected components, the Brauer–Manin pairing of $\pi((y_v))$ with any element of $\Br(X)$ is same as that of $z \in X(k) \subset X(\mathbb{A})$, hence it is orthogonal to $\Br(X)$. The irreducibility of $\phi^*g_1 = 0$ implies that there exists some codimension one point $Q$ on $X$ such that for any other codimension one point $Q \neq P$ on $X$, the fiber $Y_{k(Q)}$ is nonsplit. Hence $\Br(Y) = \pi^*\Br(X)$ by [CTPS16, Prop 2.2], and so $(y_v) \in Y(\mathbb{A})^{\Br}$. Thus, there is no obstruction arising from $\Br(Y)$. 

\[\square\]

**Remark 2.2.** The proof of Theorem 2.1 necessitates the existence of at least 2 real embeddings of the ground field $k$. In particular, it does not work over $k = \mathbb{Q}$. The proof furthermore requires $X$ to have dimension at least 2, but this condition is likely not necessary. However, in order to obtain examples for which the \textit{étale-Brauer} obstruction is insufficient to explain failures of the Hasse principle, we restrict our focus to a class of conic bundle surfaces.

### 2.2. Châtelet conic bundles over elliptic curves.

Let $E/k$ be an elliptic curve of positive rank over number field $k$ with short Weierstrass equation $y^2 = x^3 + bx + c$, and let $\pi: E \to \mathbb{P}^1$ be the morphism sending $(x, y)$ to $x$. Consider the Châtelet surface $Y \to \mathbb{P}^1$ defined by

$$u_0^2 - au_1^2 = f(x)u_2^2,$$

where $f(x)$ is a separable polynomial in $k[x]$ and $a \in k^x \setminus k^{x^2}$ is square free. Let $X$ be the fiber product $Y \times_{\mathbb{P}^1} E$. We will henceforth refer to such $\phi: X \to E$ as a Châtelet conic bundle over an elliptic curve.

The following theorem is motivated by the construction in [CTPS16, §5], in which they produced a conic bundle over an elliptic curve with a single rational point such that the \textit{étale} Brauer–Manin obstruction was insufficient. We construct such an example of Châtelet conic bundle over an elliptic curve of positive rank following their techniques.

**Theorem 2.3.** There exists a real quadratic field $k$, an elliptic curve $E$ with a point $Q \in E$ and a Châtelet conic bundle $\phi: X \to E$ satisfying the following properties:

- the fibres of $\phi: X \to E$ are conics;
- $E(k) = \mathbb{Z}$ and all fibers of $\phi: X \setminus X_Q \to E \setminus Q$ are split;
• $X(k) = \emptyset$ and $X(\mathbb{A})^{et,Br} \neq \emptyset$.

Proof. Let $E$ be the elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 - 432x + 15120$. Then $E(\mathbb{Q}) \simeq \mathbb{Z}$, and $E(\mathbb{R})$ is connected. Let $k = \mathbb{Q}(\sqrt{5})$ so that $E(k) \simeq E(\mathbb{Q})$. Write the defining equation of $E$ as $y^2 = r(x)$. Let $a' = 3 + 9\sqrt{5}$. Then $r(a') = 17496$ and let $K := k(\sqrt{17496})$ so that $P := (3 + 9\sqrt{5}, \sqrt{17496})$ is a point on $E(K)$. Write $P = mQ$ for some $Q \in E(K)$ where $Q$ is nondivisible. Let $\sigma \in \text{Gal}(K/k)$ be the unique nontrivial element. Then $P^\sigma = -P$ implies that $m(Q^\sigma + Q) = 0$. A Magma [BCP97] computation shows that $E(K)$ is torsion free, so $Q^\sigma = -Q$. Hence the $x$-coordinate $a := x(Q)$ is defined over $k$, but not $\mathbb{Q}$ since $k(Q)$ is a biquadratic extension of $\mathbb{Q}$. Let $\tau \in \text{Gal}(k/\mathbb{Q})$ be a generator. Choose a rational number $b \in \mathbb{Q}$ such that $b$ lies in the interval between $a$ and $a^\tau$ and such that $v_5(b) = 0$. Then $r(b) \equiv b(b^2 - 2) \pmod{5}$ whence $v_5(r(b)) = 0$. Since $K$ is a totally real field, we have $r(a) > 0$. Moreover by continuity of $r(x)$ we can choose $b$ sufficiently close to $a$ so that $r(b) > 0$ as well. Let $n$ be the product of all primes appearing in $r(b)$. Let $p$ be a prime such that $-p \equiv 1 \pmod{8n}$ and $p \equiv 2 \pmod{5}$. Note that $p$ is inert in $k$. Then the quaternion algebra over $k$ defined by

$$(-r(b), -p)_2$$

is ramified only at the two real places. Indeed it is unramified at all primes appearing in $2r(b)$ by construction, so the only possibilities for ramification are at $p$ and the two real places. Since it is clearly ramified at the two real places, by Hilbert’s reciprocity law, it must be unramified at $p$.

Fix a point $P_0 := (x_0, y_0) \in E(k)$ such that $(x_0 - a)(x_0 - b)$ is totally positive; this is possible since $E(k)$ is dense in $E(\mathbb{R})$. Let $\phi : X \to E$ be the Châtelet conic bundle over $E$ defined by

$$u^2 + r(b)v^2 = -p\frac{(x-a)(x-b)}{(x_0-a)(x_0-b)}w^2.$$

We first show that $X$ is everywhere locally soluble. Note that the fiber above $P_0$ has local points at all the finite places by the calculation above. For each finite place $v$, let $M_v$ be any $k_v$ point on the fiber above $P_0$. Let $v_1$ and $v_2$ denote the two real places, where $k \to k_{v_1} \simeq \mathbb{R}$ sends $\sqrt{5}$ to itself while $k \to k_{v_2} \simeq \mathbb{R}$ sends $\sqrt{5}$ to $-\sqrt{5}$. By choosing $x \in \mathbb{R}$ with $r(x) > 0$ in the interval between $a$ and $b$ for $v_1$ (resp. in the interval between $a^\tau$ and $b$ for $v_2$) we find that $(x-a)(x-b) < 0$ (resp. $(x-a^\tau)(x-b) < 0$). Hence the fiber above $(x, y)$ has a $k_{v_i}$-point $M_{v_i}$ for $i = 1, 2$. This defines a point $\{M_v\} \in X(\mathbb{A})$.

To show $X$ has no $k$-rational points, note that for any $R := (x, y) \in E(k)$, the quantity

$$-p\frac{(x-a)(x-b)}{(x_0-a)(x_0-b)}$$

is always negative in at least one real place, since $x \in \mathbb{Q}$. Hence the conic $X_R$ has no $k$-rational point.

By [CTPS16, Proposition 2.2], $\phi^* : \text{Br}(E) \to \text{Br}(X)$ is surjective since all fibers of $\phi$ away from the fiber over the closed point of $E$ corresponding to $x = a$ have a geometrically integral
component of multiplicity one defined over \( k \). Since \( \phi(\{M_v\}) \) is orthogonal to \( \text{Br}(E) \) as it pairs in the same way as \( P_0 \in E(k) \), we have \( \{M_v\} \in X(\mathbb{A})^\text{Br}. \)

The remainder of the proof, that is, showing that \( X(\mathbb{A})^{\text{et},\text{Br}} \neq \emptyset \), will follow from Theorem 2.4 below, applied to the conic bundle \( X' := X \times_E E \rightarrow E \) where \( E \rightarrow E \) is given by translation by \( P_0 \). Since \( E \) is a Serre curve \([\text{Ser72}, \S 5.2] \), \( E \) has large Galois image (see below). Since \( X' \) is isomorphic to \( X \) over \( k \), \( X'(\mathbb{A})^{\text{et},\text{Br}} \neq \emptyset \) implies \( X(\mathbb{A})^{\text{et},\text{Br}} \neq \emptyset \), as desired. \( \Box \)

In \([\text{CTPS16}] \), an elliptic curve over \( k \) is said to have \emph{large Galois image} if the image of \( \rho: \text{Gal}(\overline{k}/k) \rightarrow \text{GL}_2(\widehat{\mathbb{Z}}) \) coming from the Galois representation of torsion points on \( E \) contains \( \text{SL}_2^+(\mathbb{Z}) \), where \( \text{SL}_2^+(\mathbb{Z}) \) is the kernel of the composition \( \text{SL}_2(\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \mathbb{Z}/2\mathbb{Z} \). The following theorem is an amalgamation of various results proved in \([\text{CTPS16}] \).

**Theorem 2.4.** Let \( k \) be a totally real field, and let \( K \) be a field such that \( k \subset K \subset k^{\text{cyc}} \). Suppose that \( E \) is an elliptic curve over \( k \) such that \( E(\mathbb{R}) \) is connected and \( E \) has large Galois image. Let \( \phi: X \rightarrow E \) be a conic bundle where each fiber contains a geometrically integral component of multiplicity one, except a single nonsplit fiber over \( P \in E(K) \) which is nondivisible. Finally, suppose that the fiber over \( O \in E(k) \) is locally soluble at all finite places of \( k \). If \( \{M_v\} \in X(\mathbb{A}) \) where \( \phi(M_v) = O \) for all finite places, then \( \{M_v\} \in X(\mathbb{A})^{\text{et},\text{Br}}. \)

**Proof.** The proof follows from \([\text{CTPS16}, \text{Thm. 5.6}] \) mutatis mutandis, however, we repeat a sketch of the argument here for the convenience of the reader. By \([\text{CTPS16}, \text{Prop. 2.2} \text{], the map} \text{Br}(E) \rightarrow \text{Br}(X) \) is surjective. By \([\text{CTPS16}, \text{Prop. 2.3} \text{], any torsor} X' \rightarrow X \) comes from some torsor \( \phi: E' \rightarrow E \). Twisting by a finite \( k \)-group scheme \( G \), we can assume \( E' \) has a point \( O' \) mapping to \( O \). Let \( C \subset E' \) be the connected component of \( O' \). Choosing \( O' \) as the origin of \( C \) makes \( C \rightarrow E \) an isogeny of elliptic curves. Then \( Y \subset X' \times C \) is a conic bundle \( g: Y \rightarrow C \). By \([\text{CTPS16}, \text{Thm. 4.1} \text{] \),} \phi^{-1}(P) \text{ is integral. Hence} Q := \phi^{-1}(P) \text{ is a closed point of} C \text{, so applying} \([\text{CTPS16}, \text{Prop. 2.2} \text{]} \text{ again gives} g^* \text{Br}(C) \rightarrow \text{Br}(Y) \text{ is surjective. For each finite place} v \text{, let} M'_v \text{ be a point on} Y \text{ on the fiber above} O' \text{ that maps to} M_v \in X(k_v). \text{ For the infinite places} v \text{, let} M'_v \text{ be any real point on} Y \text{ mapping into} M_v. \text{ Since} \text{Br}(Y) = g^*\text{Br}(C) \text{, we have} \{M'_v\} \in Y(\mathbb{A})^\text{Br} \text{ so that} \{M'_v\} \in X'(\mathbb{A})^\text{Br} \text{. Hence} \{M_v\} \in X(\mathbb{A})^{\text{et},\text{Br}}. \( \Box \)

3. Distribution of rational points

The results of the previous section, in particular Theorem 2.3, demonstrated the insufficiency of the Brauer–Manin obstruction for varieties fibered over positive rank elliptic curves. In this section we consider those varieties \( X \) with a dominant morphism \( \phi: X \rightarrow E \) for which \( X(k) \neq \emptyset \), and study properties of the image of \( X(k) \) inside of \( E(k) \).

For the remainder of this section, we fix \( k = \mathbb{Q} \) and assume that \( \phi \) does not have a section over \( \mathbb{Q} \) and \( X(\mathbb{Q}) \neq \emptyset \). We are interested in the following questions concerning the set \( \phi(X(\mathbb{Q})) \subseteq E(\mathbb{Q}) \):
(1) Can \( \phi(X(\mathbb{Q})) \) be finite or infinite?

(2) Does \( \phi(X(\mathbb{Q})) \) contain a translate of a finite index subgroup in \( E(\mathbb{Q}) \), i.e., does the closure \( \phi(X(\mathbb{Q})) \subseteq E(\mathbb{A}) \) contain an open subset of \( E(\mathbb{Q}) \cong \hat{\mathbb{Z}}^r \) (see e.g., [Sko99, p. 126])

**Remark 3.1.** The motivation in asking (2) is that for any finite set of primes \( S \), the subset
\[
\{ P \in E(\mathbb{Q}) \mid \text{the fiber above } P \text{ contains } \mathbb{Q}_p\text{-points for } p \in S \} \subseteq E(\mathbb{Q}) \quad (3.1)
\]
always contains a translate of a finite index subgroup in \( E(\mathbb{Q}) \). To see this, let \( P \in E(\mathbb{Q}) \) be a point such that the fiber above \( P \) contains a rational point. If \( \phi^{-1}(P) \) is singular, there is another point \( P' \) such that \( \phi^{-1}(P') \) is smooth, and has \( \mathbb{Q}_p \)-points for each \( p \in S \). Hence we may assume \( \phi^{-1}(P) \) is smooth and has \( \mathbb{Q}_p \)-points for each \( p \in S \), though it need not have a rational point. By the implicit function theorem, for each \( p \in S \), there exist \( p \)-adic analytic open neighborhoods \( U_p \subset X(\mathbb{Q}_p) \) containing \( P \) such that for any point \( Q \in U_p(\mathbb{Q}_p) \), the fiber above \( Q \) has \( \mathbb{Q}_p \)-points. We can find a finite set of points \( Q_i = (x_{Qi}, y_{Qi}) \in E(\mathbb{Q}) \) such that \( -v_p(x_{Qi}) \) is large for every \( p \in S, 1 \leq i \leq r \), and \( \{ Q_i \} \) generates a finite index subgroup of \( E(\mathbb{Q}) \). By continuity in the \( p \)-adic topology of the group law on elliptic curves, we can assume that \( P + nQ_i \) lies in \( U_p \) for any \( n \in \mathbb{Z}, p \in S \), and \( 1 \leq i \leq r \). It follows that \( \phi^{-1}(P + nQ_i) \) also has \( \mathbb{Q}_p \)-points for every \( p \in S \). Hence (3.1) contains \( P + H \) where \( H \) is the subgroup generated by \( \{ Q_i \} \).

We first consider (1) and give some new examples, including conic bundles, for which the image of the rational points is finite. In Proposition 3.7, we provide an example for which \( \phi(X(\mathbb{Q})) \) is infinite. We then consider (2) for Châtelet conic bundles over an elliptic curve with a nonsplit fiber over a nonzero rational point on \( E \). We show that in this case, (2) is false in general, but there are examples for which it is true.

### 3.1. Examples of finiteness of \( \phi(X(\mathbb{Q})) \).

Let \( V \) be a smooth projective variety equipped with a morphism \( \pi: V \to \mathbb{P}^1 \) with geometrically integral generic fiber. If \( \pi \) has at least 6 geometric double fibers, then the \( k \)-points of \( V \) are contained in only finitely many fibers [CTSSD97, Cor. 2.2]. In fact, more is true; only finitely many fibers are everywhere locally soluble [LM19, Thm. 1.4]. Moreover, if \( E \) is an elliptic curve, then under the double cover \( E \to \mathbb{P}^1 \), one finds that the image of the rational points of \( V \times_{\mathbb{P}^1} E \to E \) is finite. This subsection contains concrete examples illustrating the finiteness of \( \phi(X(\mathbb{Q})) \) which do not follow from these results.

**Proposition 3.2.** Let \( E \) be the elliptic curve over \( \mathbb{Q} \) with Weierstrass equation \( y^2 = x^3 + 2x - 2 \). Consider the Châtelet conic bundle over an elliptic curve \( \phi: X \to E \) given by the equation
\[
u_0^2 + u_1^2 = 3xu_2^2.
\]
Then \( X \) has rational points over the origin \( O \in E(\mathbb{Q}) \) but no rational point on any other fiber.
Proof. The fiber over the origin \( O \in E(\mathbb{Q}) \) has a singular point defined over \( \mathbb{Q} \). We show that no other fiber has a rational point. Let \( O \neq P \in E(\mathbb{Q}) \) with \( P = (x, y) \). Write \( x = 2^r s \) with \( s \in \mathbb{Z}_2^\times \). Then the equality
\[
y^2 = 2^{3r}s^3 + 2 \cdot 2^r s - 2
\]
shows that \( r \leq 0 \) and even, and so \( s \equiv 1 \pmod{4} \). Hence \( 3s \equiv 3 \pmod{4} \). Any real solution must have \( x > 0 \), hence there exists a prime \( p \equiv 3 \pmod{4} \) such that \( v_p(3s) \) is odd. Thus, the conic
\[
u_0^2 + u_1^2 - 3xu_2^2 = 0
\]
does not have solutions over \( \mathbb{Q}_p \). \( \square \)

Remark 3.3. We do not know whether \( \phi(X(\mathbb{Q})) \) can be finite for conic bundles if there is a smooth fiber with rational points.

We give an analogous example showing that the image of the rational points can be finite for fibrations where the fibers are higher genus curves. In this case, we permit rational points to be on smooth fibers as well.

Proposition 3.4. Let \( n > 2 \) be an integer. \( E \) be the elliptic curve given by the equation \( y^2 = x^3 + 2 \). Note that \( E(\mathbb{Q}) \) has rank 1. Let \( V \) be a smooth projective model of the variety defined by
\[
\{ [u, v, w] \times (x, y) \in \mathbb{P}^2 \times E \mid u^n + xv^n + x^2w^n = 0 \}.
\]
Then \( V \) has only finitely many fibers containing rational points.

Proof. Let \( \pi : V \to E \) be projection. The fiber above \((-1, \pm 1) \in E(\mathbb{Q})\) contains rational points over \( \mathbb{Q} \). Suppose a rational point \((x, y) \in E(\mathbb{Q})\), satisfies the condition that for each prime \( p \), \( v_p(x) \equiv 0 \pmod{n} \). Then \( x = z^3 \) for some \( z \in \mathbb{Q} \) and we obtain a point on the curve \( y^2 = z^{3n} - 1 \). This is a smooth curve of genus at least 2, hence has only finitely many rational points by Faltings’ theorem. Thus for all but finitely many rational points \( P \in E \), we have \( x(P) \) is not an \( n \)th power. Let \((x, y) \in E(\mathbb{Q})\) be such a point, and let \( p \) be a prime where \( v_p(x) \equiv c \neq 0 \pmod{n} \). We show that the fiber above \((x, y)\) is insoluble over \( \mathbb{Q}_p \). Suppose on the contrary that it has \( \mathbb{Q}_p \)-points; assume \( u, v, w \in \mathbb{Q}_p \) is a solution. Then
\[
\begin{align*}
v_p(u^n) & \equiv 0 \pmod{n} \\
v_p(xv^n) & \equiv c \pmod{n} \\
v_p(x^2w^n) & \equiv 2c \pmod{n}
\end{align*}
\]
Since not all three of the above valuations can equal \( \infty \), exactly one of the terms \( u^n, xv^n, x^2w^n \) must achieve minimum valuation. Hence the sum cannot be 0, a contradiction. Thus only finitely many rational points of \( E \) have everywhere locally soluble fibers in \( V \). \( \square \)

3.2. Translates of finite index subgroups of \( E(\mathbb{Q}) \). We focus our attention again on Châtelet conic bundles over an elliptic curve, \( \phi : X \to E \) defined by an equation of the form (2.1). We answer question (2) in the negative when \( E \) has a point \( P = (x, y) \in E(\mathbb{Q}) \) such
that \( f(x) = 0 \), i.e. when \( X \) has a rational singular fiber which is nonsplit over \( \mathbb{Q} \). By applying an automorphism of \( E \), we can assume \( P = O \), the identity in \( E(\mathbb{Q}) \). This is equivalent to \( f \) having odd degree. For each prime \( p \) of good reduction, define \( n_p := |E_p(\mathbb{F}_p)| \). Let \( E_1(\mathbb{Q}_p) := \ker( E(\mathbb{Q}_p) \to E_p(\mathbb{F}_p)) \). Then any \( P \neq O \in E_1(\mathbb{Q}_p) \) has \( 3v_p(x(P)) = 2v_p(y(P)) = -6i \) for some integer \( i \geq 1 \) [Sil09, VII.2 Prop. 2.2].

**Lemma 3.5.** Let \( E/\mathbb{Q} \) be an elliptic curve given by a short Weierstrass equation and \( p \) be a prime of good reduction. Let \( O \neq P \in E_1(\mathbb{Q}_p) \) and let \( i \geq 1 \) be the integer such that \( v_p(x(P)) = -2i \). If \( Q \in (w, z) \in E(\mathbb{Q}_p) \) where \( w, z \in \mathbb{Z}_p^\times \), then \( x(P + Q) = w + pu \) for some \( u \in \mathbb{Z}_p^\times \).

**Proof.** Let \( P = (\frac{w}{p^x}, \frac{y}{p^x}) \) where \( x, y \in \mathbb{Z}_p^\times \). By the addition formula,

\[
x(P + Q) = \left( \frac{y - p^{3i}z}{p^i x - p^{3i}w} \right)^2 - \frac{x}{p^{2i}} - w
\]

\[
= \frac{1}{p^{2i}} \left( \frac{y^2 - x^3 + 2p^{2i}x^2w + p^{3i}u}{(x - p^{2i}w)^2} - w \right)
\]

\[
= \frac{1}{p^{2i}} \left( \frac{2p^{2i}x^2w + p^{3i}u'}{(x - p^{2i}w)^2} - w \right)
\]

\[
= (2x^2w + pu')(x^2 + p^{2i}v) - w
\]

\[
= w + pu''
\]

where \( u, u', u'', v \in \mathbb{Z}_p^\times \). \( \square \)

We define an elliptic curve \( E \) over \( \mathbb{Q} \) to be **almost surjective** if it satisfies the following conditions:

- For any isogenous \( E' \), \( E'(\mathbb{Q}) \) is torsion free.
- \( \rho_\ell \) is surjective for all \( \ell > 2 \) except for possibly one prime.
- If \( \rho_\ell \) is not surjective for some \( \ell > 2 \), then \( k_2 \cap k_\ell = \mathbb{Q} \).

Any elliptic curve with no exceptional prime (i.e. \( \rho_\ell \) is surjective for every prime \( \ell \)) will satisfy these conditions (e.g., Serre curves). Almost all elliptic curves satisfy these conditions [Duk97, Jon10].

**Theorem 3.6.** Let \( E/\mathbb{Q} \) be an almost surjective elliptic curve of positive rank defined by \( y^2 = r(x) \). Let \( \phi: X \to E \) be the Châtelet conic bundle over \( E \) given by

\[
u_0^2 - au_1^2 = f(x)u_2^2
\]

where \( \sqrt{a} \notin k_2(\sqrt{-3}) \). Suppose \( X \) has a singular fiber over \( P_0 = (w, z) \in E(\mathbb{Q}) \).

Then \( \phi(X(\mathbb{Q})) \) does not contain a translate of a finite index subgroup of \( E(\mathbb{Q}) \).

**Proof.** Suppose that \( \phi(X(\mathbb{Q})) \) contains a subset \( P + H \) where \( P \in E(\mathbb{Q}) \) and \( H \subset E(\mathbb{Q}) \) is finite index subgroup. Since \( H \) contains the subgroup \( nE(\mathbb{Q}) \subset E(\mathbb{Q}) \) for some \( n \), we can
assume that $H = nE(\mathbb{Q})$. By Corollary 4.15, there are infinitely many primes $p$ of good reduction such that $\sqrt{a} \notin \mathbb{Q}_p$ and $E_p(\mathbb{F}_p)[n] = 0$. Choose such a prime $p$ not dividing $a, n$, or $g(w)$, where $g(x) = f(x)/(x - w)$. By the theory of formal groups of elliptic curves, there is an isomorphism of groups

$$\xi: E_1(\mathbb{Q}_p) \to p\mathbb{Z}_p = \hat{E}(p\mathbb{Z}_p), \quad (x, y) \mapsto -\frac{x}{y}$$

such that $v_p(\xi(Q)) = -v_p(x(Q))/2$ [Sil09, VII Prop. 2.2, Prop. 6.3].

By replacing $P$ by $P + nQ$ for some $Q \in E(\mathbb{Q})$ if necessary, we may assume that $P - P_0 = \mathcal{O}$ and set $R := P - P_0$. Let $\tilde{R}$ be the image of $R$ in the reduction $E_p$ of $E$ modulo $p$. Let $m_p$ be the order of $\tilde{R}$, which is relatively prime to $n$ since $E_p(\mathbb{F}_p)[n] = 0$, so that $m_pR ∈ E_1(\mathbb{Q}_p)$ and $v_p(x(m_pR)) \leq -2$. By the isomorphism (3.2), for any $Q ∈ E_1(\mathbb{Q}_p)$ and any integer $m$, we have $v_p(\xi(mQ)) = v_p(m) + v_p(\xi(Q))$, and hence $v_p(x(mQ))/2 = -v_p(m) + v_p(x(Q))/2$. Thus, setting either $s = m_p$ or $pm_p$, we find that $v_p(x(sR)) = -2i$ where $i > 0$ is odd. Since $(s, n) = 1$, there exist integers $t, t'$ with $t$ relatively prime to $p$ such that $st + nt' = 1$. We obtain $stR = P - P_0 + nQ$, with $Q := -t'R ∈ E(\mathbb{Q})$. Since $v_p(x(sR)) = v_p(x(sR')) = -2i$, by Lemma 3.5, $stR + P_0$ has $x$-coordinate $w + p^i w'$ for some $w' ∈ \mathbb{Z}_p^\times$. Hence the fiber above $P + nQ = stR + P_0$ is given by the conic

$$u_0^2 - au_1^2 = f(w + p^i w')u_2^2.$$ 

By construction, $v_p(f(w + p^i w')) = v_p(p^i w'g(w + p^i w')) = i$, which is odd. Hence this conic does not have any $\mathbb{Q}_p$ points, since $a \notin \mathbb{Q}_p^2$. \hfill $\square$

Theorem 3.6 may not hold if $E$ is allowed to have nontrivial torsion over $\mathbb{Q}$, as the following proposition shows.

**Proposition 3.7.** Let $E$ be the elliptic curve

$$y^2 = x(x - 1)(x - 7)$$

which has rank 1 and full 2–torsion subgroup defined over $\mathbb{Q}$. Let $X$ be the Châtelet conic bundle over $E$ defined by

$$u^2 + 3v^2 = xw^2.$$ 

Then $\phi(X(\mathbb{Q}))$ contains a translate of a finite index subgroup inside $E(\mathbb{Q})$.

**Proof.** The point $P = (1/4, 9/8)$ is a generator of the infinite subgroup of $E(\mathbb{Q})$. Let $\tilde{P}$ be the reduction of $P$ modulo $p$. Then the order of $\tilde{P}$ is divisible by 2 if there does not exist a point $\tilde{Q}$ such that $2\tilde{Q} = \tilde{P}$. For any field $K$ of characteristic not 2, the point $P$ is divisible by 2 if and only if $1/4 - 1$ and $1/4 - 7$ are both squares in $K$ ([Cas6601, p. 269–270]). Let $p > 3$ be a prime for which $E$ has good reduction. If $\sqrt{-3} \notin \mathbb{F}_p$, then $\tilde{P}$ is not divisible by 2 in $E_p(\mathbb{F}_p)$. Hence $\tilde{P}$ has order divisible by 2. Thus no point in the set $\{(1 + 2k)P\}$ will reduce to $\tilde{O}$ mod $p$ for any $p > 7$. Let $R = (0, 0)$ be a 2-torsion point on $E(\mathbb{Q})$ and set $M := P + R$. Then, no point in the set $\{(1 + 2k)M\}$ will reduce to $\tilde{R}$ mod $p$ for any $p > 7$. 

\hfill 11
By the discussion above, any point in \{(1 + 2k)M\} has even valuation for primes \(p > 3, p \neq 7\), so the fiber above will have \(\mathbb{Q}_p\)-points. For \(p = 7\), since \(\sqrt{-3} \in \mathbb{Q}_7\), any fiber will have a \(\mathbb{Q}_7\)-point. Finally, the fiber above \(M\) has rational points, e.g., \((u, v, w) = (4, 2, 1)\), so in particular it has \(\mathbb{Q}_p\)-points for \(p = 2, 3\). There exists integers \(n_2, n_3\) such that for any integer \(k\), \(kn_2P\) and \(kn_3P\) are very close to \(O\) in the analytic topology induced by \(\mathbb{Q}_2\) and \(\mathbb{Q}_3\) respectively. Hence \(P\) and \((1 + kn_2)P\) are sufficiently close in the 2-adic topology, and by the implicit function theorem, the fibers above \((1 + kn_2)P\) all have \(\mathbb{Q}_2\)-points. Similarly for \(\mathbb{Q}_3\). Hence the fibers above points in \{(1 + 2n_2n_3k)P\} will each be everywhere locally soluble at all the finite primes, and so will also be soluble at infinity. Hence they have \(\mathbb{Q}\)-rational points by the Hasse–Minkowski Theorem. 

4. Torsion points on elliptic curves

Let \(E\) be an elliptic curve over \(\mathbb{Q}\). In [Kat81, Thm. 2], Katz proved that given any integer \(n > 1\), \([\#E_p(\mathbb{F}_p)]n \neq 0\) for all but finitely many primes \(p\), then does there exist a curve \(E'\) \(\mathbb{Q}\)-isogenous to \(E\) such that \([\#E'(\mathbb{Q})]n \neq 0\)?

Note that this does not follow directly from Katz’s result when \(n\) is not a prime. For example if \(n = \ell_1\ell_2\), we must consider the possibility that \(E_p(\mathbb{F}_p)\) contains either \(\ell_1\)-torsion or \(\ell_2\)-torsion for almost all \(p\).

We shall need the following notation. For any positive integer \(n\), let \(k_n\) denote the \(n\)th division field of \(E\), i.e., \(k_n := \mathbb{Q}(E[n])\). Let \(\rho_n : \text{Gal}(k_n/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/n\mathbb{Z})\) be the Galois representation on the \(n\)-torsion points. Let \(NF_n \subset \text{Gal}(k_n/\mathbb{Q})\) be the subset of elements \(\sigma\) such that \([E[n]]^\sigma = 0\). If \(L, M\) are Galois extensions of a field \(K\) and \(\sigma \in \text{Gal}(L/K), \tau \in \text{Gal}(M/K)\) then we say \(\sigma\) and \(\tau\) are compatible if \(\sigma|_{L\cap M} = \tau|_{L\cap M}\).

Lemma 4.2. Let \(\ell > 2\) be a prime and \(G\) be the image of \(\rho_\ell : \text{Gal}(k_\ell/\mathbb{Q}) \to \text{GL}_2(\mathbb{F}_\ell)\). Suppose there is a point \(P \in E[\ell]\) such that \(\text{det}(\rho_\ell(\text{Gal}(k_\ell/\mathbb{Q}(P)))) = \mathbb{F}_\ell^\times\). Then \(G\) is conjugate to one of the following groups:

(1) \(G : \text{GL}_2(\mathbb{F}_\ell)\)

(2) \(B : \left\{ \begin{bmatrix} x & * \\ 0 & y \end{bmatrix} \mid x \in (\mathbb{F}_\ell^\times)^{\ell - 1}, y \in \mathbb{F}_\ell^\times \right\}, d \mid \ell - 1\)

(3) \(Cs : \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \mid x \in (\mathbb{F}_\ell^\times)^{\ell - 1}, y \in \mathbb{F}_\ell^\times \right\}, d \mid \ell - 1\)

Note that this does not follow directly from Katz’s result when \(n\) is not a prime. For example if \(n = \ell_1\ell_2\), we must consider the possibility that \(E_p(\mathbb{F}_p)\) contains either \(\ell_1\)-torsion or \(\ell_2\)-torsion for almost all \(p\).
(4) B : \{\begin{bmatrix} x & * \\ 0 & y \end{bmatrix} | x \in \mathbb{F}_\ell^\times, y \in (\mathbb{F}_\ell^\times)^{\ell - 2} \} , \ell \mid d \mid \ell^2 - \ell

(5) \text{Ns} : \{\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}, \begin{bmatrix} 0 & x \\ y & 0 \end{bmatrix} | x \in \mathbb{F}_\ell^\times, y \in \mathbb{F}_\ell^\times\}

(6) S_4 : \ell = 5 and G has projective image isomorphic to $S_4$ is exceptional. It is generated by $\begin{bmatrix} 0 & 3 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 4 & 4 \end{bmatrix}$

where $d = \text{deg}(\mathbb{Q}(P)/\mathbb{Q})$ [Sut16, Table 3].

**Proof.** There are $\ell^2 - \ell$ points in $E[\ell] \setminus \{O, P, 2P, \ldots, (\ell - 1)P\}$ which divide into Galois orbits over $\mathbb{Q}(P)$. Since $k_\ell/\mathbb{Q}(P)$ must have degree divisible by $\ell - 1$, there is either one Galois orbit of size $\ell^2 - \ell$ or there are $\ell$ orbits of size $\ell - 1$.

**Case 1** (there exists an orbit of size $\ell^2 - \ell$). Either the Galois closure of $\mathbb{Q}(P)$ is itself or it is $k_\ell$. Suppose $\mathbb{Q}(P)$ is Galois over $\mathbb{Q}$ of degree $d > 1$. Let $Q$ be any point in the orbit of size $\ell^2 - \ell$. With respect to the basis $\{P, Q\}$, $G$ is a subgroup of the matrix group

\[ \left\{ \begin{bmatrix} x & * \\ 0 & y \end{bmatrix} | x \in (\mathbb{F}_\ell^\times)^{\frac{d}{\ell - 1}}, y \in \mathbb{F}_\ell^\times \right\}. \]

Since $\text{deg}(k_\ell/\mathbb{Q}) = \text{deg}(k_\ell/\mathbb{Q}(P)) \cdot \text{deg}(\mathbb{Q}(P)/\mathbb{Q}) = (\ell^2 - \ell)d$, it follows that $G$ is in fact equal to the matrix group above.

Now suppose the Galois closure of $\mathbb{Q}(P)$ is $k_\ell$. Then we must have that $P$ is conjugate to every point in $E[\ell] \setminus \{O\}$. Hence

\[ \text{deg}(k_\ell/\mathbb{Q}) = \text{deg}(k_\ell/\mathbb{Q}(P)) \cdot \text{deg}(\mathbb{Q}(P)/\mathbb{Q}) = (\ell^2 - \ell)(\ell^2 - 1). \]

By order considerations, this forces $G$ to be $\text{GL}_2(\mathbb{F}_\ell)$.

**Case 2** (there exist $\ell$ orbits of size $\ell - 1$). Fix a basis $\{P, Q'\}$ of $E[\ell]$, such that a generator of $\text{Gal}(k_\ell/\mathbb{Q}(P))$ is mapped to $\begin{bmatrix} 1 & x \\ 0 & y \end{bmatrix}$ for some $x \in \mathbb{F}_\ell$ and $y \in \mathbb{F}_\ell^\times$, $y \neq 1$. Then since $\left(\frac{x}{y - 1}, 1\right)$ is an eigenvector with eigenvalue $y$, we have that the orbit of $Q := \frac{x}{y - 1}P + Q'$ is $\{Q, 2Q, \ldots, (\ell - 1)Q\}$. Hence, over $\mathbb{Q}(P)$, the points of $E[\ell] \setminus \{O, P, \ldots, (\ell - 1)P\}$ break up into the following $\ell$ orbits of size $\ell - 1$:

\[ O_0 = \{Q, 2Q, \ldots, (\ell - 1)Q\} \]
\[ O_1 = \{P + Q, P + 2Q, \ldots, P + (\ell - 1)Q\} \]
\[ \vdots \]
\[ O_{\ell-1} = \{(\ell - 1)P + Q, \ldots, (\ell - 1)P + (\ell - 1)Q\} \]
Suppose first that $Q(P)$ is Galois over $\mathbb{Q}$, of degree $d > 1$. With respect to the basis \{P, Q\}, $G$ is a subgroup of the matrix group
\[
\begin{bmatrix}
x & 0 \\
0 & y
\end{bmatrix} \mid x, y \in (\mathbb{F}_\ell^\times)^{\frac{\ell-1}{d}}.
\]
By degree considerations again, we must have that $G$ is equal to the group above.

For the remainder of the proof, suppose the Galois closure of $Q(P)$ is $k_\ell$. First suppose that $O_0$ is a Galois orbit over $\mathbb{Q}$. Let $T := \{1 \leq n \leq \ell - 1 \mid P \sim nP\}$, where $\sim$ denotes Galois conjugate points. There exists some $0 < i \leq \ell - 1$ such that $P$ is conjugate to points in $O_i$. Then
\[
\bigcup_{n \in T} O_{in} \cup \{nP\}
\]
is a Galois orbit over $\mathbb{Q}$. From this we find that $\ell | d | \ell(\ell - 1)$. Hence by degree count, $G$ must be conjugate to the matrix group
\[
\begin{bmatrix}
x & * \\
0 & y
\end{bmatrix} \mid x, y \in (\mathbb{F}_\ell^\times)^{\frac{\ell^2 - 1}{d}}.
\]

Now suppose that $O_0$ is not a Galois orbit over $\mathbb{Q}$, i.e., $Q(Q)$ is not Galois over $\mathbb{Q}$. Suppose $Q \sim aP + bQ$ for some $a \neq 0$. If $b = 0$, there exists some suitable $e$ such that $Q \sim eQ \sim eaP = P$, so $Q \sim P$. If $b > 0$, then $Q \sim aP + bQ \sim a(P + Q)$, since the latter two are both in the orbit $O_a$. Since the Galois closure of $k(P)$ is $k_\ell$, $P$ must be conjugate to some point $cP + dQ$ where $d \neq 0$. But then for some suitable $e$, we have $Q \sim eQ \sim ea(P + Q) = c(P + Q) \sim cP + dQ \sim P$.

Since all multiples of $Q$ are Galois conjugate, we have that the orbit of $Q$ over $\mathbb{Q}$ must at least contain
\[
\{Q, \ldots, (\ell - 1)Q, P, \ldots, (\ell - 1)P\}. \tag{4.1}
\]

If this is not the whole orbit, then we claim that in fact the orbit must contain all points of $E[\ell] \setminus \mathcal{O}$. To see this, note that if the orbit is larger than (4.1), then $Q \sim aP + bQ \sim a(P + Q)$, since the latter two are both in the orbit $O_a$. Thus there exists a multiple of $Q$ conjugate to $P + Q$, whence $Q \sim P + Q$. Finally, for any $c, d \geq 1$, we have $Q \sim cQ \sim c(P + Q) \sim cP + dQ$, as desired. Thus $|G| = (\ell^2 - 1)(\ell - 1)$. The classification of subgroups of $GL_2(\mathbb{F}_\ell)$ of order prime to $\ell$ tell us that the only possibilities for $G$ are the following:

(i) $G$ is contained in a Cartan subgroup
(ii) $G$ is contained in the normalizer of a Cartan group
(iii) $G$ is exceptional.

When $\ell > 3$, (i) and (ii) are impossible by order considerations; since a non-split Cartan subgroup has order $\ell^2 - 1$, a split Cartan has order $(\ell - 1)^2$, and any Cartan subgroup has index 2 in its normalizer. Hence we are in the case of (iii), and the possibilities are either $A_4$, $S_4$, or $A_5$. By order considerations, the only case possible is $S_4$ and $\ell = 5$. By [Sut16], the
group listed in (6) occurs, e.g., for the elliptic curve \( y^2 = x^3 + 9x - 18 \). By [Sut16, Lemma 3.21], this is the only conjugacy class for \( G \) that could occur.

Finally, suppose that (4.1) is precisely the orbit of \( Q \) over \( \mathbb{Q} \). Then the remaining \( \ell - 1 \) orbits over \( \mathbb{Q}(P) \) must combine to give orbits of size \( n(\ell - 1) \) over \( \mathbb{Q} \), where \( n \mid (\ell - 1) \). (The orbits must all have the same size since each multiple of \( P + Q \) generates the same degree extension of \( \mathbb{Q} \).) We shall see that \( n = \ell + 1 \). So, consider the elements of \( G \) given by the following matrices with respect to the basis \( \{P, Q\} \):

\[
\begin{bmatrix}
x & a \\
0 & b
\end{bmatrix},
\begin{bmatrix}
1 & 0 \\
0 & y
\end{bmatrix}. \tag{4.2}
\]

The first exists as \( P \) and every nonzero multiple of \( P \) are in the same orbit over \( \mathbb{Q} \). The latter exists since there are elements of \( G \) fixing \( P \). In the former, \( a \) a priori depends on \( x \).

Then consider the product which sends \( P + Q \mapsto (x + ay)P + (by)Q \). If \( a \neq 0 \) for some \( x \), then there exists \( y \) such that \( x + ay \equiv 0 \pmod{\ell} \). Thus \( P + Q \mapsto (by)Q \), but this is impossible as the orbit of \( Q \) was assumed to be (4.1). Thus \( a = 0 \) for all \( x \), so that \( P + Q \sim xP + byQ \), whence \( n = \ell - 1 \) by the same arguments as above. Note that then \( \#G = 2(\ell - 1)^2 \), since \( \#G = \left[ k_\ell : \mathbb{Q}(P) \right] \cdot [\mathbb{Q}(P) : \mathbb{Q}] = (\ell - 1) \cdot 2(\ell - 1) \), where the latter is the size of the orbit of \( P \) over \( \mathbb{Q} \). Moreover, since since the orbit of \( Q + P \) has size \( (\ell - 1)^2 \), there must be an element of \( G \) of order 2 which fixes \( P + Q \). We claim that such an element is of the form \( \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \) so that \( G \) is the normalizer of a split Cartan subgroup. Any element of order 2 of \( \text{GL}_2(\mathbb{F}_\ell) \) must have the form \( \begin{bmatrix} w & 1 - w \\ 1 + w & -w \end{bmatrix} \) for some \( w \in \mathbb{F}_\ell \). If \( w \neq 0 \), then for any \( x, y \neq 0 \), \( G \) will contain elements of the form

\[
\begin{bmatrix}
xw & x(1-w) \\
y(1+w) & -y \end{bmatrix},
\begin{bmatrix}
xw & y(1-w) \\
x(1+w) & -yw \end{bmatrix}.
\]

There are \( (\ell - 1)^2 \) such elements of the first kind, and for \( x \neq y \), there are \( (\ell - 1)(\ell - 2) \) elements of the second kind. Since these elements are all distinct from (4.2), this gives a contradiction as the size of \( G \) is too large.

We now collect a few group theoretic lemmas which we will need in order to prove our main results.

**Lemma 4.3 ([Jor89]).** Let \( \mathbb{F}_q \) be a finite field with \( q > 3 \), the only proper normal subgroups of \( \text{SL}_2(\mathbb{F}_q) \) are \( \{I\}, \{\pm I\} \).

**Lemma 4.4.** Suppose \( \rho_n \) is surjective for some odd square-free integer \( n > 0 \). If \( K \subseteq k_n \) such that \( K/\mathbb{Q} \) is an abelian extension, then \( K \subseteq \mathbb{Q}(\zeta_n) \).

**Proof.** Let \( H \subset \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \) be any normal subgroup with abelian quotient corresponding to \( \text{Gal}(K/\mathbb{Q}) \). Recall that \( \det(\rho_n) = \chi_n \), the cyclotomic character, hence for any \( \sigma \in \text{Gal}(k_n/\mathbb{Q}) \) we have \( \sigma(\zeta_n) = \zeta_n^{\det(\rho_n(\sigma))} \). Thus, it suffices to show that \( H \) contains \( \text{SL}_2(\mathbb{Z}/n\mathbb{Z}) \). As \( n \) is
square-free,
\[ \text{SL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{p|n} \text{SL}_2(\mathbb{Z}/p\mathbb{Z}), \]
so we may assume that \( n = p \) is prime. For \( p > 3 \), the only abelian quotient of \( \text{SL}_2(\mathbb{Z}/p\mathbb{Z}) \) is the trivial group by Lemma 4.3 and the fact that \( \text{PSL}_2(\mathbb{Z}/p\mathbb{Z}) \) is non-abelian, so we are done. For \( p = 3 \), the commutator subgroup of \( \text{GL}_2(\mathbb{Z}/3\mathbb{Z}) \) is \( \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \), so it follows that \( H \) contains \( \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \).

**Lemma 4.6.** Let \( \ell \) be an odd prime. Then any proper normal subgroup \( H \subseteq \text{SL}_2(\mathbb{Z}/\ell \mathbb{Z}) \) has index divisible by \( \ell \). In particular, if \( H' \subseteq \text{GL}_2(\mathbb{Z}/\ell \mathbb{Z}) \) is a proper normal subgroup with \( \det(H') = (\mathbb{Z}/\ell \mathbb{Z})^\times \) then its index is divisible by \( \ell \).

**Proof.** For \( \ell > 3 \), the result follows from Lemma 4.3 and the fact that \( \ell \mid \# \text{SL}_2(\mathbb{Z}/\ell \mathbb{Z}) \). That is, \( H' \) cannot contain \( \text{SL}_2(\mathbb{Z}/\ell \mathbb{Z}) \) or else the determinant would fail to be surjective. So, consider \( H' \cap \text{SL}_2(\mathbb{Z}/\ell \mathbb{Z}) \). It is a normal subgroup properly contained in \( \text{SL}_2(\mathbb{Z}/\ell \mathbb{Z}) \) hence by Lemma 4.3, it is either trivial or \( \{\pm 1\} \). Thus \( \#H' \mid 2(\ell - 1) \), and the index is therefore divisible by \( \ell \). For \( \ell = 3 \), the result follows from the classification of subgroups of \( \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \).

**Proposition 4.5.** Let \( K/\mathbb{Q} \) be an abelian extension and suppose that \( n \) is an odd square-free integer such that \( \rho_n \) is surjective. Then for any \( \tau \in \text{Gal}(K/\mathbb{Q}) \), there exists \( \sigma \in NF_n \) such that \( \sigma \) is compatible with \( \tau \).

**Proof.** Let \( L := K \cap k_n \). Let \( a \in (\mathbb{Z}/n\mathbb{Z})^\times \) be such that \( \zeta_n \rightarrow \zeta_n^a \) is compatible with \( \tau \). Let \( \sigma \in \text{Gal}(k_n/\mathbb{Q}) \) be so that \( \rho_n(\sigma) \) is the following matrix,
\[
\begin{bmatrix}
a & -a \\
1 & 0
\end{bmatrix}.
\]

Then it is straightforward to check that \( \sigma \in NF_n \) and \( \det(\rho(\sigma)) = a \). By applying Lemma 4.4 to \( L \), we have \( \sigma \) and \( \tau \) are compatible. \( \square \)

**Corollary 4.7.** Let \( \ell_1, \ldots, \ell_s \) be distinct odd primes and let \( n = \ell_1 \cdots \ell_s \). Suppose that \( \rho_{E,\ell_i} \) is surjective for each \( i \). Then \( \rho_{E,n} \) is also surjective. Equivalently, \( k_m \cap k_n = \mathbb{Q} \) for any odd relatively prime integers \( m, n \).

**Proof.** Without loss of generality, assume that \( \ell_i < \ell_j \) for \( i < j \). Let \( 1 \leq i < s \) and \( m = \ell_1 \cdots \ell_i \), and suppose that \( \rho_{E,m} \) is surjective. We show that the fields \( k_m \) and \( k_{\ell_i+1} \) intersect trivially over \( \mathbb{Q} \). By assumption, \( \text{Gal}(k_m/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}/m\mathbb{Z}) \) and \( \text{Gal}(k_{\ell_i+1}/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}/\ell_{i+1}\mathbb{Z}) \). Let \( K = k_m \cap k_{\ell_{i+1}} \) and let \( H \subset \text{GL}_2(\mathbb{Z}/\ell_{i+1}\mathbb{Z}) \) be the normal subgroup such that \( \text{GL}_2(\mathbb{Z}/\ell_{i+1}\mathbb{Z})/H \cong \text{Gal}(K/\mathbb{Q}) \).

If \( K \cap \mathbb{Q}(\zeta_{\ell_{i+1}}) \neq \mathbb{Q} \) then Lemma 4.4 would imply \( K \cap \mathbb{Q}(\zeta_{\ell_{i+1}}) \cap \mathbb{Q}(\zeta_m) \neq \mathbb{Q} \) which is a contradiction. Hence \( K \cap \mathbb{Q}(\zeta_{\ell_{i+1}}) = \mathbb{Q} \), so then \( \det(H) = (\mathbb{Z}/\ell_{i+1}\mathbb{Z})^\times \). If \( H \) is proper, then by Lemma 4.6, \( \ell_{i+1} \mid [\text{GL}_2(\mathbb{Z}/\ell_{i+1}\mathbb{Z}) : H] = |\text{Gal}(K/\mathbb{Q})| \). However since \( \text{GL}_2(\mathbb{Z}/m\mathbb{Z}) \) has
order
\[ \prod_{1 \leq j \leq i} \ell_j(\ell_j - 1)^2(\ell_j + 1), \]
its quotient cannot have order divisible by \( \ell_{i+1} \). Hence we must have \( H = \text{GL}_2(\mathbb{Z}/\ell_{i+1}\mathbb{Z}) \) and so \( K = \mathbb{Q} \). Thus
\[ \text{Gal}(k_{\ell_1 \cdots \ell_i+1}/\mathbb{Q}) = \text{Gal}(k_m/\mathbb{Q}) \times \text{Gal}(k_{\ell_{i+1}}/\mathbb{Q}) \simeq \text{GL}_2(\mathbb{Z}/(\ell_1 \cdots \ell_{i+1})\mathbb{Z}). \]

**Corollary 4.8.** Let \( K/\mathbb{Q} \) be an abelian extension and \( n \) a square-free odd integer. Suppose that \( \rho_n \) and \( \rho_2 \) are surjective. If \( k_2 \subset k_n K \), then \( 3 \mid n \) and \( k_2 \subset k_3 \).

**Proof.** By Lemma 4.4, \( K \cap k_n \subset \mathbb{Q}(\zeta_n) \), so we have the exact sequence
\[ 1 \longrightarrow \text{Gal}(k_n/\mathbb{Q}(\zeta_n)) \longrightarrow \text{Gal}(k_n K/\mathbb{Q}) \longrightarrow \text{Gal}(K(\zeta_n)/\mathbb{Q}) \longrightarrow 1, \]
which induces
\[ 1 \longrightarrow \text{Gal}(k_2/\mathbb{Q}(\zeta_n) \cap k_2) \longrightarrow \text{Gal}(k_2/\mathbb{Q}) \longrightarrow \text{Gal}(K(\zeta_n) \cap k_2/\mathbb{Q}) \longrightarrow 1. \]

Now
\[ \text{Gal}(k_2/\mathbb{Q}(\zeta_n) \cap k_2) \simeq \prod_{\ell \mid n, \ell \text{ prime}} \text{Gal}(k_\ell \cap k_2/\mathbb{Q}(\zeta_\ell) \cap k_2) \]
is a normal subgroup of \( \text{Gal}(k_2/\mathbb{Q}) \simeq S_3 \). By Lemma 4.6, this forces each factor in the product to be trivial except possibly when \( \ell = 3 \). Since at least one factor must be non-trivial, otherwise \( S_3 \simeq \text{Gal}(K(\zeta_n) \cap k_2/\mathbb{Q}) \) would be abelian, we must have \( 3 \mid n \). Since \( \text{Gal}(k_3 \cap k_2/\mathbb{Q}(\zeta_3) \cap k_2) \) must simultaneously be a normal subgroup of \( S_3 \) and a quotient of \( \text{Gal}(k_3/\mathbb{Q}(\zeta_3)) \simeq \text{SL}_2(\mathbb{F}_3) \), the only possibility is that it is isomorphic to \( \mathbb{Z}/3\mathbb{Z} \). Finally we have \( \text{Gal}(k_2 \cap k_3/\mathbb{Q}) \) is a quotient of \( \text{Gal}(k_2/\mathbb{Q}) \simeq S_3 \) and contains normal subgroup of order 3. The only possibility is \( \text{Gal}(k_2 \cap k_3/\mathbb{Q}) \simeq S_3 \), i.e., \( k_2 \subset k_3 \). \( \square \)

**Corollary 4.9.** Assume the hypotheses of Corollary 4.8. Then for any \( \tau \in \text{Gal}(K(\zeta_3)/\mathbb{Q}) \) such that \( \bar{\zeta}_3^n = \zeta_3 \), there exists \( \sigma \in NF_{2n} \) such that \( \sigma \) is compatible with \( \tau \).

**Proof.** By Corollary 4.8, we have \( 3 \mid n \) and \( k_2 \subset k_3 \). The unique normal subgroup \( H \) of order 8 inside \( \text{GL}_2(\mathbb{F}_3) \simeq \text{Gal}(k_3/\mathbb{Q}) \) such that \( \text{GL}_2(\mathbb{F}_3)/H \simeq S_3 \) is generated by
\[ \left\langle \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix} \right\rangle. \]

A computation shows that the matrix
\[ \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} \]
maps to an element of order 3 in \( S_3 \simeq \text{Gal}(k_3/\mathbb{Q}) \). Choose \( \sigma' \in \text{Gal}(k_3/\mathbb{Q}) \) so that \( \rho(\sigma') \) is the matrix above. Then a computation shows \( \sigma' \in NF_3 \) and \( \sigma' \mid k_2 \in NF_2 \). Let \( a \in (\mathbb{Z}/n\mathbb{Z})^\times \) be such that \( \zeta_n \rightarrow \zeta_n^a \) is compatible with \( \tau \). Since \( \zeta_3^a = \zeta_3 \), the image of \( a \) under \( (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/3\mathbb{Z})^\times \) is trivial. Let \( \sigma = (\sigma_1, \sigma_2) \in \text{Gal}(k_{2n}/\mathbb{Q}) \simeq \text{Gal}(k_3/\mathbb{Q}) \times \text{Gal}(k_{n/3}/\mathbb{Q}) \) be so that
\[ \rho_{2n}(\sigma_1, \sigma_2) \] is
\[ \left( \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} a & -a \\ 1 & 0 \end{bmatrix} \right). \]

It is straightforward to check that \( \sigma \in NF_{2n} \) and \( \det(\rho(\sigma)) = a \). By Lemma 4.4, \( \sigma \) and \( \tau \) are compatible. \( \square \)

We now give the main results of this section on some local-to-global properties of torsion points of elliptic curves. We first consider the case of a single prime \( \ell > 3 \), and then treat 2 and 3 separately. We then prove the general case of a composite integer \( n \). For the remainder of the section, \( K/Q \) will denote a nontrivial Galois extension, which we sometimes additionally require to be abelian. To prove Theorem 3.6, we only need to consider the case when \( K \) is a quadratic extension, but the results will hold for a general \( K \).

**Proposition 4.10.** Let \( K/Q \) be a nontrivial Galois extension and \( \ell > 3 \) a prime. The following are equivalent

1. \( E(\mathbb{F}_p)[\ell] \neq 0 \) for all but finitely many primes \( p \) that do not split completely in \( K \).
2. There exists a curve \( E' \) isogenous to \( E \) such that \( E'(\mathbb{Q})[\ell] \neq 0 \).

**Proof.** The implication (2) \( \implies (1) \) is immediate. Assume (1) is true. Let \( \sigma \in \text{Gal}(K(\zeta_\ell)/Q) \) be such that \( \sigma|_{Q(\zeta_\ell)} \) generates \( \text{Gal}(Q(\zeta_\ell)/Q) \) and \( \sigma \) does not act as the identity on \( K \). Let \( p \) be a prime of good reduction for \( E \) such that \( \sigma \) is in the conjugacy class of \( \text{Frob}_p \) and \( E(\mathbb{F}_p)[\ell] \neq 0 \). Let \( P \in E[\ell] \) so that the reduction mod \( p \), \( \text{red}_p(P) \in E(\mathbb{F}_p)[\ell] \). Hence there is an embedding \( Q(P) \hookrightarrow \mathbb{Q}_p \). Since the only subfield of \( Q(\zeta_\ell) \) with an embedding into \( Q_p \) is \( Q \), it follows that \( Q(P) \cap Q(\zeta_\ell) = Q \). Hence the image of \( \rho_\ell \) is one of the groups listed in Lemma 4.2. Suppose that we are not in the case of group (4) with \( d = \ell \). Then, since \( \ell > 3 \), one can check that \( G \) is generated by the subset
\[ J := \{ g \in G \mid \det(g - 1) \neq 0 \}. \]

In particular, there must be some element \( g \in J \) such that \( g = \rho(\tau) \) for some \( \tau \in \text{Gal}(k_\ell K/Q) \) which acts nontrivially on \( K \). Moreover \( \tau|_{k_\ell} \in NF_\ell \) since \( \rho(\tau) \in J \). Let \( p \neq \ell \) be any prime of good reduction such that \( \tau \) is in the conjugacy class of \( \text{Frob}_p \). Then \( \text{Frob}_p \) does not fix any nontrivial \( \ell \)-torsion point in \( E_p(\overline{\mathbb{F}}_p)[\ell] \), so \( E_p(\overline{\mathbb{F}}_p)[\ell] = \{ O \} \) and \( p \) does not split completely in \( K \). Since there are infinitely many such primes \( p \), we get a contradiction. That is, if (1) holds, then \( G \) must be a Borel subgroup of the form (4).

Now suppose we are in the case of (4) in Lemma 4.2 with \( d = \ell \). Let \( P, Q \in E[\ell] \) be the basis giving the matrix representation of (4). The subgroup generated by \( P \) is Galois invariant, so there exists an elliptic curve \( E' \) and an isogeny \( \varphi: E \to E' \) whose kernel is the subgroup generated by \( P \). Then \( \varphi(Q) \) is fixed by \( G_Q \), so defines a rational \( \ell \)-torsion point on the isogenous curve \( E' \). \( \square \)

Proposition 4.10 does not hold if we replace \( \ell \) by 2 or 3. However, we can determine precisely when it fails as the next two propositions show.
Proposition 4.11. Let $K/Q$ be a nontrivial Galois extension. Suppose that for all but finitely many primes $p$ such that $p$ does not split completely in $K$, we have $E(F_p)[2] \neq 0$. Then either $E[2](Q) \neq 0$ or $\text{Gal}(k_2/Q) = S_3$ and $K \subset k_2$ has degree 2 over $Q$.

Proof. Let $y^2 = f(x)$ be the short Weierstrass equation for $E$ over $Q$, and suppose that $E[2](Q) = 0$. Let $L = K \cap k_2$. It suffices to show there exists an element in $\text{Gal}(k_2/Q)$ which fixes no 2-torsion point and does not fix $K$, since otherwise there are infinitely many primes $p$ whose lift of the Frobenius equals this element giving a contradiction. If the splitting field of $f$ is a cyclic degree 3 extension, then $\text{Gal}(k_2/Q)$ is also cyclic. If $L = Q$, $\text{Gal}(k_2/Q) = \text{Gal}(K/Q) \times \text{Gal}(k_2/Q)$ so choosing nontrivial elements in each component produces a Galois action which fixes no 2-torsion point and does not fix $K$. If $L = E[2]$, then we get the generator of $\text{Gal}(k_2/Q)$ does the job as well.

Now assume $\text{Gal}(k_2/Q) = S_3$. If $L = Q$, then the same argument as above applies. If $L/Q$ has degree 3, then the generator of $\text{Gal}(L/Q)$ fixes no 2-torsion point and does not fix $K$. If $L = k_2$, the same argument applies by choosing any element of order 3 in $\text{Gal}(L/Q)$. Hence $L/Q$ must be of degree 2.

Proposition 4.12. Let $K/Q$ be a nontrivial Galois extension. Suppose that for all but finitely many primes $p$ such that $p$ does not split completely in $K$, we have $E(F_p)[3] \neq 0$. Then either $E[3](Q) \neq 0$ or $K = Q(\sqrt{-3})$.

Proof. Let $L = K \cap k_3$. As in the proof of Proposition 4.11, if $K \neq L$ or $L = Q$, then we get a contradiction. Hence assume $Q \neq K \subset k_3$. Define

$$J := \{g \in G \mid \det(g - 1) \neq 0\}$$

and let $H$ be the normal subgroup generated by $J$. Then $K \subseteq k_3^H$. By the same argument as in the beginning of Proposition 4.10, the image of $\rho$ is one of the non-exceptional subgroups in Lemma 4.2. In the case $G = \text{GL}_2(F_3)$, it is straightforward to check that $G$ is generated by $J$, so $G = H$ which is a contradiction.

Since $\ell = 3$, there are only three cases left to consider:

Case 1 (B). $G$ is of the form

$$\left\{ \begin{bmatrix} x & * \\ 0 & y \end{bmatrix} \mid x, y \in F_3^x \right\}.$$

The set $J$ contains

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$$

the above elements generate the index 2 subgroup $H = \{g \in G \mid \det(g) = 1\}$. Hence $K \subset k_3^H = Q(\sqrt{-3})$, so we must have $K = Q(\sqrt{-3})$.

Case 2 (Cs). $G$ is of the form

$$\left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \mid x, y \in F_3^x \right\}.$$
The set $J$ contains
\[
\begin{bmatrix}
-1 & 0 \\
0 & -1
\end{bmatrix},
\]
which again generates the index 2 subgroup $H = \{g \in G \mid \det(g) = 1\}$, so $K = \mathbb{Q}(\sqrt{-3})$.

**Case 3 (ns).** $G$ is the normalizer of a split Cartan. The set $J$ contains
\[
\begin{bmatrix}
0 & 1 \\
-1 & 0
\end{bmatrix},
\]
which generates a cyclic normal subgroup of order 4. One checks that this subgroup is precisely $H = \{g \in G \mid \det(g) = 1\}$, so $K = \mathbb{Q}(\sqrt{-3})$.

We now prove the general case for a composite integer $n$, which is used to prove Theorem 3.6. We require additional assumptions on $K$ if 2 or 3 divides $n$, as demonstrated by the previous two propositions.

**Theorem 4.13.** Let $K/\mathbb{Q}$ be a nontrivial abelian extension not contained in $k_2$ or $\mathbb{Q}(\zeta_3)$. Let $n > 1$ be an integer. Suppose that for all except possibly one odd prime $\ell \mid n$, we have $\rho_\ell$ is surjective. If $\rho_\ell$ is not surjective and $2\ell \mid n$, assume $k_2 \cap k_\ell = \mathbb{Q}$. Then the following are equivalent:

1. $E(\mathbb{F}_p)[n] \neq 0$ for all but finitely many primes $p$ that do not split completely in $K$.
2. There exists a curve $E'$ isogenous to $E$ such that $E'(\mathbb{Q})[n] \neq 0$.

**Proof.** As before, $(2) \implies (1)$ is clear. Now assume that $(1)$ holds. Note that it suffices to consider when $n$ is a product of distinct primes. Furthermore, if there exists $\tau \in \text{Gal}(k_n K/\mathbb{Q})$ such that $\tau|_{k_n} \in NF_n$ and $K^\tau \neq K$, then for any prime $p$ of good reduction such that Frob$_p$ is in the conjugacy class of $\tau$, we have $E_p(\mathbb{F}_p)[n] = 0$ and $p$ does not split completely in $K$. Our proof will show that either (2) is true, or there exists such an element $\tau \in \text{Gal}(k_n K/\mathbb{Q})$, thereby contradicting (1).

**Case 1** ($\rho_\ell$ is surjective for all odd $\ell$). If $n$ is odd, then by Proposition 4.5, there exists $\tau \in \rho(\text{Gal}(k_n K/\mathbb{Q}))$ such that $\tau|_{k_n} \in NF_n$ and $K^\tau \neq K$.

Now assume $n = 2m$. If $m = 1$, then our result follows from Proposition 4.11, so assume $m > 1$. Since $E(\mathbb{Q})[2] = 0$, we have $\text{Gal}(k_2/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ or $S_3$. Hence, $\text{Gal}(k_2 \cap k_m/\mathbb{Q}) \simeq \{1\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$, or $S_3$. Let $L := k_2 \cap k_m K$.

If $L/\mathbb{Q}$ is abelian: By hypothesis on $K$, there exists $s \in \text{Gal}(L K/\mathbb{Q})$ such that $K^s \neq K$, and $L^s = L$ if $L/\mathbb{Q}$ is at most quadratic or $L^s = \mathbb{Q}$ if $L/\mathbb{Q}$ is cubic. By Proposition 4.5, there exists $\sigma \in \rho(\text{Gal}(k_m L K/\mathbb{Q}))$ such that $\sigma|_{k_m} \in NF_m$ and $\sigma$ restricts to $s$. Then there exists a lift $\sigma$ to $\tau \in \text{Gal}(k_n K/\mathbb{Q})$ that satisfies $\tau|_{k_n} \in NF_n$.

If $L/\mathbb{Q}$ is $S_3$: By Corollary 4.8, we have $3 \mid m$ and $k_2 \subset k_3$. By Lemma 4.4, the only quadratic extension contained in $k_3$, and hence in $k_2$, is $\mathbb{Q}(\zeta_3)$. Since $K \not\subset k_2$ by hypothesis, this implies $K \neq \mathbb{Q}(\zeta_3)$. Hence, Corollary 4.9 shows there exists $\tau \in \text{Gal}(k_n K/\mathbb{Q})$ such that $\tau|_{k_n} \in NF_n$ and $K^\tau \neq K$.
Case 2 ($\rho_\ell$ is not surjective for some $\ell$). Let $\ell \mid n$ be a prime such that $\rho_\ell$ is not surjective.

Lemma 4.14. The image of $\rho_\ell$ is given by one of the groups in Lemma 4.2

Proof. Assume first that $2 \nmid n$. By Proposition 4.5, there exists $\sigma \in \text{Gal}(k_{n/\ell}K(\zeta_\ell)/\mathbb{Q})$ such that $\sigma \in NF_{n/\ell}$ and $K^s \neq K, \mathbb{Q}(\zeta_\ell)^s = \mathbb{Q}$. Then for any prime $p$ of good reduction such that $\text{Frob}_p$ is in the conjugacy class of $\sigma$, we have $E_p(\mathbb{F}_p)[n/\ell] = 0$ and $p$ does not split completely in $K$. Hence by (1), $E_p(\mathbb{F}_p)$ contains an $\ell$-torsion point, i.e., $\sigma$ fixes an $\ell$-torsion point on $E$. Since $\sigma$ also generates $\text{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$, the hypothesis of Lemma 4.2 are satisfied.

Now assume $n = 2\ell m$ for some integer $m$ where $\ell$ again is an odd prime such that $\rho_\ell$ is not surjective. Set $L := k_2 \cap k_m K(\zeta_\ell)$ and recall that $\text{Gal}(L/\mathbb{Q}) \simeq \{1\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z},$ or $S_3$.

If $L/\mathbb{Q}$ is abelian: By hypothesis on $K$, there exists $s \in \text{Gal}(LK(\zeta_\ell)/\mathbb{Q})$ such that $K^s \neq K$ and $= \mathbb{Q}(\zeta_\ell)^s = \mathbb{Q}$ and $L^s = L$ if $L/\mathbb{Q}$ is quadratic or $L^s = \mathbb{Q}$ if $L/\mathbb{Q}$ is cubic. By Proposition 4.5, there exists $\sigma \in \text{Gal}(k_m KL(\zeta_\ell)/\mathbb{Q})$ such that $\sigma|_{k_m} \in NF_m$ and $\sigma$ restricts to $s$. By construction, any lift of $\sigma$ to $\tau \in \text{Gal}(k_{2m} K(\zeta_\ell)/\mathbb{Q})$ satisfies $\tau|_{k_2} \in NF_2$.

If $L/\mathbb{Q}$ is $S_3$: By Corollary 4.8, we have $3 \mid m$ and $k_2 \subset k_3$. By Lemma 4.4, the only quadratic extension contained in $k_3$, and hence in $k_2$, is $\mathbb{Q}(\zeta_3)$. Recall $K \cap k_2 = \mathbb{Q}(\zeta_3) \cap k_2 = \mathbb{Q}$ by hypothesis. Hence any $s \in \text{Gal}(K(\zeta_3)/\mathbb{Q})$ such that $K^s = \mathbb{Q}(\zeta_3)^s = \mathbb{Q}$ can be lifted to fix $\zeta_3$. Hence, Corollary 4.9 shows there exists $\tau \in \text{Gal}(k_{2m} K(\zeta_\ell)/\mathbb{Q})$ such that $\tau|_{k_2} \in NF_{2m}$ and $K^\tau \neq K$ and $\mathbb{Q}(\zeta_\ell)^\tau = \mathbb{Q}$.

In either case, the claim is proved by the same argument as in the case $2 \nmid n$ using $\tau$ to produce primes $p$ with $\ell$-torsion in the reduction mod $p$. \qed

Now we resume the proof of Theorem 4.13. We consider two cases based on whether the image of $\rho_\ell$ is exceptional or not.

Subcase 1 (The image of $\rho_\ell$ is not exceptional). Let $k'_\ell$ be the maximal abelian subextension of $k_\ell$. We can identify under $\rho_\ell$,

$$\text{Gal}(k'_\ell/\mathbb{Q}) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/(\ell - 1)\mathbb{Z}$$

where $1 \leq m \leq \ell - 1$. For (1)–(4), this is clear. In the case of (5), $m = 2$ and the Galois group is isomorphic to the quotient by the normal subgroup

$$\left\lbrace \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} \bigg| x \in \mathbb{F}_\ell^\times \right\}.$$

The only case in which $m = 1$ is possible is for (4), and $\rho_\ell(\text{Gal}(k_\ell/\mathbb{Q}))$ is conjugate to

$$\left\lbrace \begin{bmatrix} x & \ast \\ 0 & 1 \end{bmatrix} \bigg| x \in \mathbb{F}_\ell^\times \right\}.$$

Then $E$ will have an isogeny of degree $\ell$ onto an elliptic curve $E'$ having an $\ell$-torsion point, giving (2).

Now assume $m > 1$. Let $N \subset \text{Gal}(k'_\ell/\mathbb{Q}) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/(\ell - 1)\mathbb{Z}$ be the subset consisting of elements of the form $(a, b)$ where $a, b \neq 0$. Then any lift of an element $g \in N$ to $\text{Gal}(k_\ell/\mathbb{Q})$
lies in $N F_\ell$. Again this is clear for (1)–(4), and in the case of (5), the lift consists of matrices of the form
\[
\begin{bmatrix} 0 & x \\ y & 0 \end{bmatrix}, \quad x, y \in \mathbb{F}_\ell^*, xy \neq 1
\]
which does not have any nontrivial eigenvector. Note that if $\ell > 3$, then $N$ generates the entire group $\text{Gal}(k'_\ell/Q)$. On the other hand, if $\ell = 3$, then $K \not\subset k_\ell$. Hence there exists $\sigma \in \text{Gal}(k'_3/K/Q)$ such that $\sigma|_{k'_3} \in N$ and $K^\sigma = Q$.

If $2 \nmid n$, then by Proposition 4.5, there exists $\tau' \in \text{Gal}(k_n/k'_3K/Q)$ such that $\tau'|_{k_n/\ell} \in N F_{n/\ell}$ and $\tau$ restricts to $\sigma$. Any lift $\tau \in \text{Gal}(k_n/K/Q)$ will then satisfy $\tau \in N F_n$ and $K^\tau \neq K$.

Now suppose $n = 2\ell m$. Let $M := k'_\ell k_m = 3$, and $L := k_2 \cap M$.

If $L/Q$ is abelian: Choose $u \in \text{Gal}(L/Q)$ to be the identity if $L/Q$ is quadratic or a generator if $L/Q$ is cubic. By the hypothesis $k_3 \cap k_\ell = Q$, we have $\text{Gal}(Lk'_3/Q) \simeq \text{Gal}(L/Q) \times \text{Gal}(k'_3/Q)$. Moreover if $K \subset Lk'_3$, then the assumption $K \cap k_2 = Q$ and the fact that $N$ generates $\text{Gal}(k'_3/Q)$ means there exists some $\sigma_1 = (s,t) \in L(k'_3/Q) \times \text{Gal}(k'_3/Q)$ such that $s = u$, $t \in N$, and $K^{(s,t)} \neq K$. By Proposition 4.5, there exists $\sigma_2 \in \text{Gal}(k_m/k'_3K/Q)$ such that $\sigma_2$ is compatible with $\sigma_1$. Let $\sigma_3 \in \text{Gal}(k_m/k'_3K/Q)$ be a lift of $\sigma_2$ so that $\sigma_3|_{k_2}$ has order 3, i.e., contained in $N F_2$ (this is possible since $k_2 \cap k_m k'_3K = L$). Finally any lift $\tau \in \text{Gal}(k_m/K/Q)$ of $\sigma_3$ satisfies $\tau \in N F_n$ and $K^\tau \neq K$.

If $L/Q$ is $S_5$: By Corollary 4.8, we have $3 \mid m$ and $k_2 \subset k_3$. The hypothesis $k_3 \cap k_\ell = Q$ implies any $s \in \text{Gal}(k'_3/K/Q)$ with $s|_{k'_3} \subset N$ and $K^s = Q$ is compatible with $1 \in \text{Gal}(Q/(\zeta_3)/Q)$. Hence, Corollary 4.9 implies there exists $\sigma \in \text{Gal}(k_n/k'_3K/Q)$ with $\sigma \in N F_{n/\ell}$ and $K^\tau = Q$. Then any lift $\tau \in \text{Gal}(k_n/K/Q)$ of $\sigma$ satisfies $\tau \in N F_2$.

Subcase 2 (Exceptional image). Now assume that $\ell = 5$ and the image is exceptional as in (6) of Lemma 4.2. Recall that $\rho_5(G_5)$ generated by
\[
A = \begin{bmatrix} 0 & 3 \\ 3 & 4 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad C = \begin{bmatrix} 3 & 0 \\ 4 & 4 \end{bmatrix}
\]
Let $k'_5 \subset k_5$ be the subextension corresponding to the image of $\rho_5$ in $\text{PGL}_2(\mathbb{F}_5)$. Then $\text{Gal}(k'_5/Q) \simeq S_4$. The possible quotients of $S_4$ are $S_4$, $S_3$, $\mathbb{Z}/2\mathbb{Z}$, $\{0\}$. We will prove the desired result under the assumption that $6 \mid n$, which is the most difficult case. If 2 and/or 3 does not divide $n$, the argument is easier, and follows the same pattern as the case $6 \mid n$, so we do not include it here. By assumption $\rho_3(G/Q) \simeq \text{GL}_2(\mathbb{F}_3)$ and the possible quotients are $\text{GL}_2(\mathbb{F}_3)$, $\text{PGL}_2(\mathbb{F}_3)$, $S_3$, $\mathbb{Z}/2\mathbb{Z}$, $\{0\}$. Recall that $\text{PGL}_2(\mathbb{F}_3) \simeq S_4$, so the possibilities for $\text{Gal}(k'_5 \cap k_3)$ are (1) $S_4 \simeq \text{PGL}_2(\mathbb{F}_3)$, (2) $S_3$, (3) $\mathbb{Z}/2\mathbb{Z}$, (4) $\{0\}$.

We claim that $k_3 \cap k'_5 = Q$. Note that $Q(\zeta_5 + \zeta_5^{-1}) \subset k'_5$ is the unique quadratic field inside $k'_5$ and $Q(\zeta_3) \subset k_3$ is the unique quadratic field inside $k_3$. But by the discussion above, if $k_3 \cap k'_5 \neq Q$, then there exists a quadratic field $J \subset k_3 \cap k'_5$, which is a contradiction.

Next we claim $k_2 \cap k_3 k'_5 = Q$, $Q(\zeta_3)$, $Q(\zeta_3(\zeta_5 + \zeta_5^{-1}))$, or $k_2 \subset k_3$ with $\text{Gal}(k_2/Q) \simeq S_3$. Let $J = k_2 \cap k_3 k'_5$ defining a normal subgroup $H \subseteq \text{Gal}(k_3/Q) \times \text{Gal}(k'_5/Q)$. Suppose first $\text{Gal}(k_2/Q) \simeq S_3$. If $H$ is of index 2, then $J \subset Q(\zeta_3, \zeta_3 + \zeta_5^{-1})$ and $k_2 \cap k'_5 = Q$ imply $J = Q(\zeta_3)$
or $Q(\zeta_3(\zeta_5 + \zeta_5^{-1}))$. If $k_2$ is not contained in $k_3$, then $H \cap \text{Gal}(k_3/Q) \times \{1\}$ is index 2 inside $\text{Gal}(k_3/Q)$. Then $H \cap \{1\} \times \text{Gal}(k_5'/Q)$ must be a normal subgroup of index dividing 3. Since $\text{Gal}(k_5'/Q)$ has no normal subgroup of index 3, it must be index 1. Hence $H$ has index 2, so $J = Q(\zeta_3)$. If $\text{Gal}(k_2/Q) \simeq \mathbb{Z}/3\mathbb{Z}$, then $\text{Gal}(k_3/Q) \times \text{Gal}(k_5'/Q)$ has no normal subgroup of index 3. Hence $J = Q$.

Let $\sigma_3 \in NF_3$ whose image in $S_3$ has order 3. Then $\sigma_2 \in NF_2$ is compatible with $\sigma_3$. Let $\sigma_5 \in \text{Gal}(k_5'/Q)$ correspond to the class of the matrix $A$ in $\text{PGL}_3(\mathbb{F}_5)$. By the two paragraphs above, there exists $\sigma' \in \text{Gal}(k_2k_3k_5'/Q)$ which lifts $\sigma_2, \sigma_3, \sigma_5$. If $K \subset k_2k_3k_5'$, then the only quadratic extension fixed by $\sigma'$ is $Q(\zeta_3)$. Thus, there exists $\sigma \in \text{Gal}(k_2k_3k_5' K/Q)$ lifting $\sigma$ and acting nontrivially on $K$. Let $\tau_1 \in \text{Gal}(k_2k_3k_5 K/Q)$ be any lift of $\sigma$. We claim that $\tau_1|_{k_5} \in NF_5$. Indeed, observe that $\rho_5(\tau_1|_{k_5})$ can be any one of the following matrices

$$\begin{bmatrix} 0 & 3 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 0 & 4 \\ 4 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix}$$

all of which lie in $NF_5$.

Finally $k_2k_3k_5 K \cap k_{n/30} \subset Q(\zeta_{30})$ by Lemma 4.6. Then by Proposition 4.5, there exists $\tau \in \text{Gal}(k_{n/30} K/Q)$ such that $\tau$ restricts to $\tau_1$, $\tau|_{k_5} \in NF_n$, and $K^\tau = Q$. \hfill \square

**Corollary 4.15.** Let $E/Q$ be an almost surjective elliptic curve. Let $a \in \mathbb{Z}$ such that $\sqrt{a} \notin k_2(\sqrt{-3})$. Then for any integer $n$, there are infinitely many primes $p$ such that $E_p(\mathbb{F}_p)[n] = 0$ and $\sqrt{a} \notin \mathbb{F}_p$.

**Proof.** This is a direct consequence of Theorem 4.13 applied to $K = Q(\sqrt{a})$. \hfill \square

**References**

[AIM14] AIM, *Open problems: Rational and integral points on higher-dimensional varieties*, 2014. [https://cims.nyu.edu/~tschinke/aim/aim14-index.html](https://cims.nyu.edu/~tschinke/aim/aim14-index.html).

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). MR1484478

[Cas6601] J. W. S. Cassels, *Diophantine Equations with Special Reference To Elliptic Curves*, Journal of the London Mathematical Society **s1-41** (1966/1), no. 1, 193–291.

[CTPS16] J.-L. Colliot-Thélène, A. Pál, and A. N. Skorobogatov, *Pathologies of the Brauer-Manin obstruction*, Mathematische Zeitschrift **282** (2016/4), no. 3, 799–817.

[CTS87] J.-L. Colliot-Thélène and J.-J. Sansuc, *La descente sur les variétés rationnelles. II*, Duke Math. J. **54** (1987), no. 2, 375–492.

[CTSSD97] J.-L. Colliot-Thélène, A. N. Skorobogatov, and P. Swinnerton-Dyer, *Double fibres and double covers: paucity of rational points*, Acta Arith. **79** (1997), no. 2, 113–135. MR1438597

[Duk97] W. Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818.

[HS14] Y. Harpaz and A. N. Skorobogatov, *Singular curves and the étale Brauer-Manin obstruction for surfaces*, Ann. Sci. Éc. Norm. Supér. (4) **47** (2014), no. 4, 765–778.

[Jon10] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570.
[Jor89] C. Jordan, *Traité des substitutions et des équations algébriques*, Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics], Éditions Jacques Gabay, Sceaux, 1989. Reprint of the 1870 original. MR1188877

[Kat81] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. 62 (1981), no. 3, 481–502.

[LM19] D. Loughran and L. Matthiesen, *Frobenian multiplicative functions and rational points in fibrations* (2019), available at arXiv:1904.12845.

[Poo10] B. Poonen, *Insufficiency of the Brauer-Manin obstruction applied to étale covers*, Ann. of Math. (2) 171 (2010), no. 3, 2157–2169.

[Ser72] J. P. Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), no. 4, 259–331.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 2009.

[Sko96] A. N. Skorobogatov, *Descent on fibrations over the projective line*, Amer. J. Math. 118 (1996), no. 5, 905–923.

[Sko99] ———, *Beyond the Manin obstruction*, Invent. Math. 135 (1999), no. 2, 399–424.

[Sut12] A. V. Sutherland, *A local-global principle for rational isogenies of prime degree*, J. Théor. Nombres Bordeaux 24 (2012), no. 2, 475–485.

[Sut16] ———, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma 4 (2016), e4, 79.

[Vog18] I. Vogt, *A local-global principle for isogenies of composite degree* (2018), available at arXiv:1801.05355.

DEPARTMENT OF MATHEMATICS, RICE UNIVERSITY MS 136, HOUSTON, TX 77251-1892, USA

E-mail address: jb93@math.rice.edu

URL: http://math.rice.edu/~jb93

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF BATH, BATH, BA2 7AY, UK

E-mail address: mn634@bath.ac.uk

URL: https://sites.google.com/view/masahiro-nakahara/home