THE LOCAL-GLOBAL PRINCIPLE FOR DIVISIBILITY IN CM ELLIPTIC CURVES

BRENDAN CREUTZ AND SHENG(VICTOR) LU

Abstract. We consider the local-global principle for divisibility in the Mordell-Weil group of a CM elliptic curve defined over a number field. For each prime p we give sharp lower bounds on the degree d of a number field over which there exists a CM elliptic curve which gives a counterexample to the local-global principle for divisibility by a power of p. As a corollary we deduce that there are at most finitely many elliptic curves (with or without CM) which are counterexamples with $p > 2d + 1$. We also deduce that the local-global principle for divisibility by powers of 7 holds over quadratic fields.

1. Introduction

Let E/k be an elliptic curve over a number field k. We say that a k-rational point $P \in E(k)$ is divisible by the integer N if there exists $Q \in E(k)$ such that $NQ = P$. The question motivating this paper is the extent to which this notion of divisibility satisfies a local-global principle. Namely, if there exists $Q_v \in E(k_v)$ such that $NQ_v = P$ for all (or all but possibly finitely many) completions k_v of k does it follow that P is divisible by N?

Over the past decades there has been substantial interest in the problem of determining conditions on N and k implying that such a local-global principle holds for all elliptic curves over k [DZ01, DZ04, DZ07, PRV12, PRV14, Cre16, LW16, Ran18]. Due to its connection with a question of Cassels [Cas62, Problem 1.3], the analogous question where $E(k) = \mathrm{H}^0(k, E)$ is replaced by the Galois cohomology group $\mathrm{H}^1(k, E)$ has also recieved much attention [ÇS15, Cre13, Cre16]. Function field analogues of these questions were studied in [CV17]. In all cases the positive results in the literature concerning local-global divisibility in the groups $E(k)$ and $\mathrm{H}^1(k, E)$ have relied on the same technique, which considers a more general local-global principle for the N-torsion subgroup of E (see Definition 1.1 below).

The approach to establishing such a local-global principle can be summarized as follows. First one aims to identify purely group-theoretic conditions on the image of the mod N Galois representation $\rho_N : \mathrm{Gal}(k) \to \mathrm{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N)$ which guarantee that the local-global principle for divisibility by N holds. Elliptic curves for which these conditions are not satisfied correspond to non-cuspidal k-rational points on some modular curve with level N structure. These curves have only finitely many points defined over number fields of degree $\leq d$, provided N is sufficiently large. In many cases one can show that all of the low degree points are cusps. This has resulted in proofs that these local-global principles for divisibility by a prime power $N = p^n$ hold for all p larger than an explicit bound depending only on the degree of the number field (See [PRV12, Corollary 2] or [ÇS15, Theorem B(1)]). In the case $k = \mathbb{Q}$, the bound is $p \geq 5$ [PRV14, Corollary 4] and it is known to be sharp [Cre16]. For degrees greater than 1 the exact bound is unknown.

Establishing an exact bound requires identifying the sporadic points on these modular curves and checking whether the local-global principle holds for the corresponding elliptic curves. To that end, we undertake a detailed analysis of the local-global principle for divisibility on CM curves, as these are a common source of low degree points on modular curves.

Before stating our main results let us define the local-global principle we refer to.

Definition 1.1. *For a set of places S of k define*

$$Ш^1(k, E[N]; S) := \ker \left(\mathrm{H}^1(k, E[N]) \to \prod_{v \notin S} \mathrm{H}^1(k_v, E[N]) \right),$$

where $\mathrm{H}^1(k, E[N])$ denotes Galois cohomology of the N-torsion subgroup of E. We say that the local-global principle holds for $(E/k, N)$ if $Ш^1(k, E[N]; S) = 0$ for every finite set of places S of k.

If the local-global principle holds for $(E/k, N)$, then the local-global principle for divisibility by N holds for $\mathrm{H}^i(k, E)$ for all $i \geq 0$ (See [Cre16, Theorem 2.1] and Lemma 2.2). The goal of this paper is to determine the minimal degree of a number field over which there is a CM elliptic curve for which the local-global principle fails for given prime power $N = p^n$. In Section 3 we prove the following.

Theorem 1.2. *Let $\mathcal{O} \subset K$ be an order of conductor f in a quadratic imaginary field K and let $j = j(\mathcal{O})$ be the j-invariant of an elliptic curve with complex multiplication by $\mathcal{O}$. Let p^n be an odd prime power, let $k = \mathbb{Q}(j)$ and set $u = 2$ if $j \neq 0$ and $u = 3$ if $j = 0$.*

- *(1) Let L be a number field and let E/L be an elliptic curve with CM by $\mathcal{O}$. Then the local-global principle for $(E/L, p^n)$ holds in any of the following cases:*
  - *(a) p does not divide f and p splits in K;*
  - *(b) p does not divide f, p is inert in K and $[L : k] < (p^2 - 1)/u$; or*
  - *(c) p divides f or p ramifies in K and $[L : k] < (p - 1)/2$.*
- *(2) These bounds above are sharp:*
  - *(b') If p does not divide f and p is inert in K, then there exists a number field L of degree $(p^2 - 1)/u$ over k and an elliptic curve E/L with $j(E) = j$ such that the local-global principle fails for $(E/L, p^2)$.*
  - *(c') If p ramifies in K but does not divide f, then there exists a number field L of degree $(p - 1)/2$ over k and an elliptic curve E/L with $j(E) = j$ such that the local-global principle fails for $(E/L, p^2)$.*

Using Theorem 1.2 one can determine the minimal degree of a number field L for which there exists a CM elliptic curve E/L for which the local-global principle for $(E/L, p^n)$ fails for some n. In Section 4 we give several explicit examples where the local-global principle fails over number fields of minimal degree. The following table gives the values $d = d(p)$ for some small values of p.

p	3	5	7	11	13	17	19	23
d	1	4	3	5	12	32	9	33

The case $p = 3$ recovers the examples given in [Cre16, LW16] showing that the local-global principle for $(E/\mathbb{Q}, 9)$ can fail. For further details see Section 4.1.

Combining the above with [Ran18] and explicit lower bounds for the gonality of modular curves [Abr96] we will prove the following.

Theorem 1.3. *Let $d \geq 1$ be an integer and let $p \geq 17$ be a prime number $p > 2d+1$. Then there are at most finitely many elliptic curves E/L defined over a number field of degree $d = [L : \mathbb{Q}]$ such that the local-global principle for $(E/L, p^n)$ fails for some $n \geq 1$. Moreover, any such counterexample to the local-global principle yields a non-cuspidal non-CM point of degree $\leq d$ on the modular curve $X(p)$ parameterizing isomorphism classes of elliptic curves with full level p structure $E[p] \simeq \mu_p \times \mathbb{Z}/p$.*

Theorem 1.3 should be compared with [PRV12, Corollary 2] and [ÇS15, Theorem B(1)] which assert that the local-global principle holds for $(E/L, p^n)$ for all $[L : \mathbb{Q}] \leq d$ provided $p > (1 + 3^{d/2})^2$. The conclusion of our corollary is weaker in that it allows finitely many possible exceptions, but our bound on p is linear rather than exponential in the degree d. We expect that our bound holds without exceptions for most (if not all) primes p. Sporadic points of degree $d \leq (p-1)/2$ on $X(p)$ should be quite rare as these curves have gonality $\Theta(p^3)$. Moreover, the existence of such a point does not necessarily imply that there is a counterexample to the local-global principle, as there are additional (and rather strict) conditions which must also be satisfied by the mod p^2 Galois representation of the corresponding elliptic curves.

The points of degree at most 2 on the Klein quartic $X(7)$ are determined in [Tze04]. The rational points are all cusps and the degree 2 points have residue field $\mathbb{Q}(\sqrt{-3})$ and lie above $j = 0$ on $X(1)$. Since 7 splits in $\mathbb{Q}(\sqrt{-3})$, Theorem 1.2 shows that the local-global principle for $(E/\mathbb{Q}(\sqrt{-3}), 7^n)$ holds for the corresponding curves. Thus the following corollary.

Corollary 1.4. *The local-global principle holds for $(E/L, 7^n)$ for every elliptic curve E/L over a quadratic number field and every $n \geq 1$.*

Note that by Theorem 1.2 the local-global principle with $N = 7^n$ can fail for elliptic curves over cubic number fields. For an explicit example, see Section 4.2.

2. Group theoretic results on H^1_*

Let p be an odd prime.

Definition 2.1. *Let $V_n := \mathbb{Z}/p^n \times \mathbb{Z}/p^n$ be the natural module with a left action of $\mathrm{GL}_2(\mathbb{Z}/p^n)$. For a subgroup $G \subset \mathrm{GL}_2(\mathbb{Z}/p^n)$ let $\mathrm{H}^i(G, V_n)$ denote the i-th cohomology group of the G-module V_n. Define*

$$\mathrm{H}^1_*(G, V_n) := \bigcap_{g \in G} \ker\left(\mathrm{H}^1(G, V_n) \overset{\mathrm{res}_g}{\to} \mathrm{H}^1(\langle g \rangle, V_n)\right),$$

where $\langle g \rangle$ denotes the cyclic subgroup of G generated by g.

The following lemma is well known in the literature on questions of local-global divisibility.

Lemma 2.2. *Let E/k be an elliptic curve over a number field and let $G \subset \mathrm{GL}_2(\mathbb{Z}/p^n)$ denote the image of the representation $\mathrm{Gal}(k) \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/p^n)$ (for some choice of isomorphism $\mathrm{Aut}(E[p^n]) \simeq \mathrm{GL}_2(\mathbb{Z}/p^n)$). Then the local global principle holds for $(E/k, p^n)$ if and only if $\mathrm{H}^1_*(G, V_n) = 0$.*

Proof. To simplify notation let $\mathbb{K} := k(E[p^n])$ and identify $G \simeq \mathrm{Gal}(\mathbb{K}/k)$. For each place v of k, choose a place $\mathfrak{v}$ of $\mathbb{K}$ above v and let $G_\mathfrak{v} = \mathrm{Gal}(\mathbb{K}_\mathfrak{v}/k_v)$ be the decomposition group. For any finite set of primes S, the inflation-restriction sequence gives the following commutative and exact diagram.

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathrm{H}^1(G, E[p^n]) & \xrightarrow{\text{inf}} & \mathrm{H}^1(k, E[p^n]) & \xrightarrow{\text{res}} & \mathrm{H}^1(\mathbb{K}, E[p^n]) \\ & \downarrow a & & \downarrow b & & \downarrow c \\ 0 \longrightarrow & \prod_{v\notin S} \mathrm{H}^1(G_v, E[p^n]) & \longrightarrow & \prod_{v\notin S} \mathrm{H}^1(k_v, E[p^n]) & \longrightarrow & \prod_{v\notin S} \mathrm{H}^1(\mathbb{K}_{\mathfrak{v}}, E[p^n]) \end{array}$$

Since $\mathrm{H}^1(\mathbb{K}, E[p^n]) = \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\mathbb{K}), E[p^n])$, Chebotarev's density theorem implies that the map c is injective. Hence $Ш^1(k, E[p^n]; S) = \ker(b) = \inf(\ker(a))$. By a second application of Chebotarev's density theorem, the groups G_v range (up to conjugacy) over all cyclic subgroups of G. From this it follows that $\ker(a) \subseteq \mathrm{H}^1_*(G, E[p^n])$. We deduce from this that $Ш^1(k, E[p^n]; S) \subset \inf\left(\mathrm{H}^1_*(G, E[p^n])\right)$ with equality in the case that S contains all of the finitely many places where the decomposition group is not cyclic. The result follows. ☐

Definition 2.3. *For an odd integer $m \geq 3$ and $\delta \in \mathbb{Z}/N$ define*

$$C_{\delta,m} := \left\{ \begin{bmatrix} a & b \\ \delta b & a \end{bmatrix} \; : \; a, b \in \mathbb{Z}/m,\; a^2 - \delta b^2 \in (\mathbb{Z}/m)^\times \right\} \subset \mathrm{GL}_2(\mathbb{Z}/m)\,, \text{ and}$$

$$N_{\delta,m} := \left\langle \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, C_{\delta,m} \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/m)\,.$$

When $m = p^n$ is a prime power, we say that $G \subset N_{\delta,p^n}$ is a **full subgroup** *if the kernels of the reduction mod p maps $N_{\delta,p^n} \to \mathrm{GL}_2(\mathbb{Z}/p)$ and $G \to \mathrm{GL}_2(\mathbb{Z}/p)$ are equal.*

Lemma 2.4. *Let $G \subset N_{\delta,p^n}$ and let $G' := G \cap C_{\delta,p^n}$. If $\mathrm{H}^1_*(G, V_n) \neq 0$, then $\mathrm{H}^1_*(G', V_n) \neq 0$.*

Proof. Note that G' has odd order and index dividing 2 in G. So $\mathrm{H}^i(G/G', V_n^{G'}) = 0$ for $i \geq 1$. Thus, the inflation-restriction sequence gives an injective map $\mathrm{H}^1(G, V_n) \to \mathrm{H}^1(G', V_n)$. This map sends $\mathrm{H}^1_*(G, V_n)$ to $\mathrm{H}^1_*(G', V_n)$ because every cyclic subgroup of G' is also a cyclic subgroup of G. ☐

2.1. **Split case.**

Lemma 2.5. *Suppose δ is a nonzero square mod p. Then for every $G \subset N_{\delta,p^n}$, we have $\mathrm{H}^1_*(G, V_n) = 0$.*

Proof. By Lemma 2.4 we may assume that $G \subset C_{\delta,p^n}$. Let $d \in \mathbb{Z}/p^n$ be a square root of δ. Then C_{δ,p^n} is conjugate to the group of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}/p^n)$. Since G is diagonal, V_n splits as a product $V_n = W_1 \times W_2$ of cylic G-modules of order p^n. Hence $\mathrm{H}^1(G, V_n) \simeq \mathrm{H}^1(G, W_1) \times \mathrm{H}^1(G, W_2)$. We will show below that $\mathrm{H}^1_*(G, W_i) = 0$ for $i = 1, 2$. It follows that $\mathrm{H}^1_*(G, V_n) = 0$ as required.

Write $G = H_1 \times H_2$ where $H_i \subset G$ is the subgroup containing all matrices whose i-th diagonal entry is 1. Note that $W_1^{H_1} = W_1$ and that H_2 acts faitfully on W_1 (i.e., through an injective map $H_2 \to \mathrm{Aut}(W_2) \simeq (\mathbb{Z}/p^n)^\times$). It follows from a standard computation in the cohomology of cyclic groups that $\mathrm{H}^1(H_2, W_1) = 0$ (see [NSW08, Lemma 9.1.4]). Let $\xi \in \mathrm{H}^1_*(G, W_1)$. Since $H_1 \subset G$ is a cyclic subgroup the restriction of ξ to H_1 is trivial. Hence ξ is in the image of the inflation map $\mathrm{H}^1(H_2, W_1) = \mathrm{H}^1(H_2, W_1^{H_1}) \to \mathrm{H}^1(G, W_1)$. As noted above, $\mathrm{H}^1(H_2, W_1) = 0$, so $\xi = 0$ showing that $\mathrm{H}^1_*(G, W_1) = 0$. Swapping indices the same argument shows that $\mathrm{H}^1_*(G, W_2) = 0$. ☐

2.2. **Inert case.**

Lemma 2.6. *Suppose that δ is not a square modulo p. Let $G \subset N_{\delta,p^n}$ and let $G_1 \subset \mathrm{GL}_2(\mathbb{Z}/p)$ denote the image of G modulo p.*

(1) If G_1 is contained in neither $\begin{bmatrix} \pm 1 & 0 \\ 0 & 1 \end{bmatrix}$ nor $\begin{bmatrix} 1 & 0 \\ 0 & \pm 1 \end{bmatrix}$, then $\mathrm{H}^1_*(G, V_n) = 0$.

(2) If G is a full subgroup of N_{δ,p^2} with $G_1 \subset \begin{bmatrix} \pm 1 & 0 \\ 0 & 1 \end{bmatrix}$ or $G_1 \subset \begin{bmatrix} 1 & 0 \\ 0 & \pm 1 \end{bmatrix}$, then $\mathrm{H}^1_*(G, V_2) \neq 0$.

Proof. Let us prove the first statement. Suppose $\mathrm{H}^1_*(G, V_n) \neq 0$. Letting $G' = G \cap C_{\delta,p^n}$ we have $\mathrm{H}^1_*(G', V_n) \neq 0$ by Lemma 2.4. Let G'_1 denote the image of G' modulo p. Since $\#C_{\delta,p} = p^2 - 1$ is prime to p, [Ran18, Theorem 2] there are two possibilities for G'_1

(a) G'_1 is generated by a element of order dividing $p-1$ with 1 as an eigenvalue, or

(b) G'_1 is generated by an element of order 3 acting irreducibly on $V_1 = p^{n-1}V_n$.

(We note that $G'_1 = S_3$ is impossible because $C_{\delta,p}$ is abelian). First consider case (a). The elements of order $p-1$ in $C_{\delta,p}$ are diagonal matrices, so the condition on the eigenvalues implies that G'_1 is trivial. Then G_1 is generated by an element of order dividing 2 which has 1 as eigenvalue, so it must be contained in one of the two groups in the statement.

Now consider case (b). Then G' is abelian of order $3p^m$, so the Sylow-3-subgroup $P \subset G'$ is normal. The inflation-restriction sequence reads

$$\mathrm{H}^1(G'/P, V_n^P) \to \mathrm{H}^1(G', V_n) \to \mathrm{H}^1(P, V_n)\,.$$

Since P acts irreducibly on $V[p]$ we have $V_n^P = 0$, so the first term in the sequence is 0. The final term in the sequence is also trivial because P and V_n have relatively prime orders. By exactness of the inflation-restriction sequence we conclude $\mathrm{H}^1(G', V_n) = 0$, contradicting the assumption $\mathrm{H}^1_*(G', V_n) \neq 0$.

We now prove part 2 of the lemma. Consider the matrices

$$\sigma_1 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, h_1 = \begin{bmatrix} 1+p & 0 \\ 0 & 1+p \end{bmatrix}, h_2 = \begin{bmatrix} 1 & p \\ \delta p & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^2)\,.$$

By assumption G is generated by h_1, h_2 and at most one of the σ_i. Then G is the semidirect product of $H = \langle h_1, h_2 \rangle$ and a subgroup of order dividing 2. Since G/H has order dividing 2 and p is odd the inflation-restriction sequence gives an isomorphism

$$\mathrm{H}^1(G, V_2[p]) \simeq \mathrm{H}^1(H, V_2[p])^{G/H} = \mathrm{Hom}_{G/H}(H, V_2[p])\,.$$

Let $\mathbf{v} \in V_2[p]^G$ be a nonzero element fixed by G and define $\phi : H \to V_2[p]$ as the homomorphism determined by $\phi(h_1) = \mathbf{v}$ and $\phi(h_2) = 0$. Since h_1 lies in the center of G and $\mathbf{v}$ is fixed by G, ϕ is a G/H-equivariant homomorphism. By the isomorphism above this determines a nonzero class in $\mathrm{H}^1(G, V_2[p])$. We claim that the image ϕ' of this class in $\mathrm{H}^1(G, V_2)$ is a nonzero element of $\mathrm{H}^1_*(G, V_2)$.

Let us give the details assuming $\sigma_1 \in G$, the other cases being handled similarly. Let $g \in G$. We will show that the restriction of ϕ to the subgroup generated by g is a coboundary. If $g \in H$, then $g = h_1^a h_2^b$ for some a, b and the condition that ϕ' restricts to a coboundary on the subgroup generated by g is that the equation

$$\begin{bmatrix} ap & bp \\ b\delta p & ap \end{bmatrix} \mathbf{x} = \begin{bmatrix} 0 \\ ap \end{bmatrix} \tag{2.1}$$

has a solution $\mathbf{x} \in V_2$. This clearly has solutions when $ap = 0$. When $ap \neq 0$, $(a^2 - \delta b^2) \in (\mathbb{Z}/p^2)^\times$ because we have assumed δ is not a square modulo p. In this case the unique solution to (2.1) is $\mathbf{x} = \frac{a}{a^2-\delta b^2}\begin{bmatrix}-b\\ a\end{bmatrix}$.

If, on the other hand, $g \notin H$, then $g = \sigma h_1^a h_2^b$ in which case the local condition becomes

$$\begin{bmatrix} ap & bp \\ -b\delta p & -2-ap \end{bmatrix}\mathbf{x} = \begin{bmatrix} 0 \\ ap \end{bmatrix}, \tag{2.2}$$

which has the solution $x = p$, $y = -ap/2$.

The fact that (2.1) and (2.2) have solutions for any choice of a, b gives that $\phi' \in \mathrm{H}^1_*(G, V_2)$. The fact that there is no common solution to (2.1) as one varies a, b shows that ϕ' is not trivial. □

2.3. **Ramified case.**

Lemma 2.7. *Suppose that $\delta \equiv 0$ mod p. Let $G \subset N_{\delta,p^n}$ and let G_1 denote the image of G modulo p.*

(1) If G_1 is contained in neither $\begin{bmatrix}1 & *\\ 0 & \pm 1\end{bmatrix}$ nor $\begin{bmatrix}\pm 1 & 0\\ 0 & 1\end{bmatrix}$, then $\mathrm{H}^1_*(G, V_n) = 0$.

(2) If $\delta \not\equiv 0 \bmod p^2$, G is a full subgroup of N_{δ,p^2} and $G_1 = \begin{bmatrix}1 & *\\ 0 & \pm 1\end{bmatrix}$, then $\mathrm{H}^1_*(G, V_2) \neq 0$.

Proof. For the first statement suppose $\mathrm{H}^1_*(G', V_n) \neq 0$ where $G' = G \cap C_{\delta,p^n}$. Let G'_1 denote the image of G' modulo p. If $p \nmid \#G'_1$, then as in the proof of the preceding lemma, [Ran18] implies that G_1 is generated by a diagonal matrix of order dividing 2 with 1 as an eigenvalue. Otherwise $p \mid \#G'_1$. Since $\delta \equiv 0 \mod p$, $C_{\delta,p}$ is a Borel subgroup. So in this case [Ran18] implies that G'_1 is the subgroup of stricly upper triangular matrices and that $G_1 = G'_1$ or G_1 is generated by G'_1 and $\mathrm{diag}(1, -1)$ as required.

The assumption in the second statement of the lemma implies that G is generated by the matrices

$$\sigma = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \; g = \begin{bmatrix}1 & 1\\ \delta & 1\end{bmatrix}, \; h = \begin{bmatrix}1+p & 0\\ 0 & 1+p\end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^2).$$

We note that any element of G can be written in the form $\sigma^a g^b h^c$ for some integers a, b, c. Let $H = \langle h, g^p \rangle$ be the kernel of reduction modulo p. Then G/H is the dihedral group of order $2p$ generated by the images $\overline{\sigma}$ and $\overline{g}$ of σ and g. A direct calculation shows that the cochain defined by

$$\overline{\sigma}^a \overline{g}^b \mapsto p \begin{bmatrix} b(b-1)/2 \\ (-1)^a b + (1 + (-1)^{a+1})/2 \end{bmatrix}$$

gives a nontrivial class in $\mathrm{H}^1(G/H, V_2[p])$. We will show that the image ξ of this class in $\mathrm{H}^1(G, V_2)$ is a nonzero element of $\mathrm{H}^1_*(G, V_2)$. The proof is similar to that found in [Ran18, Lemma 11].

By induction one proves that

$$g^b = \begin{bmatrix} 1 + \delta\frac{b(b-1)}{2} & b + \delta\sum_{i=1}^{b}\frac{i(i-1)}{2} \\ \delta b & 1 + \delta\frac{b(b-1)}{2} \end{bmatrix}.$$

If $C \subset G$ is a cyclic subgroup generated by $\gamma = g^b h^c$, the condition that ξ is the class of a coboundary on C is that the equation

$$\begin{bmatrix} cp + \delta\frac{b(b-1)}{2} & b + cp + \delta\sum_{i=1}^{b}\frac{i(i-1)}{2} \\ \delta b & cp + \delta\frac{b(b-1)}{2} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p\frac{b(b-1)}{2} \\ pb \end{bmatrix}. \tag{2.3}$$

has a solution with $x, y \in \mathbb{Z}/p^2$ for any choice of integers b, c. Since the right hand side lies in $pV_2 = V_2[p]$ and the determinant of the matrix on the left hand side is $\delta b^2 \not\equiv 0 \bmod p^2$, this equation has a solution. Namely, $x = p/\delta, y = -cp^2/\delta b$ (which is well defined in $\mathbb{Z}/p^2$ since $\delta \not\equiv 0 \bmod p^2$).

Similarly, if C is generated by $\sigma g^b h^c$, the local condition gives rise to the equation

$$\begin{bmatrix} cp + \delta\frac{b(b-1)}{2} & b + bcp + \delta\sum_{i=1}^{b}\frac{i(i-1)}{2} \\ -\delta b & -2 - cp - \delta\frac{b(b-1)}{2} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p\frac{b(b-1)}{2} \\ -pb + p \end{bmatrix}.$$

in which case $x = 0, y = (b-1)p/2$ is a solution. We conclude that ξ lies in $\mathrm{H}^1_*(G, V_2)$. As the solutions to (2.3) depend on b, ξ is nontrivial. $\square$

3. Proofs of the theorems

Before beginning the proof let us recall some relevant results concerning the mod N representations attached to CM elliptic curves.

Let $E/\mathbb{Q}(j(E))$ be an elliptic curve over $k = \mathbb{Q}(j(E))$ with complex multiplication by an order $\mathcal{O} \subset K$ where K is a quadratic imaginary field. Let $H = K(j(E))$ and let $h : E \to E/\operatorname{Aut}(E) = \mathbb{P}^1$ be a Weber function. All elliptic curves with CM by $\mathcal{O}$ are twists of one another and the field $H_N := H(h(E[N]))$ does not depend on the choice of twist.

As $E[N]$ is an $\operatorname{End}(E) = \mathcal{O}$ module of rank 1 there is an isomorphism $\operatorname{Aut}_{\mathcal{O}}(E[N]) \simeq (\mathcal{O}/N)^\times$. Assuming N is odd, the natural map $\mathcal{O}^\times \to (\mathcal{O}/N)^\times$ is injective and its image identifies with $\operatorname{Aut}(E)$ as a subgroup of $\operatorname{Aut}_{\mathcal{O}}(E[N])$. The restriction of $\rho_{H,N}$ to G_{H_N} induces a representation $\rho_{H_N} : G_{H_N} \to \operatorname{Aut}(E) \simeq \mathcal{O}^\times$. In particular, $\operatorname{Gal}(H(E[N])/H_N)$ may be viewed as a subgroup of $\operatorname{Aut}(E)$. On the other hand, any choice of basis for $E[N]$ determines an isomorphism of groups $\operatorname{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The main theorems of class field theory allow one to classify the possibilities for the image of the mod N representation $\rho_{k,N} : \operatorname{Gal}(k) \to \operatorname{Aut}(E[N])$. The following is taken from [LR].

Theorem 3.1 ([LR, Theorem 1.1]). *Suppose N is odd and let $\delta = \Delta_K f^2/4$, where Δ_K is the fundamental discriminant of K and f is the conductor of $\mathcal{O}$. Then there is a basis for $E[N]$ such that the image of $\rho_{k,N} : \operatorname{Gal}(k) \to \mathrm{GL}_2(\mathbb{Z}/N)$ lies in the group $N_{\delta,N}$ (see Definition 2.3) and is generated by $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $C_{\delta,N} = \operatorname{image}(\rho_{H,N})$. Moreover the index of the image of $\rho_{H,N}$ in $C_{\delta,N}$ is equal to the index of $\operatorname{Gal}(H(E[N])/H_N)$ as a subgroup of $\operatorname{Aut}(E) \simeq \mathcal{O}^\times$.*

Lemma 3.2. *Suppose $N = p$ is an odd prime and the mod p representation attached to E/k surjects onto $N_{\delta,p}$. Let $A \subset \operatorname{Aut}(E) \subset N_{\delta,p}$ and $G \subset N_{\delta,p}$ with $A \cap G = 1$. Let $L \subset k(E[p])$ be the fixed field of the group $AG \subset N_{\delta,p}$. There exists a twist E'/L of E/L by a character $\chi : \operatorname{Gal}(L) \to A \subset \operatorname{Aut}(E)$ such that the mod p image attached to E'/L is equal to G if and only if G is a normal subgroup of AG.*

Remark 3.3. *The subgroup $A = \mu_2 \subset \operatorname{Aut}(E)$ lies in the center of $N_{\delta,p}$ so in this case G is always normal in AG.*

Proof. To ease notation let $\mathbb{K} = k(E[p])$ and identify $N_{\delta,p} = \mathrm{Gal}(\mathbb{K}/k)$. If G is a normal subgroup of AG, then the extension $\mathbb{K}^G/L$ is Galois with Galois group isomorphic to A, which may be identified with a subgroup of $\mathrm{Aut}(E) = \mu_m$. Then there is a character $\chi : \mathrm{Gal}(L) \to \mu_m$ with kernel $\mathrm{Gal}(\mathbb{K}^G)$ whose restriction to $\mathrm{Gal}(\mathbb{K}^A)$ is the inverse of $\rho_{E/\mathbb{K}^A} : \mathrm{Gal}(\mathbb{K}^A) \to A \subset \mu_m$. Let E'/L be the twist of E/L by χ. The mod p representations are related by $\rho_{E/L,p} \otimes \chi = \rho_{E'/L,p}$. So $\mathbb{K}^A = \ker(\rho_{E'/L,p}) = L(E'[p])$ and the image of $\rho_{E'/L,p}$ is equal to G.

Conversely, if there exists a twist as in the statement, then $M = \ker(\chi)$ is a Galois extension of L and $\mathrm{Gal}(\mathbb{K}/M) = G$, so G is normal in $AG = \mathrm{Gal}(\mathbb{K}/L)$. □

Proof of Theorem 1.2.
Part (1): Let L/k be a finite extension and let E/L be an elliptic curve with CM by $\mathcal{O}$. By [LR, Theorem 4.6] there exists an elliptic curve E'/k with CM by $\mathcal{O}$ such that (under a suitable choice of basis for $E'[p^n]$) the image $G_{E/k,p^n}$ of the representation $\rho_{E'/k,p^n} : \mathrm{Gal}(k) \to \mathrm{Aut}(E'[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/p^n)$ is equal to N_{δ,p^n}. The image $G_{E'/L,p^n}$ of the mod p^n representation attached to the base change E'/L is the restriction of $\rho_{E'/k,p^n}$ to the subgroup $\mathrm{Gal}(L) \subset \mathrm{Gal}(k)$. Galois theory gives $[N_{\delta,p^n} : G_{E'/L,p^n}] \le [L : k]$.

There is a character $\chi : \mathrm{Gal}(L) \to \mu_m = \mathrm{Aut}(E)$ such that $E' = E^\chi$ is the twist of E/L by χ. The mod p^n representations are related by $\rho_{E/L,p^n} = \rho_{E'/L,p^n} \otimes \chi$. The images $G_{E/L,p^n}$ and $G_{E'/L,p^n}$ of these representations are subgroups of N_{δ,p^n} whose sizes differ by a factor which divides $\ell := \#\mathrm{image}(\chi)$. Thus $[N_{\delta,p^n} : G_{E/L,p^n}] \le \ell[L : k]$. In particular, if $j \neq 0, 1728$, then $[N_{\delta,p^n} : G_{E/L,p^n}] \le 2[L : k]$.

(a) Assume that p does not divide f and that p splits in K. Then $\delta = \Delta_K f^2/4$ is a nonzero square modulo p. By Lemma 2.5 we have $\mathrm{H}^1_*(G_{E/L,p^n}, V_n) = 0$. So the local-global principle holds for $(E/L, p^n)$ by Lemma 2.2.

(b) Assume that p does not divide f, p is inert in K and $[L : k] < (p^2 - 1)/2$. First assume $j \neq 0, 1728$. Then by the discussion above we have

$$[N_{\delta,p} : G_{E/L,p}] \le [N_{\delta,p^n} : G_{E/L,p^n}] \le 2[L : k] < p^2 - 1\,.$$

The assumption on p implies that $\delta = \Delta_K f^2/4$ is not a square modulo p. So $\#N_{\delta,p} = 2(p^2 - 1)$ and the estimate above gives $\#G_{E/L,p} > 2$. In particular $G_{E/L,p}$ cannot be contained in either of the subgroups appearing in Lemma 2.6. We conclude from this and Lemma 2.2 that the local-global principle holds for $(E/L, p^n)$.

Now we consider the cases $j = 0$ or $j = 1728$. Let $m = \#\mathrm{Aut}(E) \in \{4, 6\}$. Suppose $\mathrm{H}^1_*(G_{E/L,p^n}, V_n) \neq 0$. We must show $[L : k] \ge 2(p^2 - 1)/u$. By Lemma 2.6, $G_{E/L,p}$ is trivial or is generated by $\mathrm{diag}(-1, 1)$ or $\mathrm{diag}(1, -1)$. If G is trivial, then the estimate $[N_{\delta,p^n} : G_{E/L,p^n}] \le u[L : k]$ gives $[L : k] \ge 2(p^2-1)/u$. If $G_{E/L,p}$ is generated by either $\mathrm{diag}(-1, 1)$ or $\mathrm{diag}(1, -1)$, then $G_{E/L,p}$ is not normal in $G_{E/L,p}\,\mathrm{Aut}(E)$. In fact, the only nontrivial subgroup $A \subset \mathrm{Aut}(E)$ for which $G_{E/L,p}$ is normal in $G_{E/L,p}A$ is $A = \mu_2$. By Lemma 3.2 we conclude that the image of χ is contained in μ_2. So $\ell := \#\mathrm{image}(\chi) = 2$ and our estimate above gives $[N_{\delta,p^n} : G_{E/L,p^n}] \le \ell[L : k] \le 2[L : k]$, which implies $[L : k] \ge (p^2 - 1)/2 \ge 2(p^2 - 1)/u$ as required.

(c) Assume that p divides f or p is ramified in K. Assume that $[L : k] < (p-1)/2$. These conditions imply $j \neq 0, 1728$ (Note that the condition on $[L : k]$ implies $p > 3$), so $\mathrm{Aut}(E) = \mu_2$. Arguing as in the previous case we have $[N_{\delta,p} : G_{E/L,p}] < (p-1)/2$. In this case $\delta = \Delta_K f^2/4$ is 0 mod p, so $\#N_{\delta,p} = 2p(p-1)$ and we conclude $\#G_{E/L,p} > 2p$.

In particular $G_{E/L,p}$ cannot be contained in either of the subgroups appearing in Lemma 2.7. We conclude from this and Lemma 2.2 that the local-global principle holds for $(E/L, p^n)$.

Part (2): We now show that the bounds obtained in Part (1) are sharp. Let E'/k be, as above, an elliptic curve such that the mod p^n representation surjects onto N_{δ,p^n}. Let $\mathbb{K} = k(E'[p])$. We identify $N_{\delta,p} = \mathrm{Gal}(\mathbb{K}/k)$. Let $H_p \subset \mathbb{K}$ be the subfield fixed by $\mathrm{Aut}(E') \subset N_{\delta,p}$. As the notation suggests, $H_p = k(h(E'[p]))$ for a Weber function h. Hence H_p is independent the choice of twist of E'. Let $H'_p \subset \mathbb{K}$ be the subfield fixed by $\mu_2 \subset \mathrm{Aut}(E) \subset N_{\delta,p}$. Then $H_p = H'_p$ if $j \neq 0, 1728$.

(b') Assume that p does not divide f and p is inert in K. Let $M \subset \mathbb{K}$ be the subfield fixed by $g = \mathrm{diag}(-1, 1) \in N_{\delta,p}$ and let $L = M \cap H'_p = \mathbb{K}^{\langle g,-1\rangle}$. Note that $[\mathbb{K} : L] = 4$ and $[\mathbb{K} : k] = \#N_{\delta,p} = 2(p^2 - 1)$, so $[L : k] = (p^2 - 1)/2$. Let $\chi : \mathrm{Gal}(L) \to \mu_2$ be the quadratic character with $\ker(\chi) = \mathrm{Gal}(M)$ and let E/L be the quadratic twist of E'/L by χ. The image $G_{E/L,p^2}$ of the mod p^2 representation attached to E/L is a full subgroup of N_{δ,p^2} whose image mod p is generated by $g = \mathrm{diag}(-1, 1)$. So by Lemma 2.6 we have that $\mathrm{H}^1_*(G_{E/L,p^2}, V_2) \neq 0$. By Lemma 2.2 we conclude that the local-global principle fails for $(E/L, p^2)$.

In the case $j = 0$ we can construct an example over a field of degree $(p^2 - 1)/3$ as follows. The field $H_p = k(E'[p])$ has degree $2(p^2-1)/6 = (p^2-1)/3$ and $\mathrm{Gal}(\mathbb{K}/H_p) = \mathrm{Aut}(E) = \mu_6$. By Lemma 3.2 (applied with $G = 1$) there exists a sextic twist of E'/H_p such that $H_p = H_p(E'[p])$. The image of the mod p^2 associated to this curve is the full subgroup of N_{δ,p^2} congruent to the trivial group modulo p. By Lemmas 2.6 and 2.2 the local-global principle fails for $(E'/H_p, p^2)$.

(c') Assume that p ramifies in K but does not divide f. Let $G \subset N_{\delta,p}$ be the subgroup generated by $\mathrm{diag}(1, -1)$ and the strictly upper triangular matrices. Let $M \subset \mathbb{K}$ be the fixed field of G and let $L = M \cap H'_p$. In this case $[\mathbb{K} : k] = 2p(p - 1)$, so $[L : k] = (p - 1)/2$.

As in the preceding case, twisting E'/L by the quadratic character $\mathrm{Gal}(L) \to \mu_2$ with kernel $\mathrm{Gal}(M)$ yields an elliptic curve E/L such that the image $G_{E/L,p^2}$ of the mod p^2 representation is the full subgroup of $N_{\delta,p}$ whose image mod p is G. By Lemma 2.7 and 2.2 we conclude that the local-global principle fails for $(E/L, p^2)$.

□

Proof of Theorem 1.3. Let E/L be an elliptic curve over the number field L of degree $d = [L : \mathbb{Q}]$. Suppose $p > 2d + 1$ and that the local-global principle for $(E/L, p^n)$ fails. The determinant of the mod p representation $\mathrm{Gal}(k) \to \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{Z}/p) \to \mathbb{Z}/p^\times$ is the p-cyclotomic character. Since $d < (p - 1)/2 = [\mathbb{Q}(\mu_p)^+ : \mathbb{Q}]$, the image of this determinant map is of size > 2. [Ran18, Theorem 2] shows that the possibilities for the image of the mod p representation are rather limited. The only possibility compatible with the image of the determinant map having size greater than 2 is that the image is contained in $\begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix}$. In other words, $E[p] \simeq \mathbb{Z}/p \times \mu_p$ as a Galois module, so E/L corresponds to a non-cuspidal point in $X(p)(L)$. By Theorem 1.2, E/L does not have CM. It remains only to prove the finiteness of the set of points of degree $\leq (p - 1)/2$ on $X(p)$. By [Fre94] it suffices to check that $X(p)$ has gonality $\gamma(X(p)) \geq (p-1)$. In [Abr96] one finds the estimate $\gamma(X(p)) \geq [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma(p)]7/800 = 7(p^3-p)/1600$, which suffices for $p \geq 17$. □

4. Explicit Examples

Proposition 4.1. *Suppose $p \equiv 3 \bmod 4$ is a prime ramifying in K and let E/k be an elliptic curve with CM by an order in K whose conductor is not divisible by p. We assume $k = \mathbb{Q}(j(E))$. Then $[k(\mu_p) : k] = p-1$. Let $k(\mu_p)^+$ be the unique intermediate field of degree $(p-1)/2$ over k. There is a twist E'/k of E/k such that the local-global principle fails for $(E'/k(\mu_p)^+, p^2)$.*

Proof. Twisting if necessary, we may assume that the mod p^n representations attached to E/k surject onto N_{δ,p^n}. Let $\mathbb{K} = k(E[p])$ and identify $N_{\delta,p} = \mathrm{Gal}(\mathbb{K}/k)$. Since $\delta \equiv 0 \bmod p$, $N_{\delta,p}$ consists of the upper triangular invertible matrices. Note that $k(\mu_p) \subset \mathbb{K}$ is the subfield fixed by $\mathrm{SL}_2(\mathbb{Z}/p) \cap N_{\delta,p}$. Since $p \equiv 3 \bmod 4$, $\mathrm{SL}_2(\mathbb{Z}/p) \cap N_{\delta,p}$ is the group generated by -1 and the strictly upper triangular matrices. The subfield $k(\mu_p)^+$ is fixed by the complex conjugation, which acts on $E[p]$ as $\mathrm{diag}(-1,1)$ or $\mathrm{diag}(1,-1)$. So $k(\mu_p)^+$ is the fixed field of the group $\begin{bmatrix} \pm 1 & * \\ 0 & \pm 1 \end{bmatrix}$ of order $4p$. The fixed field $M \subset \mathbb{K}$ of the group $G = \begin{bmatrix} 1 & * \\ 0 & \pm 1 \end{bmatrix}$ is a quadratic extension of $k(\mu_p)^+$. Let $E'/k(\mu_p)^+$ be the twist of $E/k(\mu_p)^+$ by the quadratic character with kernel $\mathrm{Gal}(M)$. Then the image of the mod p representation attached to $E'/k(\mu_p)$ is equal to G. By Lemma 2.7 we have $\mathrm{H}^1_*(G_{E'/k,p^2}, E[p^2]) \neq 0$. The only primes that ramify in the extension $k(\mu_p)^+/k$ are those lying above p. □

4.1. **The case $p = 3$.** Proposition 4.1 shows that there is an elliptic curve $E/\mathbb{Q}$ of j-invariant 0 (so $K = \mathbb{Q}(\sqrt{-3})$) such that the local-global principle fails for $(E/\mathbb{Q}, 9)$. Examples of such were first given in [Cre16] and then in [LW16]. In fact the proposition recovers these examples as all have j-invariant 0 and mod 9 image the full subgroup of $N_{6,9}$ congruent to $\begin{bmatrix} 1 & * \\ 0 & \pm 1 \end{bmatrix}$ modulo 3. In light of the fact that $\mathrm{Aut}(E) \simeq \mu_6$ for these curves, one can obtain infinitely many counterexamples to the local-global principle for $(E/\mathbb{Q}, 9)$ by taking cubic twists (which was already evident from [Cre16, Corollary 4.3]). This family of twists also contains the modular curve $X_0(27)$ whose mod 9 image is the full subgroup of $N_{6,9}$ congruent to $\begin{bmatrix} 1 & 0 \\ 0 & \pm 1 \end{bmatrix}$ modulo 3, giving a counterexample to the local-global principle for $(E/\mathbb{Q}, 9)$ with a different mod 3 image.

For an example with a different j-invariant one can consider the family of curves $E/\mathbb{Q}$ with j-invariant $2^4 3^3 5^3$ which have CM by the order of conductor 2 in $\mathbb{Q}(\sqrt{-3})$. In this case $\mathrm{Aut}(E) \simeq \mu_2$ so there is a unique curve in the family whose mod 9 representation is the full subgroup of $N_{-3,9}$ congruent to $\begin{bmatrix} 1 & * \\ 0 & \pm 1 \end{bmatrix}$ modulo 3; it is the curve with Cremona reference 36.a2 and is a counterexample to the local-global principle for $(E/\mathbb{Q}, 9)$.

4.2. **The case $p = 7$.** There are two elliptic curves of conductor 49 over $\mathbb{Q}$ with CM by the maximal order in $\mathbb{Q}(\sqrt{-7})$. One is the modular curve $X_0(49)$ and the other, [LMFDB, Elliptic Curve 49.a2], is its twist by the quadratic character corresponding to $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$. The images of the mod 7 representations attached to the base changes of these curves to $\mathbb{Q}(\mu_7)^+$ are

$$\begin{bmatrix} \pm 1 & * \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & * \\ 0 & \pm 1 \end{bmatrix},$$

respectively. For both curves the local-global principle for $(E/\mathbb{Q}(\mu_7), 49)$ fails, while only for the twist E of $X_0(49)$ does it fail for $(E/\mathbb{Q}(\mu_7)^+, 49)$. This gives the unique example of a CM elliptic curve over a cubic number field for which the local-global principle fails with $N = 7^n$. Since the conductor is $49 = 7^2$, the decomposition groups $D_{\mathfrak{q}} \subset \mathrm{Gal}(\mathbb{Q}(E[49])/\mathbb{Q}(\mu_7)^+)$ are cyclic for all primes $\mathfrak{q} \nmid 7$. Moreover, 7 is totally ramified in the degree 42 extension $\mathbb{Q}(E[49])/\mathbb{Q}$ and so if $\mathfrak{p}$ is the prime of $\mathbb{Q}(\mu_7)^+$ lying above 7, then the restriction map $\mathrm{H}^1(\mathbb{Q}(\mu_7^+), E[7]) \to \mathrm{H}^1(\mathbb{Q}(\mu_7)^+_{\mathfrak{p}}, E[7])$ is an isomorphism. We conclude that

$$\text{Ш}^1(\mathbb{Q}(\mu_7)^+, E[49]; S) \neq 0 \quad \Leftrightarrow \quad \mathfrak{p} \in S\,.$$

So while the local-global principle fails for $(E/\mathbb{Q}(\mu_7)^+, 49)$ the local-global principle for divisibility by 7^n holds in the groups $E(\mathbb{Q}(\mu_7)^+)$ and $\mathrm{H}^1(\mathbb{Q}(\mu_7)^+, E)$.

4.3. **The case $p = 5$.** There is no rational j-invariant $j = j(\mathcal{O})$ of an order in a quadratic imaginary field such that 5 divides the conductor or ramifies in $\mathcal{O}$. So by Theorem 1.2 the local-global principle with $N = 5^n$ holds for CM curves over quadratic and cubic fields. The class number of $\mathbb{Q}(\sqrt{-5})$ is 2, so there are elliptic curves with CM by the maximal order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-5})$ defined over a quadratic field, namely $k = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(j(\mathcal{O}))$. Theorem 1.2(c') implies that there is a CM elliptic curves over some quadratic extension L/k such that the local-global principle for $(E/L, 5^2)$ fails. Here we provide an explicit example.

Consider the curve E/k [LMFDB, Elliptic Curve 4096.1-k1] with Weierstrass equation

$$E : y^2 = f(x) := x^3 - \phi x^2 + (-\phi - 9)x + (-6\phi - 15)\,,$$

where $\phi \in \mathbb{Q}(\sqrt{5})$ satisfies $\phi^2 + \phi + 1 = 0$. The image of the mod 5 Galois representation is $\begin{bmatrix} \pm 1 & * \\ 0 & \pm 1 \end{bmatrix}$ (note that $k = \mathbb{Q}(\mu_5)^+$, so the diagonal entries must be squares in $\mathbb{F}_5^\times$). The 5-division polynomial of E/k has a root θ in a quadratic extension L/k, which turns out to be $L = \mathbb{Q}(\mu_{20})^+$. The root θ is the x-coordinate of a 5-torsion point on E. The quadratic twist of E by $d = f(\theta) \in L^\times/L^{\times 2}$ yields the curve [LMFDB, Elliptic Curves 25.a2] which has an L-rational 5-torsion point. The image of the mod 5 Galois representation attached to E^d is

$$\begin{bmatrix} 1 & * \\ 0 & \pm 1 \end{bmatrix}$$

and so, by Lemma 2.7, the local-global principle fails for $(E^d/L, 25)$. As 5 is the only prime of bad reduction and 5 is totally ramified in $L(E^d[5])$ we conclude (similarly to the $p = 7$ case) that $\text{Ш}^1(L, E^d[25]; S) \neq 0$ if and only if S contains the prime of L above 5.

5. Acknowledgements

Some of the content in this article is based on the second author's MSc Thesis at the University of Canterbury which includes a detailed proof of Corollary 1.4.

References

[Abr96] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices **20** (1996), 1005–1011.

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *III. The Tate-Šafarevič and Selmer groups*, Proc. London Math. Soc. (3) **12** (1962), 259–296.

[ÇS15] Mirela Çiperiani and Jakob Stix, *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels*, J. Reine Angew. Math. **700** (2015), 175–207.

[Cre13] Brendan Creutz, *Locally trivial torsors that are not Weil-Châtelet divisible*, Bull. Lond. Math. Soc. **45** (2013), no. 5, 935–942.

[Cre16] Brendan Creutz, *On the local-global principle for divisibility in the cohomology of elliptic curves*, Math. Res. Lett. **23** (2016), no. 2, 377–387.

[CV17] Brendan Creutz and José Felipe Voloch, *Local-global principles for Weil-Châtelet divisibility in positive characteristic*, Math. Proc. Cambridge Philos. Soc. **163** (2017), no. 2, 357–367.

[DZ01] Roberto Dvornicich and Umberto Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France **129** (2001), no. 3, 317–338 (English, with English and French summaries).

[DZ04] Roberto Dvornicich and Umberto Zannier, *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Math. Acad. Sci. Paris **338** (2004), no. 1, 47–50 (English, with English and French summaries).

[DZ07] Roberto Dvornicich and Umberto Zannier, *On a local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lond. Math. Soc. **39** (2007), no. 1, 27–34.

[Fre94] Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83.

[Gre12] Ralph Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), no. 5, 1167–1196.

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database*. [Online; accessed 22 October 2021].

[LR] Álvaro Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication*, available at `arXiv:1809.02584v2`.

[LW16] Tyler Lawson and Christian Wuthrich, *Vanishing of some Galois cohomology groups for elliptic curves*, Elliptic curves, modular forms and Iwasawa theory, Springer Proc. Math. Stat., vol. 188, Springer, Cham, 2016, pp. 373–399.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[PRV12] Laura Paladino, Gabriele Ranieri, and Evelina Viada, *On local-global divisibility by p^n in elliptic curves*, Bull. Lond. Math. Soc. **44** (2012), no. 4, 789–802.

[PRV14] Laura Paladino, Gabriele Ranieri, and Evelina Viada, *On the minimal set for counterexamples to the local-global principle*, J. Algebra **415** (2014), 290–304.

[Ran18] Gabriele Ranieri, *Counterexamples to the local-global divisibility over elliptic curves*, Ann. Mat. Pura Appl. (4) **197** (2018), no. 4, 1215–1225.

[Tze04] Pavlos Tzermias, *Low-degree points on Hurwitz-Klein curves*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 939–951.