EXAMPLES OF ABELIAN SURFACES WITH NON-SQUARE TATE-SHAFAREVICH GROUP

STEFAN KEIL

Abstract. In this article we show the existence of abelian surfaces $B/\mathbb{Q}$ with Tate-Šafarevič groups having orders five times a square and seven times a square. To obtain this result, we explore the invariance under isogenies of the Birch and Swinnerton-Dyer conjecture.

Contents

1. Introduction

Let A/K be an abelian variety over a number field K. Consider its Tate-Šafarevič group $Ш(A/K)$. If A is an elliptic curve E, then the order of $Ш(E/K)$ is a perfect square, if it is finite. But in higher dimensions, even for principally polarized abelian varieties, this is no longer true in general. Denote by $A^\vee$ the dual abelian variety. The Cassels-Tate pairing [Cas62], [Tat63]

$$\langle \cdot, \cdot \rangle : Ш(A/K) \times Ш(A^\vee/K) \to \mathbb{Q}/\mathbb{Z},$$

which is non-degenerate in case $Ш(A/K)$ is finite, combined with a result of Flach [Fla90] gives a strong restriction on the non-square part of the order of the Tate-Šafarevič group [Ste04, Theorem 1.2].

Theorem 1.1. *Assume $Ш(A/K)$ is finite. If an odd prime p divides the non-square part of $\#Ш(A/K)$, then p divides the degree of all polarizations of A/K.*

Date: June 11, 2012.
The author is supported by a scholarship from the Berlin Mathematical School (BMS).

Corollary 1.2. *If A/K is a principally polarized abelian variety, then*

$$\#Ш(A/K) = \square \text{ or } 2\square.$$

More precisely, assuming the finiteness of $Ш(A/K)$, Poonen and Stoll [PS99] associated to each principal polarization λ of A/K a unique element $c \in Ш(A/K)[2]$, and showed that the order of $Ш(A/K)$ is a square if and only if $\langle c, \lambda(c)\rangle = 0$. In this case, the induced pairing on $Ш(A/K)$ is alternating, but otherwise the Cassels-Tate pairing is only antisymmetric. They also showed that $c = 0$ if and only if λ arises from a K-rational divisor. It was already known by Tate [Tat63] that the order of finite Ш is a square, if such a K-rational divisor exists.

In end of 1996, Stoll constructed the first example of an abelian variety having $\#Ш = 2\square$, see [Ste03] for some historical remarks. His example was the Jacobian of a genus 2 curve over $\mathbb{Q}$. Then, for every prime $p < 25000$, Stein [Ste04] constructed an abelian variety $A_p/\mathbb{Q}$ of dimension $p-1$, such that $\#Ш(A_p/\mathbb{Q}) = p\square$. Hence, Stein came up with the following

Conjecture 1.3. *As one ranges over all abelian varieties $A/\mathbb{Q}$, then every square-free natural number can appear as the non-square part of the order of $Ш(A/\mathbb{Q})$.*

So one might naturally ask the following

Question 1.4. *What are the possible non-square parts of the order of finite Tate-Šafarevič groups for abelian varieties of fixed dimension over a fixed number field? (Or over number fields of bounded degree.) Is this a finite list?*

So far, in case of abelian surfaces $B/\mathbb{Q}$, the only known primes which possibly divide the non-square parts of some $\#Ш(B/\mathbb{Q})$ are 2 and 3. The purpose of this paper is to extend this list by 5 and 7. We will explore an equation of Cassels and Tate, which is a consequence of the invariance under isogenies of the Birch and Swinnerton-Dyer conjecture. The left hand side of this equation is the order of the Tate-Šafarevič group in question up to squares. We will explain how to calculate the right hand side and then give explicit examples to prove the following

Theorem 1.5. *There exist abelian surfaces $B_1/\mathbb{Q}$ and $B_2/\mathbb{Q}$, such that $\#Ш(B_1/\mathbb{Q}) = 5\square$ and $\#Ш(B_1/\mathbb{Q}) = 7\square$.*

The outline of this paper is the following. In Chapter 2 we present the utilized equation of Cassels and Tate. This equation will break into two parts - a local and a global one. The remaining part of Chapter 2 is devoted to explain the local quotient. In Chapter 3 we present the familiy of abelian surfaces we consider and prove how to calculte the local and the global part of the Cassels-Tate equation. Finally, in Chapter 4 we will do explicit calculations for the primes 5 and 7 and give examples.

2. Preliminaries

Throughout let A/K be an abelian variety A over a number field K, i.e., a proper group scheme which is geometrically integral and of finite type over Spec K, where $K/\mathbb{Q}$ is a finite field extension. For any K-scheme T, the group of T-rational points is denoted by $A(T)$, where if $T = \text{Spec } L$, for L a field, we write $A(L)$. The dual abelian variety of A/K is denoted by $A^\vee := \text{Pic}^0_{A/K}$ and a polarization of A/K is a symmetric isogeny $\lambda : A \to A^\vee$, such that over $\overline{K}$ we have $\lambda = \lambda_{\mathcal{L}}$, for an ample line bundle $\mathcal{L}$ on $A/\overline{K}$.

With v we denote a place of K, i.e., an equivalence class of valuations of K, and with M_K the set of all places of K. We have the subset M_K^0 of all finite places (or primes) of K and the subset M_K^∞ of all infinite places of K. With K_v we denote the completion of K at v, and with k_v its residue field, i.e., the quotient of the valuation ring $\mathcal{O}_v$ of K_v by its maximal ideal $\mathfrak{m}_v = \pi_v \mathcal{O}_v$, for a uniformizer π_v. We normalize the absolute value $|\cdot|_v$ on K_v, such that $|\pi_v|_v = (\#k_v)^{-1}$. If $v \in M_K^0$ is a prime lying over $p \in M_{\mathbb{Q}}^0$, we denote this with $v|p$ and call K_v a p-adic field. Denote by K_v^{nr} the maximal unramified extension of K_v, thus K_v^{nr} is obtained by adjoining to K_v all n-th roots of unity, for n coprime to the characteristic p of k_v.

Since all fields considered will be perfect we do not pay attention to seperability and with $\overline{K}$ we denote a once and for all fixed algebraic closure of K. The absolute Galois group of a field K will be denoted by G_K. For Galois cohomology we use the usual abbreviation $H^i(K, M) := H^i(G_K, M)$, for a Galois module M. The Tate-Šafarevič group of A/K is defined as

$$Ш(A/K) := \ker\left(H^1(K, A(\overline{K})) \to \prod_{v \in M_K} H^1(K_v, A(\bar{K}_v)) \right).$$

With ℓ we denote a prime and by $\mathbb{Z}/\ell\mathbb{Z}$ we either mean a cyclic group of order ℓ or a Galois module of order ℓ with trivial Galois action. By $\boldsymbol{\mu}_\ell$ we denote the ℓ-th roots of unity as a Galois module of order ℓ, and we write $\xi = \xi_\ell$ for a primitive ℓ-th root of unity. The trivial group is denoted by 0. By $\square \in \{1, 4, 9, 16, \ldots\}$, we denote a square natural number.

2.1. **An equation of Cassels and Tate.** Cassels [Cas65] (the elliptic curve case) and Tate [Tat95] (the general case) proved the following theorem to show the invariance of the Birch and Swinerton-Dyer conjecture under isogenies, see also [Mil06, Theorem I.7.3]. Denote by R_A the regulator and by P_A the period of A. By $c_{A,v}$ we denote the local Tamagawa number of A at a finite place v.

Theorem 2.1. *Let $\varphi : A \to B$ be an isogeny between two abelian varieties A and B over a number field K. Assume that either $Ш(A/K)$ or $Ш(B/K)$ is finite, then $Ш(A/K)$ and $Ш(B/K)$ are both finite and*

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{R_B}{R_A} \cdot \frac{\#A(K)_{\mathrm{tors}} \#A^\vee(K)_{\mathrm{tors}}}{\#B(K)_{\mathrm{tors}} \#B^\vee(K)_{\mathrm{tors}}} \cdot \frac{P_B}{P_A} \cdot \prod_{v \in M_K^0} \frac{c_{B,v}}{c_{A,v}}.$$

The product over the Tamagawa numbers is actually finite, since $c_{A,v} = 1$, in case v is a place of good reduction of A. We define $A(K)_{\mathrm{free}}$ as the quotient group $A(K)/A(K)_{\mathrm{tors}}$. Consider the following induced group homomorphisms.

$$\varphi_K : A(K) \to B(K),\ \varphi_K^\vee : B^\vee(K) \to A^\vee(K),\ \varphi_v : A(K_v) \to B(K_v),$$
$$\varphi_{K,\mathrm{tors}} : A(K)_{\mathrm{tors}} \to B(K)_{\mathrm{tors}},\quad \varphi_{K,\mathrm{tors}}^\vee : B^\vee(K)_{\mathrm{tors}} \to A^\vee(K)_{\mathrm{tors}},$$
$$\varphi_{K,\mathrm{free}} : A(K)_{\mathrm{free}} \to B(K)_{\mathrm{free}},\quad \varphi_{K,\mathrm{free}}^\vee : B^\vee(K)_{\mathrm{free}} \to A^\vee(K)_{\mathrm{free}}.$$

Now we can reformulate the above quotients in terms of the isogeny φ, which is part of the proof of the above theorem. This reformulation turns out to be easier to handle for computational purposes and we are going to use the Cassels-Tate equation only in this description. There are two trivial equalities

$$\frac{\#A(K)_{\mathrm{tors}}}{\#B(K)_{\mathrm{tors}}} = \frac{\#\ker \varphi_K}{\#\mathrm{coker}\ \varphi_{K,\mathrm{tors}}},\quad \frac{\#A^\vee(K)_{\mathrm{tors}}}{\#B^\vee(K)_{\mathrm{tors}}} = \frac{\#\mathrm{coker}\ \varphi_{K,\mathrm{tors}}^\vee}{\#\ker \varphi_K^\vee},$$

and two more interesting ones

$$\frac{R_B}{R_A} = \frac{\#\text{coker } \varphi^\vee_{K,\text{free}}}{\#\text{coker } \varphi_{K,\text{free}}}, \quad \frac{P_B}{P_A} \cdot \prod_{v \in M_K^0} \frac{c_{B,v}}{c_{A,v}} = \prod_{v \in M_K} \frac{\#\text{coker } \varphi_v}{\#\ker \varphi_v}.$$

Hence we have

$$\frac{R_B}{R_A} \cdot \frac{\#A(K)_{\text{tors}} \#A^\vee(K)_{\text{tors}}}{\#B(K)_{\text{tors}} \#B^\vee(K)_{\text{tors}}} = \frac{\#\ker \varphi_K}{\#\text{coker } \varphi_K} \frac{\#\text{coker } \varphi^\vee_K}{\#\ker \varphi^\vee_K},$$

and we call the right-hand side of this equation the *global quotient*. The global quotient obviously breaks into the *regulator quotient* and the *torsion quotient*. The product $\prod_v \frac{\#\text{coker } \varphi_v}{\#\ker \varphi_v}$ runs over all places v of K and is called the *local quotient*. It is in fact a finite product, since $\#\text{coker } \varphi_v = \#\ker \varphi_v$, for all but finitely many places v, see Corollary 2.8. The rest of section 2 will only concern the local quotient.

2.2. **Isogenies on K_v-rational points.** We will use the following notation. Let $\varphi : A \to B$ be an isogeny of prime degree ℓ between two abelian varieties A and B over a number field K and let $v \in M_K^0$ be a finite place of K lying over a prime p. Consider the induced group homomorphism on K_v-rational points

$$\varphi_v : A(K_v) \to B(K_v).$$

Our aim is to compute the quotient $\frac{\#\text{coker } \varphi_v}{\#\ker \varphi_v}$, which mainly consists in determining the cardinality of coker φ_v. The cokernel of φ_v can naturally be identified with a subgroup of $H^1(K_v, A(\overline{K}_v)[\varphi])$, since the short exact sequence of Galois modules

$$0 \longrightarrow A(\overline{K}_v)[\varphi] \longrightarrow A(\overline{K}_v) \xrightarrow{\varphi} B(\overline{K}_v) \longrightarrow 0\ ,$$

gives the long exact Galois cohomology sequence

$$0 \longrightarrow \text{coker } \varphi_v \xrightarrow{\delta_v} H^1(K_v, A(\overline{K}_v)[\varphi]) \longrightarrow \cdots$$

Lemma 2.2. *Set $n := [K_v : \mathbb{Q}_p]$. With notation as above, if φ or $\varphi^\vee$ is obtained by dividing out a K_v-rational point, then*

$$H^1(K_v, A(\overline{K}_v)[\varphi]) \cong \begin{cases} \mathbb{Z}/\ell\mathbb{Z}, & v \nmid \ell, \boldsymbol{\mu}_\ell \nsubseteq K_v, \\ (\mathbb{Z}/\ell\mathbb{Z})^2, & v \nmid \ell, \boldsymbol{\mu}_\ell \subseteq K_v, \\ (\mathbb{Z}/\ell\mathbb{Z})^{n+1}, & v|\ell, \boldsymbol{\mu}_\ell \nsubseteq K_v, \\ (\mathbb{Z}/\ell\mathbb{Z})^{n+2}, & v|\ell, \boldsymbol{\mu}_\ell \subseteq K_v, \end{cases}$$

and if both φ and $\varphi^\vee$ are not obtained by dividing out a K_v-rational point, then

$$H^1(K_v, A(\overline{K}_v)[\varphi]) \cong \begin{cases} 0, & v \nmid \ell, \\ (\mathbb{Z}/\ell\mathbb{Z})^n, & v|\ell. \end{cases}$$

Proof. It is clear that $H^1(K_v, A(\overline{K}_v)[\varphi])$ is abelian and has exponent ℓ. Let M be a finite K_v-Galois module and denote by $M^\vee := \text{Hom}(M, \boldsymbol{\mu}_\ell)$ the dual of M. By [Ser02, II.5 Theorem 2, Proposition 17 and Theorem 5], we have

$$\#H^1(K_v, M) = \begin{cases} \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee), & v \nmid \ell, \\ \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee) \cdot \ell^n, & v \mid \ell. \end{cases}$$

If φ (resp. $\varphi^\vee$) is obtained by dividing out a K_v-rational point, then $A(\overline{K}_v)[\varphi] \cong \mathbb{Z}/l\mathbb{Z}$ (resp. $\boldsymbol{\mu}_\ell$) as Galois modules. Since

$$H^0(K_v, \mathbb{Z}/\ell\mathbb{Z}) \cong \mathbb{Z}/\ell\mathbb{Z}, \text{ and } H^0(K_v, \boldsymbol{\mu}_\ell) \cong \begin{cases} 0, & \boldsymbol{\mu}_\ell \nsubseteq K_v, \\ \mathbb{Z}/\ell\mathbb{Z}, & \boldsymbol{\mu}_\ell \subseteq K_v, \end{cases}$$

and $\mathbb{Z}/\ell\mathbb{Z}$ and $\boldsymbol{\mu}_\ell$ are dual to each other, we get the first statement.

If both φ and $\varphi^\vee$ are not obtained by dividing out a K_v-rational point, then $A(\overline{K}_v)[\varphi])$ and its dual are both $\ncong \mathbb{Z}/\ell\mathbb{Z}$. Therefore

$$H^0(K_v, A(\overline{K}_v)[\varphi]) = H^0(K_v, A(\overline{K}_v)[\varphi]^\vee) = 0,$$

which completes the proof. □

Corollary 2.3.

$$H^1(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z}) \cong H^1(\mathbb{Q}_p, \boldsymbol{\mu}_\ell) \cong \begin{cases} \mathbb{Z}/\ell\mathbb{Z}, & p \neq \ell, p \not\equiv 1 \bmod \ell, \ell \neq 2, \\ (\mathbb{Z}/\ell\mathbb{Z})^2, & (p = \ell \text{ or } p \equiv 1 \bmod \ell), \ell \neq 2, \\ (\mathbb{Z}/\ell\mathbb{Z})^3, & p = \ell = 2, \end{cases}$$

Proof. This follows immediately from the facts, that $\boldsymbol{\mu}_2 \subseteq \mathbb{Q}_p$, for all p, and $\boldsymbol{\mu}_\ell \nsubseteq \mathbb{Q}_p$ if and only if $p \not\equiv 1 \bmod \ell$ and $\ell \neq 2$. □

Now we introduce unramified Galois cohomology, which is an important subgroup. Let M be a G_{K_v}-module and K_v^{nr} be the maximal unramified extension of K_v. We have that $G_{K_v^{\mathrm{nr}}}$ is a (normal) subgroup of G_{K_v}, thus the usual restriction homomorphism

$$\mathrm{Res}_{\mathrm{nr}} : H^1(K_v, M) \to H^1(K_v^{\mathrm{nr}}, M)$$

is definied and we denote its kernel by $H^1_{\mathrm{nr}}(K_v, M)$.

Lemma 2.4. *If φ is obtained by dividing out a K_v-rational point, then*

$$H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi]) \cong \mathbb{Z}/\ell\mathbb{Z}.$$

If φ is not obtained by dividing out a K_v-rational point, then

$$H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi]) = 0.$$

Proof. The order of $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$ equals the order of $H^0(K_v, A(\overline{K}_v)[\varphi])$, see [SS01, Lemma 4.2]. See also [Ser02, II Proposition 18(b)]. □

By $\tilde{\mathcal{A}}$ we denote the reduction of A modulo v, i.e., the special fiber at v of the Néron model $\mathcal{A}/\mathcal{O}_K$ of A, and by $\tilde{\mathcal{A}}_0(k_v)$ we denote the smooth part of the k_v-rational points of the reduction at v, i.e., the k_v-rational points of the connected component of $\tilde{\mathcal{A}}$ intersecting the zero-section. Denote by $A_0(K_v)$ the preimage of $\tilde{\mathcal{A}}_0(k_v)$ under the reduction-mod-v map, and by $A_1(K_v)$ the kernel of $A_0(K_v) \to \tilde{\mathcal{A}}_0(k_v)$. We have the following two commutative diagrams with exact rows and induced group homomorphisms as vertical arrows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1(K_v) & \longrightarrow & A_0(K_v) & \longrightarrow & \tilde{\mathcal{A}}_0(k_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_v^1} & & \downarrow{\scriptstyle \varphi_v^0} & & \downarrow{\scriptstyle \tilde{\varphi}_v^0} & & \\ 0 & \longrightarrow & B_1(K_v) & \longrightarrow & B_0(K_v) & \longrightarrow & \tilde{\mathcal{B}}_0(k_v) & \longrightarrow & 0 \end{array} \tag{1}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_0(K_v) & \longrightarrow & A(K_v) & \longrightarrow & A(K_v)/A_0(K_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_v^0} & & \downarrow{\scriptstyle \varphi_v} & & \downarrow{\scriptstyle \bar{\varphi}_v} & & \\ 0 & \longrightarrow & B_0(K_v) & \longrightarrow & B(K_v) & \longrightarrow & B(K_v)/B_0(K_v) & \longrightarrow & 0 \end{array} \tag{2}$$

Note that all kernels and cokernels of the vertical maps in the above two commutative diagrams are finite groups and their cardinalities are powers of ℓ. The quantity $c_{A,v} := A(K_v)/A_0(K_v)$ is the local Tamagawa number of A at v and the quotient $c_{B,v}/c_{A,v}$ is also a power of ℓ.

In the unramified case we get the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1(K_v^{\mathrm{nr}}) & \longrightarrow & A_0(K_v^{\mathrm{nr}}) & \longrightarrow & \tilde{\mathcal{A}}_0(\overline{k}_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_{v,\mathrm{nr}}^1} & & \downarrow{\scriptstyle \varphi_{v,\mathrm{nr}}^0} & & \downarrow{\scriptstyle \tilde{\varphi}_{\overline{k}_v}^0} & & \\ 0 & \longrightarrow & B_1(K_v^{\mathrm{nr}}) & \longrightarrow & B_0(K_v^{\mathrm{nr}}) & \longrightarrow & \tilde{\mathcal{B}}_0(\overline{k}_v) & \longrightarrow & 0 \end{array} \tag{3}$$

Now we apply the snake lemma on diagrams 1 and 2 to get a basic lemma, which we will use often.

Lemma 2.5. *With notation as above,*

$$\frac{\#\mathrm{coker}\ \varphi_v}{\#\ker \varphi_v} = \frac{\#\mathrm{coker}\ \varphi_v^1}{\#\ker \varphi_v^1} \cdot \frac{c_{B,v}}{c_{A,v}}.$$

Proof. Applying the snake lemma on the kernels and cokernels in the first diagram we get

$$\frac{\#\ker \varphi_v^1}{\#\mathrm{coker}\ \varphi_v^1} \cdot \frac{\#\ker \tilde{\varphi}_v^0}{\#\mathrm{coker}\ \tilde{\varphi}_v^0} = \frac{\#\ker \varphi_v^0}{\#\mathrm{coker}\ \varphi_v^0}.$$

Since $\tilde{\mathcal{A}}_0(k_v)$ and $\tilde{B}_0(k_v)$ are finite groups with same cardinality, we get $\#\ker \tilde{\varphi}_v^0 = \#\mathrm{coker}\ \tilde{\varphi}_v^0$, therefore

$$\frac{\#\ker \varphi_v^1}{\#\mathrm{coker}\ \varphi_v^1} = \frac{\#\ker \varphi_v^0}{\#\mathrm{coker}\ \varphi_v^0}.$$

Applying the snake lemma on the second diagram gives

$$\frac{\#\mathrm{coker}\ \varphi_v}{\#\ker \varphi_v} = \frac{\#\mathrm{coker}\ \varphi_v^0}{\#\ker \varphi_v^0} \cdot \frac{\#\mathrm{coker}\ \bar{\varphi}_v}{\#\ker \bar{\varphi}_v}.$$

By definition we have

$$\frac{\#\mathrm{coker}\ \bar{\varphi}_v}{\#\ker \bar{\varphi}_v} = \frac{c_{B,v}}{c_{A,v}},$$

which completes the proof. □

We continue with examining the quotient $\#\mathrm{coker}\ \varphi_v^1/\#\ker \varphi_v^1$. As we will see, this is mostly 1, since φ_v^1 will be an isomorphism for all but finitely many places v. We start by recalling two basic lemmas.

Lemma 2.6. *The kernel of reduction $A_1(K_v)$ is a pro-p group.*

Proof. We have that $A_1(K_v)$ is isomorphic to the group $\hat{A}(\mathfrak{m}_v)$ associated to the formal group $\hat{A}$ of A defined over the valuation ring $\mathcal{O}_v$ of K_v with maximal ideal $\mathfrak{m}_v$. If m is coprime to the characteristic p of the residue field, then the multiplication-by-m-endomorphism on $\hat{A}(\mathfrak{m}_v)$ is an isomorphism. It is an easy excercise to check

that any profinite group, such that for all primes $\ell \neq p$ the multiplication-by-ℓ-map is an isomorphism, is a pro-p group. Hence $A_1(K_v)$ is, and we are done. □

Lemma 2.7. *With notation as above, if $v \nmid \ell$, then φ_v^1 and $\varphi_{v,\mathrm{nr}}^1$ are isomorphisms.*

Proof. There are isogenies $\alpha : B \to A$ and $\beta : A \to B$, such that $\alpha \circ \varphi : A \to A$ and $\beta \circ \alpha : B \to B$ are the multiplication-by-ℓ-maps. Hence we get the following induced group homomorphisms on the level of kernels of reduction.

$$A_1(K_v) \xrightarrow{\varphi_v^1} B_1(K_v) \xrightarrow{\alpha_v^1} A_1(K_v) \xrightarrow{\beta_v^1} B_1(K_v)$$

with $[\ell]_v^1 : A_1(K_v) \to A_1(K_v)$ and $[\ell]_v^1 : B_1(K_v) \to B_1(K_v)$.

As $v \nmid \ell$, by the previous lemma, we have that both maps $[\ell]_v^1$ are isomorphisms. Hence it follows that all three homomorphisms α_v^1, β_v^1 and φ_v^1 are isomorphisms. Now for any finite (unramified) extension L_w/K_v, by the same argument, we get φ_w^1 is an isomorphism, thus $\varphi_{v,\mathrm{nr}}^1$ also is. □

We conclude that the local quotient actually is a finite product. Let S be a finite set of places of K containing the infinite primes, the bad primes of A and the primes dividing the degree of the isogeny φ.

Corollary 2.8. *With notation as above, if $v \nmid \ell$ and v is a place of good reduction, then*

$$\frac{\#\mathrm{coker}\ \varphi_v}{\#\ker \varphi_v} = 1,$$

thus

$$\prod_{v \in M_K} \frac{\#\mathrm{coker}\ \varphi_v}{\#\ker \varphi_v} = \prod_{v \in S} \frac{\#\mathrm{coker}\ \varphi_v}{\#\ker \varphi_v}.$$

Proof. Combine Lemmas 2.5 and 2.7 with the fact, that the Tamagawa quotient equals 1 in case of good reduction. □

Now we present a slightly stronger generalization of [SS01, Lemmas 4.3 and 4.5]. Proposition 2.10 will be an important ingredient to calculate the local quotient (see Theorem 3.6).

Lemma 2.9. *With notation as above, if $\varphi_{v,\mathrm{nr}}^1$ is surjective, then* coker φ_v^0 *can be naturally maped onto a subgroup of $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$.*

Proof. In the above diagram 3, the first vertical map $\varphi_{v,\mathrm{nr}}^1$ is surjective by assumption. The third vertical map $\tilde{\varphi}^0_{\overline{k}_v}$ is surjective, since $\overline{k}_v$ is algebraically closed, therefore the middle vertical map $\varphi^0_{v,\mathrm{nr}}$ is also surjective, i.e., $B_0(K_v^{\mathrm{nr}})/\varphi^0_{v,\mathrm{nr}}(A_0(K_v^{\mathrm{nr}}))$ is trivial. The following diagram commutes.

$$\begin{array}{ccc} B_0(K_v)/\varphi_v^0(A_0(K_v)) & \xrightarrow[\delta_v]{} & H^1(K_v, A(\overline{K}_v)[\varphi]) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Res}_{\mathrm{nr}}} \\ B_0(K_v^{\mathrm{nr}})/\varphi^0_{v,\mathrm{nr}}(A_0(K_v^{\mathrm{nr}})) & \xrightarrow[\delta_{v,\mathrm{nr}}]{} & H^1(K_v^{\mathrm{nr}}, A(\overline{K}_v)[\varphi]) \end{array}$$

Since the lower left group is trivial, the image of the upper left group in the lower right group must be trivial, i.e., the image of δ_v lies in $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$. □

Note, that since the natural map coker $\varphi_v^0 \to$ coker φ_v need not to be injective, also the natural map coker $\varphi_v^0 \to H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$ may not be injective.

Proposition 2.10. *With notation as above, consider the following long exact sequence obtained by Galois cohomology*

$$0 \longrightarrow \text{coker } \varphi_v \xrightarrow{\delta_v} H^1(K_v, A(\overline{K}_v)[\varphi]) \longrightarrow \cdots$$

If $\varphi^1_{v,\mathrm{nr}}$ is surjective and φ^1_v and $\bar{\varphi}_v$ are isomorphisms, then δ_v indentifies coker φ_v *with $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$.*

Proof. If $\bar{\varphi}_v$ is an isomorphism, then the natural map coker $\varphi_v^0 \to$ coker φ_v is also an isomorphism, thus by the previous lemma we have that coker φ_v maps injectively onto a subgroup of $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$. But these two groups have same cardinality, since $\#H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi]) = \#\ker\varphi_v = \#\text{coker } \varphi_v$, by Lemmas 2.4 and 2.5. □

In [SS01, Lemmas 4.3 and 4.5] our assumptions on φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ were replaced by $v \nmid \ell$. We have seen in Lemma 2.7 that $v \nmid \ell$ is a stronger assumption. The tricky part in the calculation of the local quotient will be to decide whether we can apply Proposition 2.10 even in the case $v \mid \ell$. For this purpose, we end this section with a reinterpretation of the quotient $\#\text{coker } \varphi^1_v / \#\ker\varphi^1_v$, which is taken from [Sch96]. In case $K = \mathbb{Q}$, this will give a criterion to decide whether φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ are isomorphism.

First we need some notation. Assume that the abelian varieties A and B are of dimension d and let $v \in M_K^0$ be a finite place. We can write the isogeny $\varphi : A \to B$ as a d-tuple of power series in d-variables in a neighbourhood of the point $\mathcal{O}$. Let $|\varphi'(0)|_v$ be the normalized v-adic absolute value of the determinant of the Jacobian matrix of partials of such a power series representation of φ evaluated at 0. Note that $|\varphi'(0)|_v$ is well definied.

Proposition 2.11. *With notation as above,*

$$|\varphi'(0)|_v^{-1} = \frac{\#\text{coker } \varphi^1_v}{\#\ker\varphi^1_v},$$

hence

$$|\varphi'(0)|_v = 1, \ \textit{if } v \nmid \ell.$$

Proof. Combine [Sch96, Lem. 3.8] with Lemmas 2.5 and 2.7. □

As a corollary we get a nice condition whether φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ are isomorphisms, even in case $v \mid \ell$.

Corollary 2.12. *With notation as above, the following holds.*

(i) If $|\varphi'(0)|_v = 1$ and $\varphi^1_{v,\mathrm{nr}}$ is injective, then φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ are isomorphisms.

(ii) If $K = \mathbb{Q}$ and $\ell \neq 2$, then φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ are injective, and we have that φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ are isomorphisms if and only if $|\varphi'(0)|_v = 1$ holds.

Proof. Assume $|\varphi'(0)|_v = 1$, then we also have that $|\varphi'(0)|_w = 1$, for all unramified finite field extensions L_w/K_v. Since all maps $\varphi^1_{w,\mathrm{nr}}$ are injective as $\varphi^1_{v,\mathrm{nr}}$ is, they are therefore isomorphisms. Hence $\varphi^1_{v,\mathrm{nr}}$ also is, which proves (i).

For (ii), use the isomorphism $A_1(K_v) \cong \hat{A}(\mathfrak{m}_v)$. Then use [Sil86, IV. Example 6.1.1] to conclude that φ^1_w is injective for any finite unramified field extension L_w/K_v. Hence $\varphi^1_{v,\mathrm{nr}}$ also is. Now apply (i). □

Remark 2.13. In case of elliptic curves, $\varphi'(0)$ is just the leading coefficent of the power series representation of φ. We can easily compute this value: Use Vélu's algorithm [Vél71] to discribe φ as coordinate functions $\varphi(x,y) = (\tilde{x}(x,y), \tilde{y}(x,y))$ and then write $-\tilde{x}/\tilde{y}$ as a power series in $z := -x/y$, see [Sil86, IV]. We will do this explicitly in Propositions 4.2 and 4.10.

In the next section we will calculate the quotient $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$ for the special case of A being an elliptic curve E. We will do this by exploring how the reduction type of E at v determines the Tamagawa quotient and the value $|\varphi'(0)|_v$.

2.3. **Bad reduction of elliptic curves.** In this section let E be an elliptic curve over a p-adic field K_v and let $\eta : E \to E'$ be an isogeny of prime degree ℓ. Consider the following two commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K_v) & \longrightarrow & E_0(K_v) & \longrightarrow & \tilde{\mathcal{E}}_0(k_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \eta_v^1} & & \downarrow{\scriptstyle \eta_v^0} & & \downarrow{\scriptstyle \tilde{\eta}_v^0} & & \\ 0 & \longrightarrow & E_1'(K_v) & \longrightarrow & E_0'(K_v) & \longrightarrow & \tilde{\mathcal{E}}_0'(k_v) & \longrightarrow & 0 \end{array} \tag{4}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_0(K_v) & \longrightarrow & E(K_v) & \longrightarrow & E(K_v)/E_0(K_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \eta_v^0} & & \downarrow{\scriptstyle \eta_v} & & \downarrow{\scriptstyle \bar{\eta}_v} & & \\ 0 & \longrightarrow & E_0'(K_v) & \longrightarrow & E'(K_v) & \longrightarrow & E'(K_v)/E_0'(K_v) & \longrightarrow & 0 \end{array} \tag{5}$$

To determine $\frac{\#\operatorname{coker}\eta_v}{\#\ker\eta_v}$, by Lemma 2.5, we have to calculate $\frac{\#\operatorname{coker}\eta_v^1}{\#\ker\eta_v^1}\cdot\frac{c_{E',v}}{c_{E,v}}$. We will descibe this value depending on the reduction type of E. In case of split multiplicative reduction we also have to consider whether $\ker\eta_v \subseteq E_0(K_v)$. We start with calculating the quotient of the Tamagawa numbers, which is easy if we restrict to $\ell \geq 5$.

Lemma 2.14. *Suppose that E has*

1. *good reduction, or*
2. *non-split multiplicative reduction and $\ell \neq 2$, or*
3. *additive reduction and $\ell \geq 5$,*

then the group homomorphism $\bar{\eta}_v$ is an isomorphism, hence $c_{E',v}/c_{E,v} = 1$.

Proof. In case of good reduction this is clear, since $c_{E,v} = c_{E',v} = 1$. From Tate's algorithm [Tat75] it follows that in the remaining cases $c_{E,v}$ and $c_{E',v}$ are at most 4 in the additive case, and at most 2 in the non-split case. Since the cardinalities of the kernel and cokernel of $\bar{\eta}_v$ are powers of ℓ, it follows that $\bar{\eta}_v$ is an isomorphism and hence $c_{E',v}/c_{E,v} = 1$. □

To calculate the Tamagawa quotient in the split multiplicative reduction case we use the theory of Tate curves.

Theorem 2.15. (Tate) *Assume that E/K_v has split multiplicative reduction. Then there is a unique $\alpha \in K_v^*$, s.t. $v(\alpha) > 0$, and we have the following Galois-equivariant p-adic analytic isomorphism*

$$E(L) \cong L^*/\alpha^{\mathbb{Z}},$$

for all algebraic field extension L/K_v. Moreover, $c_{E,v} = v(\alpha)$.

Proof. See [Sil94, V Thm. 5.3]. The last statement follows from the proof of the surjectivity of the Tate map [Sil94, V.4]. □

If E/K_v is an elliptic curve having split multiplicative reduction we have $E(\overline{K}_v) \cong \overline{K}_v^*/\alpha^{\mathbb{Z}}$, for $\alpha \in K_v^*$ and $v(\alpha) > 0$. We want to classify which Galois invariant subgroups of prime order ℓ exist and whether they are contained in the connected component of the identity $E_0(\overline{K}_v)$. Since they are all subgroups of $E(\overline{K}_v)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, there are at most $\ell + 1$ of such groups. The ℓ-th roots of unity ξ_ℓ^i in $\overline{K}_v^*$ always generate a Galois invariant subgroup of $\overline{K}_v^*/\alpha^{\mathbb{Z}}$, which is contained in the connected component of the identity, and a generator is definied over K_v if and only if $\boldsymbol{\mu}_\ell \subseteq K_v$. The remaining ℓ subgroups are definied over $K_v(\sqrt[\ell]{\alpha}, \boldsymbol{\mu}_\ell)$. None of these ℓ groups are contained in the connected component of the identity. They are generated by $\xi_\ell^i \sqrt[\ell]{\alpha}$, for $i = 0, \dots, \ell - 1$, hence all of these groups are galois invariant if and only if $\sqrt[\ell]{\alpha} \subseteq K_v$, i.e. $\ell \mid v(\alpha)$. In this case, the generator of at least one of these groups is definied over K_v. The generators for the other $\ell - 1$ groups are definied over K_v if and only if $\ell \mid v(\alpha)$ and $\boldsymbol{\mu}_\ell \subseteq K_v$.

Proposition 2.16. *With notation as above, if E/K_v has split multiplicative reduction, then*

$$\frac{c_{E'}}{c_E} = \begin{cases} 1/\ell, & \ker \eta_v \nsubseteq E_0(\overline{K}_v), \\ \ell, & \ker \eta_v \subseteq E_0(\overline{K}_v). \end{cases}$$

Further, in case that η is obtained by dividing out a K_v-rational point and $\ker \eta_v \nsubseteq E_0(\overline{K}_v)$, we also have that η_v^1 is an isomorphism and that $\eta_{v,\mathrm{nr}}^1$ is surjective.

Proof. By theorem 2.15 we have $E(\overline{K}_v) \cong \overline{K}_v^*/\alpha_1^{\mathbb{Z}}$ and $E'(\overline{K}_v) \cong \overline{K}_v^*/\alpha_2^{\mathbb{Z}}$. If $\ker \eta_v \nsubseteq E_0(\overline{K}_v)$ then $\ker \eta_v = \langle [\xi_\ell^i \sqrt[\ell]{\alpha_1}] \rangle$, for an $i \in \{0, \dots, \ell - 1\}$, and $\eta_v : \overline{K}_v^*/\alpha_1^{\mathbb{Z}} \to \overline{K}_v^*/\alpha_2^{\mathbb{Z}}$ is given by $[x] \mapsto [x]$ and $\alpha_2 = \xi_\ell^i \sqrt[\ell]{\alpha_1}$. Therefore

$$\frac{c_{E'}}{c_E} = \frac{v(\alpha_2)}{v(\alpha_1)} = \frac{v(\xi_\ell^i \sqrt[\ell]{\alpha_1})}{v(\alpha_1)} = 1/\ell.$$

If $\ker \eta_v \subseteq E_0(\overline{K}_v)$ then $\ker \eta_v = \langle [\xi_\ell] \rangle$ and $\eta_v : \overline{K}_v^*/\alpha_1^{\mathbb{Z}} \to \overline{K}_v^*/\alpha_2^{\mathbb{Z}}$ is given by $[x] \mapsto [x^\ell]$ and $\alpha_2 = \alpha_1^\ell$. Therefore

$$\frac{c_{E'}}{c_E} = \frac{v(\alpha_2)}{v(\alpha_1)} = \frac{v(\alpha_1^\ell)}{v(\alpha_1)} = \ell.$$

For the last statement note, that η_v is surjective, since the map on representatives is given by the identity. The maps η_v^0 and η_v^1 are injective, because $\ker \eta_v \nsubseteq E_0(\overline{K}_v)$. Applying the snake lemma on Diagram 5 gives the surjectivity of η_v^0 and then by Diagram 4 and the snake lemma we get the surjectivity of η_v^1, thus η_v^1 is an isomorphism. We can use the same strategy to show that η_w^1 is surjective, for every finite (unramified) field extension L_w/K_v, hence $\eta_{v,\mathrm{nr}}^1$ is surjective. □

In case that η is obtained by dividing out a K_v-rational point, we only have to distinguish between $\ker \eta_v \nsubseteq E_0(K_v)$ and $\ker \eta_v \subseteq E_0(K_v)$. If we additionally assume that η_v^1 is injective, then we get a strong connection between the reduction type and the arithmetic of K_v.

Proposition 2.17. *With notation as above, if η is obtained by dividing out a K_v-rational point, we have:*

(i) If $\ker \eta_v \nsubseteq E_0(K_v)$, then exactely one of the following three cases holds

(1) *E has split multiplicative reduction,*
(2) *E has non-split multiplicative reduction and $l = 2$,*
(3) *E has additive reduction and $l = 2$ or 3.*

(ii) If $\ker \eta_v \subseteq E_0(K_v)$, assume additionally that η_v^1 is injective. If E/K_v has bad reduction and $\ell \neq 2$, then

(1) *E has split multiplicative reduction $\Leftrightarrow \ \boldsymbol{\mu}_\ell \subseteq K_v, v \nmid \ell$,*
(2) *E has non-split multiplicative reduction $\Leftrightarrow \ \boldsymbol{\mu}_\ell \nsubseteq K_v, v \nmid \ell$,*
(3) *E has additive reduction $\Leftrightarrow \ v|\ell$.*

(iii) If η_v^1 is injective and the reduction type of E/K_v is multiplicative, then η_v^1 is an isomorphism and $\eta_{v,\mathrm{nr}}^1$ is surjective.

Proof. Let P be a generator of $\ker \eta_v$. If $\ker \eta_v \nsubseteq E_0(K_v)$ then $\bar{P}$ is a singular point, the reduction type is bad and $\ker \eta_v$ injects into $\ker \bar{\eta}_v$. This gives $\ell | c_E$. Since c_E is ≤ 2 in the non-split multiplicative case and ≤ 4 in the additive case, we get (i).

If $\ker \eta_v \subseteq E_0(K_v)$ then P generates $\ker \eta_v^0$. Since we assumed η_v^1 to be injective, the order of $\bar{P}$ is ℓ. Set $|k_v| =: p^f$. The order of $\bar{P}$ divides the cardinality of $\tilde{\mathcal{E}}_0(k_v)$, which is either $p^f - 1, p^f + 1$ or p^f, depending on whether the reduction type is split multiplicative, non-split multiplicative or additive, respectively [Tat75, §7]. Therefore we get the following implications.

(1) split $\Rightarrow \ p^f \equiv 1(\ell) \ \Rightarrow \ p \neq \ell, \ \Rightarrow \ v \nmid \ell$,
(2) non-split $\Rightarrow \ p^f \equiv -1(\ell) \ \Rightarrow \ p \neq \ell, \ \Rightarrow \ v \nmid \ell$,
(3) additive $\Rightarrow \ p^f \equiv 0(l) \ \Rightarrow \ p = \ell, \ \Rightarrow \ v \mid \ell$.

Hence, if $\ker \eta_v \subseteq E_0(K_v)$, we have $v \nmid \ell$ in the multiplicative case. Thus we can use Lemma 2.7 and Proposition 2.16 to get (iii). If $\ell \neq 2$ and we omit the case of good reduction, the above implications yield

(1) split $\Leftrightarrow \ p^f \equiv 1(\ell) \Leftrightarrow \ \boldsymbol{\mu}_\ell \subseteq k_v, p \neq \ell \Leftrightarrow \ \boldsymbol{\mu}_\ell \subseteq K_v, v \nmid \ell$,
(2) non-split $\Leftrightarrow \ p^f \not\equiv 0, 1(\ell) \Leftrightarrow \ \boldsymbol{\mu}_\ell \nsubseteq k_v, p \neq \ell \Leftrightarrow \ \boldsymbol{\mu}_\ell \nsubseteq K_v, v \nmid \ell$,
(3) additive $\Leftrightarrow \ p^f \equiv 0(\ell) \Leftrightarrow \ p = \ell \Leftrightarrow \ v|\ell$,

which proves (ii). □

In the special case $K_v = \mathbb{Q}_p$ and $\ell \geq 5$ we summarize and get two corollaries.

Corollary 2.18. *Let E be an elliptic curve over $\mathbb{Q}_p$ and let $\eta : E \to E'$ be an isogeny of prime degree $\ell \geq 5$ and assume that η is obtained by dividing out a $\mathbb{Q}_p$-rational point. Then*

$$\begin{cases} E \text{ has split reduction and } \ker \eta_p \subseteq E_0(\mathbb{Q}_p) & \Rightarrow \ p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p, \\ E \text{ has non-split reduction} & \Rightarrow \ p \neq \ell, \boldsymbol{\mu}_\ell \nsubseteq \mathbb{Q}_p, \\ E \text{ has additive reduction} & \Rightarrow \ p = \ell. \end{cases}$$

Therefore, with respect to the reduction type of $E/\mathbb{Q}_p$, we get

$$\frac{\#\mathrm{coker}\ \eta_p}{\#\ker \eta_p} = \begin{cases} 1/\ell, & \text{split multiplicative reduction}, \ker \eta_p \nsubseteq E_0(\mathbb{Q}_p), \\ \ell, & \text{split multiplicative reduction}, \ker \eta_p \subseteq E_0(\mathbb{Q}_p), \\ 1, & \text{non-split multiplicative reduction}, \\ 1, & \text{good reduction}, p \neq \ell, \\ |\eta'(0)|_p^{-1}, & \text{good reduction}, p = \ell, \\ |\eta'(0)|_p^{-1}, & \text{additive reduction}. \end{cases}$$

Proof. By Corollary 2.12 we have that η_p^1 is injective, hence the first implications follow with Proposition 2.17. For the second part use Lemma 2.5, i.e., $\frac{\#\text{coker } \eta_p}{\#\ker \eta_p} = \frac{\#\text{coker } \eta_p^1}{\#\ker \eta_p^1} \cdot \frac{c_{E',p}}{c_{E,p}}$. The Tamagawa quotient is calculated in Lemma 2.14 and Proposition 2.16. By Proposition 2.11 we have $\#\text{coker } \eta_p^1/\#\ker \eta_p^1 = |\eta'(0)|_p^{-1}$. If $p \neq \ell$ or in the multiplicative case, we know $|\eta'(0)|_p^{-1} = 1$ by Propositions 2.11 and 2.17, which completes the proof. □

Corollary 2.19. *Let E be an elliptic curve over $\mathbb{Q}_p$ and let $\eta : E \to E'$ be an isogeny of prime degree $\ell \geq 5$ and assume that η is obtained by dividing out a $\mathbb{Q}_p$-rational point. Consider the following long exact sequence of Galois cohomology.*

$$0 \longrightarrow \text{coker } \eta_p \xrightarrow{\delta_p} H^1(\mathbb{Q}_p, E(\bar{\mathbb{Q}}_p)[\eta]) \xrightarrow{\iota_p^1(E)} H^1(\mathbb{Q}_p, E(\bar{\mathbb{Q}}_p)) \longrightarrow \cdots$$

Then, with respect to the reduction type of $E/\mathbb{Q}_p$, we have

$$\iota_p^1(E) \text{ is } \begin{cases} \text{injective}, & \text{split multiplicative and } \ker \eta_p \nsubseteq E_0, \\ \equiv 0, & \text{split multiplicative and } \ker \eta_p \subseteq E_0, \\ \equiv 0, & \text{non-split multiplicative}, \\ \text{not injective and } \not\equiv 0, & \text{good}, p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p, \\ \equiv 0, & \text{good}, p \neq \ell, \boldsymbol{\mu}_\ell \nsubseteq \mathbb{Q}_p, \\ \text{not injective and } \not\equiv 0, & \text{good}, p = \ell, |\eta'(0)|_p = 1, \\ \equiv 0, & \text{good}, p = \ell, |\eta'(0)|_p \neq 1, \\ \text{not injective and } \not\equiv 0, & \text{additive}, |\eta'(0)|_p = 1, \\ \equiv 0, & \text{additive}, |\eta'(0)|_p \neq 1. \end{cases}$$

Proof. Combine Lemma 2.2 with Corollary 2.18. □

3. Controlling $\#Ш(B/\mathbb{Q})$ modulo squares

We want to find examples of abelian surfaces B, such that the order of their Tate-Šafarevič groups is not a square. We start with a principally polarized abelian surface $A = E_1 \times E_2$, which is the product of two elliptic curves $E_i/\mathbb{Q}$. The order of $Ш(A/\mathbb{Q})$ is a square, provided it is finite, since $Ш(A/\mathbb{Q}) \cong Ш(E_1/\mathbb{Q}) \times Ш(E_2/\mathbb{Q})$. Then we construct an isogeny $\varphi : A \to B$ of prime degree ℓ in such a way, that the resulting abelian surface B fulfills the conditions in Theorem 1.1, i.e., the degree of every polarization of B is divisible by ℓ. This gives us the possibility that ℓ might divide the non-square part of the order of $Ш(B/\mathbb{Q})$. Then one uses the Cassels-Tate equation

$$\frac{\#Ш(A/\mathbb{Q})}{\#Ш(B/\mathbb{Q})} = \frac{\#\ker \varphi_{\mathbb{Q}}}{\#\text{coker } \varphi_{\mathbb{Q}}} \frac{\#\text{coker } \varphi_{\mathbb{Q}}^\vee}{\#\ker \varphi_{\mathbb{Q}}^\vee} \prod_{p \in M_{\mathbb{Q}}} \frac{\#\text{coker } \varphi_p}{\#\ker \varphi_p}$$

and determines the global and local quotient on the right hand side, which gives the order of $Ш(B/\mathbb{Q})$ up to squares. This is done in the rest of this section. We begin with the construction of an abelian surface having the property that the degree of every polarization it possesses is divisible by a given prime ℓ. For the proof we follow a sketch of Brian Conrad.

Proposition 3.1. *Let K be a any field and let E_1 and E_2 be two non-isogenous elliptic curves over K. Let G be a finite group scheme of prime order ℓ over K*

and assume G occurs inside both E_1 and E_2. Fix embeddings $G \hookrightarrow E_1, E_2$. These embeddings induce a natural embedding of G into the product $A := E_1 \times_K E_2$. Denote its image by $\tilde{G}$. Then any polarization of the quotient $B := A/\tilde{G}$ has degree divisible by ℓ.

Proof. Let $\lambda : B \to B^\vee$ be any polarization and consider the quotient map $\varphi : A \to B = A/\tilde{G}$ and its dual $\varphi^\vee : B^\vee \to A^\vee = A$. The composition

$$\Psi : A \xrightarrow{\varphi} B \xrightarrow{\lambda} B^\vee \xrightarrow{\varphi^\vee} A^\vee = A$$

is a polarization of A. Since E_1 and E_2 are not isogenous, Ψ breaks into

$$\Psi = \Psi_1 \times \Psi_2 : E_1 \times_K E_2 \to E_1 \times_K E_2,$$

where Ψ_i is a polarization of E_i. If we denote by $\iota_i : E_i \hookrightarrow A \xrightarrow{\varphi} B$ the natural embedding of E_i as a closed subvariety of B, then it is clear that

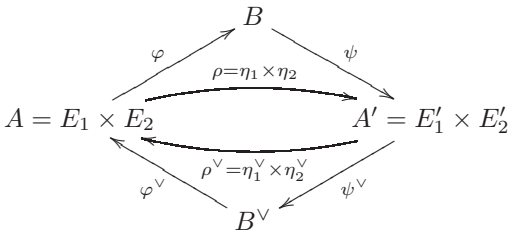
$$\Psi_i : E_i \xrightarrow{\iota_i} B \xrightarrow{\lambda} B^\vee \xrightarrow{\iota_i^\vee} E_i^\vee = E_i.$$

By construction $\tilde{G}$ lies in the kernel of Ψ and we have that G has to be in either both kernels of the Ψ_i or in none, because $\tilde{G}$ lies diagonally in $G \times G$.

Now assume to the contrary that $\ell \nmid \deg \lambda$. As $\deg \varphi = \deg \varphi^\vee = \ell$ we have $\deg \Psi_1 \cdot \deg \Psi_2 = \deg \Psi = \deg \varphi \cdot \deg \lambda \cdot \deg \varphi^\vee = \ell^2 \cdot \square$, with $\ell \nmid \square$. Hence it follows that one of the degrees of the Ψ_i is divisible by ℓ and the other is not, because the degree of a polarization is always a square. As the degree of (let's say) Ψ_2 is not divisible by ℓ, its kernel is a finite group of order not divisible by ℓ, hence it cannot contain G. Now recall that every elliptic curve has a unique polarization of each square degree ℓ^2 whose kernel is the full ℓ-torsion. Since the degree of Ψ_1 is divisible by ℓ and hence by ℓ^2, we have that $(\ker \Psi_1)[\ell] = E[\ell]$. Therefore $G \subseteq \ker \Psi_1$, which gives a contradiction. □

From now on we will always assume the following

Setting 3.2. Let $\ell \geq 5$ be a prime number and let E_1 and E_2 be two elliptic curves over $\mathbb{Q}$ having a rational point T_i of exact order ℓ. Set $G := \langle T_i \rangle$ to be the subgroup generated by this point and denote by $E_i' := E_i/G$ the quotient and by $\eta_i : E_i \to E_i'$ the corresponding quotient isogeny. Set $A := E_1 \times E_2$ to be the product and embed G diagonally into A, denoted by $\tilde{G}$. Hence $\tilde{G} \cong \langle (T_1, nT_2) \rangle$, for some $n \in \{1, 2, \ldots, \ell - 1\}$. Define $B := A/\tilde{G}$ to be the quotient and denote the corresponding isogeny by $\varphi : A \to B$. Now set $A' := E_1' \times E_2'$ and denote by $\rho := \eta_1 \times \eta_2 : A \to A'$ the isogeny having as kernel $G \times G$. We call $\psi : B \to A'$ the isogeny, such that $\rho = \psi \circ \varphi$. Note, that as elliptic curves are principally polarized, we have $A \cong A^\vee$ and $A' \cong A'^\vee$. To summarize, we have a commutative diagram:



By construction $\ker\eta_1 \cong \ker\eta_2 \cong \ker\varphi \cong \mathbb{Z}/\ell\mathbb{Z}$, therefore $\ker\rho \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and $\ker\psi \cong \mathbb{Z}/\ell\mathbb{Z}$. Since the kernels of the dual isogenies are the Cartier duals, we have $\ker\eta_1^\vee \cong \ker\eta_2^\vee \cong \ker\varphi^\vee \cong \ker\psi^\vee \cong \boldsymbol{\mu}_\ell$ and $\ker\rho^\vee \cong \boldsymbol{\mu}_\ell \times \boldsymbol{\mu}_\ell$.

Remark 3.3. The constructed surface B depends on the choice of the diagonal embedding of G in A, i.e., on the choice of n, but it turns out that the order of the Tate-Šafarevič group of B is independent of that choice.

3.1. **The local quotient.** We start by using the results of the previous section to compute the quotients $\#\mathrm{coker}\ \varphi_p/\#\ker\varphi_p$, for $p \in M_\mathbb{Q}$. The infinite case is very easy, as we see now.

Lemma 3.4. *Assume setting 3.2, then*

$$\frac{\#\mathrm{coker}\ \varphi_\infty}{\#\ker\varphi_\infty} = \frac{1}{\ell}.$$

Proof. The kernel has ℓ elements by construction, and $\varphi_\infty : A(\mathbb{R}) \to B(\mathbb{R})$ is surjective, since $\deg\varphi = \ell$ is not divisible by 2. □

Suppose p is a finite place. Consider the long exact sequences of Galois cohomology for A and for the two elliptic curves E_i.

$$0 \longrightarrow \mathrm{coker}\ \varphi_p \longrightarrow H^1(\mathbb{Q}_p, A(\bar{\mathbb{Q}}_p)[\varphi]) \xrightarrow{\iota_p^1(A)} H^1(\mathbb{Q}_p, A(\bar{\mathbb{Q}}_p)) \longrightarrow \cdots$$

$$0 \longrightarrow \mathrm{coker}\ \eta_{i,p} \longrightarrow H^1(\mathbb{Q}_p, E_i(\bar{\mathbb{Q}}_p)[\eta_i]) \xrightarrow{\iota_p^1(E_i)} H^1(\mathbb{Q}_p, E_i(\bar{\mathbb{Q}}_p)) \longrightarrow \cdots$$

Since we know $H^1(\mathbb{Q}_p, A(\bar{\mathbb{Q}}_p)[\varphi])$, it suffices to calculate $\iota_p^1(A)$ in order to determine coker φ_p. Thus the aim will be to describe $\iota_p^1(A)$ in terms of the elliptic curves E_i.

Proposition 3.5. *Assume setting 3.2 and let $p \in M_\mathbb{Q}^0$ be a finite place. Then we have the following properties for $\iota_p^1(A)$ given properties of both $\iota_p^1(E_i)$.*

$\iota_p^1(E_i)$	$\iota_p^1(A)$
at least one injective	*injective*
both $\equiv 0$	$\equiv 0$
one $\equiv 0$, *one not injective and* $\not\equiv 0$	*not injective and* $\not\equiv 0$
both not injective and $\not\equiv 0$	*not injective and* $\not\equiv 0$

Proof. There are natural isomorphisms between $A[\varphi]$ and $E_i[\eta_i]$, given by $(T_1, nT_2) \mapsto T_1$ and $(T_1, nT_2) \mapsto nT_2$. Using these isomorphisms we can identify the map $\iota_p(A) : A[\varphi] \to E_1 \times E_2$ with $\iota_p(E_1) \oplus \iota_p(E_2)$. The functoriality of Galois cohomology gives

$$\iota_p^1(A) = \iota_p^1(E_1) \oplus \iota_p^1(E_2).$$

Now the first three lines of the table are immediate. The last line needs explanation for the non-injectivity. Combine Corollaries 2.12 and 2.19 to conclude that if $\iota_p^1(E_i)$ is not injective and $\not\equiv 0$, then the reduction type of E_i at p is either additive or good, $|\eta_i'(0)|_p = 1$ and $\eta_{i,p}^1$ and $\eta_{i,p,\mathrm{nr}}^1$ are isomorphisms. By Lemma 2.14 we have that $\bar{\eta}_{i,p}$ is an isomorphism. Now apply Proposition 2.10 to see that coker $\eta_{i,p}$ maps bijectively onto $H^1_{\mathrm{nr}}(\mathbb{Q}_p, E_i(\bar{\mathbb{Q}}_p)[\eta_{i,p}])$. Hence the kernels of $\iota_p^1(E_1)$ and $\iota_p^1(E_2)$ both equal $H^1_{\mathrm{nr}}(\mathbb{Q}_p, A(\bar{\mathbb{Q}}_p)[\varphi])$, which is non-trivial. Thus $\iota_p^1(A)$ is not injective. □

Now we can express $\frac{\#\text{coker }\varphi_p}{\#\ker\varphi_p}$ in terms of the type of reduction of both E_i's at p. In case of split multiplicative reduction we additionally have to consider whether $\ker\eta_{i,p}\subseteq(E_i)_0(\mathbb{Q}_p)$. In case of $p=\ell$ and the reduction is additive or good, the local quotient also depends on the values of $|\eta_i'(0)|_p$.

Theorem 3.6. *Assume setting 3.2 and let $p\in M_{\mathbb{Q}}^0$ be a finite place. Then*

$$\frac{\#\text{coker }\varphi_p}{\#\ker\varphi_p}=\begin{cases}\ell, & \text{split-split with both kernels } \subseteq E_0,\\ 1/\ell, & \text{at least one } E_i \text{ has split with kernel } \not\subseteq E_0,\\ 1, & \text{all other cases with } p\neq\ell.\end{cases}$$

The remaining cases are additive-additive, additive-good or good-good with $p=\ell$.

$$\frac{\#\text{coker }\varphi_p}{\#\ker\varphi_p}=\begin{cases}1, & \text{remaining case and at least one } |\eta_i'(0)|_p=1,\\ \ell, & \text{remaining case and both } |\eta_i'(0)|_p\neq 1.\end{cases}$$

Proof. Apply Corollary 2.19 on the table of the previous proposition to deduce from the reduction type of both E_i at p the properties of $\iota_p^1(A)$. Then use Corollary 2.18 and Lemma 2.2 to deduce from the reduction type of both E_i the dimension of $H^1(\mathbb{Q}_p,A(\bar{\mathbb{Q}}_p)[\varphi])$. This gives the cardinality of coker φ_p. To summarize we have the following three collums with respect to the conditions on the left.

reduction type of E_1 and E_2	$\iota_p^1(A)$	$\dim H^1$	$\#\text{coker }\varphi_p$
split-split, both kernels $\subseteq E_0$	$\equiv 0$	2	ℓ^2
at least one E_i split with kernel $\not\subseteq E_0$	injective	1 or 2	1
split-good, kernel $\subseteq E_0$, $(\Rightarrow p\neq l)$	not inj., $\not\equiv 0$	2	ℓ
non-split-good, $(\Rightarrow p\neq l)$	$\equiv 0$	1	ℓ
non-split-non-split, $(\Rightarrow p\neq l)$	$\equiv 0$	1	ℓ
good-good, $p\neq l, \boldsymbol{\mu}_l\subseteq\mathbb{Q}_p$	not inj., $\not\equiv 0$	2	ℓ
good-good, $p\neq l, \boldsymbol{\mu}_l\not\subseteq\mathbb{Q}_p$	$\equiv 0$	1	ℓ
good-good, $p=l, \lvert\eta_i'(0)\rvert_p=1$, one i	not inj., $\not\equiv 0$	2	ℓ
good-good, $p=l, \lvert\eta_i'(0)\rvert_p\neq 1$, both i	$\equiv 0$	2	ℓ^2
additive-good, $\lvert\eta_i'(0)\rvert_p=1$, one i	not inj., $\not\equiv 0$	2	ℓ
additive-good, $\lvert\eta_i'(0)\rvert_p\neq 1$,both i	$\equiv 0$	2	ℓ^2
additive-additive, $\lvert\eta_i'(0)\rvert_p=1$, one i	not inj., $\not\equiv 0$	2	ℓ
additive-additive, $\lvert\eta_i'(0)\rvert_p\neq 1$,both i	$\equiv 0$	2	ℓ^2

Since $\#\ker\varphi_v=\ell$ we are done. □

3.2. **The global quotient.** Now we investigate the global quotient

$$\frac{\#\ker\varphi_{\mathbb{Q}}}{\#\text{coker }\varphi_{\mathbb{Q}}}\frac{\#\text{coker }\varphi_{\mathbb{Q}}^\vee}{\#\ker\varphi_{\mathbb{Q}}^\vee}.$$

The kernels are clear by construction, hence we need a strategy to compute the cokernels. We will not come up with a formula as for the local quotient, but instead we will describe a method how to compute the global quotient in case one knows generators of the cokernels of $\eta_{i,\mathbb{Q}}$ and $\eta_{i,\mathbb{Q}}^\vee$. Clearly, one knows such generators in case one has a Mordell-Weil basis for $E_i(\mathbb{Q})$ and $E_i'(\mathbb{Q})$. We have the following two long exact sequences.

$$0\to\ker\psi_{\mathbb{Q}}^\vee\to\ker\rho_{\mathbb{Q}}^\vee\to\ker\varphi_{\mathbb{Q}}^\vee\to\text{coker }\psi_{\mathbb{Q}}^\vee\to\text{coker }\rho_{\mathbb{Q}}^\vee\to\text{coker }\varphi_{\mathbb{Q}}^\vee\to 0$$

$$0\to\ker\varphi_{\mathbb{Q}}\to\ker\rho_{\mathbb{Q}}\to\ker\psi_{\mathbb{Q}}\to\text{coker }\varphi_{\mathbb{Q}}\to\text{coker }\rho_{\mathbb{Q}}\to\text{coker }\psi_{\mathbb{Q}}\to 0$$

By construction the maps $\ker \rho_{\mathbb{Q}}^{\vee} \to \ker \varphi_{\mathbb{Q}}^{\vee}$ and $\ker \rho_{\mathbb{Q}} \to \ker \psi_{\mathbb{Q}}$ are surjective, therefore we have two short exact sequences of the cokernels.

$$0 \to \operatorname{coker} \psi_{\mathbb{Q}}^{\vee} \to \operatorname{coker} \rho_{\mathbb{Q}}^{\vee} \to \operatorname{coker} \varphi_{\mathbb{Q}}^{\vee} \to 0$$

$$0 \to \operatorname{coker} \varphi_{\mathbb{Q}} \to \operatorname{coker} \rho_{\mathbb{Q}} \to \operatorname{coker} \psi_{\mathbb{Q}} \to 0$$

We first have a look at the dual case, which is simpler. There are long exact sequences of Galois cohomology.

$$0 \longrightarrow \operatorname{coker} \rho_{\mathbb{Q}}^{\vee} \longrightarrow H^1(\mathbb{Q}, (E_1' \times E_2')(\bar{\mathbb{Q}})[\rho^{\vee}]) \longrightarrow \dots$$

$$0 \longrightarrow \operatorname{coker} \varphi_{\mathbb{Q}}^{\vee} \longrightarrow H^1(\mathbb{Q}, B^{\vee}(\bar{\mathbb{Q}})[\varphi^{\vee}]) \longrightarrow \dots$$

The Kummer sequence for $\mathbb{Q}$ and Hilbert's Theorem 90 yield

$$\delta_{\mathbb{Q}} : H^1(\mathbb{Q}, \boldsymbol{\mu}_{\ell}) \cong \mathbb{Q}^*/\mathbb{Q}^{*\ell}.$$

Since $E_i'(\bar{\mathbb{Q}})[\eta_i^{\vee}]$ and $B^{\vee}(\bar{\mathbb{Q}})[\varphi^{\vee}])$ are isomorphic to $\boldsymbol{\mu}_{\ell}$ as Galois modules for $G_{\mathbb{Q}}$, we obtain isomorphisms from $H^1(\mathbb{Q}, E_i'(\bar{\mathbb{Q}})[\eta_i^{\vee}])$ and $H^1(\mathbb{Q}, B^{\vee}(\bar{\mathbb{Q}})[\varphi^{\vee}])$ to $H^1(\mathbb{Q}, \boldsymbol{\mu}_{\ell})$. Hence, composing with $\delta_{\mathbb{Q}}$ we get natural injective group homomorphisms

$$\operatorname{coker} \eta_{i,\mathbb{Q}}^{\vee} \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*\ell}, \ \operatorname{coker} \varphi_{\mathbb{Q}}^{\vee} \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*\ell}.$$

Note that the images of these embeddings are independent of all choices made. We get a commutative diagram.

$$\begin{array}{ccc} \operatorname{coker} \rho_{\mathbb{Q}}^{\vee} = \operatorname{coker} \eta_{1,\mathbb{Q}}^{\vee} \times \operatorname{coker} \eta_{2,\mathbb{Q}}^{\vee} & \hookrightarrow & \mathbb{Q}^*/\mathbb{Q}^{*\ell} \times \mathbb{Q}^*/\mathbb{Q}^{*\ell} \\ \downarrow & & \downarrow \\ \operatorname{coker} \varphi_{\mathbb{Q}}^{\vee} & \hookrightarrow & \mathbb{Q}^*/\mathbb{Q}^{*\ell} \end{array}$$

In this diagram the natural surjection $\operatorname{coker} \rho_{\mathbb{Q}}^{\vee} \twoheadrightarrow \operatorname{coker} \varphi_{\mathbb{Q}}^{\vee}$ becomes $(x, y) \mapsto x^m/y$ as a map from $\mathbb{Q}^*/\mathbb{Q}^{*\ell} \times \mathbb{Q}^*/\mathbb{Q}^{*\ell}$ to $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$, for a suitable $m \in \{1, \dots, \ell-1\}$. It is clear that the image of $\operatorname{coker} \rho_{\mathbb{Q}}^{\vee}$ in the lower right group $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$ is independent of m, and for determining the image we can simply set $m = 1$. The next proposition explains how to calculate the images of $\operatorname{coker} \eta_{i,\mathbb{Q}}^{\vee}$ in $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$, i.e., how to calculate the upper horizontal map. Combining afterwards with $(x, y) \mapsto x/y$ gives $\operatorname{coker} \varphi_{\mathbb{Q}}^{\vee}$.

Proposition 3.7. *Let E and E' be elliptic curves over a number field K and $\eta : E \to E'$ an isogeny of prime degree ℓ. Assume that η is obtained by dividing out a K-rational point T. Let $f_T \in K(E)$ be a K-rational function on E, such that $\operatorname{div}(f_T) = \ell(T) - \ell(\mathcal{O})$. Then there is a unique constant $c \in K^*/K^{*\ell}$, such that*

$$\operatorname{coker} \eta_K^{\vee} \to K^*/K^{*\ell}$$

$$P \mapsto c \cdot f_T(P) \bmod K^{*\ell}, \ \textit{for } P \neq \mathcal{O}, T,$$

is a well-definied and injective group homomorphism, and its image is independent of the choice of the point T and function f_T and agrees with the image of the natural injection $\operatorname{coker} \eta_K^{\vee} \hookrightarrow K^*/K^{*\ell}$ described above. Furthermore the image lies in the finite set

$$K(S, \ell) := \{x \in K^*/K^{*\ell} \mid \ v_{\mathfrak{p}}(x) \equiv 0 \bmod \ell, \ \forall \mathfrak{p} \notin S\},$$

where S is the set of all primes $\mathfrak{p} \subset \mathcal{O}_K$ dividing the minimal discriminant of E and the degree of η.

Proof. This is Exercise 10.1 in [Sil86]. □

Remark 3.8. By Riemann-Roch the vector space of functions $f_T \in K(E)$ with $\operatorname{div}(f_T) = \ell(T) - \ell(\mathcal{O})$ is 1-dimensional, hence such a function always exists. Given such a f_T it is easy to determine $c \in K^*/K^{*\ell}$ and to find the value for the image of T in $K^*/K^{*\ell}$ by using the fact, that the map $c \cdot f_T \bmod K^{*\ell}$ is a group homomorphism. We will do this explicitly in Propositions 4.4 and 4.12.

Now we consider the remaining case, i.e., determining coker $\varphi_{\mathbb{Q}}$. There is no natural injection of coker $\eta_{i,\mathbb{Q}}$ into $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$ as before, since $E_i(\bar{\mathbb{Q}})[\eta_i]$ is not isomorphic to $\boldsymbol{\mu}_\ell$ as a Galois module for $G_{\mathbb{Q}}$. But $E_i(\bar{\mathbb{Q}})[\eta_i]$ is isomorphic to $\boldsymbol{\mu}_\ell$ as a Galois module for G_L, for $L := \mathbb{Q}(\boldsymbol{\mu}_\ell)$. Note that the natural restriction map

$$H^1(\mathbb{Q}, E_i(\bar{\mathbb{Q}})[\eta_i]) \to H^1(L, E_i(\bar{\mathbb{Q}})[\eta_i]) \cong L^*/L^{*\ell}$$

is injective, as the kernel, which equals $H^1(\operatorname{Gal}(L/\mathbb{Q}), E_i(\bar{\mathbb{Q}})[\eta_i])$, is trivial, since $[L : \mathbb{Q}] = \ell - 1$ is coprime to $\#E_i(\bar{\mathbb{Q}})[\eta_i] = \ell$. Thus we have the following commutative diagram.

$$\begin{array}{ccc}
\operatorname{coker} \varphi_{\mathbb{Q}} & \hookrightarrow & L^*/L^{*\ell} \\
\downarrow & & \downarrow \\
\operatorname{coker} \eta_{1,\mathbb{Q}} \times \operatorname{coker} \eta_{2,\mathbb{Q}} & \hookrightarrow & L^*/L^{*\ell} \times L^*/L^{*\ell} \\
\downarrow & & \downarrow \\
\operatorname{coker} \psi_{\mathbb{Q}} & \hookrightarrow & L^*/L^{*\ell}
\end{array}$$

In this diagram the natural surjection coker $\eta_{1,\mathbb{Q}} \times$ coker $\eta_{2,\mathbb{Q}} \twoheadrightarrow$ coker $\psi_{\mathbb{Q}}$ is $(a, b) \mapsto a^m/b$ as a map from $L^*/L^{*\ell} \times L^*/L^{*\ell}$ to $L^*/L^{*\ell}$, for a suitable $m \in \{1, \ldots, \ell - 1\}$. As before, all images are independent of m, thus we can simply set $m = 1$. Hence the kernel, i.e., coker $\varphi_{\mathbb{Q}}$, is easy to determine provided we know the images of coker $\eta_{i,\mathbb{Q}}$ in $L^*/L^{*\ell}$.

To obtain a map, which computes the images of coker $\eta_{i,\mathbb{Q}}$ in $L^*/L^{*\ell}$, we note that the dual isogeny $\eta_i^\vee : E_i' \to E_i$ is obtained by dividing out a L-rational point. Hence by the previous proposition we need a generator $\check{T}$ of $E_i'[\eta_i^\vee]$ and a L-rational function $f_{\check{T}} \in L(E_i')$, such that $\operatorname{div}(f_{\check{T}}) = \ell(\check{T}) - \ell(\mathcal{O})$. Again, the image lies in the finite set

$$L(S, \ell) := \{x \in L^*/L^{*\ell} \mid \ v_{\mathfrak{p}}(x) \equiv 0 \bmod \ell, \ \forall \mathfrak{p} \notin S\},$$

where S is the set of all primes $\mathfrak{p} \subset \mathcal{O}_L$ dividing the minimal discriminant of E/L and the degree of η.

At the end of this section we will describe the torsion quotient in terms of the Galois module structure of the ℓ-torsion of the elliptic curves E_i'.

Proposition 3.9. *Assume setting 3.2, then*

$$\frac{\#A(\mathbb{Q})_{\text{tors}}\,\#A^\vee(\mathbb{Q})_{\text{tors}}}{\#B(\mathbb{Q})_{\text{tors}}\,\#B^\vee(\mathbb{Q})_{\text{tors}}} = \begin{cases} 1 \text{ or } \ell, & \text{both } E_i'(\bar{\mathbb{Q}})[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \boldsymbol{\mu}_\ell, \\ \ell^3, & \text{both } E_i'(\bar{\mathbb{Q}})[\ell] \ncong \mathbb{Z}/\ell\mathbb{Z} \oplus \boldsymbol{\mu}_\ell, E_1'(\bar{\mathbb{Q}})[\ell] \ncong E_2'(\bar{\mathbb{Q}})[\ell], \\ \ell^2, & \text{otherwise.} \end{cases}$$

Proof. Since the four torsion groups are isomorphic at the p-primary parts, for p a prime $\neq \ell$, we only have to consider the ℓ-primary parts. By Mazur's theorem

[Maz77] we have that $E_i(\mathbb{Q})[\ell^\infty] \cong \mathbb{Z}/\ell\mathbb{Z}$, and that $E_i'(\mathbb{Q})[\ell^\infty] \cong \mathbb{Z}/\ell\mathbb{Z}$ if and only if $E_i'(\bar{\mathbb{Q}})[l] \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \boldsymbol{\mu}_\ell$, otherwise it is trivial. It is obvious that

$$A(\mathbb{Q})[\ell^\infty] \cong A^\vee(\mathbb{Q})[\ell^\infty] \cong (\mathbb{Z}/\ell\mathbb{Z})^2.$$

We claim that

$$B(\mathbb{Q})[\ell^\infty] \cong \begin{cases} \mathbb{Z}/\ell\mathbb{Z} \text{ or } (\mathbb{Z}/\ell\mathbb{Z})^2 \text{ or } \mathbb{Z}/\ell^2\mathbb{Z}, & \text{both } E_i'(\bar{\mathbb{Q}})[l] \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \boldsymbol{\mu}_\ell, \\ \mathbb{Z}/\ell\mathbb{Z}, & \text{otherwise,} \end{cases}$$

and that

$$B^\vee(\mathbb{Q})[\ell^\infty] \cong \begin{cases} (\mathbb{Z}/\ell\mathbb{Z})^2, & \text{both } E_i'(\bar{\mathbb{Q}})[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \boldsymbol{\mu}_\ell, \\ 0, & \text{both } E_i'(\bar{\mathbb{Q}})[\ell] \ncong \mathbb{Z}/\ell\mathbb{Z} \oplus \boldsymbol{\mu}_\ell, E_1'(\bar{\mathbb{Q}})[\ell] \ncong E_2'(\bar{\mathbb{Q}})[\ell], \\ \mathbb{Z}/\ell\mathbb{Z}, & \text{otherwise,} \end{cases}$$

and leave the justification as an exercise, because we are not going to use these results further. □

Now we will apply our results on two precise families of elliptic curves for the primes $\ell = 5$ and $\ell = 7$ respectively.

4. Elliptic curves over $\mathbb{Q}$ with rational ℓ-torsion

For a prime $\ell \neq 2$, Mazur's theorem [Maz77] tells us, that the rational ℓ-torsion subgroup $E(\mathbb{Q})[\ell]$ of an elliptic curve $E/\mathbb{Q}$ is either trivial or cyclic of order ℓ, where the non-trivial case can only happen, if $\ell = 3, 5$ or 7. Unfortunately this reduces the method described in the previous sections to be applicable only for the two primes $\ell = 5$ or 7.

4.1. **Prime $\ell = 5$.** It is a well-known fact that all elliptic curves over a number field K with non-trivial 5-torsion are parametrized by the Weierstraß equations

$$E_d : y^2 + (d+1)xy + dy = x^3 + dx^2,$$

for $d \in K$. Clearly the discriminant

$$\Delta_d = -d^5(d^2 + 11d - 1)$$

has to be different from zero. For $K = \mathbb{Q}$ this is exactly the case when $d \neq 0$ holds. The curve E_d is isogenous to the elliptic curve

$$E_d' : y^2 + (d+1)xy + dy = x^3 + dx^2 + (5d^3 - 10d^2 - 5d)x + (d^5 - 10d^4 - 5d^3 - 15d^2 - d),$$
$$\Delta_d' = -d(d^2 + 11d - 1)^5,$$

via the isogeny η_d which has exactly the five rational 5-torsion points as kernel. These points are

$$E_d(\mathbb{Q})[5] = \{\mathcal{O}, T = (0,0), 2T = (-d, d^2), 3T = (-d, 0), 4T = (0, -d)\}.$$

Now assume $K = \mathbb{Q}$. If we write $d = u/v$, with $u, v \in \mathbb{Z}$ coprime, then E_d is isomorphic to

$$E_{u,v} : y^2 + (u+v)xy + uv^2 y = x^3 + uvx^2,$$
$$\Delta_{u,v} = -(uv)^5(u^2 + 11uv - v^2),$$

and E_d' is isomorphic to

$$E_{u,v}' : y^2 + (u+v)xy + uv^2 y =$$
$$x^3 + uvx^2 + (5u^3v - 10u^2v^2 - 5uv^3)x + (u^5v - 10u^4v^2 - 5u^3v^3 - 15u^2v^4 - uv^5),$$

$$\Delta'_{u,v} = -uv(u^2 + 11uv - v^2)^5,$$
$$c'_{4,u,v} = u^4 - 228u^3v + 494u^2v^2 + 228uv^3 + v^4.$$

To determine the local quotient we have to know the reduction type of E_d at p and the value $|\eta'_d(0)|_p$.

Lemma 4.1. *Let p be a prime number and let $E := E_d$ be an elliptic curve as above parametrized by $d = u/v \in \mathbb{Q}^*$, with $u, v \in \mathbb{Z}$ coprime.*

(i) If $p|uv$ then E has split multiplicative reduction at p with $E(\mathbb{Q})[5] \nsubseteq E_0(\mathbb{Q}_p)$.

(ii) If $p|u^2 + 11uv - v^2$ then $E(\mathbb{Q})[5] \subseteq E_0(\mathbb{Q}_p)$, and E has split multiplicative reduction at p if and only if $p \equiv 1 \bmod 5$, additive reduction if and only if $p = 5$, and otherwise non-split multiplicative reduction with $p \equiv -1 \bmod 5$.

(iii) a) $v_5(u^2 + 11uv - v^2) \in \{0, 2, 3\}$,

b) $v_5(u^2 + 11uv - v^2) = 0 \Leftrightarrow u \not\equiv 2v \bmod 5$,

c) $v_5(u^2 + 11uv - v^2) = 3 \Leftrightarrow u \equiv 7v \bmod 25$,

d) $u \equiv 2v \bmod 5 \Rightarrow 5^4 \mid c'_{4,u,v}$

Proof. Consider the reduction-mod-p map $E(\mathbb{Q}) \to \tilde{\mathcal{E}}(\mathbb{F}_p)$ and the point $T = (0, 0)$, which generates $E(\mathbb{Q})[5]$. If $p|uv$ then $\tilde{\mathcal{E}} : \bar{y}^2 + \alpha\bar{x}\bar{y} = \bar{x}^3$, for a non-zero $\alpha \in \mathbb{Z}/p\mathbb{Z}$. In particular $\bar{T}$ is a node of $\tilde{\mathcal{E}}$ and the tangent cone is generated by $\bar{x} = -\alpha\bar{y}$ and by $\bar{y} = 0$. Thus the reduction type is split multiplicative and $T \notin E_0(\mathbb{Q}_p)$, which proves (i).

If $p|u^2 + 11uv - v^2$ then $\bar{T}$ is non-singular, hence $E(\mathbb{Q})[5] \subseteq E_0(\mathbb{Q}_p)$. Also $\bar{T}$ is non-trivial, therefore it has order 5. Since the order of $\bar{T}$ divides $\#\tilde{\mathcal{E}}_0(\mathbb{F}_p)$, which equals $p-1$ if the reduction is split multiplicative, $p+1$ if the reduction is non-split multiplicative, and p if the reduction is additive, we get (ii).

Part (iii) is an easy calculation. Note, that any pair of integers u and v making the expression $u^2+11uv-v^2$ divisible by 5^4 is not coprime, since u and v will both be divisible by 5. □

Proposition 4.2. *Let $\eta_d : E_d \to E'_d$ be the isogeny described above, for $d = u/v$. Then*

$$|\eta'_d(0)|_p = \begin{cases} 1/5, & p = 5 \text{ and } u \equiv 7v \bmod 25, \\ 1, & \text{otherwise.} \end{cases}$$

Proof. It is clear that $|\eta'_d(0)|_p$ equals 1, if $p \neq 5$ or if p is a place of multiplicative reduction, see Proposition 2.11 and Corollary 2.18. So it only remains the case $p = 5$ and p is good or additive, by the previous lemma. For places of good reduction the Weierstrass equations $E_{u,v}$ and $E'_{u,v}$ are minimal. In case $p = 5$ is additive, combining Lemma 4.1 with [Sil86, Exercise 7.1] gives that the Weierstrass equation for $E_{u,v}$ is minimal and the one for $E'_{u,v}$ is not minimal if and only if $u \equiv 7v \bmod 25$. In this case $v_5(\Delta'_{u,v}) = 15$ and $c'_{4,u,v}$ is divisible at least by 5^4, so the Weierstrass equation of $E'_{u,v}$ will become minimal if we make the following change of variables, $x \mapsto x/5^2$ and $y \mapsto y/5^3$. For the moment assume that the equation for $E'_{u,v}$ is minimal. We will now compute the p-adic valuation of the leading coefficent of the power series representation of η_d. We claim that $\eta_d(z) = z + ...$ as a power series in z in a neighbourhood of $\mathcal{O}$.

Set $\eta_d(x, y) =: (\tilde{x}(x, y), \tilde{y}(x, y))$, then by [Vél71] we have $-\frac{\tilde{x}(x,y)}{\tilde{y}(x,y)} = \frac{p(x)}{q(x,y)}$, for

$$p(x) := x(d + x)[d^4 + (3d^3 + d^4)x + (3d^2 + 3d^3)x^2 + (d + 3d^2 - d^3)x^3 + 2dx^4 + x^5]$$

$$= x^7 + \dots,$$
$$q(x,y) := d^6 + (5d^5 + 2d^6)x + (10d^4 + 8d^5 + d^6)x^2 + (10d^3 + 13d^4 + 4d^5)x^3$$
$$+(5d^2 + 10d^3 + 4d^4)x^4 + (d + 3d^2 + d^3 - d^4)x^5$$
$$+y[2d^5+(7d^4+d^5)x+(9d^3+3d^4)x^2+(5d^2+3d^3+d^4)x^3+(d-d^2-d^3)x^4-3dx^5-x^6]$$
$$= -yx^6 + \dots$$

For $z := -x/y$, we have $x(z) = z^{-2} + \dots$ and $y(z) = -z^{-3} + \dots$ as Laurent series for x and y (see [Sil86, IV.1]), therefore $\eta_d(z) = \frac{z^{-14}+\dots}{z^{-15}+\dots} = z + \dots$ as power series in z. Hence $\eta_d'(0) = 1$, and therefore $|\eta_d'(0)|_p = 1$.

In case the equation for $E'_{u,v}$ was not minimal, we have to replace z by $5z$, which gives $\eta_d(z) = 5z + \dots$, and therefore $\eta_d'(0) = 5$. Hence $|\eta_d'(0)|_5 = 1/5$. □

Combining the above lemma and proposition with Theorem 3.6 gives complete control of the local quotient.

Theorem 4.3. *Assume Setting 3.2 with $\ell = 5$. Let E_i be given by $d_i = u_i/v_i$, for $d_i \in \mathbb{Q}^*, u_i, v_i \in \mathbb{Z}$ coprime. If $p \in M_\mathbb{Q}$ is a place, then*

$$\frac{\#\text{coker } \varphi_p}{\#\ker \varphi_p} = \begin{cases} 1/5, & p = \infty, \\ 1/5, & p \mid u_1v_1u_2v_2, \\ 5, & p \mid \gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2), p \equiv 1(5), \\ 5, & u_1 \equiv 7v_1 \bmod 25, u_2 \equiv 7v_2 \bmod 25, p = 5, \\ 1, & \textit{otherwise.} \end{cases}$$

Next comes the global quotient. As the η_i are obtained by dividing out the $\mathbb{Q}$-rational point $T_i = (0,0)$, we will use Proposition 3.7 to calculate coker $\eta_{i,\mathbb{Q}}^\vee$ in $\mathbb{Q}^*/\mathbb{Q}^{*5}$.

Proposition 4.4. *For $T = (0,0)$ set*

$$f_T := -x^2 + xy + y \in K(E_d).$$

The image of the natural embedding coker $\eta_{d,\mathbb{Q}}^\vee \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*5}$ *equals the image of*

$$f_T(x,y) \bmod \mathbb{Q}^{*5}, \text{ for } P = (x,y) \neq \mathcal{O}, T.$$

By linearity $f_T(T) = d^4$, and $f_T(\text{coker } \eta_{d,\mathbb{Q},\text{tors}}^\vee) = \langle d \rangle$ in $\mathbb{Q}^*/\mathbb{Q}^{*5}$.

Proof. For functions $x, y, x + y + d \in K(E)$ one easily sees, that $\text{div}(x) = (T) + (4T) - 2(\mathcal{O})$, $\text{div}(y) = 2(T) + (3T) - 3(\mathcal{O})$, and $\text{div}(x+y+d) = 2(3T) + (4T) - 3(\mathcal{O})$, hence $\text{div}((xy^2)/(x + y + d)) = 5(T) - 5(\mathcal{O})$. Multiplying $(xy^2)/(x + y + d)$ with $(-y - dx)/(-y - dx)$ yields $-x^2 + xy + y$ in $K(E)$. By Proposition 3.7 we obtain $f_T = c(-x^2 + xy + y)$. Since $(f_T(2T))^2 = f_T(4T)$, we deduce $c = 1$ and that $f_T(T) \equiv f_T(2T)^3 \equiv d^4 \bmod \mathbb{Q}^{*5}$. □

Corollary 4.5. *With notation as above, $E'_d(\mathbb{Q})[5] \cong \mathbb{Z}/5\mathbb{Z} \Leftrightarrow d \in \mathbb{Q}^{*5}$.*

Proof. We have that $E'_d(\mathbb{Q})[5]$ is non-trivial if and only if coker $\eta_{d,\mathbb{Q}}^\vee$ is trivial on the torsion part, i.e., the injective map $\eta_{d,\mathbb{Q},\text{tors}}^\vee : E'_d(\mathbb{Q})_{\text{tors}} \to E_d(\mathbb{Q})_{\text{tors}}$ is an isomorphism. The cokernel of $\eta_{d,\mathbb{Q},\text{tors}}^\vee$ is generated by d in $\mathbb{Q}^*/\mathbb{Q}^{*5}$. Hence $E'_d(\mathbb{Q})[5]$ is non-trivial if and only if d is trivial in $\mathbb{Q}^*/\mathbb{Q}^{*5}$. □

Now we calculate coker $\eta_\mathbb{Q}$ in L^*/L^{*5}, for $L = \mathbb{Q}(\xi)$, with ξ a fifth root of unity. Fix a generator $\check{T}$ of $E'(\bar{\mathbb{Q}})[\eta^\vee]$. Since $\check{T}$ is defined over L, we have that

$E'(L)[\eta^\vee] \cong \mathbb{Z}/5\mathbb{Z}$ and hence $(E'/L, \check{T})$ is isomorphic over L to an $(E_{\tilde{d}}, (0,0))$ as above, for $\tilde{d} \in L$. Such an isomorphism τ is given by four values $r, s, t \in L$ and $w \in L^*$ and has the form $x = w^2x' + r$ and $y = w^3y' + w^2sx' + t$, compare [Sil86, III.1]. Having such an isomorphism τ and the formula of f_T from Proposition 4.4, we can determine $f_{\check{T}}$, since

$$f_{\check{T}}(x,y) \equiv \tau^* f_T(x',y') \bmod L^{*5}.$$

To obtain τ we use [Sil86, III Table 1.2]. As the a_6 of the Weierstraß equation of $(E_{\tilde{d}}, (0,0))$ vanishes, we get $(r,t) = \check{T}$. The kernel polynomial of the dual isogeny $\eta_d^\vee : E'_d \to E_d$ is

$$x^2 + (d^2+d+1)x + \frac{1}{5}(d^4 - 3d^3 - 26d^2 + 8d + 1),$$

thus, for $\vartheta := \xi + \xi^{-1} = (\sqrt{5}-1)/2$, we may chose

$$r = \frac{1}{5}[(-\vartheta - 3)d^2 + (-11\vartheta - 8)d + (\vartheta - 2)] \in \mathbb{Q}(\vartheta) = \mathbb{Q}(\sqrt{5}),$$

$$t = \frac{1}{5}[(\xi^2 + 2\xi + 2)d^3 + (\xi^3 + 10\xi^2 + 23\xi + 11)d^2$$

$$+(11\xi^3 - 12\xi^2 + 9\xi + 2)d + (-\xi^3 + \xi^2 - \xi + 1)] \in L.$$

Since a_4 of $(E_{\tilde{d}}, (0,0))$ also vanishes we deduce

$$s = \frac{1}{5}[(-4\xi^3 - 3\xi^2 - 7\xi - 6)d + (3\xi^3 - 4\xi^2 - \xi - 3)],$$

and since $a_3 = a_2$ we deduce

$$w = \frac{1}{5}[(-\xi^3 - 7\xi^2 - 8\xi - 4)d + (7\xi^3 - \xi^2 + 6\xi + 3)].$$

Also one can use the conditions on the a_i to calculate $\tilde{d} = \frac{(5\vartheta-3)d+1}{d-(5\vartheta-3)}$. All in all we described an algorithm to compute $f_{\check{T}}$. If one multiplies the obtained result by w^5 to get rid of denominators one obtains

$$f_{\check{T}}(x,y) = \frac{1}{25}[(3 + 6\xi - \xi^2 + 7\xi^3) + (80 + 235\xi - 60\xi^2 + 245\xi^3)d$$

$$+(220 + 465\xi + 185\xi^2 + 205\xi^3)d^2 + (15 + 55\xi - 55\xi^2 + 160\xi^3)d^3$$

$$+(140 + 280\xi + 245\xi^2 + 35\xi^3)d^4 + (-4 - 8\xi - 7\xi^2 - \xi^3)d^5]$$

$$+[(-1 + \xi - \xi^2) + (3 + 9\xi + 2\xi^2 + 2\xi^3)d + (2 + 6\xi + 8\xi^2 - 3\xi^3)d^2$$

$$+(-1 - \xi + \xi^3)d^3]x + [(-\xi + \xi^2 - 2\xi^3) + (2 + 3\xi + 2\xi^2 + \xi^3)d]x^2$$

$$+[(-3 - 2\xi^2 - 2\xi^3) + (-1 - 3\xi^2 - 3\xi^3)d + (-1 + 2\xi^2 + 2\xi^3)d^2]y + xy \in L(E'_{u,v}).$$

Now we can state the torsion quotient in terms of the d_i. Recall, that if the two elliptic curves E_i have both rank equal to zero the regulator quotient equals 1, hence the global quotient is just the torsion quotient. If elliptic curves of positive rank are involved, we need generators for the cokernels of $\eta_{i,\mathbb{Q}}$ and $\eta_{i,\mathbb{Q}}^\vee$ in order to use the above described procedure to calculate the global quotient.

Proposition 4.6. *Assume Setting 3.2 with $\ell = 5$. Let E_i be given by $d_i \in \mathbb{Q}^*$. Then the following holds.*

$$\frac{\#A(\mathbb{Q})_{\mathrm{tors}}\,\#A^\vee(\mathbb{Q})_{\mathrm{tors}}}{\#B(\mathbb{Q})_{\mathrm{tors}}\,\#B^\vee(\mathbb{Q})_{\mathrm{tors}}} = \begin{cases} 1 \text{ or } 5, & d_1, d_2 \in \mathbb{Q}^{*5}, \\ 5^2, & d_i \in \mathbb{Q}^{*5}, d_j \notin \mathbb{Q}^{*5}, i \neq j, \\ 5^2, & \langle 1\rangle \neq \langle d_1\rangle = \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}, \\ 5^3, & \langle 1\rangle \neq \langle d_1\rangle \neq \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}. \end{cases}$$

To be more precise, in case both $d_i \in \mathbb{Q}^{*5}$, set $d_i =: D_i^5$, for $D_i \in \mathbb{Q}^*$, and define $U_1 := -\xi^4(\xi+1)$, $U_2 := -\xi(\xi+1)$, $U_3 := -\xi^3(\xi+1)$ and $U_4 := -(\xi+1)$. Then the torsion quotient equals 1 if and only if

$$\left\langle \prod_{j=1}^{4} (D_1 + U_j)^j (D_1 - 1/U_j)^j \right\rangle = \left\langle \prod_{j=1}^{4} (D_2 + U_j)^j (D_2 - 1/U_j)^j \right\rangle \text{ in } L^*/L^{*5}.$$

Proof. Recall that the torsion quotient equals $5 \cdot \#\mathrm{coker}\ \varphi^\vee_{\mathbb{Q},\mathrm{tors}} / \#\mathrm{coker}\ \varphi_{\mathbb{Q},\mathrm{tors}}$, and that coker $\varphi^\vee_{\mathbb{Q},\mathrm{tors}}$ equals the image of coker $\eta^\vee_{1,\mathbb{Q},\mathrm{tors}} \times \mathrm{coker}\ \eta^\vee_{2,\mathbb{Q},\mathrm{tors}}$ in $\mathbb{Q}^*/\mathbb{Q}^{*5}$. As coker $\eta^\vee_{i,\mathbb{Q},\mathrm{tors}}$ is generated by d_i mod $\mathbb{Q}^{*5}$ and the map on coker $\varphi^\vee_{\mathbb{Q},\mathrm{tors}}$ is $(x,y) \mapsto x/y$, we get

$$\#\mathrm{coker}\ \varphi^\vee_{\mathbb{Q},\mathrm{tors}} = \begin{cases} 1, & d_1, d_2 \in \mathbb{Q}^{*5}, \\ 5, & d_i \in \mathbb{Q}^{*5}, d_j \notin \mathbb{Q}^{*5}, i \neq j, \\ 5, & \langle 1\rangle \neq \langle d_1\rangle = \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}, \\ 5^2, & \langle 1\rangle \neq \langle d_1\rangle \neq \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}. \end{cases}$$

We have seen above that $E'_d(\mathbb{Q})[5] \cong \mathbb{Z}/5\mathbb{Z}$ if and only if $d \in \mathbb{Q}^{*5}$, hence coker $\eta_{i,\mathbb{Q},\mathrm{tors}}$ is trivial in case $d_i \notin \mathbb{Q}^{*5}$, otherwise it is 1-dimensional. Looking at the kernel of $(x,y) \mapsto x/y$ gives

$$\#\mathrm{coker}\ \varphi_{\mathbb{Q},\mathrm{tors}} = \begin{cases} 1 \text{ or } 5, & d_1, d_2 \in \mathbb{Q}^{*5}, \\ 1, & \text{otherwise}, \end{cases}$$

which finishes the first part.

For the second part note, that if $d_i = D_i^5$, then $E'_d(\mathbb{Q})[5]$ is generated by the point $P_i = (x_i, y_i)$, where

$$x_i = D_i + 2D_i^2 + 3D_i^2 + 5D_i^4 + 2D_i^5 + 2D_i^6 - D_i^7 + D_i^8,$$

$$y_i = D_i^2 + 3D_i^3 + 5D_i^4 + 11D_i^5 + 13D_i^6 + 10D_i^7 + D_i^8 - D_i^{10} + D_i^{11} + D_i^{12}.$$

The image of $\langle P_i \rangle$ under $f_{\tilde{T}}$ in L^*/L^{*5}, i.e., the image of coker $\eta_{i,\mathbb{Q},\mathrm{tors}}$ in L^*/L^{*5}, is

$$\left\langle \prod_{j=1}^{4} (D_i + U_j)^j (D_i - 1/U_j)^j \right\rangle,$$

which completes the second part. □

Finally, we give two unconditional examples of an abelian surface B over $\mathbb{Q}$ of rank 0, respectively of rank 1, such that $\#Ш(B/\mathbb{Q}) = 5$.

Example 4.7. If $d_1 = u_1/v_1 = 1/11$ and $d_2 = u_2/v_2 = 2/9$, then $\#Ш(B/\mathbb{Q}) = 5$.

Proof. We start with the local quotient. There are three different primes dividing $u_1v_1u_2v_2 = 2 \cdot 3^2 \cdot 11$. Then we have the contribution of the prime at infinity and that's it, as $u_i \not\equiv 7 \cdot v_i \bmod 25$, for both i, and $\gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2) = 1$. Hence the local quotient equals $1/5^4$. Both elliptic curves E_{d_i} have analytic rank equal to 0, hence we know that $Ш(A/\mathbb{Q})$ and $Ш(B/\mathbb{Q})$ are finite and that the global quotient equals the torsion quotient. Thus the global quotient equals 5^3. We conclude that $\#Ш(B/\mathbb{Q}) = 5 \cdot \#Ш(A/\mathbb{Q})$.

It remains to show, that both $Ш(E_i/\mathbb{Q})$ are trivial. The predicted size by the Birch and Swinnerton-Dyer formula is 1. Both E_i are non-CM curves of conductor ≤ 1000, hence we can apply [Ste09, Theorem 3.31 and Theorem 4.4]. This gives us that $\#Ш(E_i/\mathbb{Q})[p^\infty] = 1$, for all primes $p \neq 5$. (The primes occurring as the degrees of cyclic isogenies or dividing any Tamagawa number are only 2 and 5.) Now use [Fis01, Theorem 1 or Table 3 in the Appendix] to calculate $\mathrm{Sel}^{\eta_i}(E_i/\mathbb{Q}) = 0$ and $\mathrm{Sel}^{\eta_i^\vee}(E_i'/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$, for both i. As $\operatorname{coker} \eta_{i,\mathbb{Q}} = 0$ and $\operatorname{coker} \eta_{i,\mathbb{Q}}^\vee \cong \mathbb{Z}/5\mathbb{Z}$ we have $Ш(E_i/\mathbb{Q})[\eta_i] = Ш(E_i'/\mathbb{Q})[\eta_i^\vee] = 0$ and thus $Ш(E_i/\mathbb{Q})[5] = 0$. Hence $Ш(E_i/\mathbb{Q})$ is trivial. □

Example 4.8. If $d_1 = u_1/v_1 = 1/10$ and $d_2 = u_2/v_2 = 3/1$, then $\#Ш(B/\mathbb{Q}) = 5$.

Proof. We have $u_1v_1u_2v_2 = 2 \cdot 3 \cdot 5$, $u_i \not\equiv 7 \cdot v_i \bmod 25$, for both i, and $\gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2) = 1$. Hence the local quotient equals $1/5^4$. The elliptic curve E_1 is of analytic rank 0 and E_2 of analytic rank 1. A generator of the free part of $E_2(\mathbb{Q})$ is the point $P = (-6, 12)$. We will now determine $\operatorname{coker} \eta_{i,\mathbb{Q}}^\vee$ as a subset of $\mathbb{Q}^*/\mathbb{Q}^{*5}$. For the first curve this equals just the torsion part of the cokernel, hence $\operatorname{coker} \eta_{1,\mathbb{Q}}^\vee$ is generated by $\{2 \cdot 5\}$. The second cokernel is generated by the image of the torsion point, which is 3, and by the image of P under $f = -x^2 + xy + y$, which is $-3 \cdot 2^5 \equiv 3 \bmod \mathbb{Q}^{*5}$. Therefore $\operatorname{coker} \eta_{2,\mathbb{Q}}^\vee$ is generated only by $\{3\}$ and hence $\operatorname{coker} \varphi_\mathbb{Q}^\vee$ has dimension equal to 2. Since both d_i are no fifth powers, we get that the dimension of $\operatorname{coker} \eta_{1,\mathbb{Q}}$ equals 0 and the one of $\operatorname{coker} \eta_{2,\mathbb{Q}}$ equals 0 or 1, thus the dimension of $\operatorname{coker} \varphi_\mathbb{Q}$ equals 0. We conclude that the global quotient equals 5^3, which gives $\#Ш(B/\mathbb{Q}) = 5 \cdot \#Ш(A/\mathbb{Q})$. Now one can use a similar strategy as in the previous example to show that $Ш(A/\mathbb{Q})$ is trivial. □

4.2. **Prime $\ell = 7$.** The situation is very similar to the case $\ell = 5$, so we mostly just state the results. The elliptic curves with non-trivial 7-torsion are parametrized by the Weierstraß equations

$$E_d : y^2 + (1 + d - d^2)xy + (d^2 - d^3)y = x^3 + (d^2 - d^3)x^2,$$
$$\Delta_d = -d^7(1 - d)^7(d^3 - 8d^2 + 5d + 1).$$

Thus for $K = \mathbb{Q}$ we have $d \neq 0, 1$. The isogenous curve is

$$E_d' : y^2 + (1 + d - d^2)xy + (d^2 - d^3)y =$$
$$x^3 + (d^2 - d^3)x^2 + (5d - 35d^2 + 70d^3 - 70d^4 + 35d^5 - 5d^7)x$$
$$+(d - 19d^2 + 94d^3 - 258d^4 + 393d^5 - 343d^6 + 202d^7 - 107d^8 + 46d^9 - 8d^{10} - d^{11}),$$
$$\Delta_d' = -d(1 - d)(d^3 - 8d^2 + 5d + 1)^7,$$

and the 7-torsion points are

$$E(\mathbb{Q})[7] = \{\mathcal{O}, T = (0, 0), 2T = (d^3 - d^2, d^5 - 2d^4 + d^3), 3T = (d^2 - d, d^3 - 2d^2 + d),$$
$$4T = (d^2 - d, d^4 - 2d^3 + d^2), 5T = (d^3 - d^2, 0), 6T = (0, d^3 - d^2)\}.$$

If we write $d = u/v$, with $u, v \in \mathbb{Z}$ coprime, we get

$$E_{u,v} : y^2 + ((v-u)(v+u) + uv)xy + (v-u)u^2v^3y = x^3 + (v-u)u^2vx^2,$$

$$\Delta_{u,v} = -(uv)^7(v-u)^7(u^3 - 8u^2v + 5uv^2 + v^3),$$

$$E'_{u,v} : y^2 + ((v-u)(v+u) + uv)xy + (v-u)u^2v^3y =$$

$$x^3 + (v-u)u^2vx^2 + (-5u^7v + 35u^5v^3 - 70u^4v^4 + 70u^3v^5 - 35u^2v^6 + 5uv^7)x$$

$$-u^{11}v - 8u^{10}v^2 + 46u^9v^3 - 107u^8v^4 + 202u^7v^5 - 343u^6v^6$$

$$+393u^5v^7 - 258u^4v^8 + 94u^3v^9 - 19u^2v^{10} + uv^{11},$$

$$\Delta'_{u,v} = -uv(v-u)(u^3 - 8u^2v + 5uv^2 + v^3)^7,$$

$$c'_{4,u,v} = u^8 + 228u^7v + 42u^6v^2 - 1736u^5v^3 + 3395u^4v^4$$

$$-3360u^3v^5 + 1666u^2v^6 - 236uv^7 + v^8.$$

As before, to determine the local quotient we have to know the reduction type of E_d at p and the value $|\eta'_d(0)|_p$.

Lemma 4.9. *Let p be a prime number and let $E := E_d$ be an elliptic curve as above parametrized by $d = u/v \in \mathbb{Q}^*$, with $u, v \in \mathbb{Z}$ coprime.*

(i) If $p|uv(v-u)$ then E has split multiplicative reduction at p with $E(\mathbb{Q})[7] \nsubseteq E_0(\mathbb{Q}_p)$.

(ii) If $p|u^3 - 8u^2v + 5uv^2 + v^3$ then $E(\mathbb{Q})[7] \subseteq E_0(\mathbb{Q}_p)$, and E has split multiplicative reduction at p if and only if $p \equiv 1 \bmod 7$, additive reduction if and only if $p = 7$, and otherwise non-split multiplicative reduction with $p \equiv -1 \bmod 7$.

(iii) a) $v_7(u^3 - 8u^2v + 5uv^2 + v^3) \in \{0, 2\}$,

b) $v_7(u^3 - 8u^2v + 5uv^2 + v^3) = 2 \Leftrightarrow u \equiv 5v \bmod 7$,

c) $u \equiv 5v \bmod 7 \Rightarrow 7^6 \mid c'_{4,u,v}$.

Proof. Analogous to the proof of Lemma 4.1. □

Proposition 4.10. *Let $\eta_d : E_d \to E'_d$ be the isogeny described above, for $d = u/v$. Then*

$$|\eta'_d(0)|_p = \begin{cases} 1/7, & p = 7 \text{ and } u \equiv 5v \bmod 7, \\ 1, & \text{otherwise.} \end{cases}$$

Proof. Analogous to the proof of Proposition 4.2. □

Hence, for the local quotient we have the following

Theorem 4.11. *Assume Setting 3.2 with $\ell = 7$. Let E_i be given by $d_i = u_i/v_i$, for $d_i \in \mathbb{Q}^*, u_i, v_i \in \mathbb{Z}$ coprime. If $p \in M_{\mathbb{Q}}$ is a place, then*

$$\frac{\#\text{coker } \varphi_p}{\#\ker \varphi_p} = \begin{cases} 1/7, & p = \infty, \\ 1/7, & p \mid u_1v_1u_2v_2(v_1 - u_1)(v_2 - u_2), \\ 7, & p \mid \gcd(u_1^3 - 8u_1^2v_1 + 5u_1v_1^2 + v_1^3, u_2^3 - 8u_2^2v_2 + 5u_2v_2^2 + v_2^3), p \equiv 1(7), \\ 7, & u_1 \equiv 5v_1 \bmod 7, u_2 \equiv 5v_2 \bmod 7, p = 7, \\ 1, & \text{otherwise.} \end{cases}$$

Next comes the global quotient.

Proposition 4.12. *For $T = (0,0)$ set*

$$f_T := d^2x^2 + x^3 + dx^3 - d^2y - xy - 2dxy - x^2y \in K(E).$$

Then the image of the natural embedding $\operatorname{coker} \eta_{\mathbb{Q}}^{\vee} \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*7}$ *equals the image of*

$$f_T(x,y) \bmod \mathbb{Q}^{*7}, \text{ for } P = (x,y) \neq \mathcal{O}, T.$$

By linearity $f_T(T) = d^3(d-1)^6$, and $f_T(\operatorname{coker} \eta_{\mathbb{Q},\mathrm{tors}}^{\vee}) = \langle d(d-1)^2 \rangle$ in $\mathbb{Q}^*/\mathbb{Q}^{*7}$.

Proof. We have that $\operatorname{div}(x) = (T) + (6T) - 2(\mathcal{O})$, $\operatorname{div}(y) = 2(T) + (5T) - 3(\mathcal{O})$, $\operatorname{div}(x(d-1) - y) = (T) + 2(3T) - 3(\mathcal{O})$, and $\operatorname{div}(x + y - d^3 + d^2) = (3T) + (5T) + (6T) - 3(\mathcal{O})$, hence $\operatorname{div}(x^2y^2(x(d-1) - y)/(x + y - d^3 + d^2)^2) = 7(T) - 7(\mathcal{O})$. Multiplying with $(-y - (1 + d - d^2)x - (d^2 - d^3))/(-y - (1 + d - d^2)x - (d^2 - d^3))$ gives $d^2x^2 + x^3 + dx^3 - d^2y - xy - 2dxy - x^2y$. Proceed as in Proposition 4.4. □

Corollary 4.13. *With notation as above, $E'_d(\mathbb{Q})[7] = 0$.*

Proof. As in Corollary 4.5, $E'_d(\mathbb{Q})[7]$ is non-trivial if and only if $d(d-1)^2$ is trivial in $\mathbb{Q}^*/\mathbb{Q}^{*7}$, which is equivalent to d and $d-1$ being a seventh power, for $d \in \mathbb{Q} \setminus \{0,1\}$. But Fermat's Last Theorem for exponent 7 says that this can never happen. □

Now set $L := \mathbb{Q}(\xi)$, for ξ a seventh root of unity. As in case $\ell = 5$, we want to compute a function $f_{\check{T}}$, which calculates the image of $\operatorname{coker} \eta_{\mathbb{Q}}$ in L^*/L^{*7}, and which depends on a point $\check{T} = (r,t) \in E'(\bar{\mathbb{Q}})[\eta^{\vee}]$. The coefficients r, t, s, w for the isomorphism $\tau : (E'_d/L, \check{T}) \to (E_{\tilde{d}}, (0,0))$ can be computed in the same manner as before. The kernel polynomial of the dual isogeny $\eta_d^{\vee} : E'_d \to E_d$ is

$$\begin{gathered}\frac{1}{7}(d^{12} + 3d^{11} - 51d^{10} + 185d^9 - 767d^8 + 2097d^7 - 2835d^6 \\ +1738d^5 - 295d^4 - 116d^3 + 55d^2 - 15d + 1) \\ +(d^8 - d^7 - 14d^6 + 32d^5 - 29d^4 + 7d^3 + 11d^2 - 7d + 1)x \\ +(2d^4 - 5d^3 + 6d^2 - 3d + 2)x^2 + x^3,\end{gathered}$$

hence for $\vartheta := \xi + \xi^{-1}$ we may chose

$$\begin{gathered}r = \frac{1}{7}[(3\vartheta^2 + 2\vartheta - 9)d^4 + (-25\vartheta^2 - 19\vartheta + 47)d^3 \\ +(23\vartheta^2 + 34\vartheta - 41)d^2 + (-2\vartheta^2 - 13\vartheta + 6)d + (-\vartheta^2 - 3\vartheta - 4)] \in \mathbb{Q}(\vartheta),\end{gathered}$$

$$\begin{gathered}t = \frac{1}{7}[(-3\xi^5 - 6\xi^4 - \xi^3 - \xi^2 - 5\xi - 5)d^6 + (28\xi^5 + 59\xi^4 + 7\xi^3 + 10\xi^2 + 45\xi + 33)d^5 \\ +(-52\xi^5 - 119\xi^4 + 6\xi^3 - 16\xi^2 - 62\xi - 51)d^4 + (56\xi^5 + 54\xi^4 - 35\xi^3 - 37\xi^2 - 9\xi + 13)d^3 \\ +(-13\xi^5 + 30\xi^4 + 54\xi^3 + 75\xi^2 + 60\xi + 32)d^2 + (-10\xi^5 - 16\xi^4 - 22\xi^3 - 25\xi^2 - 22\xi - 17)d \\ +(-\xi^5 - 3\xi^4 - 5\xi^3 - 6\xi^2 - 5\xi - 1)] \in L.\end{gathered}$$

Using the conditions on the a_i gives

$$\begin{gathered}s = \frac{1}{7}[(3\xi^5 + 6\xi^4 - 5\xi^3 - 2\xi^2 + \xi + 4)d^2 + (-16\xi^5 - 11\xi^4 - 6\xi^3 - \xi^2 - 17\xi - 12)d \\ +(5\xi^5 + 3\xi^4 + 8\xi^3 + 6\xi^2 + 11\xi + 2)],\end{gathered}$$

$$\begin{gathered}w = \frac{1}{7}[(-3\xi^5 - 6\xi^4 - \xi^3 - \xi^2 - 5\xi - 5)d^6 + (28\xi^5 + 59\xi^4 + 7\xi^3 + 10\xi^2 + 45\xi + 33)d^5 \\ +(-52\xi^5 - 119\xi^4 + 6\xi^3 - 16\xi^2 - 62\xi - 51)d^4 + (56\xi^5 + 54\xi^4 - 35\xi^3 - 37\xi^2 - 9\xi + 13)d^3 \\ +(-13\xi^5 + 30\xi^4 + 54\xi^3 + 75\xi^2 + 60\xi + 32)d^2 + (-10\xi^5 - 16\xi^4 - 22\xi^3 - 25\xi^2 - 22\xi - 17)d \\ +(-\xi^5 - 3\xi^4 - 5\xi^3 - 6\xi^2 - 5\xi - 1)],\end{gathered}$$

$$\tilde{d} = \frac{(\vartheta^2+3\vartheta+2)d - (\vartheta^2+3\vartheta+1)}{d-(\vartheta^2+3\vartheta+2)}.$$

Now putting everything together gives

$$f_{\tilde{T}} \equiv w^7 \cdot f_T((x-r)/w^2, (y-t-s(x-r))/w^3)$$

$$= w^3\tilde{d}^2(x-r)^2 + w(x-r)^3 + w\tilde{d}(x-r)^3 - w^4\tilde{d}^2(y-t-s(x-r)) - w^2(x-r)(y-t-s(x-r)),$$

which yields a one page long formula for $f_{\tilde{T}}$.

For the torsion quotient we get the following

Proposition 4.14. *Assume Setting 3.2 with $\ell = 7$. Let E_i be given by $d_i \in \mathbb{Q} \setminus \{0,1\}$. Then*

$$\frac{\#A(\mathbb{Q})_{\text{tors}}\,\#A^\vee(\mathbb{Q})_{\text{tors}}}{\#B(\mathbb{Q})_{\text{tors}}\,\#B^\vee(\mathbb{Q})_{\text{tors}}} = \begin{cases} 7^2, & \langle d_1(d_1-1)^2\rangle = \langle d_2(d_2-1)^2\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*7}, \\ 7^3, & \text{otherwise.} \end{cases}$$

Proof. Since $A(\mathbb{Q})[7^\infty] \cong (\mathbb{Z}/7\mathbb{Z})^2$ and $A'(\mathbb{Q})[7^\infty] = 0$ we have $B(\mathbb{Q})[7^\infty] \cong \mathbb{Z}/7\mathbb{Z}$, and hence

$$\#\text{coker } \varphi_{\mathbb{Q},\text{tors}} = 1.$$

We know that coker $\eta^\vee_{i,\mathbb{Q},\text{tors}}$ is generated by $d_i(d_i-1)^2$ in $\mathbb{Q}^*/\mathbb{Q}^{*7}$ and as the product of these two cokernels maps surjectively onto coker $\varphi^\vee_{\mathbb{Q},\text{tors}}$ via the map $(x,y) \mapsto x/y$, we conclude that

$$\#\text{coker } \varphi^\vee_{\mathbb{Q},\text{tors}} = \begin{cases} 7, & \langle d_1(d_1-1)^2\rangle = \langle d_2(d_2-1)^2\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*7}, \\ 7^2, & \text{otherwise,} \end{cases}$$

which completes the proof. □

We finish by giving an unconditional example of an abelian surface B over $\mathbb{Q}$ of rank equal to 0, such that $\#Ш(B/\mathbb{Q}) = 7$.

Example 4.15. If $d_1 = u_1/v_1 = 1/3$ and $d_2 = u_2/v_2 = 1/4$, then $\#Ш(B/\mathbb{Q}) = 7$.

Proof. We have $u_1v_1u_2v_2(v_1-u_1)(v_2-u_2) = 2^3 \cdot 3^2$, $u_1 \equiv 5 \cdot v_1 \bmod 7$, $u_2 \not\equiv 5 \cdot v_2 \bmod 7$, and $\gcd(u_1^3 - 8u_1^2v_1 + 5u_1v_1^2 + v_1^3, u_2^3 - 8u_2^2v_2 + 5u_2v_2^2 + v_2^3) = 1$. Hence the local quotient equals $1/7^3$. Both elliptic curves E_i have analytic rank equal to 0, hence we know that $Ш(A/\mathbb{Q})$ and $Ш(B/\mathbb{Q})$ are finite and that the global quotient equals the torsion quotient. For $a = 4$ we have that $d_1^a(d_1-1)^{2a} \equiv 2 \cdot 3^2 \equiv d_2(d_2-1)^2 \bmod \mathbb{Q}^{*7}$, thus the global quotient equals 7^2. We conclude that $7 \cdot \#Ш(A/\mathbb{Q}) = \#Ш(B/\mathbb{Q})$. As in the examples of $\ell = 5$, one can use [Ste09] and [Fis01] to show that $Ш(A/\mathbb{Q})$ is trivial. □

References

[Cas62] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.

[Cas65] J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.

[Fis01] Tom Fisher. Some examples of 5 and 7 descent for elliptic curves over **Q**. *J. Eur. Math. Soc. (JEMS)*, 3(2):169–201, 2001.

[Fla90] Matthias Flach. A generalisation of the Cassels-Tate pairing. *J. Reine Angew. Math.*, 412:113–127, 1990.

[Maz77] Barry Mazur. Modular curves and the eisenstein ideal. *IHES Publ. Math.*, 47:33–186, 1977.

[Mil06] J.S. Milne. *Arithmetic Duality Theorems*. BookSurge, LLC, second edition, 2006.

[PS99] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[Sch96] Edward F. Schaefer. Class groups and Selmer groups. *J. Number Theory*, 56(1):79–114, 1996.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, English edition, 2002.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[SS01] Edward F. Schaefer and Michael Stoll. How to do a p-descent on an elliptic curve. long online version, 2001.

[Ste03] William A. Stein. Possibilities for shafarevich-tate groups of modular abelian varieties, March 2003.

[Ste04] William A. Stein. Shafarevich-Tate groups of nonsquare order. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 277–289. Birkhäuser, Basel, 2004.

[Ste09] William A. Stein. Computational verfication of the birch and swinnerton-dyer conjecture for individual elliptic curves. *Math. Comp.*, 78:2397–2425, 2009.

[Tat63] John Tate. Duality theorems in Galois cohomology over number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 288–295. Inst. Mittag-Leffler, Djursholm, 1963.

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[Tat95] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages 415–440. Soc. Math. France, Paris, 1995.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

Institut für Mathematik, Humboldt-Universität zu Berlin, Unter den Linden 6, D-10099 Berlin, Germany

E-mail address: keil@math.hu-berlin.de