Accepted Manuscript

Examples of non-simple abelian surfaces over the rationals with non-square order Tate-Shafarevich group

Stefan Keil

PII: S0022-314X(14)00157-7
DOI: 10.1016/j.jnt.2014.04.018
Reference: YJNTH 4870

To appear in: *Journal of Number Theory*

Received date: 10 August 2012
Revised date: 24 February 2014
Accepted date: 16 April 2014

Please cite this article in press as: S. Keil, Examples of non-simple abelian surfaces over the rationals with non-square order Tate-Shafarevich group, *J. Number Theory* (2014), http://dx.doi.org/10.1016/j.jnt.2014.04.018

Examples of non-simple abelian surfaces over the rationals with non-square order Tate-Shafarevich group

Stefan Keil[1]

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

Abstract

Let A be an abelian surface over a fixed number field. If A is principally polarised, then it is known that the order of the Tate-Shafarevich group of A must, if finite, be a square or twice a square. For each $k \in \{1, 2, 3, 5, 6, 7, 10, 13\}$ we construct a non-simple non-principally polarised abelian surface $B/\mathbb{Q}$ having Tate-Shafarevich group of order k times a square. To obtain this result, we explore the invariance under isogeny of the Birch and Swinnerton-Dyer conjecture.

Keywords:
Abelian surface, Tate-Shafarevich group, Cassels-Tate equation
2000 MSC: 11G10, 11G07, 11G35

Contents

Email address: `keil@math.hu-berlin.de` (Stefan Keil)
URL: `http://www.mathematik.hu-berlin.de/~keil/` (Stefan Keil)

[1]The author is supported by a scholarship from the Berlin Mathematical School (BMS) and wants to thank the referee for his or her very helpful comments and suggestions.

1. Introduction

Let A/K be an abelian variety over a number field K. Consider its Tate-Shafarevich 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 polarised abelian varieties, this is no longer true in general. Denote by $A^\vee$ the dual abelian variety. The Cassels-Tate pairing [1], [26]

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

which is non-degenerate in case $Ш(A/K)$ is finite, combined with a result of Flach [7], gives a strong restriction on the non-square part of the order of the Tate-Shafarevich group [23, Theorem 1.2].

Theorem 1.1 (Tate, Flach)**.** *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 every polarisation of A/K.*

Corollary 1.2 (Poonen, Stoll)**.** *If A/K is a principally polarised abelian variety, then*

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

More precisely, assuming the finiteness of $Ш(A/K)$, Poonen and Stoll [17] associated to each principal polarisation λ of A/K a canonical element $c \in Ш(A/K)[2]$, and showed that the order of $Ш(A/K)$ is a square if and only if $\langle c, \lambda(c)\rangle = 0$. This is clearly the case if $c = 0$. They showed that $c = 0$ is equivalent to the induced pairing on $Ш(A/K)$ being alternating and also equivalent to the polarisation λ arising from a K-rational divisor. It was already known by Tate [26] that the order of $Ш$ is a square, if such a K-rational divisor exists. In case $c \neq 0$ the induced pairing is anti-symmetric, due to Flach [7].

In 1996, Stoll constructed the first example of an abelian variety having $\#Ш = 2 \cdot \square$; see [22] for some historical remarks. His example was the Jacobian of a genus 2 curve over $\mathbb{Q}$, a principally polarised abelian surface over $\mathbb{Q}$. Thereafter, for every prime $p < 25000$, William Stein [23] constructed an abelian variety $A_p/\mathbb{Q}$ of dimension $p-1$, such that $\#Ш(A_p/\mathbb{Q}) = p \cdot \square$. This result led Stein to make the following conjecture.

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

The following question is then natural.

Question 1.4. *What are the possible non-square parts of the orders of finite Tate-Shafarevich groups for abelian varieties of fixed dimension over a fixed number field? Is this a finite list?*

So far, in the case of abelian surfaces $B/\mathbb{Q}$, the only known square-free positive integers k which equal the non-square part of the order of some $Ш(B/\mathbb{Q})$

are 1, 2, and 3. The purpose of this paper is to extend this list by 5, 6, 7, 10, and 13. The construction we use is an isogeny applied to a product of two elliptic curves, and hence is different from the construction used by Poonen and Stoll, and by Stein. To understand the image of this isogeny we will explore an equation of Cassels and Tate, which is a consequence of the isogeny invariance of the Birch and Swinnerton-Dyer conjecture. The non-square part of the left hand side of this equation will be equal to the non-square part of the order of the Tate-Shafarevich group in question. We will explain how to calculate the right hand side and then we will give explicit examples to prove the following

Theorem 1.5. *For each* $k \in \{1, 2, 3, 5, 6, 7, 10, 13\}$ *there exists a non-simple non-principally polarised abelian surface* $B/\mathbb{Q}$ *such that* $\#Ш(B/\mathbb{Q}) = k \cdot \square$.

The outline of this paper is the following. In the rest of this section we fix notation. In Section 2 we present the aforementioned equation of Cassels and Tate. This equation will break into two parts – a local part and a global part. The remaining part of Section 2 is devoted to explaining the local part and to introduce non-simple abelian surfaces. In Section 3 we will work with elliptic curves possessing a $\mathbb{Q}$-rational N-torsion point. Such curves lead to two parameter families of abelian surfaces and we prove how to calculate the local and global part of the Cassels-Tate equation for these families. Finally, we present explicit calculations and give examples to prove the above theorem.

Notation 1.6. Let A/K be an abelian variety A over a field K, i.e. a proper group scheme of positive dimension which is geometrically integral and of finite type over Spec K. Usually, K is a number field, or a (p-adic) local field, or a finite field. Since all fields considered are perfect we do not pay attention to separability, and with $\overline{K}$ we denote a once and for all fixed algebraic closure of K. For a field L containing K, the group of L-rational points is denoted by $A(L)$, with $\mathcal{O} \in A(L)$ being the identity element of the group law. The dual abelian variety of A/K is denoted by $A^\vee := \mathrm{Pic}^0_{A/K}$ and a polarisation 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 $A/\overline{K}$. If $\varphi : A \to B$ is an isogeny between abelian varieties over a field K, then for a field extension L/K we say that φ has a *L-kernel*, if all points in $A(\overline{K})[\varphi]$ are already defined over L, i.e. $A(\overline{K})[\varphi] = A(L)[\varphi]$. If we do not specify the field of definition of an isogeny φ between two abelian varieties which are defined over a field K, then we want φ to be also defined over K.

If K is a number field, then with v we denote a place 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 $\mathcal{O}_v$ by its maximal ideal $\mathfrak{m}_v = \pi_v \mathcal{O}_v$, for a uniformiser π_v. We normalise the absolute value $|\cdot|_v$ on K_v so that $|\pi_v|_v = (\#k_v)^{-1}$. If $v \in M_K^0$ is a place lying over $p \in M_{\mathbb{Q}}^0$, we denote this by $v|p$ and call K_v a p-adic field. Denote by K_v^{nr} the maximal unramified extension of K_v. It is obtained by adjoining to K_v all n-th roots of unity, for n coprime to the characteristic of k_v.

The absolute Galois group of a field K will be denoted by Gal_K. For Galois cohomology we use the usual abbreviation $H^i(K, M) := H^i(\mathrm{Gal}_K, M)$, for a K-Galois module M. The Tate-Shafarevich group of A/K is defined as

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

With ℓ we denote a prime number 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. We sometimes refer to computations carried out with the software package Sage [25].

2. Controlling the order of Tate-Shafarevich groups modulo squares

We want to construct abelian surfaces $B/\mathbb{Q}$ such that the order of their Tate-Shafarevich groups is not a square. To archieve this objective we start with an abelian surface $A/\mathbb{Q}$ being the product of two elliptic curves E_1 and E_2 over $\mathbb{Q}$. Hence it is known that the order of the Tate-Shafarevich group $Ш(A/\mathbb{Q})$ is a square, provided it is finite. Then we consider cyclic isogenies $\varphi : A \to B$ and the goal is to understand $Ш(B/\mathbb{Q})$ in terms of $Ш(A/\mathbb{Q})$ and φ. The precise situation we consider is summarised in Setting 2.33. The isogeny φ naturally induces a group homomorphism between $Ш(A/\mathbb{Q})$ and $Ш(B/\mathbb{Q})$ which is an isomorphism between ℓ-primary parts for primes ℓ not dividing the degree of the isogeny. In particular this means, that if $Ш(A/K)$ is of square order, then a necessary condition for a prime ℓ to divide the non-square part of the order of $Ш(B/K)$ is that ℓ divides the degree of φ.

In the next subsection we will present the Cassels-Tate equation, which expresses the relative change of the orders of the Tate-Shafarevich groups of A and B under φ. It consists of a local and a global part, which will be called the *local quotient* and the *global quotient*. We will spend the following two subsections computing the local quotient, one for general abelian varieties and one for elliptic curves. The main result is Theorem 2.28. The isogenies constructed in Setting 2.33 are then subsumed into the so-called *isogenies with diagonal kernel* in the last subsection of this chapter. We also introduce the general concept of non-simple abelian surfaces and we present the Key Lemma 2.30 for the computation of the local quotient. In Section 3 we will use the results obtained in this section to actually compute explicit examples of abelian surfaces $B/\mathbb{Q}$ having Tate-Shafarevich group of non-square order.

2.1. An equation of Cassels and Tate

Cassels [2] (the elliptic curve case) and Tate [28] (the general case) proved the following theorem to show the invariance of the Birch and Swinnerton-Dyer conjecture under isogeny. Denote by R_A the regulator and by P_A the period of an abelian variety A/K over a number field K, see pages 37 and 52 in [8]. By $c_{A,v}$ we denote the local Tamagawa number of A at a finite place $v \in M_K^0$.

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 at least one of $Ш(A/K)$ or $Ш(B/K)$ is finite. Then $Ш(A/K)$ and $Ш(B/K)$ are both finite, and*

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

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

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

We may now reformulate the above quotients in terms of these induced group homomorphisms. This reformulation, which is part of the proof of the above theorem, 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, namely

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

and two more interesting ones, see the proof of Theorem I.7.3 in [16];

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

Hence the Cassels-Tate equation becomes

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{\#\ker\varphi_K}{\#\operatorname{coker}\varphi_K}\,\frac{\#\operatorname{coker}\varphi_K^\vee}{\#\ker\varphi_K^\vee} \prod_{v \in M_K} \frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v}. \tag{1}$$

In particular we have

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

and we call the right-hand side of this equation the *global quotient*. The global quotient clearly breaks into the *regulator quotient* and the *torsion quotient*. The product

$$\prod_{v \in M_K} \frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v}$$

runs over all places v of K and is called the *local quotient*. It is in fact a finite product, since $\#\operatorname{coker}\varphi_v = \#\ker\varphi_v$ for all but finitely many places v, as will be recalled in Corollary 2.12. In the next two subsections we will study the local quotient $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$ for a finite place $v \in M_K^0$.

2.2. Isogenies between abelian varieties over local fields

In this section we will use the following notation. Let $\varphi : A \to B$ be an isogeny 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 fixed 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 $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$, which mainly consists in determining the cardinality of $\operatorname{coker}\varphi_v$, as the size of the kernel is usually obvious by the definition of φ. On a few occasions we will focus on isogenies having a K_v-kernel, i.e. $A(\overline{K}_v)[\varphi] = A(K_v)[\varphi]$, and thus $\#\ker\varphi_v = \deg\varphi$ and Gal_{K_v} acts trivially on $A(\overline{K}_v)[\varphi]$.

In general, 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

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

The next lemma determines the size of $H^1(K_v, A(\overline{K}_v)[\varphi])$ and in particular shows that it is finite. Hence $\operatorname{coker}\varphi_v$ is also finite.

Lemma 2.2. *Let K_v be a p-adic field and let M be a finite K_v-Galois module of order $\#M$ and with dual $M^\vee := \mathrm{Hom}(M, \mathbb{G}_m(\overline{K}_v))$. The size of the first cohomology group of M can be computed as follows.*

$$\#H^1(K_v, M) = \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee) \cdot p^{v_p(\#M)\cdot[K_v:\mathbb{Q}_p]}.$$

Proof. This follows from Theorems 2 and 5 in Chapter II.5 in [20]. Define the Euler-Poincaré characteristic by $\chi(K_v, M) := \#H^0(K_v, M) \cdot \#H^2(K_v, M)/\#H^1(K_v, M)$. By the duality Theorem 2 from [20], we get $\#H^2(K_v, M) = \#H^0(K_v, M^\vee)$, and by Theorem 5, we get $\chi(K_v, M) = (\mathcal{O}_v : \#M\mathcal{O}_v)^{-1}$, where $\mathcal{O}_v$ is the valuation ring of K_v. Hence, $\chi(K_v, M) = p^{-v_p(\#M)\cdot[K_v:\mathbb{Q}_p]}$ and we are done. □

Corollary 2.3. *Let φ be of prime degree ℓ. If φ or $\varphi^\vee$ has a K_v-kernel, then*

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

and if neither φ nor $\varphi^\vee$ has a K_v-kernel, then

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

Proof. By definition $H^1(K_v, A(\overline{K}_v)[\varphi])$ is abelian and has exponent ℓ. By the previous lemma, for $M := A(\overline{K}_v)[\varphi]$, we have

$$\#H^1(K_v, M) = \begin{cases} \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee), & v \nmid \ell \\ \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee) \cdot \ell^{[K_v:\mathbb{Q}_p]}, & v \mid \ell. \end{cases}$$

If φ, respectively $\varphi^\vee$, has a K_v-kernel, then $A(\overline{K}_v)[\varphi] \cong \mathbb{Z}/l\mathbb{Z}$, respectively $\boldsymbol{\mu}_\ell$, 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 neither φ nor $\varphi^\vee$ has a K_v-kernel, then neither $A(\overline{K}_v)[\varphi]$ nor its dual is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. 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 2.4.

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

Proof. This is immediate from Corollary 2.3 upon observing 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 $\ell \neq 2$. □

For a finite K_v-module M we will now introduce the unramified Galois cohomolgy group which is an important subgroup of $H^1(K_v, M)$. Denote by K_v^{nr} the maximal unramified extension of K_v. We have that the inertia group $I_v := \mathrm{Gal}_{K_v^{\mathrm{nr}}}$ is a normal subgroup of Gal_{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 defined and by the Inflation-Restriction sequence its kernel is isomorphic to $H^1(\mathrm{Gal}(K_v^{\mathrm{nr}}/K_v), M^{I_v})$. We denote the kernel of $\mathrm{Res}_{\mathrm{nr}}$ by $H^1_{\mathrm{nr}}(K_v, M)$ and call it the *unramified subgroup* of $H^1(K_v, M)$. Consider again the following Galois cohomology sequence with respect to an isogeny $\varphi : A \to B$.

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

We say that $\operatorname{coker} \varphi_v$ is *maximal*, respectively *maximally unramified*, respectively *trivial*, if δ_v is an isomorphism, respectively if δ_v induces an isomorphism between $\operatorname{coker} \varphi_v$ and the unramified subgroup $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$, respectively if $\operatorname{coker} \varphi_v$ is the trivial group.

Remark 2.5. If $K = \mathbb{Q}$ and $(p, \ell) \neq (2, 2)$, the last two corollaries show that if the isogeny $\varphi : A \to B$ is of prime degree ℓ and has a $\mathbb{Q}_p$-kernel, then

$H^1(\mathbb{Q}_p, A(\overline{\mathbb{Q}}_p)[\varphi])$ is either isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ or $(\mathbb{Z}/\ell\mathbb{Z})^2$. In the former case, either $\operatorname{coker}\varphi_p$ is the trivial group, or is isomorphic to $H^1(\mathbb{Q}_p, A(\overline{\mathbb{Q}}_p)[\varphi])$. In the latter case there is a third possibility, namely that $\operatorname{coker}\varphi_p$ has ℓ elements and thus is one of the $\ell+1$ subgroups of $H^1(\mathbb{Q}_p, A(\overline{\mathbb{Q}}_p)[\varphi])$ of order ℓ. By the next lemma, the unramified subgroup is one of these $\ell+1$ subgroups of order ℓ.

Besides merely determing the size of $\operatorname{coker}\varphi_v$ our goal is further to specify it as a subgroup of $H^1(K_v, A(\overline{K}_v)[\varphi])$, and hence the main purpose of this subsection is to give criteria to check whether $\operatorname{coker}\varphi_v$ is maximally unramified.

Lemma 2.6. *Let K_v be a p-adic field and let M be a finite K_v-module. Then the order of $H^1_{\mathrm{nr}}(K_v, M)$ equals the order of $H^0(K_v, M)$.*

Proof. Follows from Lemma 4.2 in [19]. □

We introduce some more notation. 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.

$$\begin{tikzcd} 0 \arrow[r] & A_1(K_v) \arrow[r] \arrow[d, "\varphi_v^1"'] & A_0(K_v) \arrow[r] \arrow[d, "\varphi_v^0"'] & \tilde{\mathcal{A}}_0(k_v) \arrow[r] \arrow[d, "\tilde{\varphi}_v^0"'] & 0 \\ 0 \arrow[r] & B_1(K_v) \arrow[r] & B_0(K_v) \arrow[r] & \tilde{\mathcal{B}}_0(k_v) \arrow[r] & 0 \end{tikzcd} \tag{2}$$

$$\begin{tikzcd} 0 \arrow[r] & A_0(K_v) \arrow[r] \arrow[d, "\varphi_v^0"'] & A(K_v) \arrow[r] \arrow[d, "\varphi_v"'] & A(K_v)/A_0(K_v) \arrow[r] \arrow[d, "\overline{\varphi}_v"'] & 0 \\ 0 \arrow[r] & B_0(K_v) \arrow[r] & B(K_v) \arrow[r] & B(K_v)/B_0(K_v) \arrow[r] & 0 \end{tikzcd} \tag{3}$$

All kernels and cokernels of the vertical maps in the above two diagrams are finite groups. In the unramified case we get the following commutative diagram.

$$\begin{tikzcd} 0 \arrow[r] & A_1(K_v^{\mathrm{nr}}) \arrow[r] \arrow[d, "\varphi_{v,\mathrm{nr}}^1"'] & A_0(K_v^{\mathrm{nr}}) \arrow[r] \arrow[d, "\varphi_{v,\mathrm{nr}}^0"'] & \tilde{\mathcal{A}}_0(\overline{k}_v) \arrow[r] \arrow[d, "\tilde{\varphi}_{\overline{k}_v}^0"'] & 0 \\ 0 \arrow[r] & B_1(K_v^{\mathrm{nr}}) \arrow[r] & B_0(K_v^{\mathrm{nr}}) \arrow[r] & \tilde{\mathcal{B}}_0(\overline{k}_v) \arrow[r] & 0 \end{tikzcd} \tag{4}$$

We recall a basic fact, which follows from Lang's Theorem [13, Theorem 1].

Lemma 2.7. *The finite groups $\tilde{\mathcal{A}}_0(k_v)$ and $\tilde{B}_0(k_v)$ have same cardinalities.*

Proof. The proof is given on page 561 in [13]. □

Now we apply the snake lemma on Diagrams (2) and (3) to get a basic lemma. Recall, that the quantity $c_{A,v}$ is defined as the order of the quotient group $A(K_v)/A_0(K_v)$ and is called the *local Tamagawa number* of A at v.

Lemma 2.8. *With notation as above, we have the equality*

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

Proof. Applying the snake lemma on Diagram (2) we get

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

Since $\#\tilde{\mathcal{A}}_0(k_v) = \#\tilde{B}_0(k_v)$ by Lemma 2.7, we get $\#\ker\tilde{\varphi}_v^0 = \#\operatorname{coker}\tilde{\varphi}_v^0$. Hence $\#\ker\varphi_v^1/\#\operatorname{coker}\varphi_v^1 = \#\ker\varphi_v^0/\#\operatorname{coker}\varphi_v^0$. Diagram (3) leads to

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

By definition $\#\operatorname{coker}\overline{\varphi}_v/\#\ker\overline{\varphi}_v = c_{B,v}/c_{A,v}$, which completes the proof. □

We continue by examining the quotient $\#\operatorname{coker}\varphi_v^1/\#\ker\varphi_v^1$. We start by recalling two basic lemmas, and then we deduce the well known fact that φ_v^1 is an isomorphism for all but finitely many places v.

Lemma 2.9. *The kernel of reduction $A_1(K_v)$ is a pro-p group.*

Proof. The multiplication-by-ℓ endomorphism $[\ell]$ on $A_1(K_v)$ is an isomorphism, for all primes ℓ different to the characteristic p of the residue field k_v, as $A_1(K_v)$ 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 $\mathfrak{m}_v$. Hence for any subgroup G of $A_1(K_v)$, $[\ell]$ is a surjective endomorphism on $A_1(K_v)/G$, for $\ell \neq p$. If in addition $A_1(K_v)/G$ is finite, then $[\ell]$ is an automorphism on $A_1(K_v)/G$, for all $\ell \neq p$, and thus $A_1(K_v)/G$ is a p-group. Hence, $A_1(K_v)$ is a pro-p group. □

Lemma 2.10. *If $v \nmid \deg\varphi$, then φ_v^1 and $\varphi_{v,\mathrm{nr}}^1$ are isomorphisms.*

Proof. Denote the degree of φ by n. There exist isogenies $\psi : B \to A$ and $\rotatebox[origin=c]{180}{ψ} : A \to B$, such that $\psi\circ\varphi : A \to A$ and $\rotatebox[origin=c]{180}{ψ}\circ\psi : B \to B$ are the multiplication-by-n maps $[n]$. Hence we get the following induced group homomorphisms on the kernels of reduction.

$$\begin{tikzcd}
A_1(K_v) \arrow[r, "\varphi_v^1"] \arrow[rr, bend left, "{[n]_v^1}"] & B_1(K_v) \arrow[r, "\psi_v^1"] \arrow[rr, bend right, "{[n]_v^1}"'] & A_1(K_v) \arrow[r, "\rotatebox[origin=c]{180}{ψ}_v^1"] & B_1(K_v)
\end{tikzcd}$$

Since $v \nmid \deg\varphi$, we have by the previous lemma that both maps $[n]_v^1$ are isomorphisms. Hence it follows that all three homomorphisms ψ_v^1, $\rotatebox[origin=c]{180}{ψ}_v^1$ and φ_v^1 are isomorphisms. Now for any finite unramified extension L_w/K_v, we get by the same argument that φ_w^1 is an isomorphism, and so also is $\varphi_{v,\mathrm{nr}}^1$. □

Corollary 2.11. *If a prime ℓ divides the cardinality of a kernel or cokernel of one of the induced group homomorphisms φ_v, φ_v^0, φ_v^1, $\overline{\varphi}_v$ or $\tilde{\varphi}_v^0$ appearing in Diagrams (2) and (3), or ℓ divides the Tamagawa quotient $c_{B,v}/c_{A,v}$, then $\ell \mid \deg\varphi$. Further, if $\gcd(\deg\varphi, c_{A,v} \cdot c_{B,v}) = 1$, then $\overline{\varphi}_v$ is an isomorphism.*

In particular, if φ is of prime degree ℓ, then the cardinalities of all kernels and cokernels of φ_v, φ_v^0, φ_v^1, $\overline{\varphi}_v$ and $\tilde{\varphi}_v^0$, as well as the Tamagawa quotient $c_{B,v}/c_{A,v}$, are powers of ℓ.

We conclude that the product over all quotients $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$ is actually a finite product. Denote by M_K the set of places of K and let S be a finite set of M_K containing the infinite places, the places of bad reduction and the places dividing the degree of the isogeny φ.

Corollary 2.12. *If $v \nmid \deg\varphi$ and v is a place of good reduction, then*

$$\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v} = 1, \quad \textit{and thus} \quad \prod_{v\in M_K}\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v} = \prod_{v\in S}\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v}.$$

Proof. Combine Lemmas 2.8 and 2.10 with the fact that the Tamagawa quotient equals 1 in case of good reduction. □

In view of the corollary, the goal of this subsection is to provide methods to compute the quotient $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$, in case v is a place of bad reduction or $v \mid \deg\varphi$. If we stick to good reduction, but do not care whether v divides the degree of φ, then the next lemma gives a very nice criterion to check whether $\operatorname{coker}\varphi_v$ is maximally unramified. The notation used in part (i) of the lemma comes from the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & A_1(\overline{K}_v) \arrow[r] \arrow[d, "\varphi^1_{\overline{K}_v}"'] & A_0(\overline{K}_v) \arrow[r] \arrow[d, "\varphi^0_{\overline{K}_v}"'] & \tilde{\mathcal{A}}_0(\overline{k}_v) \arrow[r] \arrow[d, "\tilde{\varphi}^0_v"'] & 0 \\
0 \arrow[r] & B_1(\overline{K}_v) \arrow[r] & B_0(\overline{K}_v) \arrow[r] & \tilde{\mathcal{B}}_0(\overline{k}_v) \arrow[r] & 0
\end{tikzcd}$$

Lemma 2.13 (Criterion for maximal unramifiedness of $\operatorname{coker}\varphi_v$ in case v is a place of good reduction)**.** *Assume v is a place of good reduction.*

(i) If $\ker\varphi^1_{\overline{K}_v}$ is trivial, then $\operatorname{coker}\varphi_v$ is maximally unramified.

(ii) If φ has a K_v-kernel and φ_v^1 is injective, then $\operatorname{coker}\varphi_v$ is maximally unramified.

Proof. Part (ii) for $K_v = \mathbb{Q}_p$, $\ell \neq 2$, and A and B are elliptic curves is Lemma A.3 in the Appendix of [4] by Tom Fisher. In general, (ii) follows directly from (i), as the assumptions imply that $\ker\varphi^1_{\overline{K}_v} = \ker\varphi_v^1 = 0$.

For (i) note, that if $[\xi] \in H^1(K_v, A[\varphi])$ is an element of $\operatorname{coker}\varphi_v$, then $[\xi]$ lies in the kernel of $H^1(K_v, A[\varphi]) \to H^1(K_v, A)$. This means that there is a point $P \in A(\overline{K}_v)$, such that $\xi(\sigma) = P^\sigma - P$, for all $\sigma \in \mathrm{Gal}_{K_v}$. As v is a place of good reduction we get that $P \in A_0(\overline{K}_v)$. Consider the reduction-mod-v map $A_0(\overline{K}_v) \to \tilde{\mathcal{A}}_0(\overline{k}_v)$, which is a group homomorphism. Hence, $\overline{P^\tau - P} =$

$\overline{P}^{\tau} - \overline{P} = \mathcal{O}$, for all $\tau \in I_v$, as I_v acts trivially on $\mathcal{A}_0(\overline{k}_v)$. Therefore for all $\tau \in I_v$, $P^{\tau} - P$ lies in the kernel of reduction $\varphi^1_{\overline{K}_v}$. As $\varphi^1_{\overline{K}_v}$ is assumed to be trivial we immediately deduce that $P^{\tau} - P = \mathcal{O}$, for all $\tau \in I_v$, which is equivalent to $P \in A_0(K_v^{\mathrm{nr}})$. By definition, $[\xi]$ lies in $H^1_{\mathrm{nr}}(K_v, A[\varphi])$ if it is in the kernel of $\mathrm{Res}_{\mathrm{nr}}$. This is clearly the case if $P \in A(K_v^{\mathrm{nr}})$, because this makes the restriction of ξ to I_v to be the zero map, and thus $\operatorname{coker} \varphi_v$ injects into $H^1_{\mathrm{nr}}(K_v, A[\varphi])$. By Lemmas 2.6 and 2.8, $\operatorname{coker} \varphi_v$ also surjects onto $H^1_{\mathrm{nr}}(K_v, A[\varphi])$, as its order is at least the order of $H^1_{\mathrm{nr}}(K_v, A[\varphi])$. □

We continue with presenting a reinterpretation of the quotient $\# \operatorname{coker} \varphi^1_v / \# \ker \varphi^1_v$ given by Schaefer in [18]. Using these results it is quite easy to compute $\# \operatorname{coker} \varphi^1_v / \# \ker \varphi^1_v$ for elliptic curves. 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 identity element $\mathcal{O}$. Let $|\varphi'(0)|_v$ be the normalised v-adic absolute value of the determinant of the Jacobian matrix of partial derivatives of such a power series representation of φ evaluated at 0. Note that $|\varphi'(0)|_v$ is well defined.

Proposition 2.14. *With notation as above,*

$$|\varphi'(0)|_v^{-1} = \frac{\# \operatorname{coker} \varphi^1_v}{\# \ker \varphi^1_v}; \quad \textit{and hence } |\varphi'(0)|_v = 1, \ \textit{if } v \nmid \ell.$$

Proof. Combine [18, Lemma 3.8] with Lemmas 2.8 and 2.10. □

Corollary 2.15. *With notation as above,*

$$\frac{\# \operatorname{coker} \varphi_v}{\# \ker \varphi_v} = |\varphi'(0)|_v^{-1} \cdot \frac{c_{B,v}}{c_{A,v}}.$$

Proof. This follows from the last proposition together will Lemma 2.8. □

Remark 2.16. In the case of elliptic curves, $\varphi'(0)$ is just the leading coefficent of the power series representation of φ. One can easily compute this value: Use Vélu's algorithm [29] to describe 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 [21, IV]. We will do this explicitly in Propositions 3.6 and 3.14.

Before we give our main criterion for checking that $\operatorname{coker} \varphi_v$ is maximally unramified we give a basic lemma about $|\varphi'(0)|_v$ and the maps φ^1_v and $\varphi^1_{v,\mathrm{nr}}$. We will consider the ramification index e_v of the place v of K. Note that if $K_v = \mathbb{Q}_p$ and $p \neq 2$, then the condition $e_v < p - 1$ is fulfilled.

Lemma 2.17. *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 the ramification index $e_v < p - 1$, then φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ are injective.

(iii) If $K = \mathbb{Q}$, then φ^1_p and $\varphi^1_{p,\mathrm{nr}}$ are injective, unless $p = 2$ and $2 \mid \deg \varphi$.

(iv) If $K = \mathbb{Q}$ and $|\varphi'(0)|_v = 1$, then φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ are isomorphisms, unless $p = 2$ and $2 \mid \deg \varphi$.

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 $\varphi^1_{v,\mathrm{nr}}$ is injective the maps $\varphi^1_w : A_1(L_w) \to B_1(L_w)$ are also injective. By Proposition 2.14, the size of the kernels and cokernels of φ^1_w agree and therefore they are isomorphisms. Hence $\varphi^1_{v,\mathrm{nr}}$ is an isomorphism, which proves (i).

For (ii) use the isomorphism $A_1(K_v) \cong \hat{A}(\mathfrak{m}_v)$. Then use [21, IV. Theorem 6.1] or the next lemma to conclude that φ^1_w is injective for any finite unramified field extension L_w/K_v. Hence $\varphi^1_{v,\mathrm{nr}}$ is injective.

For (iii) apply (ii) in case $p \neq 2$. In case $2 \nmid \deg \varphi$ this is due to Lemma 2.10. Combing (i) and (iii) gives (iv). □

Lemma 2.18. *If the ramification index $e_v < p - 1$, then the reduction-mod-v map $A_0(K_v) \to \tilde{A}_0(k_v)$ has torsion-free kernel, i.e. $A_1(K_v)$ is torsion-free. In particular, this gives an injection $A(K)_{\mathrm{tors}} \hookrightarrow \tilde{A}_0(k_v)$, thus if in addition v is a place of good reduction there is an injection $A(K)_{\mathrm{tors}} \hookrightarrow \tilde{\mathcal{A}}(k_v)$.*

Proof. This is essentially the content of the Appendix of [9]. □

The next lemma and theorem are a slight generalisation of Lemmas 4.3 and 4.5 of [19]. Theorem 2.20 provides our main criterion to check whether $\operatorname{coker} \varphi_v$ is maximally unramified. To state the lemma we introduce the map

$$\delta^0_v : \operatorname{coker} \varphi^0_v \to H^1(K_v, A(\overline{K}_v)[\varphi]).$$

It is obtained by composing the natural map $\operatorname{coker} \varphi^0_v \to \operatorname{coker} \varphi_v$ from Diagram (3) with the connecting homomorphism $\delta_v : \operatorname{coker} \varphi_v \to H^1(K_v, A(\overline{K}_v)[\varphi])$. Note that since $\operatorname{coker} \varphi^0_v \to \operatorname{coker} \varphi_v$ need not be injective, δ^0_v may also not be injective. Similarly one defines the map

$$\delta^0_{v,\mathrm{nr}} : \operatorname{coker} \varphi^0_{v,\mathrm{nr}} \to H^1(K^{\mathrm{nr}}_v, A(\overline{K}_v)[\varphi]).$$

Lemma 2.19. *If $\varphi^1_{v,\mathrm{nr}}$ is surjective, then the image of $\operatorname{coker} \varphi^0_v$ under δ^0_v lies in $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$.*

Proof. In the above Diagram (4), the first vertical map $\varphi^1_{v,\mathrm{nr}}$ 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. $\operatorname{coker} \varphi^0_{v,\mathrm{nr}}$ is trivial. The following diagram commutes.

$$\begin{tikzcd} \operatorname{coker} \varphi^0_v \arrow[r, "\delta^0_v"'] \arrow[d] & H^1(K_v, A(\overline{K}_v)[\varphi]) \arrow[d, "\mathrm{Res}_{\mathrm{nr}}"'] \\ \operatorname{coker} \varphi^0_{v,\mathrm{nr}} \arrow[r, "\delta^0_{v,\mathrm{nr}}"'] & H^1(K^{\mathrm{nr}}_v, A(\overline{K}_v)[\varphi]) \end{tikzcd}$$

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

Theorem 2.20 (Main criterion for maximal unramifiedness of $\operatorname{coker}\varphi_v$)**.** *If $\varphi^1_{v,\mathrm{nr}}$ is surjective and φ^1_v and $\overline{\varphi}_v$ are isomorphisms, then $\operatorname{coker}\varphi_v$ is maximally unramified.*

Proof. As $\overline{\varphi}_v$ is an isomorphism, $\operatorname{coker}\varphi^0_v \to \operatorname{coker}\varphi_v$ is also an isomorphism, and so by the above lemma we have that $\operatorname{coker}\varphi_v$ 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 $\# H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi]) = \#\ker\varphi_v$ by Lemma 2.6, and $\#\ker\varphi_v = \#\operatorname{coker}\varphi_v$ by Lemma 2.8, as $\overline{\varphi}_v$ and φ^1_v are isomorphisms. □

Our assumptions on φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ in Lemma 2.19 and Theorem 2.20 replaced the assumption $v \nmid \deg\varphi$ in Lemmas 4.3 and 4.5 of [19]. We have seen in Lemma 2.10 that $v \nmid \deg\varphi$ is a stronger assumption, hence we can easily deduce the original result of Schaefer and Stoll.

Corollary 2.21 (Criterion for maximal unramifiedness of $\operatorname{coker}\varphi_v$ in case $v \nmid \deg\varphi$)**.** *If $v \nmid \deg\varphi$ and $\gcd(\deg\varphi, c_{A,v}\cdot c_{B,v}) = 1$ then $\operatorname{coker}\varphi_v$ is maximally unramified.*

Proof. This is Lemma 4.5 of [19]. The corollary follows directly from Theorem 2.20 together with Lemma 2.10 and Corollary 2.11. □

We also want to apply Theorem 2.20 in case $v \mid \deg\varphi$. As already seen in Lemma 2.17 we can replace $v \nmid \deg\varphi$ with the condition that the ramification index $e_v < p-1$ and that $|\varphi'(0)|_v = 1$.

Corollary 2.22 (Criteria for maximal unramifiedness of $\operatorname{coker}\varphi_v$ in case $v \mid \deg\varphi$)**.** *Assume that the ramification index $e_v < p-1$.*

(i) If $|\varphi'(0)|_v = 1$ and $\gcd(\deg\varphi, c_{A,v}\cdot c_{B,v}) = 1$, then $\operatorname{coker}\varphi_v$ is maximally unramified.

(ii) If v is a place of good reduction, then $\operatorname{coker}\varphi_v$ is maximally unramified if and only if $|\varphi'(0)|_v = 1$.

(iii) If v is a place of good reduction and φ has a K_v-kernel, then $|\varphi'(0)|_v = 1$ and $\operatorname{coker}\varphi_v$ is maximally unramified.

Proof. For (i) combine Lemma 2.17 with Theorem 2.20 and Corollary 2.11.

For (ii) note that v being a place of good reduction implies that $c_{A,v} = c_{B,v} = 1$. If $|\varphi'(0)|_v = 1$, then by (i) we get that $\operatorname{coker}\varphi_v$ is maximally unramified. Now assume that $\operatorname{coker}\varphi_v$ is maximally unramified, hence its cardinality equals the cardinality of $\ker\varphi_v$. By Corollary 2.15 we get that $|\varphi'(0)|_v = c_{B,v}/c_{A,v} = 1$, which completes (ii). For (iii), combine (ii) with Lemmas 2.13 and 2.17. □

Corollary 2.23 (Criteria for maximal unramifiedness of $\operatorname{coker}\varphi_p$ in case $K = \mathbb{Q}$)**.** *Let $\varphi : A \to B$ be an isogeny between two abelian varieties A and B over $\mathbb{Q}$ and let p be a prime such that $p \neq 2$ if $2 \mid \deg\varphi$.*

(i) If $|\varphi'(0)|_p = 1$ and $\gcd(\deg\varphi, c_{A,p}\cdot c_{B,p}) = 1$, then $\operatorname{coker}\varphi_p$ is maximally unramified.

(ii) If p is a place of good reduction and φ has a $\mathbb{Q}_p$-kernel, then $|\varphi'(0)|_p = 1$ and $\operatorname{coker}\varphi_p$ is maximally unramified.

Proof. Follows directly from Lemma 2.17, Theorem 2.20, and Corollary 2.22. □

2.3. Isogenies of prime degree between elliptic curves over local fields

Let E and E' be elliptic curves over a p-adic field K_v and let $\eta : E \to E'$ be an isogeny of prime degree ℓ. We will use the notations from Diagrams (2), (3), and (4) with $A = E$ and $B = E'$. Assuming that η has a K_v-kernel, the goal of this subsection is to determine under which further assumptions the reduction type of E at v determines whether $\operatorname{coker} \eta_v$ is maximal, maximally unramified, or trivial. In the case when $K_v = \mathbb{Q}_p$ and $\ell \geq 5$ we can give a complete classification, which will be stated in the main theorem 2.28.

We start with computing the quotient $c_{E'}/c_E$ of Tamagawa numbers with respect to the reduction type at v. In most cases $c_{E'}/c_E$ can easily be computed with Tate's algorithm and the theory of Tate curves. See for example the Appendix of [4] by Tom Fisher or [3, §6 and §9] by Tim and Vladimir Dokchitser.

Lemma 2.24. *Suppose that E/K_v 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 $\overline{\eta}_v$ is an isomorphism, and hence $c_{E'}/c_E = 1$.

Proof. This is standard and follows from Tate's algorithm [27]. □

Lemma 2.25. *Suppose that E/K_v has split multiplicative reduction, then*

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

Proof. This is Lemma A.2 of the appendix of [4] by Tom Fisher. □

Now we study the implications of $\ker \eta_v$ being or not being part of the connected component of the identity $E_0(\overline{K}_v)$. The result is essentially a corollary of Tate's algorithm [27] and explores the fact that η is of prime degree.

Lemma 2.26. *With notation as above, we have:*

(i) If $\ker \eta_v \nsubseteq E_0(\overline{K}_v)$, then η has a K_v-kernel, η_v^1 is an isomorphism, $|\eta'(0)|_v = 1$, $\ell \mid c_E$, and exactly one of the following three cases holds.

1. *E has split multiplicative reduction,*
2. *E has non-split multiplicative reduction and $\ell = 2$,*
3. *E has additive reduction and either $\ell = 2$ or $\ell = 3$.*

(ii) If $\ker \eta_v \subseteq E_0(\overline{K}_v)$, assume additionally that η has a K_v-kernel and that η_v^1 is injective. We have the following implications.

1. *E has multiplicative reduction $\Rightarrow$ $v \nmid \ell$ and $|\eta'(0)|_v = 1$,*
2. *E has split multiplicative reduction $\Rightarrow$ $\boldsymbol{\mu}_\ell \subseteq K_v$,*
3. *E has non-split multiplicative reduction and $\ell \neq 2 \Rightarrow$ $\boldsymbol{\mu}_\ell \nsubseteq K_v$,*
4. *E has additive reduction $\Rightarrow$ $v|\ell$.*

Proof. If $\ker \eta_v$ is trivial, then it is contained in $E_0(\overline{K}_v)$. Hence, $\ker \eta_v \nsubseteq E_0(\overline{K}_v)$ implies that $\ker \eta_v$ is non-trivial, and therefore η has a K_v-kernel as its degree is prime. It also implies that $\eta^0_{\overline{K}_v}$, η^0_v, and thus η^1_v are injective. From the triviality of $\eta^0_{\overline{K}_v}$ is follows that $H^1(K_v, E_0(\overline{K}_v)[\eta])$ is trivial and hence $\operatorname{coker} \eta^0_v$ is also trivial. Thus η^0_v is an isomorphism, and therefore $\tilde{\eta}^0_v$ is surjective. By Lemma 2.7, $\tilde{\eta}^0_v$ is an isomorphism, as its kernel and cokernel have equal cardinalities. This implies that η^1_v is an isomorphism, which gives $|\eta'(0)|_v = 1$ by Proposition 2.14. Again by the fact that η^0_v is an isomorphism, it follows that $\# \ker \overline{\eta}_v = \ell$, which gives that $\ell \mid c_E$. In particular, the reduction type is bad. By [27], c_E is ≤ 2 in the non-split multiplicative case and ≤ 4 in the additive case, giving (i).

For (ii) let $P \in E(K_v)$ be a generator of $\ker \eta_v$. If $\ker \eta_v \subseteq E_0(\overline{K}_v)$ and η has a K_v-kernel, then P generates $\ker \eta^0_v$. Since we assumed η^1_v to be injective, the order of $\overline{P}$ is ℓ. Set $|k_v| =: p^f$. The order of $\overline{P}$ 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 [27, §7]. Therefore we get the following implications:

1. multiplicative $\Rightarrow\ p^f \not\equiv 0 \bmod \ell \ \Rightarrow\ p \neq \ell \ \Rightarrow\ v \nmid \ell$,
2. split $\Rightarrow\ p^f \equiv 1 \bmod \ell \ \Rightarrow\ \boldsymbol{\mu}_\ell \subseteq k_v \ \Rightarrow\ \boldsymbol{\mu}_\ell \subseteq K_v$,
3. non-split and $\ell \neq 2 \Rightarrow\ p^f \not\equiv 0, 1 \bmod \ell \Rightarrow\ \boldsymbol{\mu}_\ell \nsubseteq k_v \Rightarrow\ \boldsymbol{\mu}_\ell \nsubseteq K_v$,
4. additive $\Rightarrow\ p^f \equiv 0 \bmod \ell \ \Rightarrow\ p = \ell, \ \Rightarrow\ v \mid \ell$.

By Proposition 2.14, $v \nmid \ell$ implies $|\eta'(0)|_v = 1$, which completes (ii). □

We summarise the case of multiplicative reduction and state under which further assumptions $\operatorname{coker} \eta_v$ is trivial, maximally unramified, or maximal.

Corollary 2.27 (Criteria to classify $\operatorname{coker} \eta_v$ is case of multiplicative reduction)**.** *Suppose the reduction type of E/K_v is split multiplicative.*

(i) If $\ker \eta_v \nsubseteq E_0(\overline{K}_v)$, then $|\eta'(0)|_v = 1$ and $\operatorname{coker} \eta_v$ is trivial.

(ii) If $\ker \eta_v \subseteq E_0(\overline{K}_v)$, η has a K_v-kernel, and η^1_v is injective, then $v \nmid \ell$, $\boldsymbol{\mu}_\ell \subseteq K_v$, $|\eta'(0)|_v = 1$, and $\operatorname{coker} \eta_v$ is maximal.

Suppose the reduction type of E/K_v is non-split multiplicative.

(iii) If $\ell \neq 2$, η has a K_v-kernel, and η^1_v is injective, then $v \nmid \ell$, $\boldsymbol{\mu}_\ell \nsubseteq K_v$, $|\eta'(0)|_v = 1$ and $\operatorname{coker} \eta_v$ is maximally unramified.

(iv) If $\ell = 2$, $v \nmid \ell$, and η has a K_v-kernel, then $\boldsymbol{\mu}_\ell \subseteq K_v$ and $|\eta'(0)|_v = 1$. Further $\operatorname{coker} \eta_v$ is trivial if $c_{E'}/c_E = 1/2$, $\operatorname{coker} \eta_v$ is maximal if $c_{E'}/c_E = 2$, and $\operatorname{coker} \eta_v$ is maximally unramified if $c_E = c_{E'} = 1$.

Proof. Lemma 2.26 already contains everything of (i)-(iii) but the statement whether $\operatorname{coker} \eta_v$ is trivial, maximally unramified, or maximal. In (iv) we get $|\eta'(0)|_v = 1$ and $\boldsymbol{\mu}_\ell \subseteq K_v$, as $v \nmid \ell$ and $\ell = 2$. It remains to classify $\operatorname{coker} \eta_v$.

By Corollary 2.15 we obtain the equation $\# \operatorname{coker} \eta_v = \ell \cdot c_{E'}/c_E$. The size of $H^1(K_v, E(\overline{K}_v)[\eta])$ is given by Corollary 2.4, and $c_{E'}/c_E$ in (i)-(iii) can be computed with Lemmas 2.24 and 2.25. This shows triviality of $\operatorname{coker} \eta_v$ in (i) and the first case in (iv), and maximality in all other cases but the third case of (iv). Note that in (iii), $H^1(K_v, E(\overline{K}_v)[\eta])$ equals the unramified subgroup. To get the maximal unramifiedness in the third part of (iv) use Corollary 2.21. □

We finish with the main theorem of this subsection. Recall that we call $\operatorname{coker}\eta_p$ *maximal* if it equals the full $H^1(\mathbb{Q}_p, E(\overline{\mathbb{Q}}_p)[\eta])$, and *maximally unramified* if it equals the unramified subgroup $H^1_{\mathrm{nr}}(\mathbb{Q}_p, E(\overline{\mathbb{Q}}_p)[\eta])$; see the discussion before Remark 2.5. The definition of $|\eta'(0)|_p$ is given before Proposition 2.14 and having a $\mathbb{Q}_p$-kernel means that $E(\overline{\mathbb{Q}}_p)[\eta] = E(\mathbb{Q}_p)[\eta]$.

Theorem 2.28 (Criteria to classify $\operatorname{coker}\eta_p$ is case η has a $\mathbb{Q}_p$-kernel and is of prime degree)**.** *Let E and E' be elliptic curves over $\mathbb{Q}_p$ and let $\eta : E \to E'$ be an isogeny of prime degree ℓ, and assume that η has a $\mathbb{Q}_p$-kernel. Then the left column of the table below implies the two columns to the right, and in all but the last row we also get that $|\eta'(0)|_p = 1$.*

reduction type of $E/\mathbb{Q}_p$, plus further assumptions	*$p =$ or $\neq \ell$, $\boldsymbol{\mu}_\ell \subseteq$ or $\nsubseteq \mathbb{Q}_p$*	$\operatorname{coker}\eta_p$ *is*
split multiplicative, $\ker\eta_p \nsubseteq E_0(\overline{\mathbb{Q}}_p)$	*no implications*	*trivial*
split multipl., $\ker\eta_p \subseteq E_0(\overline{\mathbb{Q}}_p)$, $p \neq 2$ *or* $\ell \neq 2$	$p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p$	*maximal*
non-split multiplicative, $\ell \neq 2$	$p \neq \ell, \boldsymbol{\mu}_\ell \nsubseteq \mathbb{Q}_p$	*max. unramified*
non-split multiplicative, $\ell = 2 \neq p$, $c_{E'}/c_E = 1/2$	$p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p$	*trivial*
non-split multiplicative, $\ell = 2 \neq p$, $c_{E'}/c_E = 2$	$p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p$	*maximal*
non-split multiplicative, $\ell = 2 \neq p$, $c_E = c_{E'} = 1$	$p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p$	*max. unramified*
good, $p \neq 2$ *or* $\ell \neq 2$	*no implications*	*max. unramified*
additive, $\ell \geq 5$, $\lvert\eta'(0)\rvert_p = 1$	$p = \ell, \boldsymbol{\mu}_\ell \nsubseteq \mathbb{Q}_p$	*max. unramified*
additive, $\ell \geq 5$, $\lvert\eta'(0)\rvert_p \neq 1$	$p = \ell, \boldsymbol{\mu}_\ell \nsubseteq \mathbb{Q}_p$	*maximal*

Proof. For all but the first row of the table we use Lemma 2.17 to deduce that η_p^1 is injective. Then the six cases of multiplicative reduction are contained in the last corollary and the case of good reduction is covered by Lemma 2.13.

In the additive case, due to $\ell \geq 5$, we get that $p = \ell$ by Lemma 2.26 and hence $\boldsymbol{\mu}_\ell \nsubseteq \mathbb{Q}_p$. This implies that $\#H^1(\mathbb{Q}_p, E(\overline{\mathbb{Q}}_p)[\eta]) = \ell^2$ by Corollary 2.4. Further $\overline{\eta}_p$ is an isomorphism by Lemma 2.24 and thus by Corollary 2.15 we have $\#\operatorname{coker} = \ell \cdot |\eta'(0)|_p^{-1}$. We know that $|\eta'(0)|_p^{-1} \geq 1$, as η_p^1 is injective. Hence, there are two possibilities. Firstly, $\#\operatorname{coker}\eta_p = \ell$, which is equivalent to $|\eta'(0)|_p = 1$, and secondly, $\#\operatorname{coker}\eta_p = \ell^2$, which is equivalent to $|\eta'(0)|_p \neq 1$, and which implies that $\operatorname{coker}\eta_p$ is maximal. It remains to show that $\operatorname{coker}\eta_p$ is maximally unramified in case the reduction type is additive and $|\eta'(0)|_p = 1$. At this point we apply Theorem 2.20, which is possible due to Lemma 2.17. □

2.4. Non-simple abelian varieties and isogenies with diagonal kernel

In this subsection K will always denote a field of characteristic 0. An abelian variety B/K is called *non-simple* if it is isogenous to a product of two abelian varieties A_1/K and A_2/K, i.e. there is an isogeny $\varphi : A_1 \times A_2 \to B$.

Recall, that we want all isogenies to be defined over K, too. Let A_1, A_2 and B be abelian varieties over a field K and let $\varphi : A_1 \times A_2 \to B$ be an isogeny. We say that φ has *diagonal kernel*, or simply say that φ is *diagonal*, if there is a finite group scheme G over K contained in both A_i, together with fixed embeddings $\iota_i : G \hookrightarrow A_i$, such that the kernel of φ is the embedding of G into the product $A_1 \times A_2$ via $\iota_1 \times \iota_2$. We denote the image of G in A_i by $G_i := \iota_i(G)$. Clearly, G, G_1, and G_2 are pairwise isomorphic as finite group schemes and the $\overline{K}$-rational points of G_1 and G_2 form isomorphic Galois modules; hence there is a Galois equivariant isomorphism $\alpha : G_1 \to G_2$ such that $\iota_2 = \alpha \circ \iota_1$ and that $\ker \varphi$ equals the graph of α. Further, both A_i possess an isogeny $\eta_i : A_i \to A_i'$ which is defined through its kernel by setting $\ker \eta_i := G_i$ and $A_i' := A_i/G_i$.

Now we state a basic lemma about Galois cohomology and then we present our Key Lemma to controll the local quotient for isogenies with diagonal kernel.

Lemma 2.29. *Let K be a field and let G_1 and G_2 be two finite K-Galois modules. Assume $\alpha : G_1 \to G_2$ is a Galois equivariant homomorphism. Then*

$$\alpha^* : H^1(K, G_1) \to H^1(K, G_2), \quad [\xi] \mapsto [\alpha \circ \xi],$$

is a well-defined group homomorphism. If in addition α is an isomorphism, then α^* is an isomorphism, too. Further, the isomorphism α^* respects the Inflation-Restriction sequence, i.e. for any Galois extension L/K, α^* induces isomorphisms $H^1(\mathrm{Gal}(L/K), G_1^{\mathrm{Gal}_L}) \to H^1(\mathrm{Gal}(L/K), G_2^{\mathrm{Gal}_L})$ and $H^1(L, G_1) \to H^1(L, G_2)$ which commute with the Inflation-Restriction sequence.

In particular, if $K = K_v$ is a local field, for every Galois equivariant isomorphism $\alpha : G_1 \to G_2$, the isomorphism $\alpha^* : H^1(K_v, G_1) \to H^1(K_v, G_2)$ induces an isomorphism between $H^1_{\mathrm{nr}}(K_v, G_1)$ and $H^1_{\mathrm{nr}}(K_v, G_2)$.

Proof. Follows directly from the functoriality of Galois cohomology. $\square$

Lemma 2.30 (Key Lemma to compute the local quotient for isogenies with diagonal kernel)**.** *Let A_1 and A_2 be two abelian varieties over a number field K and let $\varphi : A_1 \times A_2 \to B$ be an isogeny with diagonal kernel. Denote by $\eta_i : A_i \to A_i'$ the isogenies for which there is a Galois equivariant isomorphism $\alpha : \ker \eta_1 \to \ker \eta_2$ whose graph equals $\ker \varphi$. Let $v \in M_K^0$ be a finite place of K.*

(i) $\operatorname{coker} \varphi_v$ is maximal if $\operatorname{coker} \eta_{1,v}$ and $\operatorname{coker} \eta_{2,v}$ are both maximal.

(ii) $\operatorname{coker} \varphi_v$ is trivial if either $\operatorname{coker} \eta_{1,v}$ or $\operatorname{coker} \eta_{2,v}$ is trivial.

(iii) $\operatorname{coker} \varphi_v$ is maximally unramified if either $\operatorname{coker} \eta_{1,v}$ or $\operatorname{coker} \eta_{2,v}$ is maximally unramified and the other one is maximally unramified or maximal.

Proof. Define the two Galois equivariant isomorphisms $\gamma_1 := (id, \alpha) : \ker \eta_1 \to \ker \varphi$ and $\gamma_2 := (\alpha^{-1}, id) : \ker \eta_2 \to \ker \varphi$. By the above lemma we get two group isomorphisms $\gamma_i^* : H^1(K_v, A_i[\eta_i]) \to H^1(K_v, (A_1 \times A_2)[\varphi])$. For $[\xi] \in H^1(K_v, (A_1 \times A_2)[\varphi])$ denote by $[\xi_1]$, respectively $[\xi_2]$, the preimage under γ_1^*, respectively γ_2^*. Thus $\xi(\sigma) = (\xi_1(\sigma), \xi_2(\sigma))$, for all $\sigma \in \mathrm{Gal}_{K_v}$. It follows that

$$[\xi] \in \operatorname{coker} \varphi_v \;\Leftrightarrow\; [\xi_1] \in \operatorname{coker} \eta_{1,v} \text{ and } [\xi_2] \in \operatorname{coker} \eta_{2,v}, \tag{5}$$

since both assertions are equivalent to the existence of $P_1 \in A_1(\overline{K}_v)$ and $P_2 \in A_2(\overline{K}_v)$, such that for all $\sigma \in \mathrm{Gal}_{K_v}$ we have $\xi_1(\sigma) = P_1^\sigma - P_1$ and $\xi_2(\sigma) = P_2^\sigma - P_2$. For (ii), recall that $[\xi]$ is the trivial class if and only if $[\xi_1]$ and $[\xi_2]$ are both the trivial class. For (iii) use the above lemma again to get that

$[\xi] \in H^1_{\mathrm{nr}}(K_v, (A_1 \times A_2)[\varphi])$ if and only if $[\xi_1] \in H^1_{\mathrm{nr}}(K_v, A_1[\eta_1])$ and $[\xi_2] \in H^1_{\mathrm{nr}}(K_v, A_2[\eta_2])$. Now everything follows directly from (5). □

Remark 2.31. The Key Lemma shows that if one knows whether $\operatorname{coker} \eta_{1,v}$ and $\operatorname{coker} \eta_{2,v}$ are maximal, maximally unramified, or trivial, then one knows whether $\operatorname{coker} \varphi_v$ is maximal, maximally unramified, or trivial. For all examples of cyclic isogenies $\varphi : E_1/\mathbb{Q} \times E_2/\mathbb{Q} \to B/\mathbb{Q}$ we consider we will compute $\operatorname{coker} \varphi_p$ by first computing $\operatorname{coker} \eta_{i,p}$ and then applying the Key Lemma.

For fixed abelian varieties A_1/K and A_2/K and fixed isomorphic finite subgroup schemes $G_1/K \subset A_1$ and $G_2/K \subset A_2$, we can define an isogeny $\varphi : A_1 \times A_2 \to B$ with diagonal kernel by setting the kernel of φ to be equal to the graph of α. Note that φ and B depend on the choice of α, which we may denote by φ_α and B_α to emphasise it. We will now show that the order of $Ш(B_\alpha/K)$ is independent of the choice of α if φ is a cyclic isogeny.

Proposition 2.32. *Let A_1 and A_2 be two abelian varieties over a number field K, such that there are isomorphic finite cyclic K-subgroup schemes $G_1 \subseteq A_1$ and $G_2 \subseteq A_2$. Choose a Galois equivariant isomorphism $\alpha : G_1 \to G_2$ and let $\varphi_\alpha : A_1 \times A_2 \to B_\alpha$ be the cyclic isogeny with diagonal kernel such that* $\ker \varphi_\alpha$ *equals the graph of α. Then $\#Ш(B_\alpha/K)$ is independent of the choice of α.*

Proof. Consider the Cassels-Tate equation

$$\frac{\#Ш(A_1 \times A_2/K)}{\#Ш(B_\alpha/K)} = \frac{\#\ker \varphi_{\alpha,K}}{\#\operatorname{coker} \varphi_{\alpha,K}} \frac{\#\operatorname{coker} \varphi^\vee_{\alpha,K}}{\#\ker \varphi^\vee_{\alpha,K}} \prod_{v \in M_K} \frac{\#\operatorname{coker} \varphi_{\alpha,v}}{\#\ker \varphi_{\alpha,v}}.$$

We will show that the cardinality of all occurring kernels and cokernels on the right hand side are independent of α. The set of $\overline{K}$-rational points of the kernels of the isogenies $\varphi_\alpha : A_1 \times A_2 \to B_\alpha$ and $\varphi_\alpha^\vee : B_\alpha^\vee \to A_1^\vee \times A_2^\vee$ depend on α. But the isomorphism class of $\ker \varphi_\alpha$ and of $\ker \varphi_\alpha^\vee$ as a Galois module is fixed, hence it is clear that the size of all occurring kernels in the Cassels-Tate equation are unaffected by α. It remains to consider the cokernels.

Fix two Galois equivariant isomorphisms $\alpha, \alpha' : G_1 \to G_2$. Then there is a Galois equivariant automorphism β_2 of G_2, such that $\alpha' = \beta_2 \circ \alpha$. The Galois equivariant automorphism $\gamma_2 := id \times \beta_2$ of $G_1 \times G_2$ induces a Galois equivariant isomorphism between $\ker \varphi_\alpha$ and $\ker \varphi_{\alpha'}$. As G_2 is cyclic, the automorphism β_2 is multiplication by some factor, hence there is an endomorphism B_2 of A_2 such that the restriction of B_2 to G_2 equals β_2. The following diagram has exact rows and commutes, with $id \times B_2$ and $[id \times B_2]$ being isogenies.

$$\begin{tikzcd}
0 \arrow[r] & \ker \varphi_\alpha \arrow[r] \arrow[d, "\gamma_2"'] & A_1 \times A_2 \arrow[r, "\varphi_\alpha"] \arrow[d, "id \times B_2"'] & B_\alpha \arrow[r] \arrow[d, "{[id \times B_2]}"'] & 0 \\
0 \arrow[r] & \ker \varphi_{\alpha'} \arrow[r] & A_1 \times A_2 \arrow[r, "\varphi_{\alpha'}"] & B_{\alpha'} \arrow[r] & 0
\end{tikzcd}$$

Applying Galois cohomology yields the following commutative diagram with exact rows, where L is either the number field K or one of its completions K_v.

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{coker}\varphi_{\alpha,L} \arrow[r] \arrow[d] & H^1(L,\ker\varphi_\alpha) \arrow[r, "\iota^1_\alpha"] \arrow[d, "\gamma_2^*"] & H^1(L, A_1\times A_2) \arrow[r] \arrow[d, "(id\times B_2)^*"] & \dots \\
0 \arrow[r] & \operatorname{coker}\varphi_{\alpha',L} \arrow[r] & H^1(L,\ker\varphi_{\alpha'}) \arrow[r, "\iota^1_{\alpha'}"] & H^1(L, A_1\times A_2) \arrow[r] & \dots
\end{tikzcd}$$

The homomorphism γ_2^* is an isomorphism by Lemma 2.29. As the diagram commutes we get that γ_2^* induces an injection $\ker\iota^1_\alpha \hookrightarrow \ker\iota^1_{\alpha'}$. Switching the roles of α and α' gives an injection $\ker\iota^1_{\alpha'} \hookrightarrow \ker\iota^1_\alpha$. Thus $\operatorname{coker}\varphi_{\alpha,L}$ and $\operatorname{coker}\varphi_{\alpha',L}$ have same cardinality. Now consider the dual picture, where $\gamma_2^\vee$ is an isomorphism making the diagram commutative.

$$\begin{tikzcd}
0 \arrow[r] & \ker\varphi^\vee_{\alpha'} \arrow[r] \arrow[d, "\gamma_2^\vee"] & B^\vee_{\alpha'} \arrow[r, "\varphi^\vee_{\alpha'}"] \arrow[d, "{[id\times B_2]^\vee}"] & A_1^\vee\times A_2^\vee \arrow[r] \arrow[d, "id\times B_2^\vee"] & 0 \\
0 \arrow[r] & \ker\varphi^\vee_{\alpha} \arrow[r] & B^\vee_{\alpha} \arrow[r, "\varphi^\vee_{\alpha}"] & A_1^\vee\times A_2^\vee \arrow[r] & 0
\end{tikzcd}$$

With the same argument as before, one gets a bijection between $\operatorname{coker}\varphi^\vee_{\alpha,K}$ and $\operatorname{coker}\varphi^\vee_{\alpha',K}$ and thus they also have the same number of elements. $\square$

Now we have a look at the special case of A_1 and A_2 being elliptic curves E_1 and E_2 over $\mathbb{Q}$, i.e. we focus on non-simple abelian surfaces $B/\mathbb{Q}$.

Setting 2.33. Let N be a positive integer and let E_1 and E_2 be two elliptic curves over $\mathbb{Q}$, each having a $\mathbb{Q}$-rational point P_i of exact order N. The point P_i generates a finite subgroup scheme $G_i := \langle P_i\rangle$ in E_i. Denote by $E_i' := E_i/G_i$ the quotient and by $\eta_i : E_i \to E_i'$ the corresponding quotient isogeny. Define in $E_1\times E_2$ the finite subgroup scheme $\tilde{G} := \langle (P_1, nP_2)\rangle$, for some $n \in (\mathbb{Z}/N\mathbb{Z})^*$. Let $B := (E_1\times E_2)/\tilde{G}$ be the quotient and denote the corresponding isogeny by $\varphi : E_2\times E_2 \to B$. Hence, φ is a cyclic N-isogeny with diagonal kernel. Further, φ has a $\mathbb{Q}$-kernel and thus φ_p has a $\mathbb{Q}_p$-kernel for every place p of $\mathbb{Q}$. Denote by $\eta_1\times\eta_2 : E_1\times E_2 \to E_1'\times E_2'$ the isogeny having as kernel $G_1\times G_2$. We let $\psi : B \to E_1'\times E_2'$ be the isogeny satisfying $\eta_1\times\eta_2 = \psi\circ\varphi$. As elliptic curves are principally polarised, we have $E_1\times E_2 \cong (E_1\times E_2)^\vee$ and $E_1'\times E_2' \cong (E_1'\times E_2')^\vee$.

$$\begin{tikzcd}
 & B \arrow[dr, "\psi"] & \\
A = E_1\times E_2 \arrow[ur, "\varphi"] \arrow[rr, bend left, "\eta_1\times\eta_2"] & & A' = E_1'\times E_2' \arrow[dl, "\psi^\vee"] \arrow[ll, bend left, "\eta_1^\vee\times\eta_2^\vee"] \\
 & B^\vee \arrow[ul, "\varphi^\vee"] &
\end{tikzcd}$$

By construction $\ker\eta_1 \cong \ker\eta_2 \cong \ker\varphi \cong \mathbb{Z}/N\mathbb{Z}$, therefore $\ker(\eta_1\times\eta_2) \cong \mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$ and $\ker\psi \cong \mathbb{Z}/N\mathbb{Z}$. Applying Cartier duality, we get $\ker\eta_1^\vee \cong \ker\eta_2^\vee \cong \ker\varphi^\vee \cong \ker\psi^\vee \cong \boldsymbol{\mu}_N$ and $\ker(\eta_1^\vee\times\eta_2^\vee) \cong \boldsymbol{\mu}_N\times\boldsymbol{\mu}_N$.

Remark 2.34. (i) Let G be a finite group scheme being isomorphic to the isomorphic group schemes G_1 and G_2, i.e. $G \cong \mathbb{Z}/N\mathbb{Z}$. Fix a generating point P, i.e. $G = \langle P \rangle$. Then there are natural embeddings ι_i of G into E_i with image G_i given by $\iota_1(P) := P_1$ and $\iota_2(P) := nP_2$, such that $\tilde{G}$ is the embedding of G into $E_1 \times E_2$ with respect to $\iota_1 \times \iota_2$. The Galois equivariant isomorphism $\alpha : G_1 \to G_2$ fulfilling the condition $\iota_2 = \alpha \circ \iota_1$ is defined by $P_1 \mapsto nP_2$. In other words the choice of n is equivalent to the choice of α. As we have seen in Proposition 2.32, the order of $Ш(B/\mathbb{Q})$ is indendent of that choice.

(ii) Due to Mazur's classification of possible torsion points of elliptic curves over $\mathbb{Q}$, see Theorem 7.5 in [21] or [14] and [15], the only possible values for N in Setting 2.33 are $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$.

(iii) If $\#Ш(B/\mathbb{Q}) = k \cdot \square$, with k square-free, then k has to divide N. Thus, the only possible values for k that one can obtain with Setting 2.33 are $k = 1, 2, 3, 5, 6, 7, 10$. In the next section we will see that indeed all these values for k are possible.

The next lemma tells us that the abelian surface $B/\mathbb{Q}$ from Setting 2.33 has the interesting property that every polarisation it possesses has degree divisible by ℓ, in case $\deg \varphi = N = \ell$ is a prime and E_1 and E_2 are not isogenous. The proof we present follows a sketch of Brian Conrad.

Lemma 2.35. *Let K be a field and let E_1 and E_2 be two non-isogenous elliptic curves over K. Let G be a finite cyclic group scheme of prime order ℓ over K together with fixed embeddings $\iota_1 : G \hookrightarrow E_1$ and $\iota_2 : G \hookrightarrow E_2$. Thus the map $\iota_1 \times \iota_2$ is a diagonal embedding of G into the product $E_1 \times E_2$. Denote its image in $E_1 \times E_2$ by $\tilde{G}$. Then any polarisation of the quotient $B := (E_1 \times E_2)/\tilde{G}$ has degree divisible by ℓ.*

Proof. Set $A := E_1 \times E_2$ and let $\lambda : B \to B^\vee$ be any polarisation and consider the quotient map $\varphi : A \to B$ and its dual $\varphi^\vee : B^\vee \to A^\vee = A$. The composition

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

is a polarisation of A. Let $\mathrm{em}_i : E_i \hookrightarrow A$ be the natural embedding of E_i into the product, and $\mathrm{pr}_i : A \to E_i$ the natural projection. Define homomorphisms

$$\Psi_1 : E_1 \xrightarrow{\mathrm{em}_1} A \xrightarrow{\Psi} A \xrightarrow{\mathrm{pr}_1} E_1 \quad \text{and} \quad \Psi_2 : E_2 \xrightarrow{\mathrm{em}_2} A \xrightarrow{\Psi} A \xrightarrow{\mathrm{pr}_2} E_2.$$

We claim that $\Psi = \Psi_1 \times \Psi_2$. The claim is equivalent to $\mathrm{pr}_2 \circ \Psi \circ \mathrm{em}_1 : E_1 \to E_2$ and $\mathrm{pr}_1 \circ \Psi \circ \mathrm{em}_2 : E_2 \to E_1$ being the zero map. By assumption E_1 and E_2 are non-isogenous, hence the only homomorphism between them is the zero map, which gives the claim.

Now we proceed as follows: for $i = 1$ and $i = 2$ we get that Ψ_i is a polarisation of E_i having $\iota_i(G)$ in its kernel. As the degree of a polarisation is always a square and ℓ is a prime we get that ℓ^2 divides the degree of Ψ_1 and of Ψ_2. Therefore, ℓ^4 divides the degree of Ψ. We conclude that ℓ^2 divides the degree of the polarisation λ, as $\deg \Psi = \deg \varphi \cdot \deg \lambda \cdot \deg \varphi^\vee = \ell^2 \cdot \deg \lambda$, which completes the proof. $\square$

Now we give a remark which says that it is enough to be able to compute the Cassels-Tate equation for isogenies of prime power degree. This enables us to deal with Setting 2.33 for the composite cases $N = 6$ and $N = 10$.

Remark 2.36. Let A and B be abelian varieties over a field K and let $\varphi : A \to B$ be an isogeny. Denote by $\prod_i \ell_i^{e_i}$ the prime factorisation of $\deg \varphi$, with the ℓ_i being pairwise different primes. The ℓ_i-primary part of the $\overline{K}$-rational points of $\ker \varphi$ forms a Galois invariant subgroup. Hence for each ℓ_i, φ factors through an isogeny $\varphi_{\ell_i} : A \to B_{\ell_i}$ of degree $\ell_i^{e_i}$ by defining $\ker \varphi_{\ell_i}$ to be the subgroup scheme of $\ker \varphi$ of order $\ell_i^{e_i}$. Therefore, there is an isogeny $\psi_{\ell_i} : B_{\ell_i} \to B$ of degree coprime to ℓ_i, such that $\varphi = \psi_{\ell_i} \circ \varphi_{\ell_i}$. Thus, the ℓ_i-primary parts of $Ш(B_{\ell_i}/K)$ and $Ш(B/K)$ are isomorphic. For the dual isogeny we get an analogous decomposition $\varphi^\vee = \psi_{\ell_i}^\vee \circ \varphi_{\ell_i}^\vee$. Note that $\varphi_{\ell_i}^\vee := (\varphi^\vee)_{\ell_i} \neq (\varphi_{\ell_i})^\vee$. Now let K be a number field. Hence, in order to compute the Cassels-Tate equation (1) for φ it suffices to compute all the Cassels-Tate equations for the φ_{ℓ_i}. As the degrees of all φ_{ℓ_i} are pairwise coprime we get that

$$\frac{\#\ker \varphi_K}{\#\operatorname{coker} \varphi_K} = \prod_i \frac{\#\ker \varphi_{\ell_i,K}}{\#\operatorname{coker} \varphi_{\ell_i,K}}, \quad \frac{\#\operatorname{coker} \varphi_K^\vee}{\#\ker \varphi_K^\vee} = \prod_i \frac{\#\operatorname{coker} \varphi_{\ell_i,K}^\vee}{\#\ker \varphi_{\ell_i,K}^\vee},$$

$$\frac{\#\operatorname{coker} \varphi_v}{\#\ker \varphi_v} = \prod_i \frac{\#\operatorname{coker} \varphi_{\ell_i,v}}{\#\ker \varphi_{\ell_i,v}}.$$

In case $\varphi : A_1 \times A_2 \to B$ is an isogeny with diagonal kernel then all the φ_{ℓ_i} also have diagonal kernel.

3. Constructing non-simple abelian surfaces over $\mathbb{Q}$ with non-square order Tate-Shafarevich groups using elliptic curves with a rational N-torsion point

In this section we will construct non-simple non-principally polarised abelian surfaces $B/\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = k \cdot \square$, for $k = 1, 2, 3, 5, 6, 7, 10$. All these examples are obtained via an isogeny $\varphi : E_1 \times E_2 \to B$ as constructed in Setting 2.33 with respect to $\deg \varphi = N = 5, 6, 7, 10$. The elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have a $\mathbb{Q}$-rational N-torsion point, thus they correspond to points on the modular curve $X_1(N)$. The genus of $X_1(N)$ equals 0 if and only if $N = 1, \ldots, 10, 12$. In this case the set of $\mathbb{Q}$-rational points of $X_1(N)$ is non-empty, hence there are infinitely many elliptic curves over $\mathbb{Q}$ possessing a $\mathbb{Q}$-rational point of order N and these curves can be parametrised by a rational number $d \in \mathbb{Q}$. The parametisations we use can be found in Proposition 1.1.2 of [11] and Section 6 of [12]. The goal is to express the local and the global quotient of the Cassels-Tate equation (1) with respect to such a parametrisation, i.e. with respect to two rational numbers d_1 and d_2, which represent the two elliptic curves E_1 and E_2. Therefore, for fixed N we will look at a two parameter family of abelian surfaces $B/\mathbb{Q}$.

In the first two subsections we will compute the local and the global quotient of the Cassels-Tate equation (1) with respect to Setting 2.33 with a focus on

N being a prime number ℓ. We provide a formula which computes the local quotient with respect to the reduction type of E_1 and E_2 at the primes p. Further, we explain how to obtain two functions with which one can compute the global quotient as long as Mordell-Weil bases for E_1 and E_2 are known.

In the two prime cases $N = 5$ and $N = 7$, then the results of Chapter 2 enable us to give a formula computing the local and the torsion quotient for any given pair of rational numbers (d_1, d_2) that correspond to the two elliptic curves via the chosen parametrisation. Further we compute the two functions to determine the global quotient once a Mordell-Weil basis of E_1 and E_2 is known. This will be discussed in the third subsection and provides examples of non-simple abelian surfaces B over $\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = k\cdot\Box$, for $k = 5, 7$. Since for any given pair (d_1, d_2) we can compute whether $\#Ш(B/\mathbb{Q})$ is five or seven times a square provided we have the corresponing Mordell-Weil bases, we are able to obtain comprehensive numerical results about the occurrence of non-square order Tate-Shafarevich groups in these two families of abelian surfaces. We did so for $N = 5$ and the results are presented in [10].

The fourth subsection treats with the composite cases $N = 6$ and $N = 10$ and we will give examples of non-simple abelian surfaces B over $\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = k \cdot \Box$, for $k = 1, 2, 3, 6, 10$. In an appendix we will have a brief look at cyclic isogenies $\varphi : E_1 \times E_2 \to B$ with diagonal kernel of degree 13 to show that the case $\#Ш(B/\mathbb{Q}) = 13 \cdot \Box$ is also possible.

3.1. The local quotient

We want to compute the quotients $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p$ with respect to Setting 2.33. If $p = \infty$ is the place at infinity this is often very easy.

Lemma 3.1. *Let E_1 and E_2 be elliptic curves over $\mathbb{R}$ and $\varphi : E_1 \times E_2 \to B$ a diagonal cyclic isogeny of degree N having a $\mathbb{R}$-kernel, i.e. $\#\ker\varphi_\infty = N$.*

(i) If $2 \nmid N$, then $\operatorname{coker}\varphi_\infty$ is trivial, and thus $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p = 1/N$.

(ii) If $2 \mid N$ assume further that both elliptic curves have negative discriminant. Then $\#\operatorname{coker}\varphi_\infty = 2$, and thus $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p = 2/N$.

Proof. As $\operatorname{coker}\varphi_\infty$ embeds into $H^1(\mathbb{R}, (E_1 \times E_2)[\varphi])$, which is trivial if the order of $\mathrm{Gal}_\mathbb{R}$ is coprime to $(E_1 \times E_2)[\varphi]$, we get (i).

For (ii) note that by assumption the Galois action on $\ker\varphi$ is trivial, hence $H^1(\mathbb{R}, (E_1 \times E_2)[\varphi])$ is just the group of homomorphisms from $\mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/N\mathbb{Z}$, which has 2 elements if $2 \mid N$. In case both discrimanants of the two elliptic curves are negative, we have that $H^1(\mathbb{R}, (E_1 \times E_2)(\mathbb{C}))$ is trivial, by Theorem V.2.4 in [21], which implies that $\operatorname{coker}\varphi_\infty$ surjects onto $H^1(\mathbb{R}, (E_1 \times E_2)[\varphi])$. $\Box$

Now we state the main theorem about the local quotient with respect to Setting 2.33 for $\deg\varphi = N = \ell$ being prime. It expresses $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p$ in terms of the type of reduction of both E_i at p. In case the reduction type is split multiplicative we additionally have to consider whether $\ker\eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p)$, and in case the reduction type is non-split multiplicative we also have to consider the value of the Tamagawa quotient $c(E_i')_p/c(E_i)_p$. In case the reduction type is additive, the local quotient also depends on the values of $|\eta_i'(0)|_p$. If $\ell \geq 5$, then the theorem determines the size of $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p$ for any p and any combination of reduction types of the two elliptic curves.

Theorem 3.2. *Assume Setting 2.33 for* $\deg\varphi = N = \ell$ *being prime and let* $p \in M_{\mathbb{Q}}^0$ *be a finite place. Then the local quotient at* p *can be computed as follows in case* $\ell \geq 5$.

$$\frac{\#\operatorname{coker}\varphi_p}{\#\ker\varphi_p} = \begin{cases} 1/\ell, & \text{at least one elliptic curve } E_i \text{ has split multiplicative} \\ & \quad \text{reduction at } p \text{ with } \ker\eta_{i,p} \nsubseteq (E_i)_0(\mathbb{Q}_p) \\ \ell, & \text{both elliptic curves have split multiplicative reduction at } p \\ & \quad \text{and both } \ker\eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p) \\ \ell, & \text{both elliptic curves have additive reduction at } p \\ & \quad \text{and both satisfy } |\eta_i'(0)|_p \neq 1 \\ 1, & \text{otherwise.} \end{cases}$$

In case $\ell = 3$ *we get the following equality.*

$$\frac{\#\operatorname{coker}\varphi_p}{\#\ker\varphi_p} = \begin{cases} 1/3, & \text{at least one elliptic curve } E_i \text{ has split multiplicative} \\ & \quad \text{reduction at } p \text{ with } \ker\eta_{i,p} \nsubseteq (E_i)_0(\mathbb{Q}_p) \\ 3, & \text{both elliptic curves have split multiplicative reduction at } p \\ & \quad \text{and both } \ker\eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p) \\ 1, & \text{all other cases, such that neither elliptic curve} \\ & \quad \text{has additive reduction at } p. \end{cases}$$

And in case $\ell = 2 \neq p$ *the situation is the following.*

$$\frac{\#\operatorname{coker}\varphi_p}{\#\ker\varphi_p} = \begin{cases} 1/2, & \text{at least one elliptic curve } E_i \text{ has split multiplicative} \\ & \quad \text{reduction at } p \text{ with } \ker\eta_{i,p} \nsubseteq (E_i)_0(\mathbb{Q}_p) \\ 1/2, & \text{at least one elliptic curve } E_i \text{ has non-split multiplicative} \\ & \quad \text{reduction at } p \text{ with } c(E_i')_p/c(E_i)_p = 1/2, \\ 2, & \text{both elliptic curves have either split multiplicative reduction} \\ & \quad \text{at } p \text{ with } \ker\eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p) \text{ or non-split multiplicative} \\ & \quad \text{reduction at } p \text{ with } c(E_i')_p/c(E_i)_p = 2, \\ 1, & \text{all other cases, such that both elliptic curves do not} \\ & \quad \text{have additive reduction at } p, \text{ and } (c(E_i')_p, c(E_i)_p) \neq (2,2) \\ & \quad \text{in case } E_i \text{ has non-split multiplicative reduction.} \end{cases}$$

In case $\ell = 2 = p$ *we get that* $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p = 1/2$*, if at least one elliptic curve* E_i *has split multiplicative reduction at* p *with* $\ker\eta_{i,p} \nsubseteq (E_i)_0(\mathbb{Q}_p)$.

Proof. Use Theorem 2.28 and the Key Lemma 2.30 to deduce from the reduction type of both E_i at p plus the stated further conditions whether $\operatorname{coker}\varphi_p$ is maximal, maximally unramified or trivial, i.e. by Corollary 2.4 has order ℓ^2, ℓ, or 1 respectively. As $\#\ker\varphi_p = \ell$ we are done. $\square$

It is not possible that one of the elliptic curves has split multiplicative reduction with $\ker \eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p)$ and the other curve has additive reduction with $|\eta_i'(0)|_p \neq 1$, as the former case implies $p \neq \ell$ and the latter implies $p = \ell$.

3.2. The global quotient

Now we investigate the global quotient $\frac{\#\ker \varphi_{\mathbb{Q}}}{\#\operatorname{coker} \varphi_{\mathbb{Q}}} \frac{\#\operatorname{coker} \varphi_{\mathbb{Q}}^\vee}{\#\ker \varphi_{\mathbb{Q}}^\vee}$ with respect to Setting 2.33 for $\deg \varphi = N = \ell$ being prime. As φ has a $\mathbb{Q}$-kernel, we only need a strategy to compute the size of the cokernels. We will not come up with a formula, but we will describe a method for computing 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 $E_i'(\mathbb{Q})$. The maps $\ker \eta_{1,\mathbb{Q}}^\vee \times \ker \eta_{2,\mathbb{Q}}^\vee \to \ker \varphi_{\mathbb{Q}}^\vee$ and $\ker \eta_{1,\mathbb{Q}} \times \ker \eta_{2,\mathbb{Q}} \to \ker \psi_{\mathbb{Q}}$ are surjective, therefore we have two short exact sequences of the cokernels.

$$0 \to \operatorname{coker} \psi_{\mathbb{Q}}^\vee \to \operatorname{coker} \eta_{1,\mathbb{Q}}^\vee \times \operatorname{coker} \eta_{2,\mathbb{Q}}^\vee \to \operatorname{coker} \varphi_{\mathbb{Q}}^\vee \to 0$$

$$0 \to \operatorname{coker} \varphi_{\mathbb{Q}} \to \operatorname{coker} \eta_{1,\mathbb{Q}} \times \operatorname{coker} \eta_{2,\mathbb{Q}} \to \operatorname{coker} \psi_{\mathbb{Q}} \to 0$$

We first compute $\operatorname{coker} \varphi_{\mathbb{Q}}^\vee$, which is simpler than the computation of $\operatorname{coker} \varphi_{\mathbb{Q}}$. We have the following long exact sequences of Galois cohomology.

$$0 \to \operatorname{coker} \eta_{1,\mathbb{Q}}^\vee \times \operatorname{coker} \eta_{2,\mathbb{Q}}^\vee \to H^1(\mathbb{Q}, (E_1' \times E_2')(\overline{\mathbb{Q}})[\eta_1^\vee \times \eta_2^\vee]) \to \dots$$

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

The Kummer sequence for a number field K and Hilbert's Theorem 90 yield

$$\delta_K : H^1(K, \boldsymbol{\mu}_\ell) \cong K^*/K^{*\ell}.$$

Since $E_i'(\overline{\mathbb{Q}})[\eta_i^\vee]$ and $B^\vee(\overline{\mathbb{Q}})[\varphi^\vee]$ are isomorphic to $\boldsymbol{\mu}_\ell$ as Galois modules for $\mathrm{Gal}_{\mathbb{Q}}$, we obtain isomorphisms from $H^1(\mathbb{Q}, E_i'(\overline{\mathbb{Q}})[\eta_i^\vee])$ and $H^1(\mathbb{Q}, B^\vee(\overline{\mathbb{Q}})[\varphi^\vee])$ to $H^1(\mathbb{Q}, \boldsymbol{\mu}_\ell)$. 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 the following commutative diagram.

$$\begin{tikzcd} \operatorname{coker} \eta_{1,\mathbb{Q}}^\vee \times \operatorname{coker} \eta_{2,\mathbb{Q}}^\vee \arrow[r, hook] \arrow[d] & \mathbb{Q}^*/\mathbb{Q}^{*\ell} \times \mathbb{Q}^*/\mathbb{Q}^{*\ell} \arrow[d] \\ \operatorname{coker} \varphi_{\mathbb{Q}}^\vee \arrow[r, hook] & \mathbb{Q}^*/\mathbb{Q}^{*\ell} \end{tikzcd} \tag{6}$$

In this diagram the natural surjection $\operatorname{coker} \eta_{1,\mathbb{Q}}^\vee \times \operatorname{coker} \eta_{2,\mathbb{Q}}^\vee \twoheadrightarrow \operatorname{coker} \varphi_{\mathbb{Q}}^\vee$ 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 $m \in \{1, \dots, \ell - 1\}$. Note that m depends on n, but it is clear that the image of $\operatorname{coker}\eta_{1,\mathbb{Q}}^{\vee} \times \operatorname{coker}\eta_{2,\mathbb{Q}}^{\vee}$ in the lower right group $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$ is independent of m and n, 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 $\operatorname{coker}\varphi_{\mathbb{Q}}^{\vee}$ as a subset of $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$.

Proposition 3.3. *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 has a K-kernel, i.e. $E(\overline{K})[\eta] = E(K)[\eta]$, and let $P \in E(K)$ be a generator of the kernel. Let $f_P \in K(E)$ be a K-rational function on E such that $\operatorname{div}(f_P) = \ell(P) - \ell(\mathcal{O})$.*

(i) There exists a unique constant $c = c(f_P) \in K^*/K^{*\ell}$ such that

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

$$[Q] \mapsto c \cdot f_P(Q) \bmod K^{*\ell}, \text{ for } Q \in E(K) \text{ with } Q \neq \mathcal{O}, P,$$

is a well-defined and injective group homomorphism.

(ii) The image of the map $c \cdot f_P$ is independent of the choice of the point P and function f_P and agrees with the image of the natural injection $\operatorname{coker}\eta_K^{\vee} \hookrightarrow K^*/K^{*\ell}$ described above.

(iii) The image of the map $c \cdot f_P$ 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 $\mathfrak{p} \subset \mathcal{O}_K$, such that $\mathfrak{p}$ divides the degree of η or $\mathfrak{p}$ is a prime of bad reduction of E.

Proof. This is Exercise 10.1 in [21]. □

Remark 3.4. By the Riemann-Roch Theorem, the vector space of functions $f_P \in K(E)$ with $\operatorname{div}(f_P) = \ell(P) - \ell(\mathcal{O})$ is 1-dimensional, hence such a function always exists. Given such a f_P it is easy to determine $c \in K^*/K^{*\ell}$ and to find the value for the image of P in $K^*/K^{*\ell}$, by using the fact that the map $c \cdot f_P \bmod K^{*\ell}$ is a group homomorphism. We will do this explicitly in Propositions 3.8 and 3.16 and Lemmas 3.20 and 3.25.

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

$$H^1(\mathbb{Q}, E_i(\overline{\mathbb{Q}})[\eta_i]) \to H^1(L, E_i(\overline{\mathbb{Q}})[\eta_i])$$

is injective, as the kernel, which equals $H^1(\mathrm{Gal}(L/\mathbb{Q}), E_i(\overline{\mathbb{Q}})[\eta_i])$, is trivial, since $[L : \mathbb{Q}] = \ell - 1$ is coprime to $\#E_i(\overline{\mathbb{Q}})[\eta_i] = \ell$. Using the isomorphism δ_L we get natural injections $\operatorname{coker}\eta_{i,\mathbb{Q}} \hookrightarrow H^1(\mathbb{Q}, E_i(\overline{\mathbb{Q}})[\eta_i]) \hookrightarrow H^1(L, E_i(\overline{\mathbb{Q}})[\eta_i]) \cong L^*/L^{*\ell}$ and hence we obtain the commutative diagram below. In this diagram the natural surjection $\operatorname{coker}\eta_{1,\mathbb{Q}} \times \operatorname{coker}\eta_{2,\mathbb{Q}} \twoheadrightarrow \operatorname{coker}\psi_{\mathbb{Q}}$ is $(x, y) \mapsto x^m/y$ as a map from $L^*/L^{*\ell} \times L^*/L^{*\ell}$ to $L^*/L^{*\ell}$, for a suitable $m \in \{1, \dots, \ell-1\}$. As before, all images are independent of m and n, and so we can simply set $m = 1$ in our computations. Hence $\operatorname{coker} \varphi_{\mathbb{Q}}$ is easy to determine provided we know the images of $\operatorname{coker} \eta_{i,\mathbb{Q}}$ in $L^*/L^{*\ell}$.

$$\begin{tikzcd}
\operatorname{coker} \varphi_{\mathbb{Q}} \arrow[r, hook] \arrow[d, hook] & L^*/L^{*\ell} \arrow[d] \\
\operatorname{coker} \eta_{1,\mathbb{Q}} \times \operatorname{coker} \eta_{2,\mathbb{Q}} \arrow[r, hook] \arrow[d] & L^*/L^{*\ell} \times L^*/L^{*\ell} \arrow[d] \\
\operatorname{coker} \psi_{\mathbb{Q}} \arrow[r, hook] & L^*/L^{*\ell}
\end{tikzcd} \tag{7}$$

To obtain functions computing the images of $\operatorname{coker} \eta_{i,\mathbb{Q}}$ in $L^*/L^{*\ell}$, note that the dual isogenies $\eta_i^\vee : E_i' \to E_i$ have L-kernels. Hence by Proposition 3.3 we need generators $\check{P}_i \in E_i'(L)$ of $E_i'[\eta_i^\vee]$ and L-rational functions $f_{\check{P}_i} \in L(E_i')$, such that $\operatorname{div}(f_{\check{P}_i}) = \ell(\check{P}_i) - \ell(\mathcal{O})$. Again, if S denotes the set of all primes $\mathfrak{p} \subset \mathcal{O}_L$, such that $\mathfrak{p}$ divides the degree of η or $\mathfrak{p}$ is a prime of bad reduction of E_i/L, then the image of $\operatorname{coker} \eta_{i,\mathbb{Q}}$ in $L^*/L^{*\ell}$ lies in the finite set

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

3.3. $N = 5$ and $N = 7$ ($k = 5, 7$)

It is a well-known fact that all elliptic curves E over a number field K with a K-rational 5-torsion point P are parametrised by the Weierstraß equation

$$E : Y^2 + (d+1)XY + dY = X^3 + dX^2, \ P = (0,0), \tag{8}$$

for $d \in K$. Clearly the discriminant $\Delta = -d^5(d^2 + 11d - 1)$ has to be different from zero. For $K = \mathbb{Q}$ this is exactly the case when $d \neq 0$ holds. Using Vélu's algorithm [29] one can show that the curve E is isogenous to the elliptic curve

$$E' : Y^2+(d+1)XY+dY = X^3+dX^2+(5d^3-10d^2-5d)X+(d^5-10d^4-5d^3-15d^2-d)$$

via the isogeny $\eta : E \to E'$ whose kernel is generated by P. Note that

$$\langle P \rangle = \{\mathcal{O}, \ P = (0,0), \ 2P = (-d, d^2), \ 3P = (-d, 0), \ 4P = (0, -d)\}.$$

If we write $d = u/v$, with $u, v \in \mathbb{Z}$ coprime, then E is isomorphic to

$$E_{u,v} : Y^2 + (u+v)XY + uv^2Y = X^3 + uvX^2, \ P = (0,0),$$

with discriminant $\Delta_{u,v} = -(uv)^5(u^2 + 11uv - v^2)$, and E' is isomorphic to

$$E'_{u,v} : Y^2 + (u+v)XY + uv^2Y =$$
$$X^3 + uvX^2 + (5u^3v - 10u^2v^2 - 5uv^3)X + (u^5v - 10u^4v^2 - 5u^3v^3 - 15u^2v^4 - uv^5).$$

We want to use Theorem 3.2 to determine the local quotient, thus for each prime p we have to know the reduction type of E at p and the value $|\eta'(0)|_p$.

Lemma 3.5. *Let E be an elliptic curve as above parametrised by $d = u/v \in \mathbb{Q} \setminus \{0\}$, with $u, v \in \mathbb{Z}$ coprime, and let p be a prime number.*

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

(ii) If $p|u^2 + 11uv - v^2$ then $\ker \eta_p \subseteq E_0(\mathbb{Q}_p)$. Further, 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) $u \equiv 2v \bmod 5 \;\Rightarrow 5^4 \mid c'_{4,u,v}$, where $c'_{4,u,v}$ is the usual coefficients of a short Weierstraß equation of $E'_{u,v}$ as given for example in [21, III.1].

Proof. Most of part (i) and (ii) follow from Lemma 1.4 and the comment thereafter of [6]. The rest is an easy exercise. □

Proposition 3.6. *Let $\eta : E \to E'$ be the isogeny described above, for the parameter $d = u/v \in \mathbb{Q} \setminus \{0\}$, with $u, v \in \mathbb{Z}$ coprime. Then*

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

Proof. By Theorem 2.28 we have that $|\eta'(0)|_p$ equals 1 if $p \neq 5$ or if p is a place of good or multiplicative reduction. If $p = 5$ is additive, combining Lemma 3.5 with [21, 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 $E'_{u,v}$ will become minimal under the following change of variables: $X \mapsto X/5^2$ and $Y \mapsto Y/5^3$. Assume that $E'_{u,v}$ is minimal. We will now compute the p-adic valuation of the leading coefficent of the power series representation of η. We claim that $\eta(Z) = Z + ...$ as a power series in Z in a neighbourhood of $\mathcal{O}$. Set $\eta(X, Y) =: (\tilde{X}(X, Y), \tilde{Y}(X, Y))$. Then by [29], we have $-\tilde{X}(X, Y)/\tilde{Y}(X, Y) = p(X)/q(X, Y)$, for

$$\begin{aligned} p(X) &:= X(d + X)[d^4 + (3d^3 + d^4)X + (3d^2 + 3d^3)X^2 \\ &\quad +(d + 3d^2 - d^3)X^3 + 2dX^4 + X^5], \\ q(X, Y) &:= d^6 + (5d^5 + 2d^6)X + (10d^4 + 8d^5 + d^6)X^2 \\ &\quad +(10d^3 + 13d^4 + 4d^5)X^3 + (5d^2 + 10d^3 + 4d^4)X^4 + (d + 3d^2 + d^3 - d^4)X^5 \\ &\quad +Y[2d^5 + (7d^4 + d^5)X + (9d^3 + 3d^4)X^2 + (5d^2 + 3d^3 + d^4)X^3 \\ &\quad +(d - d^2 - d^3)X^4 - 3dX^5 - X^6]. \end{aligned}$$

For $Z := -X/Y$, we have $X(Z) = Z^{-2} + \ldots$ and $Y(Z) = -Z^{-3} + \ldots$ as Laurent series for X and Y, see [21, IV.1], thus $\eta(Z) = \frac{Z^{-14}+\ldots}{Z^{-15}+\ldots} = Z + \ldots$ as power series in Z. Hence $\eta'(0) = 1$, and therefore $|\eta'(0)|_p = 1$.

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

Combining both the above lemma and proposition with Lemma 3.1 and Theorem 3.2 gives complete control of the local quotient.

ACCEPTED MANUSCRIPT

Theorem 3.7. *Assume Setting 2.33 with $N = 5$. Let E_i be given by $d_i = u_i/v_i$, for $d_i \in \mathbb{Q} \setminus \{0\}$, with $u_i, v_i \in \mathbb{Z}$ coprime. If $p \in M_\mathbb{Q}$ is a place, then*

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

Next comes the global quotient. We will use Proposition 3.3 to calculate $\operatorname{coker}\eta^\vee_{i,\mathbb{Q}}$ in $\mathbb{Q}^*/\mathbb{Q}^{*5}$. Note that $\operatorname{coker}\eta^\vee_{i,\mathbb{Q},\mathrm{tors}}$ is generated by the point P_i.

Proposition 3.8. *For $P = (0, 0)$ set*

$$f_P := -X^2 + XY + Y \in K(E).$$

The image of the natural embedding $\operatorname{coker}\eta^\vee_\mathbb{Q} \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*5}$ equals the image of

$$f_P(X, Y) \bmod \mathbb{Q}^{*5},\ \textit{for } Q = (X, Y) \neq \mathcal{O}, P.$$

By linearity $f_P(P) = d^4$, and $f_P(\operatorname{coker}\eta^\vee_{\mathbb{Q},\mathrm{tors}}) = \langle d\rangle$ in $\mathbb{Q}^*/\mathbb{Q}^{*5}$.

Proof. For $X, Y, X + Y + d \in K(E)$, we have $\operatorname{div}(X) = (P) + (4P) - 2(\mathcal{O})$, $\operatorname{div}(Y) = 2(P) + (3P) - 3(\mathcal{O})$, and $\operatorname{div}(X + Y + d) = 2(3P) + (4P) - 3(\mathcal{O})$. As $(XY^2)/(X+Y+d)\cdot(-Y-dX)/(-Y-dX)$ equals $-X^2+XY+Y$ in $K(E)$, we get $\operatorname{div}(f_P) = 5(P) - 5(\mathcal{O})$. Apply Proposition 3.3. Since $(f_P(2P))^2 = f_P(4P)$, we get $c = 1$. As $f_P(P) \equiv f_P(2P)^3 \equiv d^4 \bmod \mathbb{Q}^{*5}$, we are done. □

Corollary 3.9. *With notation as above, $E'(\mathbb{Q})[5] \cong \mathbb{Z}/5\mathbb{Z} \Leftrightarrow d \in \mathbb{Q}^{*5}$.*

Proof. We have that $E'(\mathbb{Q})[5]$ is non-trivial if and only if $\operatorname{coker}\eta^\vee_\mathbb{Q}$ is trivial on the torsion part. The cokernel of $\eta^\vee_{\mathbb{Q},\mathrm{tors}}$ is generated by d in $\mathbb{Q}^*/\mathbb{Q}^{*5}$. Hence $E'(\mathbb{Q})[5]$ is non-trivial if and only if d is trivial in $\mathbb{Q}^*/\mathbb{Q}^{*5}$. □

Now we calculate $\operatorname{coker}\eta_\mathbb{Q}$ in L^*/L^{*5}, for $L := \mathbb{Q}(\xi)$, with $\xi \in \boldsymbol{\mu}_5$ a primitive fifth root of unity. Fix a generator $\check{P}$ of $E'(\overline{\mathbb{Q}})[\eta^\vee]$. Since $\check{P} \in E'(L)$, we have that $(E', \check{P})$ is isomorphic over L to a pair $(E_{\tilde{d}}, (0, 0))$, where $E_{\tilde{d}}$ is the elliptic curve over L for the parameter $\tilde{d} \in L$ given by equation (8). Such a L-isomorphism $\epsilon : (E', \check{P}) \tilde{\to} (E_{\tilde{d}}, (0, 0))$ is given by $r, s, t \in L$ and $w \in L^*$ and has the form $X = w^2X' + r$ and $Y = w^3Y' + w^2sX' + t$; see [21, III.1]. Knowing ϵ and the formula of f_P from Proposition 3.8, we can determine $f_{\check{P}}$, since

$$f_{\check{P}}(X, Y) \equiv \epsilon^* f_P(X', Y') \bmod L^{*5}.$$

To obtain ϵ we use [21, III Table 1.2]. As a_6 of the Weierstraß equation of $E_{\tilde{d}}$ vanishes, we get $(r, t) = \check{P}$. The kernel polynomial of the dual isogeny $\eta^\vee : E' \to E$ 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 choose

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

$$t = \frac{1}{5}[(\xi^2+2\xi+2)d^3 + (\xi^3+10\xi^2+23\xi+11)d^2$$
$$+(11\xi^3-12\xi^2+9\xi+2)d + (-\xi^3+\xi^2-\xi+1)] \in L.$$

Since a_4 of $E_{\tilde{d}}$ also vanishes and $a_3 = a_2$ we deduce

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

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

We also deduce $\tilde{d} = ((5\vartheta-3)d+1)/(d-(5\vartheta-3))$ and we obtain

$$f_{\check{P}}(X,Y) \equiv \frac{1}{25}[(3+6\xi-\xi^2+7\xi^3) + (80+235\xi-60\xi^2+245\xi^3)d$$
$$+(220+465\xi+185\xi^2+205\xi^3)d^2 + (15+55\xi-55\xi^2+160\xi^3)d^3$$
$$+(140+280\xi+245\xi^2+35\xi^3)d^4 + (-4-8\xi-7\xi^2-\xi^3)d^5]$$
$$+[(-1+\xi-\xi^2) + (3+9\xi+2\xi^2+2\xi^3)d + (2+6\xi+8\xi^2-3\xi^3)d^2$$
$$+(-1-\xi+\xi^3)d^3]X + [(-\xi+\xi^2-2\xi^3) + (2+3\xi+2\xi^2+\xi^3)d]X^2$$
$$+[(-3-2\xi^2-2\xi^3) + (-1-3\xi^2-3\xi^3)d + (-1+2\xi^2+2\xi^3)d^2]Y + XY \in L(E').$$

Now we can state the torsion quotient in terms of the pair (d_1, d_2).

Proposition 3.10. *Assume Setting 2.33 with $N = 5$. Let E_i be given by $d_i \in \mathbb{Q} \setminus \{0\}$. Then the following holds.*

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

In case both $d_i \in \mathbb{Q}^{*5}$, then the torsion quotient equals 1 if and only if

$$\left\langle \prod_{j=1}^{4} (\delta_1+\zeta_j)^j (\delta_1 - 1/\zeta_j)^j \right\rangle = \left\langle \prod_{j=1}^{4} (\delta_2+\zeta_j)^j (\delta_2 - 1/\zeta_j)^j \right\rangle \text{ in } L^*/L^{*5},$$

with $d_i =: \delta_i^5$, for $\delta_i \in \mathbb{Q}^*$, and $\zeta_1 := -\xi^4(\xi+1)$, $\zeta_2 := -\xi(\xi+1)$, $\zeta_3 := -\xi^3(\xi+1)$ and $\zeta_4 := -(\xi+1)$, where $\xi \in \boldsymbol{\mu}_5$ is a primitive fifth root of unity.

Proof. Recall Diagrams (6) and (7) and that the torsion quotient equals $5 \cdot \#\operatorname{coker}\varphi^\vee_{\mathbb{Q},\text{tors}}/\#\operatorname{coker}\varphi_{\mathbb{Q},\text{tors}}$. We have seen above that $E'(\mathbb{Q})[5] \cong \mathbb{Z}/5\mathbb{Z}$ if and only if $d \in \mathbb{Q}^{*5}$, hence $\operatorname{coker}\eta_{i,\mathbb{Q},\text{tors}}$ 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 that $\operatorname{coker}\varphi_{\mathbb{Q},\text{tors}}$ might have five elements in case $d_1, d_2 \in \mathbb{Q}^{*5}$, and is trivial otherwise. Since coker $\eta^\vee_{i,\mathbb{Q},\mathrm{tors}}$ is generated by d_i mod $\mathbb{Q}^{*5}$ and the map onto coker $\varphi^\vee_{\mathbb{Q},\mathrm{tors}}$ is given by $(x,y) \mapsto x/y$, we get

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

which finishes the first part. For the second part, note that if $d_i = \delta_i^5$, then $E'(\mathbb{Q})[5]$ is generated by the point $P'_i = (x_i, y_i)$, where

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

The image of $\langle P'_i\rangle$ under $f_{\check{T}}$ in L^*/L^{*5}, i.e. the image of coker $\eta_{i,\mathbb{Q},\mathrm{tors}}$, is $\left\langle \prod_{j=1}^4 (\delta_i + \zeta_j)^j (\delta_i - 1/\zeta_j)^j \right\rangle$, which completes the second part. □

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

Example 3.11. If $d_1 = u_1/v_1 = 1/11$, $d_2 = u_2/v_2 = 2/9$, then $\#Ш(B/\mathbb{Q}) = 5$.

Proof. There are three different primes dividing $u_1v_1u_2v_2 = 2 \cdot 3^2 \cdot 11$. We also have the contribution of the prime at infinity, and no contribution from any other prime, as $u_i \not\equiv 7 \cdot v_i$ mod 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_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 [24, 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 [6, 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 coker $\eta_{i,\mathbb{Q}} = 0$ and coker $\eta^\vee_{i,\mathbb{Q}} \cong \mathbb{Z}/5\mathbb{Z}$ 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 3.12. If $d_1 = u_1/v_1 = 1/10$, $d_2 = u_2/v_2 = 3/1$, then $\#Ш(B/\mathbb{Q}) = 5$.

Proof. We have $u_1v_1u_2v_2 = 2 \cdot 3 \cdot 5$, $u_i \not\equiv 7 \cdot v_i$ mod 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 $(-6, 12)$. We will now determine coker $\eta^\vee_{i,\mathbb{Q}}$ as a subset of $\mathbb{Q}^*/\mathbb{Q}^{*5}$. For the first curve this equals just the torsion part of the cokernel, hence 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 $(-6,12)$ under $f=-X^2+XY+Y$, which is $-3\cdot 2^5\equiv 3 \bmod \mathbb{Q}^{*5}$. Therefore coker $\eta_{2,\mathbb{Q}}^\vee$ is generated only by $\{3\}$ and hence coker $\varphi_{\mathbb{Q}}^\vee$ has dimension equal to 2. Since neither d_i are fifth powers, we get that the dimension of coker $\eta_{1,\mathbb{Q}}$ equals 0 and the dimension of coker $\eta_{2,\mathbb{Q}}$ equals 0 or 1, thus the dimension of 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. □

The situation for $N=7$ is similar to the case $N=5$. The elliptic curves E with a rational 7-torsion point P are parametrised by the Weierstraß equation

$$E: Y^2+(1+d-d^2)XY+(d^2-d^3)Y = X^3+(d^2-d^3)X^2,\ P=(0,0),$$

with discriminant $\Delta=-d^7(1-d)^7(d^3-8d^2+5d+1)$. Thus for $K=\mathbb{Q}$ we have $d\neq 0,1$. The isogenous curve is

$$\begin{gathered}E': Y^2+(1+d-d^2)XY+(d^2-d^3)Y = \\ X^3+(d^2-d^3)X^2+(5d-35d^2+70d^3-70d^4+35d^5-5d^7)X \\ +(d-19d^2+94d^3-258d^4+393d^5-343d^6+202d^7-107d^8+46d^9-8d^{10}-d^{11}),\end{gathered}$$

and the points in the kernel of $\eta: E\to E'$ are

$$\begin{gathered}\langle P\rangle = \{\mathcal{O},\ P=(0,0),\ 2P=(d^3-d^2,d^5-2d^4+d^3),\ 3P=(d^2-d,d^3-2d^2+d), \\ 4P=(d^2-d,d^4-2d^3+d^2),\ 5P=(d^3-d^2,0),\ 6P=(0,d^3-d^2)\}.\end{gathered}$$

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

$$E_{u,v}: Y^2+((v-u)(v+u)+uv)XY+(v-u)u^2v^3Y = X^3+(v-u)u^2vX^2,\ P=(0,0),$$

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

Lemma 3.13. *Let E be an elliptic curve as above parametrised by $d=u/v\in\mathbb{Q}\setminus\{0,1\}$, with $u,v\in\mathbb{Z}$ coprime, and let p be a prime number.*

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

(ii) If $p|u^3-8u^2v+5uv^2+v^3$ then $\ker\eta_p\subseteq E_0(\mathbb{Q}_p)$. Further, 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) $u\equiv 5v \bmod 7 \ \Rightarrow 7^6 \mid c'_{4,u,v}$.

Proposition 3.14. *Let $\eta: E\to E'$ be the isogeny described above, for the parameter $d=u/v\in\mathbb{Q}\setminus\{0,1\}$, with $u,v\in\mathbb{Z}$ coprime. Then*

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

Hence, for the local quotient we have the following

Theorem 3.15. *Assume Setting 2.33 with $N = 7$. Let E_i be given by $d_i = u_i/v_i$, for $d_i \in \mathbb{Q} \setminus \{0,1\}$, with $u_i, v_i \in \mathbb{Z}$ coprime. If $p \in M_{\mathbb{Q}}$ is a place, then*

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

Next comes the global quotient.

Proposition 3.16. *For $P = (0,0)$ set*

$$f_P := d^2X^2 + X^3 + dX^3 - d^2Y - XY - 2dXY - X^2Y \in K(E).$$

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

$$f_P(X,Y) \bmod \mathbb{Q}^{*7},\ \textit{for } Q = (X,Y) \neq \mathcal{O}, P.$$

By linearity $f_P(P) = d^3(d-1)^6$, and $f_P(\operatorname{coker}\eta^\vee_{\mathbb{Q},\mathrm{tors}}) = \langle d(d-1)^2\rangle$ in $\mathbb{Q}^*/\mathbb{Q}^{*7}$.

Proof. We have that $\operatorname{div}(X) = (P)+(6P)-2(\mathcal{O})$, $\operatorname{div}(Y) = 2(P)+(5P)-3(\mathcal{O})$, $\operatorname{div}(Xd-1)-Y) = (P)+2(3P)-3(\mathcal{O})$, and $\operatorname{div}(X+Y-d^3+d^2) = (3P)+(5P)+(6P)-3(\mathcal{O})$, hence $\operatorname{div}(Y^2X^2(X(d-1)-Y)/(X+Y-d^3+d^2)^2) = 7(P)-7(\mathcal{O})$. Multiplying with $(-Y-(1+d-d^2)X-(d^2-d^3))/(-Y-(1+d-d^2)X-(d^2-d^3))$ gives $d^2X^2 + X^3 + dX^3 - d^2Y - XY - 2dXY - X^2Y$. □

Corollary 3.17. *With notation as above, $E'(\mathbb{Q})[7] = 0$.*

Proof. As in Corollary 3.9, $E'(\mathbb{Q})[7]$ 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. □

Set $L := \mathbb{Q}(\xi)$, for $\xi \in \boldsymbol{\mu}_7$ a primitive seventh root of unity. As in case $N = 5$, we want to compute a function $f_{\check{P}}$, which calculates the image of $\operatorname{coker}\eta_{\mathbb{Q}}$ in L^*/L^{*7}, and which depends on a point $\check{P} = (r,t) \in E'(\overline{\mathbb{Q}})[\eta^\vee]$. The coefficients r,t,s,w for the L-isomorphism $\epsilon : (E', \check{P}) \tilde{\to} (E_{\tilde{d}}, (0,0))$ can be computed in the same manner as before. The kernel polynomial of $\eta^\vee : E' \to E$ is

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

Using the conditions on the a_i and setting $\vartheta := \xi + \xi^{-1}$ gives

$$r = \frac{1}{7}[(3\vartheta^2 + 2\vartheta - 9)d^4 + (-25\vartheta^2 - 19\vartheta + 47)d^3$$
$$+(23\vartheta^2 + 34\vartheta - 41)d^2 + (-2\vartheta^2 - 13\vartheta + 6)d + (-\vartheta^2 - 3\vartheta - 4)] \in \mathbb{Q}(\vartheta),$$
$$t = \frac{1}{7}[(-3\xi^5 - 6\xi^4 - \xi^3 - \xi^2 - 5\xi - 5)d^6 + (28\xi^5 + 59\xi^4 + 7\xi^3 + 10\xi^2 + 45\xi + 33)d^5$$
$$+(-52\xi^5 - 119\xi^4 + 6\xi^3 - 16\xi^2 - 62\xi - 51)d^4 + (56\xi^5 + 54\xi^4 - 35\xi^3 - 37\xi^2 - 9\xi + 13)d^3$$
$$+(-13\xi^5 + 30\xi^4 + 54\xi^3 + 75\xi^2 + 60\xi + 32)d^2 + (-10\xi^5 - 16\xi^4 - 22\xi^3 - 25\xi^2 - 22\xi - 17)d$$
$$+(-\xi^5 - 3\xi^4 - 5\xi^3 - 6\xi^2 - 5\xi - 1)] \in L,$$
$$s = \frac{1}{7}[(3\xi^5 + 6\xi^4 - 5\xi^3 - 2\xi^2 + \xi + 4)d^2 + (-16\xi^5 - 11\xi^4 - 6\xi^3 - \xi^2 - 17\xi - 12)d$$
$$+(5\xi^5 + 3\xi^4 + 8\xi^3 + 6\xi^2 + 11\xi + 2)],$$
$$w = \frac{1}{7}[(-3\xi^5 - 6\xi^4 - \xi^3 - \xi^2 - 5\xi - 5)d^6 + (28\xi^5 + 59\xi^4 + 7\xi^3 + 10\xi^2 + 45\xi + 33)d^5$$
$$+(-52\xi^5 - 119\xi^4 + 6\xi^3 - 16\xi^2 - 62\xi - 51)d^4 + (56\xi^5 + 54\xi^4 - 35\xi^3 - 37\xi^2 - 9\xi + 13)d^3$$
$$+(-13\xi^5 + 30\xi^4 + 54\xi^3 + 75\xi^2 + 60\xi + 32)d^2 + (-10\xi^5 - 16\xi^4 - 22\xi^3 - 25\xi^2 - 22\xi - 17)d$$
$$+(-\xi^5 - 3\xi^4 - 5\xi^3 - 6\xi^2 - 5\xi - 1)],$$
$$\tilde{d} = \frac{(\vartheta^2 + 3\vartheta + 2)d - (\vartheta^2 + 3\vartheta + 1)}{d - (\vartheta^2 + 3\vartheta + 2)}.$$

Now putting everything together yields

$$f_{\tilde{P}} \equiv w^7 \cdot f_P((X - r)/w^2, (Y - t - s(X - r))/w^3)$$
$$= w^3\tilde{d}^2(X-r)^2 + w(X-r)^3 + w\tilde{d}(X-r)^3 - w^4\tilde{d}^2(Y-t-s(X-r)) - w^2(X-r)(Y-t-s(X-r)).$$

The torsion quotient can be computed as follows.

Proposition 3.18. *Assume Setting 2.33 with $N = 7$. 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 $\#\operatorname{coker}\varphi_{\mathbb{Q},\text{tors}} = 1$. We know that $\operatorname{coker}\eta^\vee_{i,\mathbb{Q},\text{tors}}$ 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 $\operatorname{coker}\varphi^\vee_{\mathbb{Q},\text{tors}}$ via the map $(x, y) \mapsto x/y$, we conclude that

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

which completes the proof. □

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

Example 3.19. If $d_1 = u_1/v_1 = 1/3$, $d_2 = u_2/v_2 = 1/4$, then $\#Ш(B/\mathbb{Q}) = 7$.

Proof. The local quotient equals $1/7^3$, as $u_1v_1u_2v_2(v_1-u_1)(v_2-u_2) = 2^3 \cdot 3^2$, $u_1 \equiv 5\cdot v_1 \bmod 7$, $u_2 \not\equiv 5\cdot v_2 \bmod 7$, and $\gcd(u_1^3-8u_1^2v_1+5u_1v_1^2+v_1^3, u_2^3-8u_2^2v_2+5u_2v_2^2+v_2^3) = 1$. Both elliptic curves have analytic rank equal to 0, thus $Ш(A/\mathbb{Q})$ and $Ш(B/\mathbb{Q})$ are finite and 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 $N = 5$, one can use [24] and [6] to show that $Ш(A/\mathbb{Q})$ is trivial. $\square$

3.4. $N = 6$ and $N = 10$ $(k = 1, 2, 3, 6, 10)$

The elliptic curves E over a number field K having a rational 6-torsion point P are parametrised by the Weierstraß equation

$$E : Y^2 + (d+1)XY - d(d-1)Y = X^3 - d(d-1)X^2,\ P = (0,0),$$

with discriminant $\Delta = d^6(9d-1)(d-1)^3$, for $d \in K \setminus \{0, 1, 1/9\}$. Denote by $\eta : E \to E'$ the cyclic isogeny of degree 6, whose kernel is $\langle P \rangle$. Then

$$2P = (d(d-1), -d^2(d-1)),\ 3P = (-d, d^2),\ 4P = (d(d-1), 0),\ 5P = (0, d(d-1)),$$

$$E' : Y^2 + (d+1)XY - d(d-1)Y = X^3 - d(d-1)X^2$$
$$-5(3d^3 - 4d^2 + d + 1)dX - (19d^5 - 33d^4 + 18d^3 - 22d^2 + 14d + 1)d.$$

Let $\check{P}$ denote a generator of the kernel of the dual isogeny $\eta^\vee : E' \to E$. Then

$$\pm\check{P} = \left(-2d^2 + 4d - 1,\ d^3 - \frac{1}{2}d^2 - 2d + \frac{1}{2} \pm \frac{1}{2}(d-1)(9d-1)\sqrt{-3}\right),$$

$$\pm2\check{P} = \left(-2d^2 - 2d - \frac{1}{3},\ d^3 + \frac{5}{2}d^2 + \frac{2}{3}d + \frac{1}{6} \pm \frac{1}{18}(9d-1)^2\sqrt{-3}\right),$$

$$3\check{P} = \left(\frac{19}{4}d^2 - \frac{14}{4}d - \frac{1}{4},\ -\frac{19}{8}d^3 - \frac{1}{8}d^2 + \frac{11}{8}d + \frac{1}{8}\right).$$

In the following four examples we will give two parameters $d_1, d_2 \in \mathbb{Q} \setminus \{0, 1, 1/9\}$ that correspond to two elliptic curves E_1 and E_2 over $\mathbb{Q}$ having a rational 6-torsion point. Hence, E_1 and E_2 fulfill Setting 2.33 with $N = 6$ and we can define $\varphi : E_1 \times E_2 \to B$ with respect to some $n \in (\mathbb{Z}/6\mathbb{Z})^*$. By Proposition 2.32 the order of $Ш(B/\mathbb{Q})$ is independent of the choice of n, thus we simply set $n = 1$. Further we get the corresponding isogenies $\varphi_{\ell=2}$ and $\varphi_{\ell=3}$, which are introduced in Remark 2.36. In all four examples the analytic rank of both elliptic curves E_1 and E_2 is 0 and the discriminant of both curves is negative. Hence, all Tate-Shafarevich groups are finite, the regulator quotient is 1, and the local quotient at infinity for $\varphi_{\ell=2}$ is 1 and for $\varphi_{\ell=3}$ is 1/3, by Lemma 3.1. Also, for both elliptic curves the reduction types at all primes p are 'nice', in the sense that we can apply Theorem 3.2. Finally, the rational torsion of E_1 and E_2 is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ and the rational torsion of E_1' and E_2' is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. By construction $\#\ker\varphi_{\mathbb{Q}}/\#\ker\varphi_{\mathbb{Q}}^{\vee} = 3$, hence we can apply the next lemma to compute the torsion quotient. Note that $\mathbb{Q}(\boldsymbol{\mu}_3) = \mathbb{Q}(\sqrt{-3})$ has degree 2 and class number 1 and that the only prime which ramifies is 3.

Lemma 3.20. *Let $E/\mathbb{Q}$ be an elliptic curves with a rational 6-torsion point $P = (0,0)$ corresponding to the parameter $d \in \mathbb{Q} \setminus \{0, 1, 1/9\}$ as given above. Assume that $E(\mathbb{Q})_{\text{tors}} = \langle P \rangle \cong \mathbb{Z}/6\mathbb{Z}$ and $E'(\mathbb{Q})_{\text{tors}} = \langle 3\check{P} \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Then*

(i) $\operatorname{coker}\eta^{\vee}_{\mathbb{Q},\text{tors}}$ *can be identified with* $\langle d \rangle \times \langle d^2(d-1) \rangle$ *in* $\mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*3}$,

(ii) $\operatorname{coker}\eta_{\mathbb{Q},\text{tors}}$ *can be identified with* $\langle (9d-1)(d-1) \rangle$ *in* $\mathbb{Q}(\boldsymbol{\mu}_3)^*/\mathbb{Q}(\boldsymbol{\mu}_3)^{*2}$.

Proof. Let $f_2 := X + d$ and $f_3 := Y + 2dX - d^2(d-1)$ be two functions in the function field of $E/\mathbb{Q}$. Then $\operatorname{div}(f_2) = 2(3P) - 2(\mathcal{O})$ and $\operatorname{div}(f_3) = 3(2P) - 3(\mathcal{O})$. As $f_2(P) \equiv d \bmod \mathbb{Q}^{*2}$, $f_3(P) \equiv d^2(d-1) \bmod \mathbb{Q}^{*3}$, $3P$ generates $\operatorname{coker}\eta^{\vee}_{\ell=2,\mathbb{Q},\text{tors}}$, and $2P$ generates $\operatorname{coker}\eta^{\vee}_{\ell=3,\mathbb{Q},\text{tors}}$, we get (i) by Proposition 3.3.

For (ii) note that by assumption on the torsion groups of E and E', we get that $\operatorname{coker}\eta_{\ell=3,\mathbb{Q},\text{tors}}$ is trivial. The map $f_2^{\vee} := X - 19/4d^2 + 14/4d + 1/4$, fulfills $\operatorname{div}(f_2^{\vee}) = 2(3\check{P}) - 2(\mathcal{O})$. From $f_2^{\vee}(\check{P}) = -3/4(d-1)(9d-1)$ it follows that $f_2^{\vee}(3\check{P}) \equiv (d-1)(9d-1) \bmod \mathbb{Q}(\boldsymbol{\mu}_3)^{*2}$. □

Example 3.21. $(k = 6)$ If $d_1 = 2/7$ and $d_2 = 4/17$, then $\#Ш(B/\mathbb{Q}) = 6\square$.

Proof. The Cremona label of E_1 is $770g1$ and of E_2 is $8398i1$ and the conductor of E_1 is $2 \cdot 5 \cdot 7 \cdot 11$ and of E_2 is $2 \cdot 13 \cdot 17 \cdot 19$. By Lemma 3.20, we get

$$\operatorname{coker}\eta^{\vee}_{1,\mathbb{Q},\text{tors}} = \langle 2 \cdot 7 \rangle \times \langle 2^2 \cdot 5 \rangle, \ \operatorname{coker}\eta^{\vee}_{2,\mathbb{Q},\text{tors}} = \langle 17 \rangle \times \langle 2 \cdot 13 \rangle,$$

$$\operatorname{coker}\eta_{1,\mathbb{Q},\text{tors}} = \langle -5 \cdot 11 \rangle, \ \operatorname{coker}\eta_{2,\mathbb{Q},\text{tors}} = \langle -13 \cdot 19 \rangle.$$

From Diagrams (6) and (7) we conclude that

$$\#\operatorname{coker}\varphi^{\vee}_{\mathbb{Q},\text{tors}} = 2^2 \cdot 3^2 \quad \text{and} \quad \#\operatorname{coker}\varphi_{\mathbb{Q},\text{tors}} = 1.$$

Thus, the torsion quotient equals $2^2 \cdot 3^3$. The first two rows of the next table provide the following data: If the reduction type at p is split multiplicative, then we indicate whether $\ker\eta_{i,\ell=2,p}$ and $\ker\eta_{i,\ell=3,p}$ are contained in $(E_i)_0(\mathbb{Q}_p)$. If the reduction type at p is non-split multiplicative then we give the Tamagawa quotient at p for $\eta_{i,\ell=2}$. The third and fourth row follow by Theorem 3.2.

$p =$	2	5	7	11	13	17	19	∞
red. type of E_1	$\not\subseteq, \not\subseteq$	$\subseteq, \not\subseteq$	$\not\subseteq, \subseteq$	$\frac{c'}{c} = 2$	good	good	good	
red. type of E_2	$\not\subseteq, \not\subseteq$	good	good	good	$\subseteq, \not\subseteq$	$\frac{c'}{c} = 1/2$	$\subseteq, \subseteq$	
$\frac{\#\operatorname{coker}\varphi_{\ell=2,p}}{\#\ker\varphi_{\ell=2,p}} =$	1/2	1	1/2	1	1	1/2	1	1
$\frac{\#\operatorname{coker}\varphi_{\ell=3,p}}{\#\ker\varphi_{\ell=3,p}} =$	1/3	1/3	1	1	1/3	1	1	1/3

Thus the local quotient equals $2^{-3} \cdot 3^{-4}$, since by Remark 2.36 we get that $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p = \#\operatorname{coker}\varphi_{\ell=2,p}/\#\ker\varphi_{\ell=2,p} \cdot \#\operatorname{coker}\varphi_{\ell=3,p}/\#\ker\varphi_{\ell=3,p}$.

In total we have $\#Ш(B/\mathbb{Q}) = 6 \cdot \#Ш(E_1 \times E_2/\mathbb{Q}) = 6\square$.

Example 3.22. $(k = 3)$ If $d_1 = 2/7$ and $d_2 = 2/13$, then $\#\text{Ш}(B/\mathbb{Q}) = 3\square$.
Proof. The Cremona label of E_1 is $770g1$ and of E_2 is $1430g1$ and the conductor of E_1 is $2 \cdot 5 \cdot 7 \cdot 11$ and of E_2 is $2 \cdot 5 \cdot 11 \cdot 13$. By Lemma 3.20, we get

$$\operatorname{coker} \eta^{\vee}_{1,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 7\rangle \times \langle 2^2 \cdot 5\rangle, \ \operatorname{coker} \eta^{\vee}_{2,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 13\rangle \times \langle 2^2 \cdot 11\rangle,$$
$$\operatorname{coker} \eta_{1,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 11\rangle, \ \operatorname{coker} \eta_{2,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 11\rangle,$$
$$\#\operatorname{coker} \varphi^{\vee}_{\mathbb{Q},\mathrm{tors}} = 2^2 \cdot 3^2 \quad \text{and} \quad \#\operatorname{coker} \varphi_{\mathbb{Q},\mathrm{tors}} = 2.$$

Hence, the torsion quotient equals $2 \cdot 3^3$. The next table implies that the local quotient equals $2 \cdot 3^{-4}$.

$p =$	2	5	7	11	13	∞
red. type of E_1	$\not\subseteq, \not\subseteq$	$\subseteq, \not\subseteq$	$\not\subseteq, \subseteq$	$\frac{c'}{c} = 2$	good	
red. type of E_2	$\not\subseteq, \not\subseteq$	$\frac{c'}{c} = 2$	good	$\subseteq, \not\subseteq$	$\not\subseteq, \subseteq$	
$\frac{\#\operatorname{coker} \varphi_{\ell=2,p}}{\#\ker \varphi_{\ell=2,p}} =$	$1/2$	2	$1/2$	2	$1/2$	1
$\frac{\#\operatorname{coker} \varphi_{\ell=3,p}}{\#\ker \varphi_{\ell=3,p}} =$	$1/3$	$1/3$	1	$1/3$	1	$1/3$

In total we have $\#\text{Ш}(B/\mathbb{Q}) = 3 \cdot \#\text{Ш}(E_1 \times E_2/\mathbb{Q}) = 3\square$.

Example 3.23. $(k = 2)$ If $d_1 = 2/7$ and $d_2 = 6/7$, then $\#\text{Ш}(B/\mathbb{Q}) = 2\square$.
Proof. The Cremona label of E_1 is $770g1$ and of E_2 is $1974l1$ and the conductor of E_1 is $2 \cdot 5 \cdot 7 \cdot 11$ and of E_2 is $2 \cdot 3 \cdot 7 \cdot 47$. By Lemma 3.20, we get

$$\operatorname{coker} \eta^{\vee}_{1,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 7\rangle \times \langle 2^2 \cdot 5\rangle, \ \operatorname{coker} \eta^{\vee}_{2,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 3 \cdot 7\rangle \times \langle 2 \cdot 3\rangle,$$
$$\operatorname{coker} \eta_{1,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 11\rangle, \ \operatorname{coker} \eta_{2,\mathbb{Q},\mathrm{tors}} = \langle -47\rangle,$$
$$\#\operatorname{coker} \varphi^{\vee}_{\mathbb{Q},\mathrm{tors}} = 2^2 \cdot 3^2 \quad \text{and} \quad \#\operatorname{coker} \varphi_{\mathbb{Q},\mathrm{tors}} = 1.$$

Hence, the torsion quotient equals $2^2 \cdot 3^3$. The next table implies that the local quotient equals $2^{-3} \cdot 3^{-3}$.

$p =$	2	3	5	7	11	47	∞
red. type of E_1	$\not\subseteq, \not\subseteq$	good	$\subseteq, \not\subseteq$	$\not\subseteq, \subseteq$	$\frac{c'}{c} = 2$	good	
red. type of E_2	$\not\subseteq, \not\subseteq$	$\not\subseteq, \not\subseteq$	good	$\not\subseteq, \subseteq$	good	$\frac{c'}{c} = 2$	
$\frac{\#\operatorname{coker} \varphi_{\ell=2,p}}{\#\ker \varphi_{\ell=2,p}} =$	$1/2$	$1/2$	1	$1/2$	1	1	1
$\frac{\#\operatorname{coker} \varphi_{\ell=3,p}}{\#\ker \varphi_{\ell=3,p}} =$	$1/3$	$1/3$	$1/3$	3	1	1	$1/3$

In total we have $\#\text{Ш}(B/\mathbb{Q}) = 2 \cdot \#\text{Ш}(E_1 \times E_2/\mathbb{Q}) = 2\square$.

Example 3.24. $(k = 1)$ If $d_1 = 2/7$ and $d_2 = 8/13$, then $\#\text{Ш}(B/\mathbb{Q}) = \square$.
Proof. The Cremona label of E_1 is $770g1$ and of E_2 is $7670i1$ and the conductor of E_1 is $2 \cdot 5 \cdot 7 \cdot 11$ and of E_2 is $2 \cdot 5 \cdot 13 \cdot 59$. By Lemma 3.20, we get

$$\operatorname{coker} \eta^{\vee}_{1,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 7\rangle \times \langle 2^2 \cdot 5\rangle, \ \operatorname{coker} \eta^{\vee}_{2,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 13\rangle \times \langle 5\rangle,$$
$$\operatorname{coker} \eta_{1,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 11\rangle, \ \operatorname{coker} \eta_{2,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 59\rangle.$$
$$\#\operatorname{coker} \varphi^{\vee}_{\mathbb{Q},\mathrm{tors}} = 2^2 \cdot 3^2 \quad \text{and} \quad \#\operatorname{coker} \varphi_{\mathbb{Q},\mathrm{tors}} = 1.$$

Hence, the torsion quotient equals $2^2 \cdot 3^3$. The next table implies that the local quotient equals $2^{-2} \cdot 3^{-3}$.

$p =$	2	5	7	11	13	59	∞
red. type of E_1	$\nsubseteq, \nsubseteq$	$\subseteq, \nsubseteq$	$\nsubseteq, \subseteq$	$\frac{c'}{c} = 2$	good	good	
red. type of E_2	$\nsubseteq, \nsubseteq$	$\subseteq, \nsubseteq$	good	good	$\nsubseteq, \subseteq$	$\frac{c'}{c} = 2$	
$\frac{\# \operatorname{coker} \varphi_{\ell=2,p}}{\# \ker \varphi_{\ell=2,p}} =$	1/2	2	1/2	1	1/2	1	1
$\frac{\# \operatorname{coker} \varphi_{\ell=3,p}}{\# \ker \varphi_{\ell=3,p}} =$	1/3	1/3	1	1	1	1	1/3

In total we have $\#Ш(B/\mathbb{Q}) = \#Ш(E_1 \times E_2/\mathbb{Q}) = \square$.

Now we have a look at $N = 10$. The elliptic curves over a number field K with a rational 10-torsion point P are given by the Weierstraß equation

$$E : Y^2 + (-d^3 + d^2 + d + 1)XY - d^2(d-1)(d+1)^2 Y = X^3 - d^2(d-1)(d+1)X^2,$$

$$P = (d^3 - d, (d^3 - d)^2),\ 2P = (0, 0),\ 5P = (-d^2, d^4),$$
$$\Delta = d^{10}(d-1)^5(d+1)^5(d^2 - 4d - 1)(d^2 + d - 1)^2.$$

Thus if $K = \mathbb{Q}$, then $d \in \mathbb{Q} \setminus \{-1, 0, 1\}$. As usual we denote the isogeny having $\langle P \rangle$ as kernel by $\eta : E \to E'$. The coefficients a'_1, a'_2, a'_3 for the dual curve E' are the same as for E. The other two coefficients are

$$a'_4 = -5d^{11} - 30d^{10} - 15d^9 + 40d^8 + 65d^7 - 25d^6 - 65d^5 + 40d^4 + 15d^3 - 30d^2 + 5d,$$

$$a'_6 = -d^{17} - 18d^{16} - 56d^{15} - 40d^{14} + 180d^{13} + 151d^{12} - 207d^{11} - 79d^{10} + 65d^9$$
$$-144d^8 + 127d^7 + 221d^6 - 170d^5 - 70d^4 + 61d^3 - 18d^2 + d.$$

Let $\check{P}$ be a generator of the kernel of the dual isogeny $\eta^\vee : E' \to E$. Thus

$$5\check{P} = (-1/4 \cdot (d^6 + 14d^5 - 5d^4 - d^2 - 14d + 1),$$
$$-1/8 \cdot (d^9 + 13d^8 - 20d^7 - 10d^6 - 14d^5 - 12d^4 + 20d^3 + 18d^2 + 13d - 1)).$$

We will give an unconditional example of a non-simple abelian surface B over $\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = 10\square$. As in all the examples for $N = 6$, both elliptic curves involved have analytic rank equal to 0, hence we can avoid computing the regulator quotient and get the finiteness of the Tate-Shafarevich groups. Further, E_1 and E_2 have negative discriminant, thus the local quotient at infinity equals 1 for $\varphi_{\ell=2}$ and 1/5 for $\varphi_{\ell=5}$, by Lemma 3.1. Finally, $E'_1(\mathbb{Q})_{\text{tors}} \cong E'_2(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$, hence we can use the next lemma to compute the torsion quotient. Note that the Galois extension $\mathbb{Q}(\boldsymbol{\mu}_5)$ has degree 4 and class number 1 and that the only prime that ramifies is 5.

Lemma 3.25. *Let $E/\mathbb{Q}$ be an elliptic curves with a rational 10-torsion point $P = (d^3 - d, (d^3 - d)^2)$ corresponding to the parameter $d \in \mathbb{Q} \setminus \{-1, 0, 1\}$ as above. Assume that $E'(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$. Then*

(i) $\operatorname{coker} \eta^\vee_{\mathbb{Q},\text{tors}}$ *can be identified with $\langle d(d^2 + d - 1)\rangle \times \langle d^4(d-1)(d+1)^3\rangle$ in $\mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*5}$, and*

(ii) $\operatorname{coker} \eta_{\mathbb{Q},\text{tors}}$ *can be identified with $\langle (d-1)(d+1)(d^2 - 4d - 1)\rangle$ in $\mathbb{Q}(\boldsymbol{\mu}_5)^*/\mathbb{Q}(\boldsymbol{\mu}_5)^{*2}$.*

Proof. We proceed as in Lemma 3.20. Let $f_2 := X + d^2$ and $f_5 := XY^2/(Y + (d+1)X - (d^5 + d^4 - d^3 - d^2))$ be two functions in the function field of E. Then $\mathrm{div}(f_2) = 2(5P) - 2(\mathcal{O})$ and $\mathrm{div}(f_5) = 5(2P) - 5(\mathcal{O})$. As $f_2(P) \equiv d(d^2 + d - 1) \bmod \mathbb{Q}^{*2}$ and $f_5(P) \equiv d^4(d-1)(d+1)^3 \bmod \mathbb{Q}^{*5}$ we get (i).

For (ii) note that $\operatorname{coker} \eta_{\ell=5,\mathbb{Q},\mathrm{tors}}$ is trivial. The map $f_2^\vee := X + 1/4 \cdot (d^6 + 14d^5 - 5d^4 - d^2 - 14d + 1)$ fulfills $\mathrm{div}(f_2^\vee) = 2(5\check{P}) - 2(\mathcal{O})$. Two of the four points of order 10 in $\ker \eta^\vee$ have X-coordinate equal to $(\xi^3 + \xi^2 - 1)d^6 + (-3\xi^3 - 3\xi^2)d^5 + (-7\xi^3 - 7\xi^2 - 1)d^4 + (6\xi^3 + 6\xi^2 + 3)d^3 + (7\xi^3 + 7\xi^2 + 5)d^2 + (-3\xi^3 - 3\xi^2 - 3)d + (-\xi^3 - \xi^2 - 2)$, where $\xi \in \boldsymbol{\mu}_5$ is a primitive fifth root of unity. It follows that $f_2^\vee(5\check{P}) \equiv (d-1)(d+1)(d^2 - 4d - 1) \bmod \mathbb{Q}(\boldsymbol{\mu}_5)^{*2}$. □

Example 3.26. ($k = 10$) If $d_1 = 5/2$ and $d_2 = 8/5$, then $\#Ш(B/\mathbb{Q}) = 10\square$.
Proof. The Cremona label of E_1 is $123690by1$, where $123690 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 31$ and the conductor of E_2 is $338910 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 79$. By Lemma 3.25, we get

$$\operatorname{coker} \eta^\vee_{1,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 5 \cdot 31 \rangle \times \langle 2^2 \cdot 3 \cdot 5^4 \cdot 7^3 \rangle,$$

$$\operatorname{coker} \eta^\vee_{2,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 5 \cdot 79 \rangle \times \langle 2^2 \cdot 3 \cdot 5^2 \cdot 13^2 \rangle,$$

$$\operatorname{coker} \eta_{1,\mathbb{Q},\mathrm{tors}} = \langle -3 \cdot 7 \cdot 19 \rangle, \ \operatorname{coker} \eta_{2,\mathbb{Q},\mathrm{tors}} = \langle -3 \cdot 13 \rangle,$$

It follows that $\# \operatorname{coker} \varphi^\vee_{\mathbb{Q},\mathrm{tors}} = 2^2 \cdot 5^2$ and $\# \operatorname{coker} \varphi_{\mathbb{Q},\mathrm{tors}} = 1$, and hence the torsion quotient equals $2^2 \cdot 5^3$. The next table implies that the local quotient equals $2^{-3} \cdot 5^{-6}$.

$p =$	2	3	5	7	11	13	19	31	79	∞
red. type of E_1	$\nsubseteq, \nsubseteq$	$\subseteq, \nsubseteq$	$\nsubseteq, \nsubseteq$	$\subseteq, \nsubseteq$	good	good	$\frac{c'}{c} = 2$	$\nsubseteq, \subseteq$	good	
red. type of E_2	$\nsubseteq, \nsubseteq$	$\subseteq, \nsubseteq$	$\nsubseteq, \nsubseteq$	good	$\subseteq, \subseteq$	$\subseteq, \nsubseteq$	good	good	$\frac{c'}{c} = 1/2$	
$\frac{\# \operatorname{coker} \varphi_{\ell=2,p}}{\# \ker \varphi_{\ell=2,p}} =$	1/2	2	1/2	1	1	1	1	1/2	1/2	1
$\frac{\# \operatorname{coker} \varphi_{\ell=3,p}}{\# \ker \varphi_{\ell=3,p}} =$	1/5	1/5	1/5	1/5	1	1/5	1	1	1	1/5

In total we have $\#Ш(B/\mathbb{Q}) = 2 \cdot 5^3 \cdot \#Ш(E_1 \times E_2/\mathbb{Q}) = 10\square$.

3.5. Appendix. Cyclic isogenies with diagonal kernel, ($k = 13$)

We will loosen an assumption in the construction undertaken in Setting 2.33. Instead of requiring that all points of the cyclic subgroup $G_i \subseteq E_i$ are $\mathbb{Q}$-rational, we will merely demand that the G_i are Galois invariant. The next example completes the proof of Theorem 1.5, as it shows the construction of a non-simple non-principally polarised abelian surface $B/\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = 13 \cdot \square$.

Example 3.27. ($k = 13$) Consider the following two elliptic curves over $\mathbb{Q}$

$$E_1 : Y^2 = X^3 - X^2 - 1829X - 32115,$$

$$E_2 : Y^2 = X^3 - X^2 - 1117108895940162813412069X$$
$$-4544555158992923683535961508147155 71.$$

The first curve has Cremona Label $2352j1$, where $2352 = 2^4 \cdot 3 \cdot 7^2$. The second curve is of conductor $135694178256 = 2^4 \cdot 3 \cdot 7^2 \cdot 13 \cdot 251 \cdot 17681$. The two elliptic curves have cyclic 13-isogenies $\eta_i : E_i \to E_i'$ with isomorphic kernels, which is due to Noam D. Elkies [5], as E_1 and E_2 are the quadratic twists with respect to $D = 7$ of Elkies' example.

Denote by $\varphi : E_1 \times E_2 \to B$ the diagonal isogeny with respect to a Galois equivariant isomorphism $\alpha : \ker \eta_1 \to \ker \eta_2$. Recall, that $\#Ш(B/\mathbb{Q})$ is independent of the choice of α by Proposition 2.32. We claim that $\#Ш(B/\mathbb{Q}) = 13 \cdot \Box$.

Proof. The Mordell-Weil groups of all four elliptic curves E_1, E_2, E_1', and E_2' are trivial and the analytic ranks are all equal to 0. It is easy to see that this implies that the global quotient equals 1 and we know that $Ш(B/\mathbb{Q})$ is finite. We claim that the local quotient at infinity equals 1. As $2 \nmid \deg \varphi = 13$, we get that $\operatorname{coker} \varphi_\infty$ is trivial. To prove the claim it is sufficient to show that $\ker \eta_{1,\infty}$ is trivial, too. The kernel polynomial of η_1 is

$$(X^3 - X^2 - 1829X + 6301)(X^3 + 195X^2 + 7187X + 71569).$$

Denote by $g_1(X)$ the first factor and by $g_2(X)$ the second factor of this kernel polynomial and by $f(X) := X^3 - X^2 - 1829X - 32115$ the defining polynomial of E_1. All six roots of g_1 and g_2 are real numbers and both factors g_1 and g_2 generate the same totally real Galois field of degree 3. Let x_0 be a zero of $g_1(X)$. As $y_0^2 = f(x_0) = g_1(x_0) - 38416 = 0 - 2^4 \cdot 7^4$, we get that $y_0 = \pm 2^2 \cdot 7^2 \cdot \sqrt{-1} \in \mathbb{C} \setminus \mathbb{R}$, which shows that $\ker \eta_{1,\infty}$ is trivial.

Among the four elliptic curves E_i and E_i', there are exactely two Tamagawa numbers which are divisible by 13. These are $c(E_2)_{13} = 13$ and $c(E_2')_{17681} = 13$. Note that $c(E_2')_{13} = 1$ and $c(E_2)_{17681} = 1$. One easily verifies that $|\eta_i'(0)|_p = 1$, for all primes p and both i, hence by Corollary 2.23 we conclude that $\operatorname{coker} \eta_{1,p}$ is maximally unramified for all primes p and that $\operatorname{coker} \eta_{2,p}$ is maximally unramified for all $p \neq 13, 17681$.

Using Hensel's Lemma one easily checks that $g_1(X)$ and $g_2(X)$ both factor into linear factors in $\mathbb{Q}_{13}[X]$ and $\mathbb{Q}_{17681}[X]$. Since $\sqrt{-1}$ also lies in $\mathbb{Q}_{13}$ and in $\mathbb{Q}_{17681}$ it follows that $\ker \eta_{i,13}$ and $\ker \eta_{i,17681}$ both have 13 elements for both i, hence $H^1(\mathbb{Q}_{13}, E_i[\eta_i]) \cong H^1(\mathbb{Q}_{17681}, E_i[\eta_i]) \cong (\mathbb{Z}/13\mathbb{Z})^2$ by Corollary 2.4. As $\# \operatorname{coker} \eta_{i,p} / \# \ker \eta_{i,p} = c(E_i')_p / c(E_i)_p$ by Corollary 2.15, we immediately deduce that $\operatorname{coker} \eta_{2,13}$ is trivial and that $\operatorname{coker} \eta_{2,17681}$ is maximal.

Applying the Key Lemma 2.30 we deduce that the local quotient equals 1, for all $p \neq 13, 17681$, as in this case $\operatorname{coker} \varphi_p$ is maximally unramified. Further the Key Lemma implies that $\operatorname{coker} \varphi_{13}$ is trivial and hence the local quotient for $p = 13$ equals $1/13$, and that $\operatorname{coker} \varphi_{17681}$ is maximally unramified and thus the local quotient for $p = 17681$ equals 1.

Putting everything together gives $\#Ш(B/\mathbb{Q}) = 13 \cdot \#Ш(E_1 \times E_2/\mathbb{Q}) = 13 \cdot \Box$.

Remark 3.28. We claim that Theorem 1.5 covers all cyclic cases, i.e. if E_1 and E_2 are elliptic curves over $\mathbb{Q}$ with finite Tate-Shafarevich groups and $\varphi : E_1 \times E_2 \to B$ is a cyclic isogeny, then the non-square part of $\#Ш(B/\mathbb{Q})$ equals one of the eight values $\{1, 2, 3, 5, 6, 7, 10, 13\}$. This is ongoing work in progress.

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

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

[3] T. Dokchitser, V. Dokchitser, Local invariants of isogenous elliptic curves, 2013. Preprint, http://arxiv.org/abs/1208.5519v3.

[4] V. Dokchitser, Root numbers of non-abelian twists of elliptic curves, Proc. London Math. Soc. (3) 91 (2005) 300–324. With an appendix by Tom Fisher.

[5] N.D. Elkies, Elliptic curves over QQ with identical 13-isogeny, 2013. Published online as an answer on math-overflow.net, http://mathoverflow.net/questions/129818/elliptic-curves-over-qq-with-identical-13-isogeny.

[6] T.A. Fisher, On 5 and 7 Descents for Elliptic Curves, Ph.D. thesis, Clare College, 2000. https://www.dpmms.cam.ac.uk/~taf1000/thesis.html.

[7] M. Flach, A generalisation of the Cassels-Tate pairing, J. Reine Angew. Math. 412 (1990) 113–127.

[8] A. Jorza, The Birch and Swinnerton-Dyer Conjecture for Abelian Varieties over Number Fields, Master's thesis, Harvard University, 2005. http://www3.nd.edu/~ajorza/.

[9] N.M. Katz, Galois properties of torsion points on abelian varieties, Invent. Math. 62 (1981) 481–502.

[10] S. Keil, R.N. Kloosterman, On the density of abelian surfaces with Tate-Shafarevich group of order five times a square, in: ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, San Diego 2012, volume 1 of *Open Book Series*, Mathematical Sciences Publishers, Berkeley, 2013, pp. 413–435.

[11] R. Kloosterman, Elliptic curves with large Selmer groups, 2001. http://www.mathematik.hu-berlin.de/~klooster/publ.php.

[12] R. Kloosterman, E.F. Schaefer, Selmer groups of elliptic curves that can be arbitrarily large, J. Number Theory 99 (2003) 148–163.

[13] S. Lang, Algebraic groups over finite fields, Amer. J. Math. 78 (1956) 555–563.

[14] B. Mazur, Modular curves and the Eisenstein ideal, IHES Publ. Math. 47 (1977) 33–186.

[15] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. 44 (1978) 129–162.

[16] J. Milne, Arithmetic Duality Theorems, BookSurge, LLC, second edition, 2006.

[17] B. Poonen, M. Stoll, The Cassels-Tate pairing on polarized abelian varieties, Ann. of Math. (2) 150 (1999) 1109–1149.

[18] E.F. Schaefer, Class groups and Selmer groups, J. Number Theory 56 (1996) 79–114.

[19] E.F. Schaefer, M. Stoll, How to do a p-descent on an elliptic curve, 2001. Long online version.

[20] J.P. Serre, Galois cohomology, Springer Monographs in Mathematics, Springer-Verlag, Berlin, English edition, 2002.

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

[22] W.A. Stein, Possibilities for Shafarevich-Tate Groups of Modular Abelian Varieties, 2003. `http://modular.math.washington.edu/papers/nonsquaresha/`.

[23] W.A. Stein, Shafarevich-Tate groups of nonsquare order, in: Modular curves and abelian varieties, volume 224 of *Progr. Math.*, Birkhäuser, Basel, 2004, pp. 277–289.

[24] W.A. Stein, Computational verfication of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves, Math. Comp. 78 (2009) 2397–2425.

[25] W.A. Stein, et al., Sage, open-source mathematics software system licensed under the GPL, version 4.6.2, `http://www.sagemath.org/`, 2013.

[26] J. Tate, Duality theorems in Galois cohomology over number fields, in: Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295.

[27] 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), Springer, Berlin, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.

[28] J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, in: Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. 415–440.

[29] J. Vélu, Isogénies entre courbes elliptiques, C. R. Acad. Sci. Paris Sér. A-B 273 (1971) A238–A241.