Arbitrarily large torsion in the Tate-Shafarevich groups

Author: Mashal Mehr
Supervisor: Valentijn Karemaker
Second reader: Soumya Sankar

Universiteit Utrecht
Faculty of Science
Mathematical Sciences

Abstract

We say that an abelian variety satisfies the Hasse principle if it has a $\mathbb{Q}$-rational point whenever it has $\mathbb{R}$-rational point and a $\mathbb{Q}_p$-rational point for all primes p. For every abelian variety it is possible to construct its Tate-Shaferevich group. The elements of this group correspond with twists of the abelian variety that violate the Hasse principle. So the study of abelian varieties that violate the Hasse principle is equivalent to the study of their Tate-Shafarevich group.

In a recent paper by Flynn and Shnidman (2022) it is shown that for any prime $p > 3$ there exist absolutely simple abelian varieties over $\mathbb{Q}$ with arbitrarily large p-torsion in their Tate-Shafarevich group. In this thesis we will examine how Flynn and Shnidman achieved this result by constructing explicit μ_p-covers of certain Jacobians that violated the Hasse principle. Furthermore, we will explore how we can generalize these results to arbitrary integers n and what the μ_n-covers of such Jacobians look like in this case.

Additionally, we examine the case $p = 2$ by approaching a paper by Lemmermeyer and Mollin (2003) using the language of μ_2-covers and contrasting the results we acquire with the results of the paper.

Acknowledgements

I would like to thank my supervisor Valentijn Karemaker for guiding me throughout the process and always offering helpful insights. She was always ready to answer my questions and uplifting me when my own confidence failed me.

I would also like to thank my second reader Soumya Sankar for reading my thesis and giving me helpful comments.

I would like to thank my partner for always being there for me in tough times and good times, and always cheering me on and believing in me.

Lastly, I would like to thank my family for their support and their interest in my thesis. Hopefully it all sounded very interesting.

1 Introduction

In mathematics one often encounters situations where a global result can be turned into a local one or vice versa. An example of turning a local result to a global one are partitions of unity, which are used in analysis and geometry to combine a collection of locally defined functions into a globally defined one. Generally however, it is more common and easier to turn a global condition into a local condition. One such example occurs in number theory when looking at rational solutions of equations. The rational numbers embed into the real numbers and the p-adic numbers for all primes p, so it is possible to find a local solutions over the real numbers and the p-adic numbers from global rational solutions. Naturally, the question arises whether it is possible to reverse this process and construct global solutions from local solutions. We say that an algebraic variety Y satisfies the Hasse principle if $Y(\mathbb{Q}) \neq \emptyset$ whenever $Y(\mathbb{Q}_p) \neq \emptyset$ for all primes $p \leq \infty$ of $\mathbb{Q}$. The Hasse-Minkowski theorem shows that the Hasse principle holds for quadratic forms over the rational numbers, but in general the principle does not hold. An example of a violation of the Hasse principle by Selmer is the cubic form $3x^3 + 4y^3 + 5z^3 = 0$ [22]. This particular is a genus one curve C, and thus represents a torsor under its Jacobian, the elliptic curve $E = \mathrm{Pic}^0(C)$. For elliptic curves the Tate-Shafarevich group $Ш(E)$ parametrizes the locally trivial E-torsors and $[C]$ is thus a non-trivial element of $Ш(E)$, whose order in $Ш(E)$ turns out to be 3. Studying the Tate-Shafarevich group thus provides an opportunity to study varieties which violate the Hasse priniciple. For an abelian variety A over $\mathbb{Q}$ the Tate-Shafarevich group $Ш(A)$ parametrizes the A-torsors which violate the Hasse principle.

In this thesis we will be looking at the paper "*Arbitrarily large p-torsion in Tate-Shafarevich groups.*"[5]. In this paper the authors Flynn and Shnidman look at Jacobians of curves of the form $y^p = x(x-1)(x-a)$. They construct μ_p-covers of these Jacobians and show that for certain values of a they can twist these covers to find covers that violate the Hasse principle. This shows that for any prime p there exist absolutely simple abelian varieties over $\mathbb{Q}$ with arbitrarily large p-torsion in the Tate-Shafarevich group.

The main result of the paper is the following theorem. To state the theorem we define $\left(\frac{q}{l}\right)_p = 1$ if q is a p-th power in $\mathbb{Q}_l^*$, otherwise we define $\left(\frac{q}{l}\right)_p = -1$.

Theorem 1.1. *Let $p > 3$ be a prime. Let $g = p-1$ and let u, v be integers not divisible by 3. Consider the variety $\tilde{A} \subset \mathbb{A}_{\mathbb{Q}}^{2g+1}$ defined by the equations*

$$y_i^p = x_i(x_i - 3uk)(x_i - 9vk) \text{ and } z^p = \prod_{i=1}^{g} x_i(x_i - 3uk). \tag{1}$$

for $i = 1, \ldots, g$. The symmetric group S_g acts on $\tilde{A}$ and the quotient $\tilde{A}/S_g$ birational to a unique g-dimensional abelian variety A over $\mathbb{Q}$.

Let U be the set of primes dividing $3puv(u-3v)$. Suppose k is the product of the primes $p_1, \ldots, p_t$, which are distinct primes not contained in U, that satisfy the following conditions:

1. $\left(\frac{p_i}{p_j}\right)_p = 1$ *for all $i \neq j$ in $\{1, 2, \ldots, t\}$,*
2. $\left(\frac{p_i}{q}\right)_p = 1$ *for all i in $\{1, 2, \ldots, t\}$ and all $q \in U$,*
3. $\left(\frac{q}{p_i}\right)_p = 1$ *for all i in $\{1, 2, \ldots, t\}$ and all $q \in U - \{3\}$,*
4. $\left(\frac{3}{p_i}\right)_p = -1$ *for all i in $\{1, 2, \ldots, t\}$.*

Let I be any proper non-empty subset of $\{1, \ldots, t\}$ and let $q = \prod_{i \in I} p_i$. Let $\tilde{X} \subset \mathbb{A}_{\mathbb{Q}}^{2g+1}$ be defined by the equations

$$y_i^p = x_i(x_i - 3uk)(x_i - 9vk) \text{ and } qz^p = \prod_{i=1}^{g} x_i(x_i - 3uk). \tag{2}$$

for $i = 1, \ldots, g$. Then $\tilde{X}/S_g$ is birational to an A-torsor X that violates the Hasse principle, and the class of X in $Ш(A)$ has order p.

This theorem gives us an explicit construction of A-torsors X which violate the Hasse principle.

From this theorem we can deduce that the Tate-Shafarevich groups of simple abelian varieties over $\mathbb{Q}$ have arbitrarily large p-torsion.

Theorem 1.2. *For every prime p and every integer $k \geq 1$, there exists an absolutely simple abelian variety A over $\mathbb{Q}$ with $\#\text{Ш}(A)[p] \geq p^k$.*

Since this gives us an explicit construction we can construct varieties whose Tate-Shafarevich group contains elements of arbitrarily large p-torsion. A minimal example for $p = 29$ of such a variety is given by the authors.

Example 1.3. *Let $\tilde{X} \subset \mathbb{A}^{28}_{\mathbb{Q}} \times \mathbb{A}^{28}_{\mathbb{Q}} \times \mathbb{A}^{1}_{\mathbb{Q}}$ be the variety defined by the 28 equations*

$$y_i^{29} = x_i(x_i - 3 \cdot 386029093 \cdot 545622299)(x_i + 9 \cdot 386029093 \cdot 545622299)$$

for $i = 1, \ldots, 28$, as well as the additional equation

$$386029093 z^p = \prod_{i=1}^{28} x_i(x_i - 3 \cdot 386029093 \cdot 545622299).$$

Then $\tilde{X}/S_g$ is birational to a torsor X for a 28-dimensional abelian variety A over $\mathbb{Q}$. Moreover, X violates the Hasse principle and represents an order 29 element of $\text{Ш}(A)$.

We will try to generalize these results and examine n-torsion in the Tate-Shafarevich group for integers of the form $n = p_1 \ldots p_t$ where $p_1, \ldots, p_t$ are distinct primes. We will construct μ_n-covers in this case and we will examine their properties. In particular, we will find that these μ_n-covers decompose uniquely into μ_{p_i}-covers by looking at how the μ_n-action on our μ_n-covers decomposes into μ_{p_i}-actions. This approach is based on equivalence of categories where we describe a μ_n-cover of a variety Y in terms of invertible sheaves on Y.

We will start in Section 2 by going over the prelimaries we will need for this thesis. We will then move on to Section 3 where we introduce μ_p-covers and μ_p-descent on these covers. We will be following the contents and structure of [5] for this section. This section serves to introduce notation and various constructions we will use. Since this section is quite technical in the original paper, we will omit most of the proofs and refer to the paper for the proofs. In Section 4 we will specialize the discussion to Jacobians of superelliptic curves. We will construct the μ_p-covers of such Jacobians and describe what the maps for μ_p-descent look like.

In Section 5 we prove Theorem 1.1. We show that the torsors violate the Hasse principle by showing that they contain $\mathbb{Q}_l$-points for all primes $l \leq \infty$, but no $\mathbb{Q}$-points. This goes well for almost all primes, but for the primes $l = p_i$ we have to be careful. Here we show that locally at these primes the torsion points $D_0 = (0, 0) - \infty$ and $D_1 = (3uk, 0) - \infty$ on J generate a certain quotient of $J(\mathbb{Q}_{p_i})$ for each prime p_i and use the special prime 3 to show these local points do not glue to a global point. The choice of 3 here is not special. In Section 6 we use the Chebotarev density theorem and a result by Masser to show that for any $t \geq 0$ we can find suitable primes $p_1, \ldots, p_t$ for Theorem 1.1 and that the variety A is absolutely simple. We can then use Theorem 1.1 to deduce Theorem 1.2.

In Section 7 we will generalize the results of Flynn and Shnidman and examine μ_n-covers for an integer n which is a product of distinct primes $p_1, \ldots, p_t$. We will show that these μ_n-covers decompose into μ_{p_i}-covers in a unique manner for all the primes p_i. We also try extend these results to find arbitrarily large n-torsion in the Tate-Shafarevich group and discuss where we fall short of proving this. Lastly, in Section 8 we apply the theory of μ_p-covers to the case where $p = 2$. In a paper by Lemmermeyer and Mollin [13] they prove that the elliptic curve $y^2 = x(x^2 - k^2)$ has arbitrarily large 2-torsion in the Tate-Shafarevich group for certain k. We examine their results through the lens of μ_2-covers and discuss the differences of working with μ_2-covers and μ_p-covers for odd primes p.

Contents

2 Preliminaries

2.1 Some scheme theory

We will use the language of algebraic varieties and schemes throughout this thesis, which can be found in Section I and Section II of [7]. In this section we will highlight some specific terms and constructions that will come up in the paper.

2.1.1 Group schemes

In this section we will go over the concepts of group schemes and introduce the main example of a group scheme that we will be working with.

For this let us recall the definition of a group.

Definition 2.1 (Group)**.** *A group is a pair (G, m), where G is a set and $m : G \times G \to G$ is a map of sets, called the multiplication map, satisfying the following properties:*

1. *The map m is associate, i.e., we have that $m(g, m(g', g'')) = m(m(g, g'), g'')$ for all $g, g', g'' \in G$.*
2. *There exists a unique element $e \in G$ such that $m(g, e) = m(e, g) = g$ for all $g \in G$.*
3. *For every element $g \in G$ there exists an element $i(g) \in G$ such that $m(g, i(g)) = m(i(g), g) = e$.*

This gives us an element $e \in G$ called the identity element and a $i : G \to G$ called the inverse map. Therefore, we can call a set G a group if we can specify that the quadruple (G, m, e, i) exists and satisfies the above axioms.

With the above definition of a group we define a group scheme as follows:

Definition 2.2 (Group scheme)**.** *A group scheme over S is a pair (G, m) where G is a scheme over S and $m : G \times_S G \to G$ is a morphism of schemes over S such that for every scheme T over S the pair $(G(T), m)$ is a group.*

We get the morphisms of schemes over S, $e : S \to G$ and $i : G \to G$, corresponding to the identity and inverse morphism respectively, such that for every scheme T over S the quadruple $(G(T), m, e, i)$ satisfies the above axioms equal to the definition of a group.

An important group scheme that is related to the primary group scheme that we will be working with is the multiplicative group scheme over F.

Example 2.3 (Multiplicative group scheme)**.** *Let F be a field. The multiplicative group scheme over F is defined as $\mathbb{G}_{m,F} :=$ Spec$F[T, T^{-1}]$. The morphism $m : \mathbb{G}_{m,F} \times_F \mathbb{G}_{m,F} \to \mathbb{G}_{m,F}$ is defined by the homomorphisms:*

$$F[T, T^{-1}] \to F[T, T^{-1}] \otimes_F F[T, T^{-1}], \tag{3}$$

$$T \mapsto T \otimes_F T. \tag{4}$$

The identity morphism $e :$ Spec$F \to \mathbb{G}_{m,F}$ is then defined by the homomorphism

$$F[T, T^{-1}] \to F, \tag{5}$$

$$T \mapsto 1, \tag{6}$$

and the inverse morphism $i : \mathbb{G}_{m,F} \to \mathbb{G}_{m,F}$ is defined by the homomorphism

$$F[T, T^{-1}] \to F[T, T^{-1}], \tag{7}$$

$$T \mapsto T^{-1}. \tag{8}$$

The primary group scheme we will be working with is the F-group scheme μ_n of the n-th roots of unity, which is a closed subvariety of the multiplicative group scheme.

Example 2.4 (Roots of unity). *Let n be a positive integer. We define the n-th roots of unity over F as the group scheme over F given by $\mu_{n,F} :=$ Spec$(F[T]/(T^n-1))$. The morphism $m : \mu_{n,F} \times_F \mu_{n,F} \to \mu_{n,F}$ is defined by the homomorphisms:*

$$\mu_{n,F} \to \mu_{n,F} \otimes_F \mu_{n,F}, \tag{9}$$
$$T \mapsto T \otimes_F T. \tag{10}$$

The identity morphism $e :$ SpecF $\to \mu_{n,F}$ is then defined by the homomorphism

$$\mu_{n,F} \to F, \tag{11}$$
$$T \mapsto 1, \tag{12}$$

and the inverse morphism $i : \mathbb{G}_{m,F} \to \mathbb{G}_{m,F}$ is defined by the homomorphism

$$\mu_{n,F} \to \mu_{n,F}, \tag{13}$$
$$T \mapsto T^{-1}. \tag{14}$$

Definition 2.5 (Algebraic variety). *An algebraic variety V over a field F is a geometrically reduced separated scheme of finite type over F, where we omit the nonclosed points of the base space.*

With this definition in mind we define a group variety as:

Definition 2.6 (Group variety). *Let F be a field. A group variety over F is an algebraic variety V over F together with regular maps*

$$m : V \times_F V \to V \text{ (multiplication)}, \tag{15}$$
$$i : V \to V \text{ (inverse)}, \tag{16}$$

and an element $e \in V(F)$ such that the structure on $V(\bar{F})$ defined by m and i is a group structure with identity element $e_V = e$.

2.2 Abelian varieties

In this section we will introduce abelian varieties and introduce important concepts and tools related to them. The approach we take will be based on Milne's notes on abelian varieties [15].

Definition 2.7 (Abelian variety). *An abelian variety A is a group variety that is complete.*

As the name implies the group structure on A turns out to be commutative, but to show this requires some technical work, so we will refer to Milne's notes [15, Corollary I.1.4]. We will write the group law additively and the identity element e will be denoted by 0.

We will introduce some basic properties of abelian varieties. A property that all group varieties share, and thus abelian varieties, is that they are smooth. For this let V be a group variety over a field F. We can define the right translation t_a by an element $a \in V$ as the composite

$$V \to V \times V \xrightarrow{m} V, \tag{17}$$
$$x \mapsto (x, a) \mapsto x + a. \tag{18}$$

On the level of points, this map is given by $x \mapsto x+a$. This map is an isomorphism $V \to V$ with inverse $t_{i(a)}$.

Lemma 2.8. *Every group variety V is smooth.*

Proof. Every variety contains a smooth dense open subvariety U. Using translates we can cover the whole of V with U. □

Another property of abelian varieties is that they are projective. Similar to showing commutativity, proving this is not trivial and we refer to Milne's notes [15, Chapter I.6].

We can now define morphisms of abelian varieties as follows.

Definition 2.9 (Homomorphisms of abelian varieties). *A homomorphism $f : A \to B$ is a morphism of varieties and also a group homomorphism. We define the kernel of f as the fibre of f over 0_B, i.e., it is the set $\ker f = f^{-1}(0_B)$.*

A particular type of homomorphisms we are interested in are isogenies.

Definition 2.10 (Isogenies)**.** *We call a homomorphism $\alpha : A \to B$ of abelian varieties an isogeny if α is surjective and has finite kernel.*

We define the degree of α as its degree as a regular map, i.e., the degree of the field extension $[F(A) : \alpha^* F(B)]$. If α is separable then the degree is equal to the size of the kernel of α. Given another isogeny $g : B \to C$ we get that $\deg(g \circ f) = \deg(g)\deg(f)$.

Proposition 2.11. *Let $\alpha : A \to B$ be a homomorphism of abelian varieties. The following statements are equivalent:*

1. *α is an isogeny,*
2. *$\dim A = \dim B$ and α is surjective,*
3. *$\dim A = \dim B$ and $\ker \alpha$ is finite,*
4. *α is finite, flat and surjective.*

Proof. For a proof we refer to Milne [15, Proposition I.7.1]. □

An example of an important isogeny is multiplication by a positive integer n.

Example 2.12 (Multiplication by n)**.** *Let A be an abelian variety of dimension g and let n be a positive integer. Then the homomorphism $n_A : A \to A$ given by*

$$a \mapsto na = a + \cdots + a, \tag{19}$$

is an isogeny of degree 2^g. Let $f : A \to B$ be an isogeny of degree n. Then we have that $\ker f \subset \ker n_A$, so we can factor n_A as $n_A = h \circ f$ for some isogeny $h : B \to A$.

Another type of abelian varieties we are interested in are absolutely simple abelian varieties.

Definition 2.13. *Let A be an abelian variety over a field F. We say that A is simple if for every abelian variety $B \subseteq A$, we have that $B = A$ or $B = \emptyset$. We say that A is absolutely simple if it is simple over the algebraic closure of F.*

The most elementary example of an absolutely simple abelian variety is an elliptic curve.

Example 2.14. *Let E be an elliptic curve. Then E is an absolutely simple abelian variety. Since E has dimension 1, every proper abelian subvariety must have dimension 0. So the only proper subvariety of E is the empty set.*

For n a positive integer not divisible by the characteristic of F we define

$$A_n(F) := \ker(n_A : A(F) \to A(F)), \tag{20}$$

has order n^{2g} and is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2g$. For a field F we denote its separable closure by F^{sep}. For a fixed prime $l \neq \text{char}(F)$, we define the Tate module as the limit

$$T_l A = \lim_{\leftarrow} A_{l^n}(F^{\text{sep}}), \tag{21}$$

and we write $V_l A = T_l A \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. For an abelian variety A one can show that $\text{End}^0(A) = \text{End}(A) \otimes \mathbb{Q}$ is a finite-dimensional algebra over $\mathbb{Q}$. We can then express an element of $\text{End}^0(A)$ as a polynomial.

Definition 2.15 (Characteristic polynomial)**.** *Let A be an abelian variety over a field F. For $\alpha \in \mathit{End}^0(A)$ there is a monic polynomial $P_\alpha(X) \in \mathbb{Q}[X]$ of degree $2g$ such that $P(n) = \deg(n_A - \alpha)$ for all $n \in \mathbb{Z}$. We call $P_\alpha(X)$ the characteristic polynomial of α. If we write $P(X) = \sum_{i=0}^{2g} a_i X^i$, then we define the trace of α as $\mathit{Tr}(\alpha) := -a_{2g-1}$ and the norm as $\mathit{Nm}(\alpha) := \deg \alpha = a_0$.*

We stated this definition as a fact, but it requires technical work to get to this statement and we refer to [15, Chapter I.10] of Milne's notes. We are primarily interested in the following result which we will state without proof.

Proposition 2.16 ([15], Proposition I.10.23)**.** *Let K be a $\mathbb{Q}$-subalgebra of $\mathit{End}(A) \otimes \mathbb{Q}$ and assume that K is a field. Let $f = [K : \mathbb{Q}]$. Then $V_l(A)$ is a free $K \otimes_{\mathbb{Q}} \mathbb{Q}_l$-module of rank $(2\dim A)/f$. Therefore, the trace of α, as an endomorphism of A, is $(2\dim A/f)\mathit{Tr}_{K/\mathbb{Q}}(\alpha)$ and $\deg(\alpha) = \mathit{Nm}_{K/\mathbb{Q}}(\alpha)^{2\dim A/f}$.*

2.2.1 The dual abelian variety

In this section we will introduce the dual variety $\widehat{A}$ of an abelian variety A. This dual variety naturally comes as a pair with A and serves to parametrize the elements of Pic$^0(A)$.

We start with the Theorem of the Square which tells us that:

Theorem 2.17 ([15], Theorem I.5.5). *For all invertible sheaves $\mathcal{L}$ on A and points $a, b \in A(k)$ we have an isomorphism of sheaves:*

$$t_{a+b}^*\mathcal{L} \otimes \mathcal{L} \simeq t_a^*\mathcal{L} \otimes t_b^*\mathcal{L}. \tag{22}$$

Remember that the Picard group of a variety X is the set of isomorphm classes of invertible sheaves of X and is denoted by Pic(X). By tensoring the isomorphism (22) with $\mathcal{L}^{-2}$ we find that

$$t_{a+b}^*\mathcal{L} \otimes \mathcal{L}^{-1} \simeq (t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}) \otimes (t_b^*\mathcal{L} \otimes \mathcal{L}^{-1}), \tag{23}$$

using the properties of the tensor product. This tells us that the map $a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is a homomorphism which we will denote by $\lambda_{\mathcal{L}} : A(k) \to \text{Pic}(A)$. We then define Pic$^0(A)$ as the subgroup of Pic(A) such that $\lambda_{\mathcal{L}} = 0$, or in other words, it is the group containing the ismorphism classes of invertible sheaves $\mathcal{L}$ on A such that $t_a^*\mathcal{L} \simeq \mathcal{L}$ for all $a \in A(\bar{F})$.

Let us consider the sheaf $m^*\mathcal{L} \otimes p * \mathcal{L}^{-1}$ on $A \times A$, where m and p are the maps sending (b, a) to $b + a$ and b respectively. Let q be the projection on the other component. Then we can think of the sheaf $m^*\mathcal{L} \otimes p * \mathcal{L}^{-1}$ as a family of invertible sheaves on $A = p(A \times A)$ parametrized by $A = q(A \times A)$. If we choose a point $a \in A(F)$ we get the invertible sheaf $(m^*\mathcal{L} \otimes p * \mathcal{L}^{-1})|_{A\times\{a\}}$. Note that on $A \times \{a\}$ the map m corresponds to t_a and p to the identity, so we find that

$$(m^*\mathcal{L} \otimes p * \mathcal{L}^{-1})|_{A\times\{a\}} = t_a^*\mathcal{L} \otimes \mathcal{L}^{-1} = \lambda_{\mathcal{L}}(a). \tag{24}$$

We can see that the sheaf $m^*\mathcal{L} \otimes p * \mathcal{L}^{-1}$ gives us another way to characterize the group Pic$^0(A)$. For this we define the following set:

$$K(\mathcal{L}) = \{a \in A \,|\, (m^*\mathcal{L} \otimes p * \mathcal{L}^{-1})|_{A\times\{a\}} \text{ is trivial}\}. \tag{25}$$

Looking at the F-points of $K(\mathcal{L})$ we find that

$$K(\mathcal{L})(F) = \{a \in A(F) \,|\, \lambda_{\mathcal{L}}(a) = 0\}. \tag{26}$$

We can now state the following result:

Proposition 2.18. *For an invertible sheaf on A, the following conditions are equivalent:*

1. *$K(\mathcal{L}) = A$,*
2. *$t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$ on $A_{\bar{F}}$, for all $a \in A(\bar{F})$,*
3. *$m^*\mathcal{L} \simeq p^*\mathcal{L} \otimes q^*\mathcal{L}$.*

Proof. For a proof we refer to Milne [15, Proposition I.8.4]. □

Thus we can now define the group Pic$^0(A)$ as follows:

Definition 2.19. *The group Pic$^0(A)$ is the set of all isomorphism classes of invertible sheaves $\mathcal{L}$ of A satisfying the conditions of Proposition 2.18.*

With the above description of Pic$^0(A)$ the elements work nicely in the following way. Let $\alpha, \beta : V \to A$ be two morphisms of varieties. We can write the sum $\alpha + \beta$ as $m \circ (\alpha \times \beta)$. The isomorphism of the third statement of Proposition 2.18 then tells us that

$$(\alpha + \beta)^*\mathcal{L} \simeq \alpha^*\mathcal{L} \otimes \beta^*\mathcal{L}. \tag{27}$$

This gives us a homomorphism of groups

$$\text{Hom}(V, A) \to \text{Hom}(\text{Pic}^0(A), \text{Pic}(V)), \tag{28}$$

and in particular if we set $V = A$ we get a homomorphism

$$\text{End}(A) \to \text{End}(\text{Pic}^0(A)). \tag{29}$$

Inductively applying (27) to the isogeny $n_A = 1_A + \cdots + 1_A$ we find that $(n_A)^*\mathcal{L} \simeq \mathcal{L}^n$.

We can now give a definition of the dual variety.

Definition 2.20 (Dual of an abelian variety). *Consider the pair $(\widehat{A}, \mathcal{P})$ with $\widehat{A}$ and abelian variety and $\mathcal{P}$ an invertible sheaf on $A \times \widehat{A}$, that satisfy the universal properties:*

1. *$\mathcal{P}_{\{0\}\times\widehat{A}}$ is trivial and for $a \in \widehat{A}$, $\mathcal{P}|_{A\times\{a\}}$ is an element of Pic$^0(A_a)$,*
2. *For any variety T over F and $\mathcal{L}$ an invertible sheaf on $A \times T$ such that $\mathcal{L}_{\{0\}\times T}$ is trivial and for $t \in T$, $\mathcal{L}|_{A\times\{t\}}$ is an element of Pic$^0(A_t)$, there is a unique morphism $f : T \to \widehat{A}$ such that $(1 \times f)^*\mathcal{P} \simeq \mathcal{L}$.*

We call $\widehat{A}$ the dual variety of A and we call $\mathcal{P}$ the Poincaré sheaf.

Remember that we described the dual variety as a way to parametrize elements of $\text{Pic}^0(A)$. Let us examine how this takes place. For this we consider a field extension $F \subseteq L$ and we set $T = \text{Spec}(L)$. Let $\mathcal{L}$ be an invertible sheaf on $A_L = A \times \text{Spec}(L)$ satisfying the universal property. Then we have that $\mathcal{L}|_{A_L}$ lies in $\text{Pic}^0(A_L)$. In particular, we have that $\widehat{A}(L) = \text{Pic}^0(A_L)$, so we get a one to one correspondence between the L-points of $\widehat{A}$ and the isomorphism classes of sheaves in $\text{Pic}^0(A_L)$. If we make the substitution $L = \bar{F}$ we get that $\widehat{A}(\bar{F}) = \text{Pic}^0(A_{\bar{F}})$. The invertible sheaf $\mathcal{L}$ described before corresponds to a unique morphism $f : \text{Spec}(\bar{F}) \to \widehat{A}$. Since $\text{Pic}^0(A_{\bar{F}})$ is parametrized by the family of sheaves $\{\mathcal{P}_a \mid a \in \widehat{A}(\bar{F})\}$, it follows that there is a unique point $a_f \in \widehat{A}(\bar{F})$ such that $\mathcal{P}_{a_f} \simeq \mathcal{L}$.

So the dual abelian variety $\widehat{A}$ has the properties we desire. Additionally, for every abelian variety A the dual variety $\widehat{A}$ exists and is unique up to unique isomorphism by the universal property. For the construction of the dual variety we refer to Milne's notes [15, Chapter I.8]. Once we have the dual of an abelian variety A, we can look at the dual variety of the dual itself and we find that $\widehat{\widehat{A}} \simeq A$.

Let $\alpha : A \to B$ be a homomorphism of abelian varieties and let $\mathcal{P}_B$ be the Poincaré sheaf on $B \times \widehat{B}$. By the universal property of the dual variety the invertible sheaf $(\alpha \times 1)^*\mathcal{P}_B$ on $A \times \widehat{B}$ gives rise to a homomorphism $\widehat{\alpha} : \widehat{B} \to \widehat{A}$ such that $(1 \times \widehat{\alpha})^*\mathcal{P}_A \simeq (\alpha \times 1)^*\mathcal{P}_B$. On the level of points, the map $\widehat{\alpha}$ is the map $\text{Pic}^0(B) \to \text{Pic}^0(A)$ that sends the isomorphism class of an invertible sheaf on B to its inverse image in A. Additionally, if α is an isogeny then we have the following result:

Theorem 2.21 ([15], Theorem I.9.1). *If $\alpha : A \to B$ is an isogeny, then the dual morphism $\widehat{\alpha} : \widehat{B} \to \widehat{A}$ is an isogeny with kernel $\widehat{\ker\alpha}$, the Cartier dual of $\ker\alpha$. Equivalently, the exact sequence*

$$0 \to \ker\alpha \to A \to B, \tag{30}$$

gives rise to a dual exact sequence

$$0 \to \widehat{\ker\alpha} \to \widehat{B} \to \widehat{A}. \tag{31}$$

Corollary 2.22. *Let $\alpha : A \to B$ be an isogeny. Then the morphism $\widehat{\widehat{\alpha}} : \widehat{\widehat{A}} \to \widehat{\widehat{B}}$ is equal to α up to post-composition with an automorphism of $B \simeq \widehat{\widehat{B}}$.*

Proof. By Theorem 2.21 the kernel of the morphism $\widehat{\widehat{\alpha}} : \widehat{\widehat{A}} \to \widehat{\widehat{B}}$ is equal to $\widehat{\widehat{\ker\alpha}}$. Note that we have an isomorphism $\widehat{\widehat{\ker\alpha}} \simeq \ker\alpha$. So the kernels of α and $\widehat{\widehat{\alpha}}$ are equal and the isogenies are equal up to automorphism. □

Definition 2.23 (Polarization). *An isogeny of an abelian variety A is an isogeny $\lambda : A \to \widehat{A}$ such that, over $\bar{F}$, λ becomes of the form $\lambda_{\mathcal{L}}$ for some ample sheaf $\mathcal{L}$ on $A_{\bar{F}}$. The degree of the polarization λ is the same as its degree as an isogeny. We call an abelian variety equipped with a polarization a polarized abelian variety. If additionally, the polarization λ has degree 1, then the pair (A, λ) is called a principally polarized abelian variety.*

For a principally polarized abelian variety (A, λ) we can identify A with its dual $\widehat{A}$ via its polarization λ, since it is an isogeny of degree 1 and thus is an isomorphism of abelian varieties.

2.2.2 Jacobian of a curve

Let C be a curve over F of genus g. It is possible to attach an abelian variety to C which inherits the group structure of $\text{Pic}^0(C)$. This abelian variety is called the Jacobian variety of C and in this section we will go over the relevant properties of Jacobians. Our approach is based on Milne's notes [15, Chapter III].

Let us first specify what we mean by a curve over F of genus g.

Definition 2.24 (Curve). *Let F be a field. We define a curve C over F as a projective, smooth algebraic variety over $\bar{F}$ of dimension 1, that is defined by polynomials with coefficients in F. We define the genus of C as the number*

$$g(C) := \dim_F H^1(C, \mathcal{O}_C). \tag{32}$$

This definition of the genus is formally the geometric genus and equal to the arithmetic genus, since we require our curves are smooth.

Recall that for varieties V and T over a field F the T-valued points of V are given by $V(T) = \mathrm{Hom}(T, V)$. For a curve C over F and T a smooth variety over F let $\mathcal{L}$ be an invertible sheaf on $C \times T$. Let $q : C \times T$ be the projectionm on the second coordinate. We can define a functor P_C^0 acting on T as follows:

$$P_C^0(T) = \mathrm{Pic}^0(C \times T)/q^*\mathrm{Pic}^0(T). \tag{33}$$

We call P_C^0 the Picard functor and it is a contravariant functor from the category of varieties over F to the category of abelian groups. We can think of the elements of $P_C^0(T)$ as families of invertible sheaves of degree zero on C parametrized by T, modulo the trivial families.

Definition 2.25 (Jacobian variety). *The Jacobian variety of C is the unique abelian variety $J = Jac(C)$ over F, for which there is a natural transformation $P_C^0 \to J$ such that $P_C^0(T) \to J(T)$ is an isomorphism whenever $C(T) \neq \emptyset$.*

The definition assumes that the Jacobian variety exists and Theorem III.1.6 of [15] ensures that this is the case.

From the definition we see that for any field $F \subseteq L$ for which $C(L) \neq \emptyset$ we have that

$$\mathrm{Pic}^0(C) = P_C^0(L) \simeq J(L). \tag{34}$$

A classic example of a Jacobian is an elliptic curve.

Example 2.26 (Elliptic curve over $\mathbb{Q}$). *An elliptic curve E over $\mathbb{Q}$ is a projective plane curve of the form $Y^2Z = X^3 + aXZ^2 + bZ^3$ over $\mathbb{Q}$ such that $4a^3 + 27b^2 \neq 0$. Equivalently, the elliptic curve E is a smooth projective curve of genus one together with a distinguished point O, which without loss of generality we take to be the point at infinity [25, Proposition III.3.1].*

Let $Div^0(E)$ be the group of divisors of degree zero and let $Pic^0(E)$ be the the quotient of $Div^0(E)$ by the group of principal divisors. This makes $Pic^0(E)$ the group of divisor classes of degree zero on E and it is equal to the Jacobian on E. The Riemann-Roch theorem tells us that the map

$$E(F) \to Pic^0(E)\,,\ P \mapsto [P - O], \tag{35}$$

is a bijection. This induces a group structure on E which coincides with the group law on E defined by the chords and tangents construction.

We can characterize the Jacobian variety of a curve via the symmetric powers of a curve. For this let r be a positive integer. Let S_r be the symmetric group of degree r. It acts on C^r, the product of r copies of C, by permuting the factors. We define the r-th symmetric powers $\mathrm{Sym}^r C$ of C as the quotient whose underlying topological space is C^r/S^r. We say that a morphism $\varphi : C^r \to T$ is symmetric if $\varphi \circ \sigma = \varphi$ for all $\sigma \in S_r$. Then there exists a symmetric morphism $\pi : C^r \to \mathrm{Sym}^r C$ such that any symmetric morphism $\varphi : C^r \to T$ over F factors through π. We also have for any affine open subset U of C, that $\mathrm{Sym}^r(U)$ is an affine open subset of $\mathrm{Sym}^r C$ and it holds that $\Gamma(\mathrm{Sym}^r(U), \mathcal{O}_{\mathrm{Sym}^r(C)}) = \Gamma(U^r, \mathcal{O}_{C^r})^{S_r}$.

For any point $P \in C(F)$ we define the map f^r which is given by

$$f^r : C^r \to J\,,\ (P_1, \ldots, P_r) \mapsto [P_1 + \cdots + P_r - rP] \tag{36}$$

on the level of points. This is a symmetric morphism so it induces a morphism $f^r_{sym} : \mathrm{Sym}^r(C) \to J$. We denote the image of f^r_{sym} with W^r, which forms a closed subvariety of J. It turns out that, for $r \leq g$, the morphism $f^r_{sym} : \mathrm{Sym}^r(C) \to W^r$ is a birational morphism [15, Theorem III.5.1].

In particular, if $r = g$ we get a surjective birational morphism $f^g_{sym} : \mathrm{Sym}^g(C) \to J$. Another important case is when $r = g - 1$. Since the closed subvariety W^{g-1} of J is birationally equivalent to $\mathrm{Sym}^{g-1}(C)$ it is of dimension $g - 1$. This turns W^{g-1} into a divisor on J which we will denote by Θ. The Θ-divisor plays an important role as it turns out that the Jacobian variety is principally polarized via the Θ-divisor.

Theorem 2.27 ([15], Theorem III.6.6). *The map $\varphi_{\mathcal{L}} : J \to \widehat{J}$ is an isomorphism.*

This means that we can identify J with its dual $\widehat{J}$ via the Θ-divisor.

2.3 The Chebotarev density theorem

In this section we will introduce the Chebotarev density theorem. The Chebotarev density theorem describes the behaviour of primes splitting in a field extension F over $\mathbb{Q}$ and tells us how such primes are distributed among the prime numbers. To almost every prime number we can assign an invariant called the Frobenius element, which is a well-defined conjugacy class in the Galois group Gal$(F/\mathbb{Q})$. The theorem then says that the asymptotic distribution of these invariants is uniform over the Galois group.

To make the notion of this distribution precise we introduce the Dirichlet density.

Definition 2.28 (Dirichlet density)**.** *Let S be a set of prime numbers. We say that S has Dirichlet density α if*

$$\lim_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{\sum_p p^{-s}} \to \alpha, \tag{37}$$

where $s \to 1^+$ means that we take the limit $s \to 1$ from above in $\mathbb{R}$.

In practical terms, the Dirichlet density describes the probability of encountering the primes that satisfy the conditions of the set S. A Dirichlet density that is easy to compute is the case when S contains all the prime numbers, as the Dirichlet density then is equal 1. The other extreme case is when S is a finite set.

Corollary 2.29. *A finite set of prime numbers has Dirichlet density 0.*

Proof. For a finite set of prime numbers S we have that $\sum_{p\in S} p^{-s}$ is a finite number when we take the limit $s \to 1^+$. On the other hand, the sum $\sum_p p^{-s}$ tends to ∞ when we take the limit $s \to 1^+$ and the result follows consequently. $\square$

To formulate the density theorem we must first introduce the Frobenius elements of prime numbers.

Definition 2.30 (Decomposition group)**.** *Let L/F be a Galois extension. Let $\mathfrak{q}$ be a prime of L above $\mathfrak{p}$ a prime of F. The decomposition group $D_\mathfrak{q} = D_{\mathfrak{q}/\mathfrak{p}}$ of $\mathfrak{q}$ is the subgroup of Gal(L/F) fixing $\mathfrak{q}$, i.e.,*

$$D_\mathfrak{q} = \{\sigma \in \mathit{Gal}(L/F) \,|\, \sigma(\mathfrak{q}) = \mathfrak{q}\}. \tag{38}$$

Let $\mathcal{O}_L$ be the ring of integers of L. An element σ of the decomposition group $D_\mathfrak{q}$ acts on the residue field $\mathcal{O}_L/\mathfrak{q}$ of $\mathfrak{q}$ by $x \pmod{\mathfrak{q}} \mapsto \sigma(x) \pmod{\mathfrak{q}}$. This map is well-defined as $\mathfrak{q}$ is fixed by σ and we get a natural map

$$\begin{aligned} D_\mathfrak{q} &\to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} \;/\; \mathcal{O}_F/\mathfrak{p}), \\ \sigma &\mapsto \overline{\sigma} : x \pmod{\mathfrak{q}} \mapsto \sigma(x) \pmod{\mathfrak{q}}. \end{aligned}$$

This map is surjective [17, Proposition 9.4]. The decomposition group measures to what extent the prime $\mathfrak{p}$ splits in $\mathcal{O}_L$ into different prime ideals. Since $D_\mathfrak{q}$ contains all the automorphisms of Gal(L/F) that fix $\mathfrak{q}$, it follows that the cosets of Gal$(L/F)/D_\mathfrak{q}$ each permute $\mathfrak{q}$ to a different prime above $\mathfrak{p}$. In particular, we see that $\mathfrak{p}$ does not split if and only if $D_\mathfrak{q}$ is equal to Gal(L/F). On the other hand, $\mathfrak{p}$ totally splits if and only if $D_\mathfrak{q}$ is equal to $\{\mathrm{id}\}$.

Related to the decomposition group we can also define the inertia group as follows.

Definition 2.31 (Inertia group)**.** *Let L/F be a Galois extension and $\mathfrak{q}$ a prime above $\mathfrak{p}$. The inertia subgroup $I_\mathfrak{q} = I_{\mathfrak{q}/\mathfrak{p}}$ of $\mathfrak{q}$ is the normal subgroup of $D_\mathfrak{q}$ that acts trivially on $\mathcal{O}_L/\mathfrak{q}$, i.e.,*

$$I_\mathfrak{q} = \ker(D_\mathfrak{q} \to \mathit{Gal}(\mathcal{O}_L/\mathfrak{q} \;/\; \mathcal{O}_F/\mathfrak{p})). \tag{39}$$

Since the map $D_\mathfrak{q} \to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} \;/\; \mathcal{O}_F/\mathfrak{p})$ is surjective we get an isomorphism of groups $D_\mathfrak{q}/I_\mathfrak{p} \simeq \mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} \;/\; \mathcal{O}_F/\mathfrak{p})$. Since $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} \;/\; \mathcal{O}_F/\mathfrak{p})$ is cyclic it is generated by the Frobenius map $\phi(x) \mapsto x^{|\mathcal{O}_F/\mathfrak{p}|}$.

Definition 2.32 (Frobenius element)**.** *The Frobenius element $\mathit{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is the element of $D_\mathfrak{q}/I_\mathfrak{p}$ that maps to ϕ.*

It is intuitively less clear at first glance, what information the inertia group and the Frobenius element contain about the splitting of primes compared to the decomposition group. The following proposition makes it clear how these two objects are related to the splitting of primes.

Proposition 2.33. *Let L/F be a Galois extension of number fields. Let $\mathfrak{q}$ be a prime of L above $\mathfrak{p}$, a prime of F. Let $e_{\mathfrak{q}/\mathfrak{p}}$ denote the ramification index of $\mathfrak{q}$ and let $f_{\mathfrak{q}/\mathfrak{p}}$ denote the inertia degree of $\mathfrak{q}$. Then we have that:*

1. $|D_{\mathfrak{q}/\mathfrak{p}}| = e_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{q}/\mathfrak{p}}$,
2. $|I_{\mathfrak{q}/\mathfrak{p}}| = e_{\mathfrak{q}/\mathfrak{p}}$,
3. *The order of Frob*$_{\mathfrak{q}/\mathfrak{p}}$ *is* $f_{\mathfrak{q}/\mathfrak{p}}$.

Proof. A proof for 1. and 2. can be found in [17, Proposition 9.6]. Note that the Frobenius element generates $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{q}\ /\ \mathcal{O}_F/\mathfrak{p})$. So we have that

$$|\langle \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \rangle| = |\mathrm{Gal}(\mathcal{O}_L/\mathfrak{q}\ /\ \mathcal{O}_F/\mathfrak{p})| = |D_{\mathfrak{q}/\mathfrak{p}}|/|I_{\mathfrak{q}/\mathfrak{p}}| = e_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{q}/\mathfrak{p}}/e_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}}. \tag{40}$$

□

Example 2.34 (Frobenius element of a cyclotomic extension). *Let ζ_n be a primitive n-th root of unity and consider the Galois extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Let p be a prime number that does not divide n and let $\mathfrak{q}$ be a prime of $\mathbb{Q}(\zeta_n)$ above p. The prime p is then unramified, so $e_{\mathfrak{q}/p} = 1$ and the inertia subgroup is equal to $I_{\mathfrak{q}/p} = \{id\}$. Thus we find that $D_{\mathfrak{q}/p} = \langle Frob_{\mathfrak{q}/p} \rangle$.*

The Frobenius element Frob$_{\mathfrak{q}/p}$ acts as $x \mapsto x^p$ on $\mathcal{O}_{\mathbb{Q}(\zeta_n)/\mathfrak{q}}$ by definition. So we find that Frob$_{\mathfrak{q}/p}(\zeta_n) \equiv \zeta_n^p \pmod{\mathfrak{q}}$. By the congrunce condition on p, the n-th roots of unity are distinct modulo p. So they are also distinct modulo $\mathfrak{q}$ and we can conclude that Frob$_{\mathfrak{q}/p}(\zeta_n) = \zeta_n^p$.

In particular, we have that

$$f_{\mathfrak{q}/p} = \text{ order of } Frob_{\mathfrak{q}/p} = \text{order of } p \text{ in } (\mathbb{Z}/n\mathbb{Z})^*. \tag{41}$$

We can now state the Chebotarev density theorem as follows.

Theorem 2.35 (Chebotarev density theorem). *Let $F/\mathbb{Q}$ be a finite Galois extension. For a conjugacy class $\mathcal{C}$ of Gal$(F/\mathbb{Q})$ the set $S_{\mathcal{C}} = \{p \text{ unramified in } F/\mathbb{Q} \text{ such that } Frob_p \in \mathcal{C}\}$ has Dirichlet density*

$$\frac{|\mathcal{C}|}{|Gal(F/\mathbb{Q})|}. \tag{42}$$

Proof. A proof can be found in [18] or [17, Theorem 13.4]. □

Example 2.36 (Dirichlet's theorem). *Let F be the field $\mathbb{Q}(\zeta_n)$. Let p be a prime number that does not divide n. There exists an isomorphism $\phi : (\mathbb{Z}/n\mathbb{Z})^* \to Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ sending $a \pmod n \mapsto (\zeta_n \mapsto \zeta_n^a)$. So Gal$(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is an abelian group and its conjugacy classes contain only one element. Let $\mathcal{C}_a$ denote the conjugacy class of $\phi(a \mod n)$. By the previous example we find that Frob$_p = \mathcal{C}_a$ if and only if $p \equiv a \pmod n$.*

Now let a be an integer that does not divide n. Then the set $\{p \text{ unramified in } F/\mathbb{Q} \text{ such that } p \equiv a \pmod n\} = \{p \text{ unramified in } F/\mathbb{Q} \text{ such that } Frob_p = \mathcal{C}_a\}$ has Dirichlet density $1/\varphi(n)$ by the Chebotarev density theorem, where φ is the Euler totient function.

2.4 Torsors and coverings

2.4.1 Galois cohomology

In this section we will introduce some of the theory of Galois cohomology and introduce the groups $H^0(G_F, A)$ and $H^1(G_F, A)$. We will do this by first looking at the cohomology of finite groups and then making the adjustment to fit that theory to the theory of Galois cohomology. Our approach is based on [25, Appendix B].

Let G be a finite group and let M be an abelian group on which G acts. We denote the action of G on M by $m \mapsto m^\sigma$ for all $m \in M$ and $\sigma \in G$.

Definition 2.37 (G-module)**.** *Let M be an abelian group with an action of G on it. We say that M is a (right) G-module if the action of G on M satisfies*

$$m^{id} = m, \tag{43}$$
$$(m + m')^\sigma = m^\sigma + m'^\sigma, \tag{44}$$
$$(m^\sigma)^\tau = m^{\sigma\tau}, \tag{45}$$

for all $m, m' \in M$ and $\sigma, \tau \in G$.

For two G-modules M and N, we say that a homomorphism $\phi : M \to N$ is a G-module homomorphism if it commutes with the action of G, i.e.,

$$\phi(m^\sigma) = \phi(m)^\sigma. \tag{46}$$

Definition 2.38 (The 0-th cohomology group)**.** *The 0-th cohomology group of the G-module M is the group $H^0(G, M)$ of G-invariant elements of M,*

$$H^0(G, M) := M^G = \{m \in M \,|\, m^\sigma = m \text{ for all } \sigma \in G\}. \tag{47}$$

If we have an exact sequence of G-modules

$$0 \to P \xrightarrow{\phi} M \xrightarrow{\psi} N \to 0, \tag{48}$$

we get an exact sequence of invariant G-modules

$$0 \to P^G \xrightarrow{\phi^G} M^G \xrightarrow{\psi^G} N^G, \tag{49}$$

with the ϕ^G and ψ^G the morphisms restricted to the invariant modules. It is clear that im$\phi \subseteq \ker\psi$. For the converse let $m \in M^G$ such that $\psi^G(m) = 0$. The previous exact sequence tells us that there exists an element $p \in P$ such that $\phi(p) = m$, but this element does not necessarily lie in P^G. To show that this element gets fixed by G we have that

$$\phi(p^\sigma) = \phi(p)^\sigma = m^\sigma = m = \phi(p). \tag{50}$$

Since ϕ is injective it follows that $p^\sigma = p$ and we have that im$\phi = \ker\psi$. Note that ψ^G is not necessarily surjective.

It is possible to measure the lack of surjectivity by examining the following object.

Definition 2.39 (The first cohomology group)**.** *Let M be a G-module. The group of 1-cochains is defined as the group*

$$C^1(G, M) = \{\text{maps } \xi : G \to M\}. \tag{51}$$

We use the notation ξ_σ to mean $\xi(\sigma)$. The group of 1-cocylces is then defined as the group

$$Z^1(G, M) = \left\{\xi \in C^1(G, M) \,|\, \xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau \text{ for all } \sigma, \tau \in G\right\}, \tag{52}$$

and the group of 1-coboundaries is the group

$$B^1(G, M) = \{\xi \in C^1(G, M) \,|\, \text{there exists an } m \in M \text{ such that } \xi_\sigma = m^\sigma - m \text{ for all } \sigma \in G\}. \tag{53}$$

Note that for all $m \in M$ and $\sigma, \tau \in G$ we have that

$$m^{\sigma\tau} - m = m^{\sigma\tau} - m^\tau + m^\tau - m = (m^\sigma - m)^\tau + (m^\tau - m), \tag{54}$$

so it follows that $B^1(G, M) \subseteq Z^1(G, M)$.

We define the first cohomology group of M as the quotient group

$$H^1(G, M) = \frac{Z^1(G, M)}{B^1(G, M)}. \tag{55}$$

In other words, two 1-cocycles are equivalent if their difference has the form $\sigma \mapsto m^\sigma - m$ for some $m \in M$.

The first cohomology group of M allows us to extend the sequence (49).

Proposition 2.40. *Let*

$$0 \to P \xrightarrow{\phi} M \xrightarrow{\psi} N \to 0, \tag{56}$$

be an exact sequence of G-modules. The there exists a long exact sequence

$$0 \to H^0(G,P) \to H^0(G,M) \to H^0(G,N) \xrightarrow{\delta} H^1(G,P) \to H^1(G,M) \to H^1(G,N). \tag{57}$$

The connecting homomorphism δ is defined as follows:

Let $n \in H^0(G,N) = N^G$. Choose an $m \in M$ such that $\psi(m) = n$ and define a cochain $\xi \in C^1(G,M)$ by $\xi_\sigma = m^\sigma - m$. Note that $\psi(m^\sigma - m) = n^\sigma - n = 0$, so the values of ξ lies in $\ker\psi = im\phi$. Thus, by the injectivity of ϕ the values of ξ lie in P and it follows that $\xi \in Z^1(G,P)$. We define $\delta(n)$ to be the cohomology class of ξ in $H^1(G,P)$.

Proof. A proof can be found in [2]. □

We will now define cohomology for the absolute Galois group. This is a profinite group so we need to take some additional considerations.

Let F be a perfect field and let $\bar{F}$ be its algebraic closure. Let $G_F := \text{Gal}(\bar{F}/F)$ be the Galois group of $\bar{F}$ over F. The group G_F is the inverse limit of Gal(L/F) as L varies over all the finite extensions of K. This makes G_F a profinite group together with the profinite topology. For a G_F-module M we require M to be an abelian group equipped with a discrete topology with an action of G_F on M such that the action is continuous with respect to the topologies on G_F and M.

The 0-th Galois cohomology group for a G_F-module M is then defined in the same way as the 0-th cohomology group for a finite group

$$H^0(G_F, M) := M^{G_F} = \{m \in M \mid m^\sigma = m \text{ for all } \sigma \in G_F\}. \tag{58}$$

The first Galois cohomology group is defined in a similar way to the finite group case, but we require additional structure on the maps we are working with.

Definition 2.41 (The first Galois cohomology group)**.** *Let M be a G_F-module. We say that a map $\xi : G_F \to M$ is continuous if it is continuous with respect to the profinite topology on G_F and the discrete topology on M.*

The group of continuous 1-cocycles from G_F to M, denoted by $Z^1_{cont}(G_F, M)$, is the subset of $Z^1(G_F, M)$ containing all the continuous cocycles, i.e.,

$$Z^1_{cont}(G_F, M) = \{\xi \in Z^1(G_F, M) \mid \xi \textit{ is continuous}\}. \tag{59}$$

Since M has the discrete topology every coboundary $\sigma \mapsto m^\sigma - m$ is automatically continuous. So we have that $B^1_{cont}(G_F, M) = B^1(G_F, M)$.

We then define the first cohomology group of the G_F-module M as the quotient group

$$H^1(G_F, M) = \frac{Z^1_{cont}(G_F, M)}{B^1(G_F, M)}. \tag{60}$$

The exact sequence from Proposition 2.40 is the same for Galois groups.

Theorem 2.42. *Let*

$$0 \to P \xrightarrow{\phi} M \xrightarrow{\psi} N \to 0, \tag{61}$$

be an exact sequence of G_F-modules. The there exists a long exact sequence

$$0 \to H^0(G_F,P) \to H^0(G_F,M) \to H^0(G_F,N) \xrightarrow{\delta} H^1(G_F,P) \to H^1(G_F,M) \to H^1(G_F,N), \tag{62}$$

with the connecting homomorphism defined as in Proposition 2.40.

Proof. The proof is the same as the theorem for finite groups. □

2.4.2 The Selmer group and the Tate-Shafarevich group

Let F be a perfect field and let A and B be abelian varieties over F. Consider the exact sequence

$$0 \to A[\phi] \to A \xrightarrow{\phi} B \to 0, \tag{63}$$

with $\phi : A \to B$ an isogeny of abelian varieties and with $A[\phi]$ denoting the kernel of ϕ. With the use of Galois cohomology we can extend this exact sequence to the long sequence

$$0 \to A[\phi](F) \to A(F) \xrightarrow{\phi} B(F) \xrightarrow{\delta} H^1(G_F, A[\phi]) \to H^1(G_F, A) \xrightarrow{\phi} H^1(G_F, B), \tag{64}$$

which gives us the short exact sequence

$$0 \to B(F)/\phi(A(F)) \xrightarrow{\delta} H^1(G_F, A[\phi]) \to H^1(G_F, A)[\phi] \to 0. \tag{65}$$

Remember that a place v of F is an equivalence class of absolute value functions on F and that F_v is a completion with respect to the place v [6, Chapter 3.5]. Let v be a place of F and let F_v denote the completion of F with respect to v. We can fix an extension of v to the algebraic closure $\bar{F}$, which gives us an embedding $\bar{F} \subset \bar{F}_v$. This gives us a decomposition group $G_v \subset G_F$ which acts on $A(\bar{F}_v)$ and $B(\bar{F}_v)$. So we can take the Galois cohomology on $A(\bar{F}_v)$ and $B(\bar{F}_v)$ as before and get the exact short sequence

$$0 \to B(F_v)/\phi(A(F_v)) \xrightarrow{\delta} H^1(G_v, A[\phi]) \to H^1(G_v, A)[\phi] \to 0. \tag{66}$$

We have the natural inclusions $G_v \subset G_F$ and $A(\bar{F}_v)$ and $B(\bar{F}_v)$. The corresponding restriction maps allows us to make the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & B(F)/\phi(A(F)) \arrow[r, "\delta"] \arrow[d] & H^1(G_F, A[\phi]) \arrow[r] \arrow[d] & H^1(G_F, A)[\phi] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v B(F_v)/\phi(A(F_v)) \arrow[r, "\delta"] & \prod_v H^1(G_v, A[\phi]) \arrow[r] & \prod_v H^1(G_v, A)[\phi] \arrow[r] & 0
\end{tikzcd} \tag{67}$$

From this commutative diagram we can construct the following two groups.

Definition 2.43 (Selmer group of ϕ). *Let $\phi : A \to B$ be an isogeny of abelian varieties. The Selmer group of ϕ of A is the subgroup of $H^1(G_F, A[\phi])$ defined by*

$$\mathit{Sel}^{(\phi)}(A/F) = \ker\left\{H^1(G_F, A[\phi]) \to \prod_v H^1(G_v, A)\right\}. \tag{68}$$

Definition 2.44 (Tate-Shafarevich group of A). *Let A be an abelian variety. The Tate-Shafarevich group of A is the subgroup of $H^1(G_F, A)$ defined by*

$$\text{Ш}(A/F) = \ker\left\{H^1(G_F, A) \to \prod_v H^1(G_v, A)\right\}. \tag{69}$$

In the next section we will discuss how the elements of the group $\text{Ш}(A/F)$ measure the extent to which the Hasse principle fails to hold for A.

Theorem 2.45. *Let $\phi : A \to B$ be an isogeny of abelian varieties defined over F. We have the following exact sequence*

$$0 \to B(F)/\phi(A(F)) \to \mathit{Sel}^{(\phi)}(A/F) \to \text{Ш}(A/F)[\phi] \to 0. \tag{70}$$

Proof. This follows directly from the commutative diagram (67) and the definition of the Selmer and Tate-Shafarevich group. □

2.4.3 Torsors

In this section we will introduce torsors. These are objects that will play an important role in our paper. We will start by looking at torsors of elliptic curves E and then generalize to torsors of abelian varieties. One important tool that torsors give us is the twisting principle, which relates twists of elliptic curves E to the first cohomology group $H^1(G_F, E)$. Our approach is based on [25, Chapter X.2-3].

Definition 2.46 (G-torsor)**.** *Let G be group. A G-torsor is a set T together with a simple transitive action $\alpha : G \times T \to T$ of G on T, i.e., for all elements $t, t' \in T$ there exists a unique $g \in G$ such that $tg = t'$ and if $gx = x$ then $g = e$.*

A morphism of G-torsors T and T' is a morphism of T and T' that respects the group action of E.

Example 2.47 (Torsors under E)**.** *Let E be an elliptic curve over a field F. A torsor under E is a pair (C, μ) where C is a smooth projective curve of genus one defined over F, together with a morphism $\mu : E \times C \to C$ defined over F that induces a simple transitive action on $\bar{F}$.*

A morphism of torsors C and C' is an isomorphism of curves $C \to C'$ that respects the action of E.

The trivial torsor under E is the torsor $(E, +)$ where $+ : E \times E \to E$ is the usual group law on E. Every torsor under E is then a twist of $(E, +)$. Remember that a twist of a curve is defined as.

Definition 2.48 (Twist of a curve)**.** *Let C be a smooth projective curve over F. A twist of C is a smooth curve C' over F that is isomorphic to C over $\bar{F}$.*

Now let (C, μ) be a torsor under E. By definition the action of E on C is defined over F. We fix a point $p_0 \in C$ and define the map $\theta : E \to C$ by $P \mapsto \mu(P, p_0)$. Then, for any $\sigma \in G_F$ such that $p_0^\sigma = p_0$ we have that

$$\theta(P)^\sigma = \mu(P, p_0)^\sigma = \mu(P^\sigma, p_0^\sigma) = \mu(P^\sigma, p_0) = \theta(P^\sigma), \tag{71}$$

so θ is defined over $F(p_0)$. Because the action on C is simply transitive the map θ has degree one and thus θ is an isomorphism. So every torsor under E is indeed a twist of $(E, +)$.

Definition 2.49 (Weil-Châtelet group for E)**.** *Let (C, μ) and (C', μ') be torsors under E. We say that (C, μ) and (C', μ') are equivalent if they are isomorphic over F. The collection of equivalence classes of torsors under E is called the Weil-Châtelet group for E and is denoted by WC(E/F).*

We have the following characterization for the trivial class of $(E, +)$ in WC(E/F).

Proposition 2.50. *Let (C, μ) be a torsor under E. Then (C, μ) is in the trivial class if and only if $C(F)$ contains a point.*

Proof. Let (C, μ) be in the trivial class. Then there is an isomorphism $\phi : E \to$ over F. So $\phi(O)$ lies in $C(F)$.

Conversely, assume there is a point p_0 in $C(F)$. Consider the map $\theta : E \to C$ given by $P \mapsto \mu(P, p_0)$. As described before, this map is an isomorphism defined over $F(p_0) = F$, so (C, μ) is in the trivial class. □

The following theorem relates the twists of curves C to the first cohomology group $H^1(G_F, C)$.

Theorem 2.51 ([25],Theorem X.2.2)**.** *Let C be a smooth projectiver curve over F. For each twist C' of C, choose an $\bar{F}$-isomorphism $\phi : C' \to C$ and define the map $\xi_\sigma = \phi^\sigma \phi^{-1} \in Aut(C)$. We then have that:*

1. *The map ξ is a 1-cocycle and its associated cohomology class in $H^1(G_F, Aut(C))$ is denoted by $\{\xi\}$.*
2. *The cohomology class $\{\xi\}$ is determined by the F-isomorphism class of C' and is independent of choice of ϕ. We thus obtain a natural map*

$$Twist(C/F) \to H^1(G_F, Aut(C)). \tag{72}$$

3. *The map in 2. is a bijection. In other words, the twists of C up to F-isomorphism, are in one-to-one correspondence with elements of the cohomology set $H^1(G_F, Aut(C))$.*

Proof. For 1, note that

$$\xi_{\sigma\tau} = \phi^{\sigma\tau}\phi^{-1} = (\phi^{\sigma}\phi^{-1})^{\tau}(\phi^{\tau}\phi^{-1}) = (\xi_{\sigma})^{\tau}\xi_{\tau}, \tag{73}$$

for all $\sigma\tau \in G_F$.

For 2, let C'' be another twist of C that is F-isomorphic to C'. We choose a $\bar{F}$-isomorphism $\psi : C'' \to C$ and we will show that the 1-cocycles $\phi^{\sigma}\phi^{-1}$ and $\psi^{\sigma}\psi^{-1}$ are cohomologous. Let $\theta : C'' \to C'$ be the F-isomorphism between C'' and C'. We consider the element $\alpha = \phi\theta\psi^{-1} \in \text{Aut}(C)$. Then we have that

$$(\alpha^{\sigma})(\psi^{\sigma}\psi^{-1}) = (\phi\theta\psi^{-1})^{\sigma}(\psi^{\sigma}\psi^{-1}) = \phi^{\sigma}\theta^{\sigma}\psi^{-1} = (\phi^{\sigma}\phi^{-1})(\phi\theta\psi^{-1}) = (\phi^{\sigma}\phi^{-1})\alpha. \tag{74}$$

So the 1-cocycle $\phi^{\sigma}\phi^{-1}$ and $\psi^{\sigma}\psi^{-1}$ differ by the 1-coboundary induced by α. So they are cohomologous.

For the proof of 3. we refer to the proof provided in [25]. □

Let $R \in E$ be a point and consider the translation map $\tau_R : E \to E$. For all points $P, Q \in E$ we have that $\tau_R(P+Q) = \tau_R(P) + Q = P + \tau_R(Q)$, so τ_R respects the group law of E and is thus an automorphism of $(E, +)$. Conversely, an automorphism of $(E, +)$ is a map $\phi : E \to E$ such that $\phi(P+Q) = \phi(P) + Q = P + \phi(Q)$ for all $P, Q \in E$. In particular, if we take Q to be the point at infinity O we get that $\phi(P) = P + \phi(O)$, so the map ϕ is the translation map by $\phi(O)$. Since the translation maps are determined by the points of E with which you translate, we get an isomorphism $\text{Aut}(E, +) \simeq E$. This observation together with Theorem 2.51 gives us the following result:

Corollary 2.52. *The torsors under E, viewed as twists of $(E, +)$, are parametrised up to isomorphism by $H^1(G_F, E)$.*

We will now introduce torsors for abelian varieties. The proofs are similar to the case of elliptic curves so we will omit them. For a detailed approach we refer to [12]

Definition 2.53 (Torsor under A)**.** *Let A be an abelian variety over a field F. A torsor under A is a pair (V, μ) where V is a variety together with an F-morphism $\mu : A \times V \to V$ such that*

$$\mu(\bar{F}) : A(\bar{F}) \times V(\bar{F}) \to V(\bar{F}), \tag{75}$$

is a simply transitive action.

A morphism of torsors V and V' is a morphism of varieties $V \to V'$ that respects the action of A.

We call the torsor $(A, +)$ the trivial torsor. Similar to the case of elliptic curves we define the Weil-Châtelet group of torsors under A.

Definition 2.54 (Weil-Châtelet group for A)**.** *Let (B, μ) and (B', μ') be torsors under A. We say that (B, μ) and (B', μ') are equivalent if they are isomorphic over F. The collection of equivalence classes of torsors under A is called the Weil-Châtelet group for A and is denoted by WC(A/F).*

Again, we can describe the Weil-Châtelet group in terms of the first Galois cohomology group $H^1(G_F, A)$.

Proposition 2.55 ([12], Proposition 4)**.** *There is a canonical bijection between the first Galois cohomology group $H^1(G_F, A)$ and the Weil-Châtelet group WC(A/F).*

We have the same characterization for the trivial class of $(A, +)$.

Proposition 2.56 ([12], Proposition 4)**.** *Let (C, μ) be a torsor under A. Then (C, μ) is in the trivial class if and only if $C(F)$ contains a point.*

Remember that we defined the Tate-Shafarevich group of A as the group

$$Ш(A/F) = \ker \left\{ H^1(G_F, A) \to \prod_v H^1(G_v, A) \right\}. \tag{76}$$

From Proposition 2.55 it follows that we can define $Ш(A/F)$ equivalently as

$$Ш(A/F) = \ker \left\{ \text{WC}(A/F) \to \prod_v \text{WC}(A/F_v) \right\}. \tag{77}$$

By Proposition 2.56 the elements of $Ш(A/F)$ represent torsors under A which contain an F_v-rational point for every place v of F. The non-trivial elements additionally contain no F-rational points, so these torsors violate the Hasse principle. In this sense the Tate-Shafarevich group measures the extent to which the Hasse principle holds for A.

2.4.4 Coverings

A covering of a topological space is defined in the following way.

Definition 2.57 (Covering)**.** *Let X be a topological space. A space over X is a topological space Y together with a continuous map $p : Y \to X$. A morphism between two spaces $p_i : Y_i \to X$, $(i = 1, 2)$ over X is given by a continuous map $f : Y_1 \to Y_2$ making the diagram commute*

$$\begin{tikzcd} Y_1 \arrow[r, "f"] \arrow[dr, "p_1"'] & Y_2 \arrow[d, "p_2"] \\ & X \end{tikzcd} . \tag{78}$$

A covering of X is a space Y over X such that the projection $p : Y \to X$ satisfies the condition: for every point x of X there is an open neighbourhood V_x of x such that the preimage $p^{-1}(V_x)$ decomposes as a disjoint union of open subsets U_i of Y, where U_i is homeomorphic to V_x under the restriction of p to each U_i.

A morphism between two coverings of X is then a morphism of spaces over X.

An important group of coverings are the coverings that arise from group actions on topological spaces. For this we need the action to satisfy the following property:

Definition 2.58 (Even group action)**.** *Let G be a group acting continuously from the left on a topological space Y. The action of G is even if each point $y \in Y$ has some open neighbourhood U such that the open sets gU are pairwise disjoint for all $g \in G$.*

For a topological space Y with a group G acting on the left, we can form the quotient space $G\backslash Y$. As a topological space it consists of the orbits under the action of G and its topology is the quotient topology. Then, the projection $Y \to Y\backslash G$ is a covering if the action of G is even.

Lemma 2.59. *If G is a group acting evenly on a connected space Y, the projection $p_G : Y \to G\backslash Y$ turns Y into a cover of $G\backslash Y$.*

Proof. The map p_G is surjective and by the definition of an even group action each $x \in G\backslash Y$ has an open neighbourhood of the form $V = p_G(U)$ as described in Definition 2.58. Taking the preimage now shows that p_G satisfies the condition of a covering. □

For a covering of a scheme we require some additional structures on the covering map.

Definition 2.60. *We call a finite morphism of schemes $\phi : X \to S$ locally free if the direct images sheaf $\phi_* \mathcal{O}_X$ is locally free of finite rank. If additionally each fibre X_P of ϕ is the spectrum of a finite étale $\kappa(P)$-algebra, where $\kappa(P)$ denotes the residue field at P, then ϕ is called a finite étale morphism.*

A finite étale cover is a surjective finite étale morphism.

To see what this additional structure achieves consider the case where $\pi : X \to Y$ is a covering of schemes, where Y is an abelian variety over a field F and X is a Y-scheme together with a simply transitive group action of F. Assume this cover is geometrically connected. Every connected finite étale cover of $Y_{\bar{F}}$ is an abelian variety by [16, §18]. This turns X into an abelian variety over the algebraic closure $\bar{F}$. Because X is isomorphic to an abelian variety over $\overline{F}$, it follows that X is a torsor under this abelian variety.

3 μ_p-covers and μ_p-descent

Let Y be an abelian variety over a field F of characteristic not p. Let μ_p be the F-group scheme of the p-th roots of unity. A μ_p-cover of Y is a Y-scheme X together with a simply transitive action of μ_p. The μ_p-covers of Y form a category $\mathcal{M}_p(Y)$ whose morphisms are isomorphisms of Y-schemes that respect the action of μ_p. It is possible to think about μ_p-covers in terms of line bundles on Y, which we will describe now.

Proposition 3.1. *There is an equivalence of categories between $\mathcal{M}_p(Y)$ and the category of pairs $(\mathcal{L}, \eta)$ where $\mathcal{L}$ is an invertible sheaf on Y and $\eta : \mathcal{L}^{\otimes p} \simeq \mathcal{O}_Y$ is an isomorphism. Here, the morphisms $(\mathcal{L}, \eta) \to (\mathcal{L}', \eta')$ are isomorphisms $g : \mathcal{L} \to \mathcal{L}'$ such that $\eta' \circ g^{\otimes p} = \eta$.*

Proof. A proof can be found in [1] or [16, Proposition II.7.3]. We will describe the functor in both directions, similar to the proof in the paper, to describe the correspondence.

If $\pi : X \to Y$ is a μ_p-cover, then there is a $\mathbb{Z}/p\mathbb{Z}$-grading on the $\mathcal{O}_Y$-module

$$\pi_* \mathcal{O}_X = \mathcal{O}_Y \oplus \bigoplus_{i=1}^{p-1} \mathcal{L}_i \tag{79}$$

where each $\mathcal{L}_i$ is the invertible subsheaf of $\pi_* \mathcal{O}_X$ on which μ_p acts by $\zeta \cdot s = \zeta^i s$. The algebra structure of $\pi_* \mathcal{O}_X$ gives isomorphisms $\mathcal{L}_i \otimes \mathcal{L}_j \simeq \mathcal{L}_{i+j}$, where indices are to be taken modulo p and where $\mathcal{L}_0 = \mathcal{O}_Y$. So, we obtain an isomorphism $\mathcal{L}_1^{\otimes p} \simeq \mathcal{O}_Y$.

Conversely, starting with a pair $(\mathcal{L}, \eta)$, we can define a sheaf of $\mathcal{O}_Y$-algebras $\mathcal{O}_Y \oplus \bigoplus_{i=1}^{p-1} \mathcal{L}^{\otimes i}$ using the isomorphism η to define the multiplication $\mathcal{L}^{\otimes i} \otimes \mathcal{L}^{\otimes} \otimes j \simeq \mathcal{L}^{\otimes i+j} \simeq \mathcal{L}^{i+j-p}$ on the factors with $i + j \geq p$. The relative spectrum of this sheaf over Y is then naturally endowed with a μ_p-action making it a μ_p-cover. $\square$

This proposition allows us to think of the μ_p-cover $\pi : X \to Y$ as the corresponding pair $(\mathcal{L}, \eta)$. The line bundle $\mathcal{L} \in \mathrm{Pic}(Y)(F)$ is called the Steinitz class of π. Because η gives us an isomorphism between $\mathcal{L}^{\otimes p} \simeq \mathcal{O}_Y$, it follows that $\mathcal{L}$ is a p-torsion line bundle. So it follows that that $\mathcal{L} \in \widehat{Y}[p](F)$, where by definition $\widehat{Y} = \mathrm{Pic}^0(Y)$ is the dual abelian variety.

Using the pair $(\mathcal{L}, \eta)$ we can construct more μ_p-covers by scaling $\eta : \mathcal{L}^{\otimes p} \to \mathcal{O}_Y$ with any element $r \in F^*$. Two such μ_p covers $(\mathcal{L}, r\eta)$ and $(\mathcal{L}, s\eta)$ are isomorphic if and only if $r/s \in F^{*p}$. Given two μ_p-covers $(\mathcal{L}, \eta)$ and $(\mathcal{L}', \eta')$, the tensor product $(\mathcal{L} \otimes \mathcal{L}', \eta \otimes \eta')$ is a μ_p-cover again. We denote the set of μ_p-covers with $H^1(Y, \mu_p)$.

Lemma 3.2. *The μ_p-cover $\pi : X \to Y$ corresponding to $(\mathcal{L}, \eta)$ is geometrically connected if and only if $\mathcal{L} \not\simeq \mathcal{O}_Y$.*

Proof. A proof can be found in [5, Lemma 2.5]. $\square$

Let $\pi : X \to Y$ be a geometrically connected μ_p-cover corresponding to $(\mathcal{L}, \eta)$, so $\mathcal{L} \not\simeq \mathcal{O}_Y$. Since every connected finite étale cover of the abelian variety $Y_{\overline{F}}$ is itself an abelian variety [16, §18], we find that X becomes an abelian variety over the algebraic closure $\overline{F}$. Because X is isomorphic to an abelian variety over $\overline{F}$, it follows that X is a torsor under this abelian variety.

The abelian variety that X is a torsor for will be the distinguished μ_p-cover with Steinitz class $\mathcal{L}$. Starting with the line bundle $\mathcal{L}$, let $\widehat{\psi} : \widehat{Y} \to \widehat{Y}/\langle \mathcal{L} \rangle$ be the degree p isogeny obtained from modding out $\mathcal{L}$. Let $\psi : A_{\mathcal{L}} \to Y$ be the dual isogeny, which is also of degree p, where $A_{\mathcal{L}}$ denotes the dual of $\widehat{Y}/\langle \mathcal{L} \rangle$. We can give ψ the structure of a μ_p-cover by considering the isomorphism:

$$\ker \psi \simeq \widehat{\ker \widehat{\psi}} \simeq \widehat{\mathbb{Z}/p\mathbb{Z}} = \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m) \simeq \mu_p \tag{80}$$

The first isomorphism is a standard result for the dual of an isogeny [15, Theorem V.9.1]. The second result follows from the fact that $\ker(\widehat{\psi}) = \langle \mathcal{L} \rangle \simeq \mathbb{Z}/p\mathbb{Z}$, since $\langle \mathcal{L} \rangle$ by a p-torsion element. For the last isomorphism, note that the homomorphisms $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_m$ are determined by which element 1 gets sent to. Since 1 has order p in $\mathbb{Z}/p\mathbb{Z}$ it follows that $\varphi(1) = \zeta_p$ where ζ_p is some p-th primitive root of unity or 1 for the trivial homomorphism φ_0. Let φ_k denote the homomorphism such that $\varphi_k(1) = \zeta_p^k$ for some $1 \leq k \leq p-1$. For $0 \leq k, k' \leq p-1$, we then have that $\varphi_k \cdot \varphi_{k'} = \varphi_{k+k'}$ and $\varphi_k^p = \varphi_0$, where the indices are taken modulo p. Identifying φ_k with some primitive p-th root of unity in μ_p, where $1 \leq k \leq p-1$, gives us an isomorphism between $\text{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{G}_m)$ and μ_p. Because we have $p-1$ different choices of k, we acquire $p-1$ different isomorphisms between $\ker(\psi)$ and μ_p. These isomorphisms correspond to the different $\mathbb{Z}/p\mathbb{Z}$-gradings we can put on $\psi_* A_{\mathcal{L}}$. There is exactly one isomorphism such that the μ_p-cover structure for ψ has Steinitz class $\mathcal{L}_1 \subset \psi_* A_{\mathcal{L}}$ isomorphic to $\mathcal{L}$, so we choose this structure for ψ.

Lemma 3.3. *Let $\pi : X \to Y$ be a μ_p-cover with non-trivial Steinitz class $\mathcal{L} \in \widehat{Y}[p](F)$. Then π is a twist of the μ_p-cover $\psi : A_{\mathcal{L}} \to Y$ and X is a torsor for $A_{\mathcal{L}}$.*

Proof. A proof can be found in [5, Lemma 2.6]. □

We have described how we acquire the distinguished μ_p-cover $A_{\mathcal{L}} \to Y$ with Steinitz class $\mathcal{L}$ for each non-zero $\mathcal{L} \in \widehat{Y}[p](F)$. Together with this cover comes a distinguished isomorphism $\eta : \mathcal{L}^{\otimes p} \simeq \mathcal{O}_Y$, which we will describe now. We will consider the case where Y is the Jacobian of a curve to simplify the process.

Let C be a smooth projective geometrically integral curve over F and let $J = \text{Pic}^0(C)$ be its Jacobian. Let g be the genus of C and thus the dimension of the abelian variety J. Let $D \in J[p](F)$ be a divisor class of order p. Let $J \to J/\langle D \rangle$ be the quotient and let $\psi : A_D \to \widehat{J}$ be the corresponding dual isogeny, where A_D is the dual of $J/\langle D \rangle$. By the above discussion, it follows that ψ is a μ_p-cover of $\widehat{J}$ corresponding to a pair $(\mathcal{L}, \eta)$. We can identify J and $\widehat{J}$ via the canonical principal polarization $\lambda : J \to \widehat{J}$. Thus we can view ψ as a μ_p-cover of J and η as an isomorphism $\mathcal{L}^{\otimes p} \to \mathcal{O}_J$. We will often refer to the μ_p-covers of the Jacobian J by the μ_p-cover of the curve that is associated to J.

By construction these μ_p-covers are abelian varieties, but in general the μ_p-covers corresponding to pairs $(\mathcal{L}, r\eta)$, where $r \in F^*$, may only be torsors for abelian varieties. The following lemmas describe which μ_p-covers have rational points, and thus are abelian varieties. For this, fix $D \in J[p](F)$ and $(\mathcal{L}, \eta)$, as above. Given $P \in J(F)$, we can construct the μ_p-cover $\psi_P = t_p \circ \psi : A_D \to J$, where $t_p : J \to J$ is translation by P. The μ_p-cover is endowed with the same μ_p-action as ψ, but with a different structure map to J. The Steinitz class of ψ_P is isomorphic to the Steinitz class of ψ, since it lies in $\text{Pic}^0(C)$ and is thus invariant under translation. If ψ_P corresponds to the pair $(\mathcal{L}', \eta')$, then we can choose an isomorphism $\mathcal{L} \simeq \mathcal{L}'$. Under this isomorphism we must have that $\eta' = r_P \eta$ for some element $r_P \in F^*$. Any other choice of isomorphism $\mathcal{L} \simeq \mathcal{L}'$ differs by a scalar, so r_P is well-defined up to F^{*p}.

Lemma 3.4. *The map $P \mapsto r_P$ induces an injective map $\partial^D : J(F)/\psi(A_D(F)) \to F^*/F^{*p}$.*

Proof. A proof can be found in [5, Lemma 3.1]. □

Lemma 3.5. *The image of ∂^D is the set of $r \in F^*/F^{*p}$ such that the μ_p-cover $(\mathcal{L}, r\eta)$ has a rational point.*

Proof. A proof can be found in [5, Lemma 3.3]. □

The following lemma can be used to give an explicit formula for the homomorphism ∂^D.

Lemma 3.6. *Let $F(J)$ be the function field of J and view $\eta^{-1} : \mathcal{O}_J \to \mathcal{L}^{\otimes p}$ as a global section of $\mathcal{L}^{\otimes p}$. Fix an embedding of $\mathcal{L}$ as a subsheaf of $F(J)$, so that η^{-1} is a non-zero element f of $F(J)$. Let Q be such that Q and $Q+P$ are in a domain of definition for f. Then $\partial^D(P) = r_P = f(P+Q)/f(Q)$, up to p-th powers.*

Proof. A proof can be found in [5, Lemma 3.5]. □

Thinking of η^{-1} as a function on J allows us to distinguish the unique μ_p-cover $(\mathcal{L}, \eta)$ corresponding to $\psi : A_D \to J$ among all μ_p-covers with Steinitz class $\mathcal{L}$.

Lemma 3.7. *A μ_p-cover corresponding to the data $(\mathcal{L}, \eta)$ is isomorphic to the μ_p-cover $A_{\mathcal{L}} = A_D \to J$ if and only if the value $f(0_J)$ of the function $f = \eta^{-1} \in F(J)$ at 0_J is a p-th power in F^*.*

Proof. A proof can be found in [5, Lemma 3.6]. □

Remember that points of $\text{Sym}^g(C)$ correspond to effective degree g divisors E on C and that the map $\text{Sym}^g(C) \to J$ sending $E \mapsto E - g \cdot \infty$ is birational. So we get an isomorphism of function fields $F(\text{Sym}^g(C)) \simeq F(J)$.

Lemma 3.8. *Suppose $pD = div(\tilde{f})$ for some $\tilde{f} \in F(C)$. Then $\mathcal{L} \simeq \mathcal{O}_J(\tilde{D})$ for a divisor $\tilde{D}$ on J such that $p\tilde{D} = div(f)$, where $f \in F(J) \simeq F(\text{Sym}^g(C))$ is the rational function $f(\sum_{i=1}^{g}(x_i, y_i) - g \cdot \infty) = \prod_{i=1}^{g} \tilde{f}(x_i, y_i)$.*

Proof. A proof can be found in [5, Lemma 3.7]. □

Let $H = \{D_1, \dots, D_m\} \subset J[p](F)$ be a subset of $\mathbb{F}_p$-linearly independent elements. For each $i = 1, \dots, m$, let $\psi_i : A_i \to J$ be the μ_p-covers corresponding to D_i. Let $A_H = \widehat{J/\langle H \rangle}$ and let $\psi_H : A_H \to J$ be the isogeny dual to $J \to J/\langle H \rangle$. Then we have the homomorphism

$$\tilde{\partial}^H : J(F) \to \prod_{i=1}^{m} F^*/F^{*p} \tag{81}$$

sending P to $(\partial^{D_1}(P), \dots, \partial^{D_m}(P))$.

Lemma 3.9. *The map $\tilde{\partial}^H$ induces an injection $\partial^H : J(F)/\psi_H(A_H(F)) \hookrightarrow \bigoplus_{i=1}^{m} F^*/F^{*p}$.*

Proof. A proof can be found in [5, Lemma 3.8]. □

Assume now that C is a curve over $\mathbb{Q}$. Everything discussed so far also holds for $F = \mathbb{Q}$ or $F = \mathbb{Q}_l$, for any prime $l \leq \infty$. For a fixed $D \in J[p](\mathbb{Q})$, let

$$\mathrm{Sel}(A_D) \subseteq \mathbb{Q}^*/\mathbb{Q}^{*p} \tag{82}$$

be the subgroup of classes r with the property that for every prime l, the class of r in $\mathbb{Q}_l^*/\mathbb{Q}_l^{*p}$ in the image of $\partial^D : J(\mathbb{Q}_l)/\psi(A_D(\mathbb{Q}_l)) \to \mathbb{Q}_l^*/\mathbb{Q}_l^{*p}$, for every prime l. In other words, an element of $\mathrm{Sel}(A_D)$ is a μ_p-cover $X \to J$ with Steinitz class D and such that $X(\mathbb{Q}_l) \neq \emptyset$ for every prime l.

For an abelian variety A over $\mathbb{Q}$ the group $Ш(A)$ is the group of A-torsors which are trivial over $\mathbb{Q}_l$ for all primes $l \leq \infty$.

Proposition 3.10. *Let $Ш(A_D)$ be the Tate-Shafarevich group of A_D. There is an exact sequence*

$$0 \to J(\mathbb{Q})/\psi(A_D(\mathbb{Q})) \to \mathit{Sel}(A_D) \to Ш(A_D)[\psi] \to 0 \tag{83}$$

where $Ш(A_D)[\psi]$ is the kernel of the map $Ш(A_D) \to Ш(J)$ induced by ψ.

Proof. A proof can be found in [5, Lemma 3.9]. □

The group $\mathrm{Sel}(A_D)$ is isomorphic to the usual Selmer group

$$\mathrm{Sel}_\psi(A) \subset H^1(F, A[\psi]) \simeq H^1(F, \mu_p) \simeq F^*/F^{*p}. \tag{84}$$

Thus it is finite, which can also be seen from the following proposition.

Proposition 3.11. *Let $l \neq p$ a prime of good reduction for J. Then the image of $\partial^D : J(\mathbb{Q}_l) \to \mathbb{Q}_l^*/\mathbb{Q}_l^{*p}$ is equal to the subgroup $\mathbb{Z}_l^*/\mathbb{Z}_l^{*p}$.*

Proof. A proof can be found in [5, Lemma 3.10]. □

4 Jacobians and μ_p-covers for curves of the form $y^p = x(x-e_1)(x-e_2)$

Let $p > 3$ a prime. Let e_0, e_1 and e_2 be distinct integers and consider the smooth projective curve C over $\mathbb{Q}$ with affine model

$$y^p = (x-e_0)(x-e_1)(x-e_2). \tag{85}$$

Without loss of generality we can assume that $e_0 = 0$. This affine model is smooth and it has a single rational point at infinity denoted by ∞. The genus of the curve is $g = p-1$ from [26, §1].

Let J be the Jacobian of C. The subgroup $J(\mathbb{Q})[p]$ has rank at least 2, because it contains $D_i = [(e_i, 0) - \infty]$ for $i \in \{0,1,2\}$. We have that $D_0 + D_1 + D_2 = \operatorname{div}(y)$ so $D_0 + D_1 + D_2$ is equal to 0 in J. Let $H := \langle D_0, D_1 \rangle$. We can define the following abelian variety:

$$\widehat{A} = J/H. \tag{86}$$

For $D := D_0 + D_1$ we define the variety

$$\widehat{B} = J/\langle D \rangle. \tag{87}$$

For these varieties we can define the quotient isogenies $\widehat{\phi} : J \to \widehat{A}$ and $\widehat{\psi} : J \to \widehat{B}$. By duality we get the dual isogenies $\phi : A \to \widehat{J}$ and $\psi : B \to \widehat{J}$. Furthermore, via the canonical principal polarization we can identify J with its dual and acquire the maps $\phi : A \to J$ and $\psi : B \to J$. This turns A and B into μ_p-covers of J. We also define the varieties $A_{D_i} = J/\langle D_i \rangle$ for $i \in \{0,1,2\}$ in this manner, with the corresponding isogenies $\psi_i : A_{D_i} \to J$. Note that $B \simeq A_{D_2}$, because $D = -D_2$.

We now get the map

$$J(\mathbb{Q})/\phi(A(\mathbb{Q})) \xrightarrow{\partial^H} \mathbb{Q}^*/\mathbb{Q}^{*p} \times \mathbb{Q}^*/\mathbb{Q}^{*p} \tag{88}$$

$$\left[\sum_{j=1}^{g} (x_j, y_j) - g \cdot \infty\right] \mapsto \left(\prod_{j=1}^{g} x_j, \prod_{j=1}^{g} (x_j - e_1)\right) \tag{89}$$

as described in the Lemmas 3.6, 3.8 and 3.9. From [21, Proposition 2.7] it follows that the divisor

$$\sum_{j=1}^{g} (x_j, y_j) - g \cdot \infty, \tag{90}$$

with $x_j, y_j \in \overline{\mathbb{Q}}$, on the left hand side is Galois stable, i.e. its divisor class can be represented by a $\mathbb{Q}$-rational divisor, because $C(\mathbb{Q}) \neq \emptyset$. This map is well-defined whenever the x_j and $x_j - e_1$ are non-zero. By [10, VI §4 Lemma 3] it is possible to find a representative in every class in $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$ such that the map ∂^H is well-defined.

We can construct similar homomorphisms for the other varieties we have defined:

$$\partial^{D_i} : J(\mathbb{Q})/\psi_i(A_{D_i}(\mathbb{Q})) \to \mathbb{Q}^*/\mathbb{Q}^{*p} \tag{91}$$

$$\left[\sum_{j=1}^{g} (x_j, y_j) - g \cdot \infty\right] \mapsto \prod_{j=1}^{g} (x_j - e_i) \tag{92}$$

for A_{D_i} with $i \in \{0,1,2\}$. Similar to ∂^H this description only makes sense whenever the $x_j - e_i$ are non-zero. However from these maps we find that

$$\partial^{D_0} \cdot \partial^{D_1} \cdot \partial^{D_2} \left(\left[\sum_{j=1}^{g} (x_j, y_j) - g \cdot \infty\right]\right) = \prod_{j=1}^{g} x_j (x_j - e_1)(x_j - e_2) = \prod_{j=1}^{g} y_j^p = 1, \tag{93}$$

since the x_j and y_j lie on the curve C. So we get the identity:

$$\partial^{D_0} \cdot \partial^{D_1} \cdot \partial^{D_2} = 1. \tag{94}$$

This allows us to describe our homomorphisms on classes where they are not well-defined. One particular example which will come up is described in the following lemma.

Lemma 4.1. *We have*

$$\partial^H([(0,0)-\infty]) = [e_1^{-1}e_2^{-1}, -e_1], \tag{95}$$

and

$$\partial^H([(e_1,0)-\infty]) = [e_1, (e_1-e_2)^{-1}]. \tag{96}$$

Proof. Note that the map ∂^H can be described by the mapping $P \mapsto (\partial^{D_0}(P), \partial^{D_1}(P))$ for $P \in J(\mathbb{Q})/\phi(A(\mathbb{Q}))$. Combining this with (94) we find that:

$$\begin{aligned}\partial^H([(0,0)-\infty]) &= [\partial^{D_1}([(0,0)-\infty])^{-1} \cdot \partial^{D_2}([(0,0)-\infty])^{-1}, \partial^{D_1}([(0,0)-\infty])] \\ &= [e_1^{-1}e_2^{-1}, -e_1].\end{aligned}$$

In a similar way, we find that $\partial^H([(e_1,0)-\infty]) = [e_1, (e_1-e_2)^{-1}]$. $\square$

Lastly, for B we have the homomorphism

$$\begin{aligned}\partial^D : &J(\mathbb{Q})/\psi(B(\mathbb{Q})) \to \mathbb{Q}^*/\mathbb{Q}^{*p}, &(97)\\ &\left[\sum_{j=1}^{g}(x_j,y_j) - g\cdot\infty\right] \mapsto \prod_{j=1}^{g} x_j(x_j-e_1). &(98)\end{aligned}$$

This gives us the following commutative diagram which we will use in the next section

$$\begin{array}{ccc} J(\mathbb{Q})/\phi(A(\mathbb{Q})) & \xrightarrow{\partial^H} & \mathbb{Q}^*/\mathbb{Q}^{*p} \times \mathbb{Q}^*/\mathbb{Q}^{*p} \\ \downarrow & & \downarrow \\ J(\mathbb{Q})/\psi(B(\mathbb{Q})) & \xrightarrow{\partial^D} & \mathbb{Q}^*/\mathbb{Q}^{*p} \end{array} \tag{99}$$

where the right vertical map is given by $[r_1, r_2] \mapsto [r_1 r_2]$.

We can find birational models for μ_p-covers of J given a Steinitz class. For our case we will look at the Steinitz class of $D = D_0 + D_1$. The distinguished μ_p-cover for this Steinitz class is the cover $B \to J$. Let this μ_p-cover correspond with the data $(\mathcal{L}, \eta)$. By Lemma 3.7 we have that $f(0_J)$ is a p-th power in $\mathbb{Q}^*$ where $f = \eta^{-1} \in \mathbb{Q}(J)$. For any point $P \in J(\mathbb{Q})/\psi(B(\mathbb{Q}))$ we have that $\partial^D(P) = r_P = f(P+Q)/f(Q)$ by Lemma 3.6. Taking $Q = 0_J$ we can rewrite this equation to get

$$f(P) = f(P+0_J) = f(0_J)r_P = 1, \tag{100}$$

since $f(0_J)$ is a p-th power. The fact that r_P is equal to 1, follows from the fact that the cover $B \to J$ is isomorphic to $(\mathcal{L}, \eta)$. Because $pD = \mathrm{div}(x(x-e_1))$, it follows from Lemma 3.8 that $1 = f(P) = [x(x-e_1)](P)$. Since P can be written in the form $\sum_{i=1}^{g}(x_i,y_i) - g\cdot\infty$ we finally get the equation

$$z^p = \prod_{i=1}^{g} x_i(x_i - e_1). \tag{101}$$

where the variable z^p comes from lifting the equation out of $\mathbb{Q}^*/\mathbb{Q}^{*p}$. Together with the birational model for J given by the equations

$$y_i^p = x_i(x_i-e_1)(x_i-e_2). \tag{102}$$

for $1 \le i \le g$, we get a birational model for B. Recall that this model has the same equations (1) of the variety $\tilde{A}$ in Theorem 1.1.

Finally for $r \in \mathbb{Q}^*$, the μ_p-cover $(\mathcal{L}, r\eta)$ is described by the equations

$$y_i^p = x_i(x_i-e_1)(x_i-e_2). \tag{103}$$

for $1 \le i \le g$, together with the additional equation

$$rz^p = \prod_{i=1}^{g} x_i(x_i - e_1). \tag{104}$$

which is twisted by r. If we identify B with the abelian variety $\tilde{A}/S_g$ of Theorem 1.1, then the above equations correspond with the equations (2) of the variety $\tilde{X}$ in Theorem 1.1.

5 The proof of Theorem 1.1

We now further specialize the curve (85) and look at the curve $C_{u,v}$ given by the affine model:

$$C = C_{u,v} : y^p = x(x-3u)(x-9v). \tag{105}$$

where u, v are integers not divisible by 3 and p is a prime larger than 3. Let J be the Jacobian of C and let A and B be the μ_p-covers from the previous section.

For certain primes q, we locally know the size of $J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q))$ from the following lemma:

Lemma 5.1. *Let q be a prime such that $q \equiv 1 \pmod p$. Then we have that $\#J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q)) = p^2$.*

Proof. The $(q-1)$-th roots of unity in $\mathbb{F}_q$ are given by $\mathbb{F}_q^\times$. By the structure of finite fields this is a cyclic group of order $q-1$. Our congruence condition on q tells us that there is an element ζ in $\mathbb{F}_q^\times$ generating a subgroup of order p. It follows that this is a primitive p-th root of unity. Because p and q are coprime it follows by Hensel's lemma that we can lift this element to an element in $\mathbb{Q}_q^*$ and we can conclude that $\mathbb{Q}_q^*$ contains a primitive p-th root of unity ζ.

For any field that contains ζ, we get an automorphism $(x, y) \mapsto (x, \zeta y)$ of C. Interpreting (x, y) as an element of div(C), we can define the pushforward $\zeta_* : \text{div(C)} \to \text{div(C)}$ as $\zeta_*(x, y) = (x, \zeta y)$ and we can extend this map $\mathbb{Z}$-linearly to other divisors. This induces a homomorphism $\zeta_* : J \to J$ sending $[D] \mapsto [\zeta_* D]$ by [25, Proposition II.3.6]. So we get a ring embedding $\iota : \mathbb{Z}[\zeta] \hookrightarrow \text{End}(J)$. For an element $n\zeta^i$ in $\mathbb{Z}[\zeta]$ with $n \in \mathbb{Z}$ and $0 \le i \le p-1$ and a divisor class $[D]$ in J the map $\iota(n\zeta^i)$ acts on $[D]$ by $\iota(n\zeta^i)(D) = [n \cdot (\zeta_* D)]$. Note that $\mathbb{Q}(\zeta) \simeq \mathbb{Z}[\zeta] \otimes \mathbb{Q}$ forms a $\mathbb{Q}$-subalgebra under this embedding. So by [15, Proposition V.10.23] it follows that $\deg(\iota(\alpha)) = \text{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha)^2$.

The kernel of $\widehat{\phi} : J \to \widehat{A}$ is then equal to the kernel of the endomorphism $1 - \iota(\zeta)$. This follows from the fact that elements in $\ker(1-\iota(\zeta))$ satisfy the relation $\zeta^* P \sim P$ for a point $P \in J$. In particular, a point P of the form $[(x, y)]$ would satisfy the relation if $y = 0$. So it follows that

$$\ker(\widehat{\phi}) = \langle D_0, D_1 \rangle \subseteq \ker(1 - \iota(\zeta)). \tag{106}$$

Since the size of the kernel of $1-\iota(\zeta)$ is equal to $\#\ker(1-\iota(\zeta)) = \text{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta)^2 = p^2 = \#\langle D_0, D_1\rangle$, we can conclude that the kernels of $\widehat{\phi}$ and $1-\iota(\zeta)$ are equal. Thus the maps $1-\iota(\zeta)$ and $\widehat{\phi}$ are equal up to post-composition with an automorphism. So A and $\widehat{A}$ are isomorphic to J over any field containing ζ and thus in particular over $\mathbb{Q}_q$. Let $\phi^{(q)} : A(\mathbb{Q}_q) \to J(\mathbb{Q}_q)$ denote the induced homomorphism on $\mathbb{Q}_q$. The local Selmer ratio is defined as

$$c_q(\phi) = \frac{\#\text{coker}\phi^{(q)}}{\#\text{ker}\phi^{(q)}} = \frac{\#J(\mathbb{Q}_q)/\phi^{(q)}(A(\mathbb{Q}_q))}{\#A(\mathbb{Q}_q)[\phi^{(q)}]}. \tag{107}$$

By [23, Corollary 3.2] we have that

$$c_q(\phi) = c_q(J)/c_q(A), \tag{108}$$

where the right hand side is the ratio of the Tamagawa numbers at q. Abstractly, the Tamagawa measure $c(G)$ of a semisimple algebraic group G defined over a global field k, is the canonical normalization of a Haar measure on $G(\mathbb{A})$ where $\mathbb{A}$ is the adele ring of k. The Tamagawa number of G is then the volume of $G(\mathbb{A})/G(k)$ under the Tamagawa measure. For the details of this construction we refer to [27, Chapter II] or [19, Chapter §5.3].

Since $J \simeq A$ over $\mathbb{Q}_q$ this ratio is 1. We also have that $\#A(\mathbb{Q}_q)[\phi] = p^2$, which gives us the result $\#J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q)) = \#A(\mathbb{Q}_q)[\phi] \cdot c_q(\phi) = p^2$. □

We would like to specialize our curves even further. To do this we introduce a non-zero integer k which is to be determined and look at the curve

$$C_k = C_{u,v,k} : y^p = x(x-3uk)(x-9vk). \tag{109}$$

Another model for this curve is $k^3 y^p = x(x-3u)(x-9v)$. From this we can see that C_k is a μ_p-twist of $C = C_{u,v} : y'^p = x'(x'-3u)(y'-9v)$ via the mapping $x \mapsto kx'$ and $y' \mapsto \sqrt[p]{k^3}$. Let J_k, A_k and B_k be the corresponding abelian varieties of C_k similar as before. These are then μ_p-twists of J, A and B as well.

For two primes q and l, let $\left(\frac{q}{l}\right)_p = 1$ if q is a p-th power in $\mathbb{Q}_l^\times$ and let it be equal to -1 otherwise. We have the exact sequence from Proposition 3.10

$$0 \to J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})) \xrightarrow{\partial^D} \text{Sel}(B_k) \to Ш(B_k)[\psi] \to 0. \tag{110}$$

Proposition 5.2. *Let U be the set of primes that divide $3puv(u-3v)$. Suppose k is a product of distinct primes $p_1,\dots,p_t$ not contained in U, which satisfy:*

1. $\left(\frac{p_i}{p_j}\right)_p = 1$ *for all $i \neq j$ in $\{1,2,\dots,t\}$,*
2. $\left(\frac{p_i}{q}\right)_p = 1$ *for all i in $\{1,2,\dots,t\}$ and all $q \in U$,*
3. $\left(\frac{q}{p_i}\right)_p = 1$ *for all i in $\{1,2,\dots,t\}$ and all $q \in U-\{3\}$,*
4. $\left(\frac{3}{p_i}\right)_p = -1$ *for all i in $\{1,2,\dots,t\}$.*

Then we have for all i that $p_i \in Sel(B_k)$ and $p_i \notin \partial^D(J_k(\mathbb{Q}))$. More generally, if $q=\prod_{i\in I} p_i^{a_i}$, with $I \subset \{1,\dots,t\}$ a proper and non-empty subset and $1 \le a_i \le p-1$, then $q \in Sel(B_k)$ and $q \notin \partial^D(J_k(\mathbb{Q}))$.

Proof. Using Lemma 4.1 we have that

$$\partial^H([(0,0)-\infty]) = [3^{-3}u^{-1}v^{-1}k^{-2}, -3uk], \tag{111}$$

$$\partial^H([(3uk,0)-\infty]) = [3uk, 3^{-2}u^{-1}(u-3v)^{-1}k^{-2}]. \tag{112}$$

For $j \neq i \in \{1,\dots,t\}$ by assumption we have that $u, v, (u-3v), p_j$ are p-th powers in $\mathbb{Q}_{p_i}^*$. So in $\mathbb{Q}_{p_i}^*/\mathbb{Q}_{p_i}^{*p} \times \mathbb{Q}_{p_i}^*/\mathbb{Q}_{p_i}^{*p}$ we have that the above elements are equal to $[3^{-3}p_i^{-2}, 3p_i]$ and $[3p_i, 3^{-2}p_i^{-2}]$ respectively. These elements are linearly independent so by Lemma 5.1 they generate $\partial^H(J_k(\mathbb{Q}_{p_i})/\phi(A_k(\mathbb{Q}_{p_i}))$. Note that we need to check if $p_i \equiv 1 \pmod p$ before we can apply the lemma. Since 3 is not a p-th power in $\mathbb{Q}_{p_i}$ we have that $\mathbb{F}_{p_i}$ contains all p-th roots of unity.

Let $[r_1, r_2]$ in $\partial^H(J_k(\mathbb{Q})/\phi(A_k(\mathbb{Q}))$. We shall consider the elements of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*p}$ as p-th power-free numbers. Proposition 3.11 tells us then that the product of $r_1 r_2$ lies in $\mathbb{Z}_l^*/\mathbb{Z}_l^{*p}$ for primes $l \neq p$ of good reduction for J. So the prime l does not divide $r_1 r_2$. By taking $r_2 = 1$ we can see that r_1 is not divisible by l, likewise for r_2 by taking $r_1 = 1$. It follows that the primes of good reduction are the primes outside $\{p_1,\dots,p_t\} \cup U$. To see this let the function $f(x,y) = y^p - x(x-3uk)(x-9vk)$ describe the curve C_k. Looking at the partial derivatives we see that $\partial_y f(x,y) = py^{p-1}$, so l possibly has bad reduction if $l = p$ or if $f(x,0)$ is not separable. If $l = p$, then we have that $f(x,y) \equiv (y - \sqrt[p]{x(x-3uk)(x-9vk)})^p$ modulo p, since $\mathbb{F}_p$ is a perfect field. So we have bad reduction at p. In the case that $y = 0$ the discriminant of $x(x-3uk)(x-9vk)$ is given by $3^8u^2v^2k^6(u-3v)^2$, so we have bad reduction if l divides $3uvk(u-3v)$. Thus the integers r_1 and r_2 are only divisible by the primes in $\{p_1,\dots,p_t\} \cup U$.

Let us assume that there is no i such that p_i divides r_1 and $1/r_2$ to the same power. Then every p_i will divide $r_1 r_2$ by a positive power, since we can multiply by $1 = p_i^p$. So $r_1 r_2$ cannot be equal to an individual prime p_i and in particular it cannot be of the form $\prod_{i\in I} p_i^{a_i}$ with I a non-empty proper subset of $\{1,\dots,t\}$ and $1 \le a_i \le p-1$.

So assume to the contrary that there exists some i such that p_i divides r_1 and $1/r_2$ to the same power. The element $[r_1, r_2]$ is a product of $[3^{-3}p_i^{-2}, 3p_i]$ and $[3p_i, 3^{-2}p_i^{-2}]$ in $\partial^H(J_k(\mathbb{Q}_{p_i})/\phi(A_k(\mathbb{Q}_{p_i}))$, since they generate the subgroup. Looking only at the p_i-adic valuation we have that

$$[r_1, r_2] \equiv [p_i^{-2}, p_i]^a \cdot [p_i, p_i^{-2}]^b \equiv [p_i^{b-2a}, p_i^{a-2b}], \tag{113}$$

for some $a, b \in \mathbb{Z}$. Passing to $\mathbb{Q}_{p_i}^*/\mathbb{Q}_{p_i}^{*p}$ we get that

$$r_1 r_2 \equiv p_i^{a-2b+b-2a} = p_i^{-b-a}, \tag{114}$$

which implies that $b = -a$. Looking back at $[r_1, r_2]$ we thus see that

$$[r_1, r_2] = [3^{-3}p_i^{-2}, 3p_i]^a \cdot [3p_i, 3^{-2}p_i^{-2}]^{-a} = [3^{-4a}p_i^{-3a}, 3^{3a}p_i^{3a}], \tag{115}$$

with $0 \le a \le p-1$. From this we find in $\mathbb{Q}_{p_i}^*/\mathbb{Q}_{p_i}^{*p}$ that

$$r_1^3 r_2^4 = 3^{-12a+12a}p_i^{-9a+12a} = p_i^{3a}. \tag{116}$$

Because 3 is not a p-th power in $\mathbb{Q}_{p_i}^*$ it implies that 3 divides r_1^3 and $1/r_2^4$ to the same power. For j an index different from j, we also have that the elements $[3^{-3}p_j^{-2}, 3p_j]$ and $[3p_j, 3^{-2}p_j^{-2}]$ generate the subgroup $\partial^H(J_k(\mathbb{Q}_{p_j})/\phi(A_k(\mathbb{Q}_{p_j}))$. Writing $[r_1, r_2]$ in terms of these elements again we see that

$$[r_1, r_2] = [3^{-3}p_j^{-2}, 3p_j]^a \cdot [3p_j, 3^{-2}p_j^{-2}]^b = [3^{b-3a}p_j^{b-2a}, 3^{a-2b}p_j^{a-2b}], \tag{117}$$

and passing to $\mathbb{Q}_{p_j}^*/\mathbb{Q}_{p_j}^{*p}$ we find that

$$r_1^3 r_2^4 = 3^{-5a-5b} p_j^{-2a-2b}. \tag{118}$$

Because we know that 3 divides r_1^3 and r_2^4 to the same power we must have that $a = -b$. From this it follows that p_j divides r_1 and $1/r_2$ to the same power following the computations of the case of p_i. Since this holds for any choice of j, we can conclude that no p_j divides $r_1 r_2$. In particular $r_1 r_2$ cannot be of the form $\prod_{i \in I} p_i^{a_i}$ as described before.

Since $\partial^H(J_k(\mathbb{Q})/\phi(A_k(\mathbb{Q}))$ maps surjectively onto $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q}))$, we can conclude that elements of the form $\prod_{i \in I} p_i^{a_i}$ with I a non-empty proper subset of $\{1, \ldots, t\}$ and $1 \leq a_i \leq p-1$ do not lie in $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q}))$.

Now to show that each p_i lies in $\mathrm{Sel}(B_k)$ we must show that p_i lies in $\partial^D(J_k(\mathbb{Q}_l)/\psi(B_k(\mathbb{Q}_l))$ for each prime l. For each prime $l \in \{p_1, \ldots, p_t\} \cup U$ different from p_i, we have that p_i is a p-th power in $\mathbb{Q}_l^*$ by the assumptions of the proposition. So p_i lies in $\partial^D(J_k(\mathbb{Q}_l)/\psi(B_k(\mathbb{Q}_l))$ since p_i is equal to the image of the identity under ∂^D. This argument also holds for the infinite prime as p_i is a p-th power in $\mathbb{R}$, since it is equal to $\sqrt[p]{p_i}$. In the case that $l = p_i$, we note that $\partial^H([(0,0)-\infty]) = [3^{-3}p_i^{-2}, 3p_i]$ and $\partial^H([(3uk,0)-\infty]) = [3p_i, 3^{-2}p_i^{-2}]$ in $\mathbb{Q}_{p_i}^*$. So it follows that $\partial^D([(0,0)-\infty]) = [3^{-2}p_i^{-1}]$ and $\partial^D([(3uk,0)-\infty]) = [3^{-1}p_i^{-1}]$. Dividing the first element by the square of the second element gives us our desired result. Lastly, for the case that $l \notin \{p_1, \ldots, p_t\} \cup U$ we note that $\partial^D(J_k(\mathbb{Q}_l)/\psi(B_k(\mathbb{Q}_l))$ is equal to $\mathbb{Z}_l^*/\mathbb{Z}_l^{*p}$ by Proposition 3.11. Since l and p_i are coprime it follows immediately that p_i lies in $\mathbb{Z}_l^*/\mathbb{Z}_l^{*p} = \partial^D(J_k(\mathbb{Q}_l)/\psi(B_k(\mathbb{Q}_l))$. So we can conclude that $p_i \in \mathrm{Sel}(B_k)$. □

Putting everything discussed so far we can give a proof of Theorem 1.1.

Proof of Theorem 1.1. Let C_k again be the smooth projective curve defined by the affine model $y^p = x(x-3uk)(x-9vk)$. Let J_k be the Jacobian of C_k and let B_k be the abelian variety that corresponds to the distinguished μ_p-cover of $D = D_0 + D_1$. From the equations (1) that define $\tilde{A}$ and our discussion of models in Section 4 we see that $\tilde{A}/S_g$ is also the distinguished μ_p-cover of the Steinitz class of D. So it is birational to B_k which has genus $p-1=g$. Since $\tilde{X}$ is a μ_p-twist of $\tilde{A}$ by the action of q, it follows that $\tilde{X}$ is an $\tilde{A}$-torsor. Thus it follows that $\tilde{X}/S_g$ is birational to a B_k-torsor X that corresponds to this twist.

By combining Lemma 3.5 and Proposition 5.2 it follows that X has no rational point since q does not lie in $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q}))$. Likewise it does have a point in $\mathbb{Q}_l^*$ for every prime l, since q lies in $\mathrm{Sel}(B_k)$ by Proposition 5.2.

Lastly, we show that the class of X has order p in $Ш(B_k)$. The B_k-torsor X arises from scaling B_k with the element q as described in Section 3. Since $q^p \in \mathbb{Q}^{*p}$ the μ_p-cover we get from scaling B_k with q^p is isomorphic to B_k and we can conclude that the class of X in $Ш(B_k)$ has order p. □

As a corollary we als have the following result for $Ш(B_k)$.

Corollary 5.3. *Let C_k be the curve as described in proposition 5.2. Then $\#Ш(B_k)[p] \geq p^{t-1}$.*

Proof. From Proposition 3.10 we have the exact sequence

$$0 \to J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})) \to \mathrm{Sel}(B_k) \to Ш(B_k)[\psi] \to 0. \tag{119}$$

The products of the form $\prod_{i \in I} p_i^{a_i}$ as described in Proposition 5.2 lie in $\mathrm{Sel}(B_k)$ but not in the subgroup $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})))$. From the exact sequence it follows that these products do not lie in the kernel and are non-trivial elements of $Ш(B_k/\mathbb{Q})[\psi]$. In particular, we can look at the single primes p_i and look at the intersection of $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})))$ with the subgroup of $\mathrm{Sel}(B_k)$ generated by $\{p_1, \ldots, p_t\}$.

This subgroup has dimension at most 1 as an $\mathbb{F}_p$-vector space. To see this we consider two linearly independent elements of this subgroup of the form $q = \prod_{i \in I} p_i^{a_i}$ and $q' = \prod_{i \in I} p_i^{a_i'}$. Since these elements lie in $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})))$ we must have that $I = \{1, \ldots, t\}$ and $1 \leq a_i, a_i' \leq p-1$. Without loss of generality we can assume that $a_1 + a_1' = 0$ modulo p, since we can scale q and q' such that this holds. But this means that their product is of the form $q = \prod_{i \in I'} p_i^{a_i + a_i'}$, where $I' = \{2, \ldots, t\}$ and $0 \leq a_i, a_i' \leq p-1$. The only way this product lies in $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})))$ is if $a_i + a_i' = 0$ modulo p. This gives us a contradiction and we can conclude that the dimension is at most 1.

By looking at the exact sequence we can see that the image of $\langle p_1, \ldots, p_t \rangle$ in $Ш(B_k)[\psi]$, denoted by $\overline{\langle p_1, \ldots, p_t \rangle}$, has dimension at least $t-1$. We have that $\deg(\psi) = p$, since $\deg(\psi) = \deg(\widehat{\psi}) = \#\ker(\widehat{\psi}) = \#\langle D \rangle$, so $Ш(B_k)[\psi] \subset Ш(B_k)[p]$. We can conclude that $\#Ш(B_k)[p] = p^{\dim_{\mathbb{F}_p}(Ш(B_k)[p])} \geq p^{\dim_{\mathbb{F}_p}(\overline{\langle p_1, \ldots, p_t \rangle})} \geq p^{t-1}$. □

6 The proof of Theorem 1.2

For the proof of Theorem 1.2 we need two additional results.

Proposition 6.1. *For any u, v as above and any $t \geq 0$, there are primes $p_1, p_2, \ldots, p_t$ satisfying the conditions of Lemma 5.1.*

Proof. Let $K = \mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p-th root of unity. We will use induction on t. If $t = 0$ we satisfy the conditions and we are done.

We will assume that $t > 0$ and that there exists primes $p_1, \ldots, p_{t-1}$ that satisfy the conditions. The case for $t = 1$ follows from the same process we will describe below, if we take $k = 1$, so from now on assume that $t \geq 2$. Let k be the product $p_1 p_2 \ldots p_{t-1}$, let N be the product of the primes that divide $puv(u - 3v)k$ and let ζ_{pN} be a primitive pN-th root of unity. Let L be the compositum of $\mathbb{Q}(\zeta_{pN})$ together with all of the fields $\mathbb{Q}(\sqrt[p]{q})$ with q a prime dividing N inside $\overline{\mathbb{Q}}$. Because L is a finite compositum of Galois extensions it is a Galois extension of $\mathbb{Q}$.

Furthermore it is an abelian extension of K. To show this we will look at extensions of K of the form $K(\zeta_N)$ and $K(\sqrt[p]{q})$ for all q dividing N. The Galois groups of these extensions are cyclic groups of order N and thus abelian. For $K(\zeta_N)$ the Galois group permutes the N-th roots of unity and for the other extensions their Galois groups permute the roots of $x^p - q$, thus effectively also permuting N-th roots of unity. Let L' be the compositum inside of $\overline{\mathbb{Q}}$ of these extensions of K and consider the restriction map:

$$\mathrm{Gal}(L'/K) \to \mathrm{Gal}(K(\zeta_N)/K) \times \prod_{q\,|N} \mathrm{Gal}(K(\sqrt[p]{q})/K), \tag{120}$$

$$\sigma \mapsto (\sigma|_{K(\zeta_N)}, (\sigma|_{K(\sqrt[p]{q})})_{q|N}). \tag{121}$$

By [11, Proposition IV.1.14.] this map is injective and we can conclude that L' is an abelian extension of K. We claim that $L' = L$. Note that $K(\zeta_N) = \mathbb{Q}(\zeta_{pN})$ and that $K(\sqrt[p]{q}) = \mathbb{Q}(\zeta_p, \sqrt[p]{q}) \supseteq \mathbb{Q}(\sqrt[p]{q})$, so we have that $L \subseteq L'$. For the other inclusion we have that $\zeta_p \in \mathbb{Q}(\zeta_{pN}) \subset L$. So it follows that $\zeta_p^n(\sqrt[p]{q})^m$ lies in L for any q dividing N. Hence L contains $\mathbb{Q}(\zeta_p, \sqrt[p]{q})$ for any prime q dividing N. So $L' \subseteq L$ and we can conclude that L is an abelian extension of K.

Finally let $E = \mathbb{Q}(\sqrt[p]{3})$ and let $F = EL$ the compositum of E and L, which is a Galois extension of $\mathbb{Q}$ by the same token.

We have that E and L are linearly disjoint over $\mathbb{Q}$. We can see this because $E/\mathbb{Q}$ is totally ramified at 3, while L is unramified at 3. This gives us the exact sequence

$$0 \to (\mathbb{Z}/p\mathbb{Z}) \to \mathrm{Gal}(F/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \to 0. \tag{122}$$

Here the first non-trivial arrow maps $n \in \mathbb{Z}/p\mathbb{Z}$ to the automorphism that sends $\zeta_p^m \sqrt[p]{3}$ to $\zeta_p^{m+n} \sqrt[p]{3}$ and acts trivially on the other basis elements. The second arrow is given by the restriction map. The Chebotarev density theorem then tells us that there exists a prime p_t whose Frobenius conjugacy class in $\mathrm{Gal}(F/\mathbb{Q})$ is not trivial but restricts to the trivial class in $\mathrm{Gal}(L/\mathbb{Q})$.

By construction, p_t splits completely in any subfield of L. In particular it splits completely in $\mathbb{Q}(\zeta_{pN})$, so we have that $p_t \equiv 1 \pmod{pN}$. From this we can find that p_t is a p-th power in $\mathbb{Q}_q^*$ for q a prime dividing $3pN$. For q a prime dividing N but not $3p$, we can reduce the above congruence to $p_t \equiv 1 \pmod{q}$. So we have that $x^p - p_t \equiv x^p - 1 \pmod{q}$ has a solution and we can conclude that p_t is a p-th power in $\mathbb{Q}_q^*$ by Hensel's lemma. For $q = p$, we have that $p^2 | pN$ and thus we get the congruence $p_t \equiv 1 \pmod{p}^2$. So q is a p-th power by applying Hensel's lemma again. For $q = 3$ every unit is a p-th power in $\mathbb{Z}_3$ so p_t is one too. Similarly, p_t splits completely in $\mathbb{Q}(\sqrt[p]{q})$ for all $q|N$, so the polynomial $x^p - q$ has solutions modulo p_t. Thus the primes q are p-th powers mod p_t.

Lastly, we need to check that 3 is not a p-th power in $\mathbb{Q}_{p_t}^*$. If it were a p-th power in $\mathbb{Q}_{p_t}^*$, then the polynomial $x^p - 3$ would have a root in $\mathbb{Q}_{p_t}^*$. This would imply that p_t has a degree 1 prime above 3 in E by Kummer-Dedekind. Remember that $p_t \equiv 1 \pmod{p}$, so it follows that $\zeta_p \in \mathbb{Q}_{p_t}^*$. Thus the polynomial $x^p - 3$ has all its roots in $\mathbb{Q}_{p_t}^*$ and consequently p_t splits completely in E. By construction p_t splits completely in L, so it also splits completely in $F = EL$. But this gives a contradiction since p_t has non-trivial Frobenius conjugacy class in $\mathrm{Gal}(F/\mathbb{Q})$, so it does not split completely in F.

□

The only thing we need to prove Theorem 1.2 now is to show that for every genus p we can find values of u, v and k such that J_k is absolutely simple, and thus B_k as well.

Lemma 6.2. *For each prime $p > 3$, there exist $u, v, k \in \mathbb{Z}$ as in Proposition 5.2 such that B_k is absolutely simple.*

Proof. We will consider the Jacobian of the curve $C : y^p = x(x-1)(x-t)$ over $\mathbb{Q}(t)$. This Jacobian is absolutely simple since there is a value of $t \in \mathbb{C}$ that makes the curve isomorphic to $y^p = x^3 - 1$, namely $t = \frac{1}{2} + \frac{\sqrt{3}}{2} i$. The Jacobian of $y^p = x^3 - 1$ is absolutely simple by [8][9]. By a result of Masser [14], the geometric endomorphism ring for 100% of specializations of $t \in \mathbb{Q}$ is the same as the generic endomorphism ring. In particular, for real numbers $d, h \geq 1$ we define $v_{\text{ex}}(d, h)$ to be the set of specializations t such that the geometric and generic endomorphism ring are not the same, satisfying $[\mathbb{Q}(t) : \mathbb{Q}] \leq d$ and $h(t) \leq h$, where $h(t)$ is the Weil height function at t. Let $\omega(S)$ be the least degree of any polynomial that vanishes on the finite subset $S \subset C(\mathbb{C})$ but not identically on C. The result then states that $\omega(v_{\text{ex}}(d, h)) \leq c(\max\{d, h\})^{\lambda}$ where c is a constant depending only on C and J, the Jacobian of C, and λ is a constant depending only on $g = p - 1$, the genus of C. Taking $d = 1$, this implies that there are only a finite amount of specializations of $\mathbb{Q}$ such that the endomorphism rings are not the same.

Since the generic abelian variety is geometrically simple, this endomorphism ring is a division field, and so 100% of the specializations are simple as well. For $t = a/b \in \mathbb{Q}$ we can take a to be divisible by exactly 3 and b not divisible by 3. In other words, we have many curves of the form $y'^p = x'(x'-1)(x'-3v/u)$ with $u, v \in \mathbb{Z}$ not divisible by 3, with absolutely simple Jacobian. Under the map we $x' \mapsto x/3u$ and $y' \mapsto y/\sqrt[p]{3^3 u^3}$, we see that this is a twist of the curve $y^p = x(x-3u)(x-9v)$ and we can conclude that there exists curves of this form with absolutely simple Jacobian. □

We can now prove Theorem 1.2.

Proof of Theorem 1.2. For the case of $p = 2$ we refer to [13] or [4]. For the case of $p = 3$ we refer to [3]. Let $p > 3$ and $k \geq 1$. Let C_k be the curve (109). From Lemma 6.2 we find $u, v, k \in \mathbb{Z}$ such that B_k is absolutely simple. By Corollary 5.3 we know that $\#\text{Ш}(B_k)[p] \geq p^{t-1}$ for a given set of primes $p_1, \ldots, p_t$. Furthermore, Proposition 6.1 tells us that for any $t \geq 0$ we can find such primes. So we can take $t = k + 1$ and get the desired result. □

7 Generalizing from p to n

We have examined p-torsion in the Tate-Shafarevich group and found that it can be arbitrarily large. A natural question to ask is whether we can also generalize this result to an arbitrary integer n. For this, we first examine the case that n has the form $n = p_1 \dots p_t$ where $p_1, \dots, p_t$ are distinct primes.

7.1 The case $n = p_1 \dots p_t$

Let $n = p_1 \dots p_t$ be a product of the distinct primes $p_1, \dots, p_t$. Let Y be an abelian variety over a field F of characteristic not dividing n. Similar as in Section 3 we will introduce μ_n-covers. For this let μ_n be the F-group scheme of the n-th roots of unity. A μ_n-cover of Y is then a Y-scheme X with a simply transitive action of μ_n and we get the category $\mathcal{M}_n(Y)$ of all μ_n-covers of Y, whose morphisms are μ_n-equivariant isomorphisms. Via Proposition 3.1, it was possible to think of a μ_p-cover as a pair $(\mathcal{L}, \eta)$ where $\mathcal{L}$ is an invertible sheaf on Y and $\eta : \mathcal{L}^{\otimes p} \simeq \mathcal{O}_Y$ an isomorphism. The same results hold for n by replacing all the p's with an n. In fact, most of the results in Section 3 hold under this substitution and we will assume that these results hold under this substitution unless specified otherwise.

While it is nice that all of these results work out for n, we still need to work locally with primes so we would like to decompose the μ_n-cover into μ_{p_i}-covers for $i \in \{1, \dots, t\}$ if possible. For this we first have the following lemma.

Lemma 7.1. *Using the notation of Proposition 3.1, let $\pi : X \to Y$ be a μ_n-cover with a corresponding pair $(\mathcal{L}, \eta)$. We can construct μ_{p_i}-covers $\pi_{p_i,j} : X_{i,j} \to Y$ of Y for $i \in \{1, \dots, t\}$ corresponding to the pair $(\mathcal{L}^{\otimes j \cdot \frac{n}{p_i}}, \eta^{\otimes j \cdot \frac{n}{p_i}})$ where $1 \leq j \leq p_i - 1$.*

Proof. By Proposition 3.1 it is sufficient to find a pair $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$ such that $\mathcal{L}_{p_i,j}$ is an invertible sheaf on Y together with an isomorphism $\eta_{p_i,j} : \mathcal{L}_{p_i,j}^{\otimes p_i} \to \mathcal{O}_Y$ where $1 \leq j \leq p_i - 1$. For this we can take $\mathcal{L}_{p_i,j}$ to be $\mathcal{L}^{\otimes j \cdot \frac{n}{p_i}}$. This is an invertible sheaf on Y as $\mathcal{L}$ is invertible. The isomorphism $\eta_{p_i,j}$ is then given by the following isomorphisms:

$$\eta_{p_i,j} : \left(\mathcal{L}^{\otimes j \cdot \frac{n}{p_i}}\right)^{\otimes p_i} \simeq \mathcal{L}^{\otimes j \cdot n} \simeq \left(\mathcal{L}^{\otimes n}\right)^j \simeq \mathcal{O}_Y^{\otimes j} \simeq \mathcal{O}_Y, \tag{123}$$

where the second to last isomorphism is given by $\eta^{\otimes j}$ and the other isomorphisms follow from the properties of tensor products of $\mathcal{O}_Y$-modules. So the isomorphism $\eta_{p_i,j}$ is given by $\eta^{\otimes j}$. By the equivalence of categories we thus find a μ_{p_i}-cover $\pi_{p_i,j} : X_{i,j} \to Y$ of Y with corresponding pair $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$. Here $X_{i,j}$ is the relative spectrum of the sheaf of algebras that is generated by $\mathcal{L}_{p_i,j}$ as described in Proposition 3.1.

Let $(\mathcal{L}, \eta) \to (\mathcal{L}', \eta')$ be a morphism of μ_n-covers where $g : \mathcal{L} \to \mathcal{L}'$ is an isomorphism such that $\eta' \circ g^{\otimes n} = \eta$. This gives us an isomorphism between $g^{\otimes j \cdot \frac{n}{p_i}} : \mathcal{L}^{\otimes j \cdot \frac{n}{p_i}} \to \mathcal{L}'^{\otimes j \cdot \frac{n}{p_i}}$, which we will denote by $g_{p_i,j}$. Consequently, this gives us a morphism between the μ_{p_i}-covers $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$ and $(\mathcal{L}'_{p_i,j}, \eta'_{p_i,j})$, since we have that

$$\eta'_{p_i,j} \circ g_{p_i,j}^{\otimes p_i} = \eta'^{\otimes j} \circ (g^{\otimes j \cdot \frac{n}{p_i}})^{\otimes p_i} = \eta'^{\otimes j} \circ g^{\otimes j \cdot n} = (\eta' \circ g^{\otimes n})^{\otimes j} = \eta^{\otimes j} = \eta_{p_i,j}. \tag{124}$$

So morphisms of μ_n-covers behave well under this construction for a fixed choice of j.

□

Note that when we were discussing the morphisms of the μ_{p_i}-covers we constructed in the above lemma, we specified that our choice of j was fixed between the μ_{p_i}-covers. The following lemma explores the situation where the choices of j differ between the μ_{p_i}-covers.

Lemma 7.2. *Let $(\mathcal{L}, \eta) \to (\mathcal{L}', \eta')$ be a morphism of μ_n-covers where $g : \mathcal{L} \to \mathcal{L}'$ is an isomorphism such that $\eta' \circ g^{\otimes n} = \eta$. Let $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$ and $(\mathcal{L}'_{p_i,j'}, \eta'_{p_i,j'})$ be the μ_{p_i}-covers of $(\mathcal{L}, \eta)$ and $(\mathcal{L}', \eta')$ respectively, as described in Lemma 7.1. Assume that j and j' are distinct integers modulo p_i. Then there exists a morphism $(\mathcal{L}_{p_i,j}, \eta_{p_i,j}) \to (\mathcal{L}'_{p_i,j'}, \eta'_{p_i,j'})$ of μ_{p_i}-covers if and only if $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$ is not geometrically connected.*

Proof. We will first assume that there exists a morphism of μ_{p_i}-covers $(\mathcal{L}_{p_i,j}, \eta_{p_i,j}) \to (\mathcal{L}'_{p_i,j'}, \eta'_{p_i,j'})$. This gives us an isomorphism between $\mathcal{L}_{p_i,j}$ and $\mathcal{L}'_{p_i,j'}$. We also have an isomorphism between $\mathcal{L}'_{p_i,j'}$ and $\mathcal{L}^{\otimes j' \cdot \frac{n}{p_i}}$ given by $(g^{-1})^{\otimes j' \cdot \frac{n}{p_i}}$. This gives us an isomorphism $\mathcal{L}_{p_i,j} \simeq \mathcal{L}^{\otimes j' \cdot \frac{n}{p_i}}$, or equivalently $\mathcal{L}^{\otimes (j-j') \cdot \frac{n}{p_i}} \simeq \mathcal{O}_Y$. Since j and j' are distinct non-zero integers modulo p_i, it follows that p_i does not divide $j - j'$. So there exists an integer k such that $k(j - j') \equiv j \pmod{p_i}$. This gives us an isomorphism $\mathcal{O}_Y \simeq \mathcal{O}_Y^{\otimes k} \simeq$

$\mathcal{L}^{\otimes k(j-j')\cdot\frac{n}{p_i}} \simeq \mathcal{L}^{\otimes j\cdot\frac{n}{p_i}}$. By Lemma 3.2 this implies that the μ_{p_i}-cover $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$ is not geometrically connected.

Now assume that $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$ is not geometrically connected, so $\mathcal{L}_{p_i,j} \simeq \mathcal{O}_Y$ by Lemma 3.2. In particular, this means that $(\mathcal{L}, \eta)$ is geometrically connected neither. This means that $\mathcal{L} \simeq \mathcal{O}_Y$ so η is scalar multiplication by some $r \in F^*$. By diagram (123) it follows then that $\eta_{p_i,j}$ is equal to r^j for all j. Let $1 \leq k \leq p_i - 1$ be the integer such that $k \cdot j = j' \pmod{p_i}$. Then we have the following isomorphisms

$$\mathcal{L}_{p_i,j} \simeq \mathcal{O}_Y \simeq \mathcal{O}_Y^{\otimes k} \simeq \mathcal{L}_{p_i,j}^{\otimes k} \simeq \mathcal{L}_{p_i,j'}, \tag{125}$$

by the properties of the tensor product of $\mathcal{O}_Y$-modules and the properties of $\mathcal{L}$. Let ρ denote the isomorphism $\mathcal{L}_{p_i,j} \to \mathcal{L}_{p_i,j'}$. Since the isomorphisms $\mathcal{L}_{p_i,j} \to \mathcal{O}_Y$ and $\mathcal{O}_Y \to \mathcal{L}_{p_i,j'}$ are given by scalar multiplication with $\sqrt[p_i]{r}^j$ and $\sqrt[p_i]{r}^{-j'}$ respectively, it follows that ρ is given by scalar multiplication with $\sqrt[p_i]{r}^j / \sqrt[p_i]{r}^{-j'}$. From this it follows that $\eta_{p_i,j'} \circ \rho = \eta_{p_i,j}$ and ρ is a morphism of μ_{p_i}-covers $(\mathcal{L}_{p_i,j}, \eta_{p_i,j}) \to (\mathcal{L}_{p_i,j'}, \eta_{p_i,j'})$. As described in the previous lemma we also have a morphism of μ_{p_i}-covers $(\mathcal{L}_{p_i,j'}, \eta_{p_i,j'}) \to (\mathcal{L}'_{p_i,j'}, \eta'_{p_i,j'})$ given by $g_{p_i,j'}$. So $g_{p_i,j'} \circ \rho$ is a morphism of μ_{p_i}-covers $(\mathcal{L}_{p_i,j}, \eta_{p_i,j}) \to (\mathcal{L}'_{p_i,j'}, \eta'_{p_i,j'})$, which gives us our desired result. □

In the proof we implicitly used the fact that the μ_n-cover $(\mathcal{L}, \eta)$ is not geometrically connected if its μ_{p_i}-cover $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$ is not geometrically connected. We will make this explicit.

Lemma 7.3. *The μ_n-cover $\pi : X \to Y$ corresponding to $(\mathcal{L}, \eta)$ is not geometrically connected if and only if the μ_{p_i}-covers $\pi_{p_i,j} : X_{i,j} \to Y$ corresponding to $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$ for one of the $i \in \{1, \dots, t\}$ and $1 \leq j \leq p_i - 1$ is not geometrically connected.*

Proof. Assume that $\pi : X \to Y$ is not geometrically connected. By Lemma 3.2 this means that $\mathcal{L} \simeq \mathcal{O}_Y$. By the properties of the tensor product of $\mathcal{O}_Y$-modules and the properties of $\mathcal{L}$ we get the isomorphisms

$$\mathcal{O}_Y \simeq \mathcal{O}_Y^{\otimes j\cdot\frac{n}{p_i}} \simeq \mathcal{L}^{\otimes j\cdot\frac{n}{p_i}} \simeq \mathcal{L}_{p_i,j}, \tag{126}$$

for all choices of $i \in \{1, \dots, t\}$ and $1 \leq j \leq p_i - 1$. So $\pi_{p_i,j} : X_{i,j} \to Y$ is not geometrically connected either.

Now assume that $\pi_{p_i,j} : X_{i,j} \to Y$ is not geometrically connected for one of the $i \in \{1, \dots, t\}$ and $1 \leq j \leq p_i - 1$. So we have an isomorphism $\mathcal{L}_{p_i,j} \simeq \mathcal{O}_Y$ and $\eta_{p_i,j}$ is scalar multiplication by some $r \in F^*$. In this case, $X_{i,j}$ is isomorphic to $Y \times_F F(\sqrt[p_i]{r})$ as an F-scheme which is not geometrically connected. Since $(X_{i,j}, \mathcal{O}_{X_{i,j}})$ is a subscheme of $(X, \mathcal{O}_X))$, it follows that $\pi : X \to Y$ is not geometrically connected. □

From Lemma 7.1 we see that given a μ_n-cover $(\mathcal{L}, \eta)$ we can construct the μ_{p_i}-covers $(\mathcal{L}_{p_i,j}, \eta_{p_i,j})$ for all $i \in \{1, \dots, t\}$ and $1 \leq j \leq p_i - 1$. When taking this approach we need to specify which μ_{p_i}-cover we are taking with respect to j when we are only considering the μ_{p_i}-covers of $(\mathcal{L}, \eta)$ for a specific prime p_i. However, it turns out that when we are considering the μ_{p_i}-covers of $(\mathcal{L}, \eta)$ for all primes p_i at once then we do not need to specify this distinction and there is a canonical way that the μ_n-cover $(\mathcal{L}, \eta)$ decomposes into μ_{p_i}-covers. We do this by looking at how the action of μ_n acts on $\mathcal{L}$ and how it decomposes in terms of actions of μ_{p_i}.

Lemma 7.4. *Let $\pi : X \to Y$ be a μ_n-cover with a corresponding pair $(\mathcal{L}, \eta)$. Then $(\mathcal{L}, \eta)$ decomposes uniquely into μ_{p_i}-covers $\pi_{p_i} : X_i \to Y$ with corresponding pair $(\mathcal{L}_{p_i}, \eta_{p_i})$, determined by the action of μ_n on $\mathcal{L}$. So π decomposes uniquely as the tensor product $\otimes_{i=1}^t \pi_{p_i}$.*

Conversely, let $\pi_{p_i} : X_i \to Y$ be a collection of μ_{p_i}-covers with corresponding pairs $(\mathcal{L}_{p_i}, \eta_{p_i})$ for $i \in \{1, \dots, t\}$. We can construct a unique μ_n-cover $\pi : X \to Y$ with corresponding pair $(\mathcal{L}, \eta)$, such that its induced μ_{p_i}-covers are π_{p_i} for all $i \in \{1, \dots, t\}$.

Proof. We will consider the sheaf of $\mathcal{O}_Y$-modules

$$\pi_* \mathcal{O}_X = \bigoplus_{i=0}^{n-1} \mathcal{L}^i. \tag{127}$$

We can write $\mathcal{L}^i$ as $\mathcal{L}^i \simeq \otimes_{j=1}^t \mathcal{L}_{p_i}^{a_{ij}}$ for some $0 \leq a_{i_j} \leq p_j - 1$. The a_{ij} need to be chosen such that the action of ζ_n on both sides of the equation is the same. The action of ζ_n on the left-hand side is given by $\zeta_n \cdot s = \zeta_n^i s$. By Lemmma 7.1 $\mathcal{L}_{p_i}$ is given by $\mathcal{L}^{\otimes j \cdot \frac{n}{p_i}}$ for some $1 \leq j \leq p_i - 1$. So the action of ζ_n on $\mathcal{L}_{p_i}^{a_{ij}}$ is given by $\zeta_n \cdot s = \zeta_n^{a_{ij} \cdot j \frac{n}{p_i}} s = \zeta_{p_i}^{a_{ij}} s$, since $\zeta_n^{j \frac{n}{p_i}}$ is some primitive p_i-th root of unity. Thus on the right-hand side the action is given by $\zeta_n \cdot s = (\prod_{j=1}^t \zeta_{p_j}^{a_{ij}}) s = \zeta_n^{\sum_{j=1}^t a_{ij} p_j} s$. Comparing the equations on both sides we need to solve $i \equiv \sum_{j=1}^t a_{ij} p_j \pmod{n}$ for all $i \in \{0, \ldots, n-1\}$. By the Chinese remainder theorem we find a unique solution for every i and it follows that

$$\pi_* \mathcal{O}_X = \bigoplus_{i=0}^{n-1} \mathcal{L}^i = \bigoplus_{i=0}^{n-1} \left(\bigotimes_{j=1}^{t} \mathcal{L}_{p_j}^{a_{ij}} \right) = \bigotimes_{j=1}^{t} \left(\bigoplus_{i=0}^{n-1} \mathcal{L}_{p_j}^{a_{ij}} \right) = \bigotimes_{j=1}^{t} \pi_{p_j *} \mathcal{O}_X \tag{128}$$

which gives us the desired result.

Let $\pi_{p_i} : X_i \to Y$ be a collection of μ_{p_i}-covers with corresponding pairs $(\mathcal{L}_{p_i}, \eta_{p_i})$ for $i \in \{1, \ldots, t\}$. Let ζ_{p_i} be the p_i-th primitive root such that the action of μ_{p_i} on $\mathcal{L}_{p_i}^j$ is given by $\zeta_{p_i} \cdot s = \zeta_{p_i}^j s$ for $0 \leq j \leq p_i - 1$. Let ζ_n be the n-th primitive root given by $\zeta_n = \prod_{i=1}^t \zeta_{p_i}$. We consider the invertible sheaf $\mathcal{L} := \bigotimes_{i=1}^t \mathcal{L}_{p_i}$. Let $s = \otimes_{i=1}^t s_i$ be an element of $\mathcal{L}$ where $s_i \in \mathcal{L}_{p_i}$. We define an action of μ_n on $\mathcal{L}$ by defining the action as $\zeta_n \cdot s = \otimes_{i=1}^t \zeta_{p_i} s_i$. This gives us a $\mathbb{Z}/n\mathbb{Z}$-grading on the sheaf $\bigoplus_{i=0}^n \mathcal{L}^i$, where $\zeta_n \cdot s \otimes_{i=1}^t \zeta_{p_i}^j s_i$ for $s \in \mathcal{L}^j$ and $0 \leq j \leq n-1$. As a final step, we need to find an isomorphism $\eta : \mathcal{L}^{\otimes n} \to \mathcal{O}_Y$. For this we will consider the isomorphism

$$\eta : \mathcal{L}^{\otimes n} = \bigotimes_{i=1}^{t} (\mathcal{L}_{p_i}^{\otimes p_i})^{\frac{n}{p_i}} \simeq \bigotimes_{i=1}^{t} \mathcal{O}_Y^{\otimes \frac{n}{p_i}} \simeq \mathcal{O}_Y, \tag{129}$$

where the first isomorphism is given by $\otimes_{i=1}^t \eta_{p_i}^{\otimes \frac{n}{p_i}}$ and the second isomoprhism follows from the properties of tensor products. Thus we find an isomorphism $\eta : \mathcal{L}^{\otimes n} \to \mathcal{O}_Y$ given by $\eta := \otimes_{i=1}^t \eta_{p_i}^{\otimes \frac{n}{p_i}}$. By the equivalence of categories the pair $(\mathcal{L}, \eta)$ gives us a μ_n-cover $\pi : X \to Y$. By the arguments earlier in this lemma we see that the induced μ_{p_i}-covers of $(\mathcal{L}, \eta)$ are given by $(\mathcal{L}_{p_i}, \eta_{p_i})$.

We will now examine how morphisms of μ_{p_i}-covers combine into a morphism of μ_n-covers. Consider the collection of μ_{p_i}-covers $(\mathcal{L}_{p_i}, \eta_{p_i}) \to (\mathcal{L}'_{p_i}, \eta'_{p_i})$ given by isomorphisms $g_{p_i} : \mathcal{L}_{p_i} \to \mathcal{L}'_{p_i}$ such that $\eta'_{p_i} \circ g^{\otimes p_i} = \eta_{p_i}$ where $i \in \{1, \ldots, t\}$. Let $(\mathcal{L}, \eta)$ and $(\mathcal{L}', \eta')$ be μ_n covers as constructed as above. We must find an isomorphism $g : \mathcal{L} \to \mathcal{L}'$ such that $\eta' \circ g^{\otimes n} = \eta$. The isomorphism $\bigotimes_{i=1}^t \mathcal{L}_{p_i} = \mathcal{L} \simeq \mathcal{L}' = \bigotimes_{i=1}^t \mathcal{L}'_{p_i}$ gives us an obvious choice for g, namely the map $g := \otimes_{i=1}^t g_{p_i}$. To see that this map satisfies our conditions we check that

$$\eta' \circ g^{\otimes n} = \otimes_{i=1}^t \eta'^{\otimes \frac{n}{p_i}}_{p_i} \circ \left(\otimes_{i=1}^t g_{p_i} \right)^{\otimes n} = \otimes_{i=1}^t \left(\eta'_{p_i} \circ g_{p_i}^{\otimes p_i} \right)^{\otimes \frac{n}{p_i}} = \otimes_{i=1}^t \eta_{p_i}^{\otimes \frac{n}{p_i}} = \eta \tag{130}$$

and we see that g satisfies $\eta' \circ g^{\otimes n} = \eta$. So morphisms behave well under this construction and we are done. $\square$

Example 7.5. *Let $n = 6 = 2 \cdot 3$. Consider a μ_6-cover $\pi : X \to Y$ over Y with a corresponding pair $(\mathcal{L}, \eta)$. Looking at the sheaf*

$$\begin{aligned}
\pi_* \mathcal{O}_X &= \mathcal{O}_Y \oplus \mathcal{L} \oplus \mathcal{L}^2 \oplus \mathcal{L}^3 \oplus \mathcal{L}^4 \oplus \mathcal{L}^5 && (131)\\
&\simeq \left(\mathcal{O}_Y \otimes \mathcal{O}_Y \right) \oplus \left(\mathcal{L}^3 \otimes \mathcal{L}^4 \right) \oplus \left(\mathcal{O}_Y \otimes \mathcal{L}^2 \right) \oplus \left(\mathcal{L}^3 \otimes \mathcal{O}_Y \right) \oplus \left(\mathcal{O}_Y \otimes \mathcal{L}^4 \right) \oplus \left(\mathcal{L}^3 \otimes \mathcal{L}^2 \right) && (132)\\
&\simeq \left(\mathcal{O}_Y \oplus \mathcal{L}^3 \right) \otimes \left(\mathcal{O}_Y \oplus \mathcal{L}^2 \oplus \mathcal{L}^4 \right) && (133)\\
&= \pi_{2*} \mathcal{O}_X \otimes \pi_{3*} \mathcal{O}_X. && (134)
\end{aligned}$$

We see that the action of ζ_6 decomposes into an action of ζ_2 and ζ_3^2, since $\mathcal{L} \simeq \mathcal{L}^3 \otimes \mathcal{L}^4$. Thus we get a decomposition into the μ_2-cover corresponding to $(\mathcal{L}_2, \eta_2)$ and the μ_3-cover $(\mathcal{L}_3, \eta_3)$, where $\mathcal{L}_2 := \mathcal{L}^3$ and $\mathcal{L}_3 := \mathcal{L}^4$.

We can now think of a μ_n-cover $\pi : X \to Y$ in terms of the pair $(\mathcal{L}, \eta)$ and its induced μ_{p_i}-covers $\pi_{p_i} : X_i \to Y$ with corresponding pairs $(\mathcal{L}_{p_i}, \eta_{p_i})$. We will call the line bundles $\mathcal{L}, \mathcal{L}_{p_i} \in \text{Pic}(Y)(F)$ the Steinitz classes of π and π_{p_i} respectively. Since these line bundles are n-torsion and p_i-torsion bundles respectively, we can continue the notation from Section 3 and let $\mathcal{L} \in \widehat{Y}[n](F)$ and $\mathcal{L}_{p_i} \in \widehat{Y}[p_i](F)$ where $\widehat{Y} = \text{Pic}^0(Y)$ is the dual abelian variety.

We now know how the action of a μ_n-cover decomposes. The next thing we will look at is how morphisms and isomorphisms are affected under this decomposition. We have seen that we could scale μ_p-covers and we can do the same in the case where we replace p with n.

Given a μ_n-cover $(\mathcal{L}, \eta)$ we acquire a different μ_n-cover $(\mathcal{L}, r\eta)$ by scaling $\eta : \mathcal{L}^{\otimes n} \to \mathcal{O}_Y$ with $r \in F^*$. Two such μ_n-covers $(\mathcal{L}, r\eta)$ and $(\mathcal{L}, s\eta)$ are isomorphic if and only if $r/s \in F^{*n}$. We can carry this process over through the decomposition and get a μ_{p_i}-cover $(\mathcal{L}_{p_i}, r\eta)$. In particular, an isomorphism of μ_n-covers in this manner induces an isomorphism of μ_{p_i}-covers. If $r/s = t^n$ was a n-th power, then it is also a p_i-th power as $t^n = (t^{n/p_i})^{p_i}$. Likewise, if $(\mathcal{L}_{p_i}, r\eta_{p_i})$ and $(\mathcal{L}_{p_i}, s\eta_{p_i})$ are isomorphic μ_{p_i}-covers for all $i \in \{1, \dots, t\}$, then r/s is a p_i-th power for all i. Since F is a field it follows that r/s is a $p_1 \dots p_t = n$-th power as well, so we get an isomorphism of μ_n-covers $(\mathcal{L}, r\eta)$ and $(\mathcal{L}, s\eta)$ this way.

Given two μ_n-covers $(\mathcal{L}, \eta)$ and $(\mathcal{L}', \eta')$, their tensor product $(\mathcal{L} \otimes \mathcal{L}', \eta \otimes \eta')$ is another μ_n-cover. This construction follows for μ_{p_i}-covers $(\mathcal{L}_{p_i}, \eta_{p_i})$ and $(\mathcal{L}'_{p_i}, \eta'_{p_i})$, and we get the tensor product $(\mathcal{L}_{p_i} \otimes \mathcal{L}'_{p_i}, \eta_{p_i} \otimes \eta'_{p_i})$ for all $i \in \{1, \dots, t\}$. We let $H^1(Y, \mu_n)$ denote the set of μ_n-covers of Y and we get an isomorphism $H^1(Y, \mu_n) \simeq \otimes_{i=1}^{t} H^1(Y, \mu_{p_i})$ from Lemma 7.4.

We have seen in Section 3 for a geometrically connected μ_p-cover $\pi : X \to Y$ corresponding to $(\mathcal{L}, \eta)$ that X is a torsor for the abelian variety $A_{\mathcal{L}}$. We will proceed with a similar construction for our μ_n-covers. By Lemma 7.3 if $\pi : X \to Y$ is a geometrically connected μ_n-cover corresponding to the pair $(\mathcal{L}, \eta)$, then the induced μ_{p_i}-covers $\pi_{p_i} : X_i \to Y$ corresponding to $(\mathcal{L}_{p_i}, \eta_{p_i})$ are geometrically connected as well. So X is a torsor for a family of abelian varieties and we will examine how these are related to each other.

Similar to Section 3, let $\widehat{\psi} : \widehat{Y} \to \widehat{Y}/\langle \mathcal{L} \rangle$ be the degree n isogeny obtained from modding out $\mathcal{L}$. Let $\psi : A_{\mathcal{L}} \to Y$ be the dual isogeny, which is also of degree n, where $A_{\mathcal{L}}$ denotes the dual of $\widehat{Y}/\langle \mathcal{L} \rangle$. We give ψ the structure of a μ_n-cover and we have that

$$\ker \psi \simeq \widehat{\ker \widehat{\psi}} \simeq \widehat{\mathbb{Z}/n\mathbb{Z}} = \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_m) \simeq \mu_n. \tag{135}$$

By the chinese remainder theorem we have that $\mu_n \simeq \prod_{i=1}^{t} \mu_{p_i}$, which suggests that there exist isogenies $\psi_{p_i} : A_{\mathcal{L}_{p_i}} \to Y$ for the induced μ_{p_i}-covers such that $\mu_{p_i} \simeq \ker \psi_{p_i}$. Indeed, let $\widehat{\psi_{p_i}} : \widehat{Y} \to \widehat{Y}/\langle \mathcal{L}_{p_i} \rangle$ be the degree p_i isogeny by modding out $\mathcal{L}_{p_i}$ and let $\psi_{p_i} : A_{\mathcal{L}_{p_i}} \to Y$ be its dual isogeny. By Lemma 7.4 every element of $\langle \mathcal{L} \rangle$ is generated by the $\mathcal{L}_{p_i}$, so we get an isomorphism $\langle \mathcal{L} \rangle \simeq \prod_{i=1}^{t} \langle \mathcal{L}_{p_i} \rangle$.

We can consider the following diagram:

$$\begin{tikzcd} \widehat{Y} \arrow[r, "\widehat{\psi}"] \arrow[dr, "\widehat{\psi_{p_i}}"'] & \widehat{Y}/\langle \mathcal{L} \rangle \\ & \widehat{Y}/\langle \mathcal{L}_{p_i} \rangle \arrow[u, "\widehat{q_i}"'] \end{tikzcd} \tag{136}$$

Here ψ and ψ_{p_i} are the usual quotient isogenies and $\widehat{q_i}$ is the projection from $\widehat{Y}/\langle \mathcal{L}_{p_i} \rangle$ to $\widehat{Y}/\langle \mathcal{L} \rangle$. The kernel of the projection is given by the image of $\langle \mathcal{L}_{p_j} \rangle_{j \neq i}$ in $\widehat{Y}/\langle \mathcal{L}_{p_i} \rangle$. Thus the degree of $\widehat{q_i}$ is equal to n/p_i and we have that $\deg(\widehat{\psi}) = n = n \cdot n/p_i = \deg(\widehat{q_i}) \deg(\widehat{\psi_{p_i}}) = \deg(\widehat{q_i} \circ \widehat{\psi_{p_i}})$. So we have a commutative diagram of isogenies and we get the dual diagram:

$$\begin{tikzcd} Y & A_{\mathcal{L}} \arrow[l, "\psi"'] \arrow[d, "q_i"] \\ & A_{\mathcal{L}_{p_i}} \arrow[ul, "\psi_{p_i}"] \end{tikzcd} \tag{137}$$

Here q_i is the isogeny dual to $\widehat{q_i}$.

These maps give us the isomorphisms

$$\ker \psi \simeq \mu_n \simeq \prod_{i=1}^{t} \mu_{p_i} \simeq \prod_{i=1}^{t} \ker \psi_{p_i}. \tag{138}$$

We get $\varphi(n) = \varphi(p_1) \dots \varphi(p_t) = (p_1 - 1) \dots (p_t - 1)$ different isomorphisms which correspond to the $\mathbb{Z}/n\mathbb{Z}$-gradings on $\psi_* A_{\mathcal{L}}$. We choose the isomorphism such that the μ_n-cover $\psi : A_{\mathcal{L}} \to Y$ has Steinitz class $\mathcal{L}_1 \subset \psi_* \mathcal{O}_{A_{\mathcal{L}}}$ isomorphic to $\mathcal{L}$. This choice of isomorphism then determines the isomorphisms $\ker \psi_{p_i} \simeq \mu_{p_i}$ such that the action of $\mathbb{Z}/p_i\mathbb{Z}$ on $\psi_* A_{\mathcal{L}_{p_i}}$ corresponds to the action of $\mathbb{Z}/p_i\mathbb{Z}$ on the μ_{p_i}-covers in the decomposition of $\mathcal{L}$. The μ_{p_i}-cover corresponding to ψ_{p_i} must have Steinitz class $\mathcal{L}_1 \subset \psi_{p_i *} \mathcal{O}_{A_{\mathcal{L}_{p_i}}}$ isomorphic to $\mathcal{L}_{p_i}$ by Lemma 7.4.

We can now prove the analogue of Lemma 3.3 for n and expand on it.

Lemma 7.6. *Let $\pi : X \to Y$ be a μ_n-cover with non-trivial Steinitz class $\mathcal{L} \in \widehat{Y}[n](F)$. Then π is a twist of the μ_p-cover $\psi : A_{\mathcal{L}} \to Y$ and we have that X is a torsor for $A_{\mathcal{L}}$. Furthermore, if $\pi_{p_i} : X_i \to Y$ are the induced μ_{p_i}-covers with non-trivial Steinitz classes $\mathcal{L}_{p_i} \in \widehat{Y}[p_i](F)$, then the π_{p_i} are twists of the μ_{p_i}-covers $\psi_{p_i} : A_{\mathcal{L}_{p_i}} \to Y$ and X_i is a torsor for $A_{\mathcal{L}_{p_i}}$.*

Proof. The proof for the first part of the lemma will be similar to the proof of [5, Lemma 2.6] and will be included for the sake of clarity.

If $\psi : A_{\mathcal{L}} \to Y$ corresponds to $(\mathcal{L}, \eta)$, then $\pi : X \to Y$ corresponds to $(\mathcal{L}, s\eta)$ for some $s \in F^*$. Over the field $F(\sqrt[n]{s})$, there is an isomorphism $\rho : A_{\mathcal{L}} \to X$ of μ_n-covers which satisfies

$$\rho^g(P) = \sqrt[n]{s}^g / \sqrt[n]{s} + \rho(P) \tag{139}$$

for all $g \in \text{Gal}(\overline{F}/F)$ and $P \in A_{\mathcal{L}}$. This makes sense since $\sqrt[n]{s}^g / \sqrt[n]{s} \in \mu_n$. The torsor $A_{\mathcal{L}} \times X \to X$ is given by $(P, Q) \mapsto \rho(P + \rho^{-1}(Q))$. Let $g \in \text{Gal}(\overline{F}/F)$ and $P, Q \in A_{\mathcal{L}}$. Then we have that

$$\begin{aligned}
\left[\rho(P + \rho^{-1}(Q))\right]^g &= \rho^g(P^g + (\rho^{-1})^g(Q^g)) && (140)\\
&= \rho(P^g + \rho^{-1}(Q^g) - \sqrt[n]{s}^g / \sqrt[n]{s}) + \sqrt[n]{s}^g / \sqrt[n]{s} && (141)\\
&= \rho(P^g + \rho^{-1}(Q^g)) - \sqrt[n]{s}^g / \sqrt[n]{s} + \sqrt[n]{s}^g / \sqrt[n]{s} && (142)\\
&= \rho(P^g + \rho^{-1}(Q^g)), && (143)
\end{aligned}$$

where we used that $(\rho^{-1})^g(P) = -\sqrt[n]{s}^g / \sqrt[n]{s} + \rho(P)^{-1}$ in (141) and the fact that ρ is μ_n-equivariant as a μ_n-cover morphism in (142). From this we see that the torsor structure is defined over F.

Let $\psi_{p_i} : A_{\mathcal{L}_{p_i}} \to Y$ be the induced μ_{p_i}-covers of ψ corresponding to the pairs $(\mathcal{L}_{p_i}, \eta_{p_i})$. Since $\pi : X \to Y$ corresponds to the pair $(\mathcal{L}, s\eta)$, we must have that the induced covers of π correspond to the pair $(\mathcal{L}_{p_i}, s\eta_{p_i})$. Let the line bundle $\mathcal{L}_{p_i}$ be given by $\mathcal{L}^{\otimes j \cdot \frac{n}{p_i}}$ for some $1 \leq j \leq p_i - 1$ as described in Lemma 7.1. Then the induced isomorphism $\rho_{p_i} : A_{\mathcal{L}_{p_i}} \to X_i$ is given by $\rho^{\otimes j}$ from (123). The action of $\text{Gal}(\overline{F}/F)$ is given by

$$\rho_{p_i}^g(P) = (\sqrt[n]{s}^g / \sqrt[n]{s})^{\otimes j} + \rho(P)_{p_i} \tag{144}$$

for all $g \in \text{Gal}(\overline{F}/F)$ and $P \in A_{\mathcal{L}_{p_i}}$. The rest of the proof is similar as before and we are done. □

Similar to Section 3 we will specialize ourselves to the situation of Jacobians. Let C be a smooth projective geometrically integral curve over F, and let $J = \text{Pic}^0(C)$ be its Jacobian. Let g be the genus of the curve and thus the dimension of the abelian variety J. We let $D \in J[n](F)$ be a divisor class of order n and we consider the quotient $\widehat{\psi} : J \to J/\langle D \rangle$. We let $\psi : A_D \to \widehat{J}$ be the dual of this isogeny, where A_D is the dual of $J/\langle D \rangle$. We identify $\widehat{J}$ with J via the canonical principal polarization and thus acquire a μ_n-cover $\psi : A_D \to J$ with corresponding pair $(\mathcal{L}, \eta)$. We can choose the μ_n-cover structure on ψ such that $\mathcal{L} \in \text{Pic}^0(\widehat{J})(F)$ gets mapped to D under the isomorphism $\hat{\hat{J}} \simeq J$. Thus we can associate $\mathcal{L}$ with D and we have for the induced μ_{p_i}-covers $(\mathcal{L}_{p_i}, \eta_{p_i})$ that $\mathcal{L}_{p_i}$ corresponds with $D_{p_i} := \frac{n}{p_i} \cdot D$. So we get the induced μ_{p_i}-covers $\psi_{p_i} : A_{D_{p_i}} \to J$.

7.2 Jacobians and μ_n-covers for curves of the form $y^n = x(x - e_1)(x - e_2)$

We will now examine the Jacobian of curves of the form $y^n = x(x-e_1)(x-e_2)$ and look at their μ_n-covers, similarly to the case where $n = p$. Additionally, we will also examine the μ_{p_i}-covers of such Jacobians.

Let $n = p_1 \dots p_t$ be a product of the distinct primes $p_1, \dots, p_t$. Let e_0, e_1 and e_2 be distinct integers and consider the smooth projective curve C over $\mathbb{Q}$ with affine model

$$y^n = (x - e_0)(x - e_1)(x - e_2). \tag{145}$$

Without loss of generality we can assume that $e_0 = 0$. This affine model is smooth and it has a single rational point at infinity denoted by ∞. The genus of the curve is equal to $g = p - 2$ if 3 divides n and equal to $g = p - 1$ otherwise by [26, §1].

Let J be the Jacobian of C. The subgroup $J(\mathbb{Q})[n]$ has rank at least 2, because it contains the elements $D_i = [(e_i, 0) - \infty]$ for $i \in \{0, 1, 2\}$. We have that $D_0 + D_1 + D_2 = \text{div}(y)$ so it is equal to 0 in J. Let $H := \langle D_0, D_1 \rangle$. We can define the following abelian variety:

$$\widehat{A} = J/H. \tag{146}$$

For $D := D_0 + D_1$ we define the variety

$$\widehat{B} = J/\langle D\rangle. \tag{147}$$

For these varieties we can define the quotient isogenies $\widehat{\phi} : J \to \widehat{A}$ and $\widehat{\psi} : J \to \widehat{B}$. By duality we get the dual isogenies $\phi : A \to \widehat{J}$ and $\psi : B \to \widehat{J}$. Furthermore, via the canonical principal polarization we can identify J with its dual and acquire the maps $\phi : A \to J$ and $\psi : B \to J$. This turns A and B into μ_n-covers of J. We also define the varieties $A_{D_i} = J/\langle D_i\rangle$ for $i \in \{0, 1, 2\}$ in this manner, with the corresponding isogenies $\psi_i : A_{D_i} \to J$. Note that $B \simeq A_{D_2}$, because $D = -D_2$.

We now get the map

$$J(\mathbb{Q})/\phi(A(\mathbb{Q})) \xrightarrow{\partial^H} \mathbb{Q}^*/\mathbb{Q}^{*n} \times \mathbb{Q}^*/\mathbb{Q}^{*n} \tag{148}$$

$$\left[\sum_{j=1}^{g}(x_j, y_j) - g \cdot \infty\right] \mapsto \left(\prod_{j=1}^{g} x_j, \prod_{j=1}^{g}(x_j - e_1)\right) \tag{149}$$

as described in the Lemmas 3.6, 3.8 and 3.9. From [21, Proposition 2.7] it follows that the class of the divisor $\sum_{j=1}^{g}(x_j, y_j) - g\cdot\infty$, with $x_i, y_i \in \overline{\mathbb{Q}}$, can be represented by a $\mathbb{Q}$-rational divisor, because $C(\mathbb{Q}) \neq \emptyset$. This map is well-defined whenever the x_j and $x_j - e_1$ are non-zero. By [10, VI §4 Lemma 3] it is possible to find a representative in every class in $J(\mathbb{Q})/\phi(A(\mathbb{Q}))$ such that the map is well-defined.

We can construct similar homomorphisms for the other varieties we have defined:

$$\partial^{D_i} : J(\mathbb{Q})/\psi_i(A_{D_i}(\mathbb{Q})) \to \mathbb{Q}^*/\mathbb{Q}^{*n} \tag{150}$$

$$\left[\sum_{j=1}^{g}(x_j, y_j) - g \cdot \infty\right] \mapsto \prod_{j=1}^{g}(x_j - e_i) \tag{151}$$

for A_{D_i} with $i \in \{0, 1, 2\}$. Here this description also only works on the classes for which the map is well-defined. However from these maps we find that

$$\partial^{D_0} \cdot \partial^{D_1} \cdot \partial^{D_2}\left(\left[\sum_{j=1}^{g}(x_j, y_j) - g \cdot \infty\right]\right) = \prod_{j=1}^{g} x_j(x_j - e_1)(x_j - e_2) = \prod_{j=1}^{g} y_j^n = 1, \tag{152}$$

since the x_j and y_j lie on the curve C. So we get the identity:

$$\partial^{D_0} \cdot \partial^{D_1} \cdot \partial^{D_2} = 1. \tag{153}$$

This allows us to describe our homomorphisms on classes where they are not well-defined. We can describe the behaviour of ∂^H on the roots similar to Lemma 4.1.

Lemma 7.7. *We have*

$$\partial^H([(0, 0) - \infty]) = [e_1^{-1}e_2^{-1}, -e_1], \tag{154}$$

and

$$\partial^H([(e_1, 0) - \infty]) = [e_1, (e_1 - e_2)^{-1}]. \tag{155}$$

Proof. The proof is similar to the proof of Lemma 4.1. $\square$

Lastly, for B we have the homomorphism

$$\partial^D : J(\mathbb{Q})/\psi(B(\mathbb{Q})) \to \mathbb{Q}^*/\mathbb{Q}^{*n}, \tag{156}$$

$$\left[\sum_{j=1}^{g}(x_j, y_j) - g \cdot \infty\right] \mapsto \prod_{j=1}^{g} x_j(x_j - e_1). \tag{157}$$

This gives us the following commutative diagram which we will use in the next section

$$\begin{array}{ccc} J(\mathbb{Q})/\phi(A(\mathbb{Q})) & \xrightarrow{\partial^H} & \mathbb{Q}^*/\mathbb{Q}^{*n} \times \mathbb{Q}^*/\mathbb{Q}^{*n} \\ \downarrow & & \downarrow \\ J(\mathbb{Q})/\psi(B(\mathbb{Q})) & \xrightarrow{\partial^D} & \mathbb{Q}^*/\mathbb{Q}^{*n} \end{array} \tag{158}$$

where the right vertical map is given by $[r_1, r_2] \mapsto [r_1 r_2]$.

We can find birational models for μ_n-covers of J given a Steinitz class. For our case we will look at the Steinitz class of $D = D_0 + D_1$. The distinguished μ_n-cover for this Steinitz class is the cover $B \to J$. Let this μ_n-cover correspond with the data $(\mathcal{L}, \eta)$. By Lemma 3.7 we have that $f(0_J)$ is an n-th power in $\mathbb{Q}^*$ where $f = \eta^{-1} \in \mathbb{Q}(J)$. For any point $P \in J(\mathbb{Q})/\psi(B(\mathbb{Q}))$ we have that $\partial^D(P) = r_P = f(P+Q)/f(Q)$ using Lemma 3.6. Taking $Q = 0_J$ we can rewrite this equation to get

$$f(P) = f(P + 0_J) = f(0_J) r_P = 1. \tag{159}$$

since $f(0_J)$ is an n-th power and the cover $B \to J$ is isomorphic to $(\mathcal{L}, \eta)$, so $r_P = 1$. Because $nD = \operatorname{div}(x(x-e_1))$, it follows from Lemma 3.8 that $1 = f(P) = [x(x-e_1)](P)$. Since P can be written in the form $\sum_{j=1}^{g}(x_j, y_j) - g \cdot \infty$ we finally get the equation

$$z^n = \prod_{j=1}^{g} x_j(x_j - e_1). \tag{160}$$

where the variable z^n comes from lifting the equation out of $\mathbb{Q}^*/\mathbb{Q}^{*n}$. Together with the birational model for J given by the equations

$$y_j^n = x_j(x_j - e_1)(x_j - e_2). \tag{161}$$

for $1 \le j \le g$, we get a birational model for B.

Finally for $r \in \mathbb{Q}^*$, the μ_n-cover $(\mathcal{L}, r\eta)$ is described by the equations

$$y_j^n = x_i(x_j - e_1)(x_j - e_2). \tag{162}$$

for $1 \le j \le g$, together with the additional equation

$$rz^n = \prod_{j=1}^{g} x_j(x_j - e_1). \tag{163}$$

which is twisted by r.

7.2.1 The μ_{p_i}-covers of $y^n = x(x-e_1)(x-e_2)$

We fix the index i for the prime p_i dividing n for this section. Let J denote the Jacobian of the curve (145) as described in the previous section. The subgroup $J(\mathbb{Q})[p_i]$ of $J(\mathbb{Q})[n]$ has rank at least 2 as well, as this subgroup contains the elements $D_{p_i,j} := \frac{n}{p_i} \cdot D_j$ for $j \in 0, 1, 2$. We also have that $D_{p_i,0} + D_{p_i,1} + D_{p_i,2} = \frac{n}{p_i}(D_0 + D_1 + D_2) = \frac{n}{p_i} \cdot \operatorname{div}(y)$, so the sum $D_{p_i,0} + D_{p_i,1} + D_{p_i,2}$ is equal to 0 in J. Let $H_{p_i} := \langle D_{p_i,0}, D_{p_i,1} \rangle$. We can define the following abelian variety:

$$\widehat{A_{p_i}} = J/H_{p_i}. \tag{164}$$

For $D_{p_i} := D_{p_i,0} + D_{p_i,1}$ we define the variety

$$\widehat{B_{p_i}} = J/\langle D_{p_i} \rangle. \tag{165}$$

For these varieties we can define the quotient isogenies $\widehat{\phi_{p_i}} : J \to \widehat{A_{p_i}}$ and $\widehat{\psi_{p_i}} : J \to \widehat{B_{p_i}}$. By duality we get the dual isogenies $\phi_{p_i} : A_{p_i} \to \widehat{J}$ and $\psi_{p_i} : B_{p_i} \to \widehat{J}$. Furthermore, via the canonical principal polarization we can identify J with its dual and acquire the maps $\phi_{p_i} : A_{p_i} \to J$ and $\psi_{p_i} : B_{p_i} \to J$. This turns A_{p_i} and B_{p_i} into μ_{p_i}-covers of J. These are the induced μ_{p_i}-covers of the μ_n-covers ϕ and ψ of the previous section. We also define the varieties $A_{p_i,D_j} = J/\langle D_{p_i,j} \rangle$ for $j \in \{0, 1, 2\}$ in this manner, with the corresponding isogenies $\psi_{p_i,j} : A_{p_i,j} \to J$. Note that $B_{p_i} \simeq A_{p_i,D_2}$, because $D_{p_i} = -D_{p_i,2}$.

This gives us the map

$$J(\mathbb{Q})/\phi_{p_i}(A_{p_i}(\mathbb{Q})) \xrightarrow{\partial^{H_{p_i}}} \mathbb{Q}^*/\mathbb{Q}^{*p_i} \times \mathbb{Q}^*/\mathbb{Q}^{*p_i} \tag{166}$$

$$\left[\sum_{j=1}^{g}(x_j, y_j) - g \cdot \infty\right] \mapsto \left(\prod_{j=1}^{g} x_j, \prod_{j=1}^{g}(x_j - e_1)\right) \tag{167}$$

as described in the Lemmas 3.6, 3.8 and 3.9. From [21, Proposition 2.7] it follows that the class of the divisor $\sum_{j=1}^{g}(x_j, y_j) - g\cdot\infty$, with $x_j, y_j \in \overline{\mathbb{Q}}$, can be represented by a $\mathbb{Q}$-rational divisor, because $C(\mathbb{Q}) \neq \emptyset$. This map is well-defined whenever the x_j and $x_j - e_1$ are non-zero. By [10, VI §4 Lemma 3] it is possible to find a representative in every class in $J(\mathbb{Q})/\phi(A_{p_i}(\mathbb{Q}))$ such that the map is well-defined.

We can construct similar homomorphisms for the other varieties we have defined:

$$\partial^{D_{p_i,j}} : J(\mathbb{Q})/\psi_{p_i,j}(A_{D_{p_i,j}}(\mathbb{Q})) \to \mathbb{Q}^*/\mathbb{Q}^{*p_i} \tag{168}$$

$$\left[\sum_{k=1}^{g}(x_k, y_k) - g\cdot\infty\right] \mapsto \prod_{k=1}^{g}(x_k - e_j) \tag{169}$$

for $A_{D_{p_i,j}}$ with $j \in \{0,1,2\}$. Here this description also only works on the classes for which the map is well-defined. However from these maps we find that

$$\partial^{D_{p_i,0}} \cdot \partial^{D_{p_i,1}} \cdot \partial^{D_{p_i,2}} \left(\left[\sum_{j=1}^{g}(x_j, y_j) - g\cdot\infty\right]\right) = \prod_{j=1}^{g} x_j(x_j - e_1)(x_j - e_2) = \prod_{j=1}^{g} y_j^n = 1, \tag{170}$$

since the x_j and y_j lie on the curve C. So we get the identity:

$$\partial^{D_{p_i,0}} \cdot \partial^{D_{p_i,1}} \cdot \partial^{D_{p_i,2}} = 1. \tag{171}$$

This allows us to describe our homomorphisms on classes where they are not well-defined and we get a direct analogue of Lemma 7.7.

Lemma 7.8. *We have*

$$\partial^{H_{p_i}}([(0,0) - \infty]) = [e_1^{-1}e_2^{-1}, -e_1], \tag{172}$$

and

$$\partial^{H_{p_i}}([(e_1,0) - \infty]) = [e_1, (e_1 - e_2)^{-1}]. \tag{173}$$

Proof. The proof is similar to the proof of Lemma 4.1. □

Lastly, for B_{p_i} we have the homomorphism

$$\partial^{D_{p_i}} : J(\mathbb{Q})/\psi(B_{p_i}(\mathbb{Q})) \to \mathbb{Q}^*/\mathbb{Q}^{*p_i}, \tag{174}$$

$$\left[\sum_{j=1}^{g}(x_j, y_j) - g\cdot\infty\right] \mapsto \prod_{j=1}^{g} x_j(x_j - e_1). \tag{175}$$

This gives us the following commutative diagram which we will use in the next section

$$\begin{array}{ccc} J(\mathbb{Q})/\phi_{p_i}(A_{p_i}(\mathbb{Q})) & \xrightarrow{\partial^{H_{p_i}}} & \mathbb{Q}^*/\mathbb{Q}^{*p_i} \times \mathbb{Q}^*/\mathbb{Q}^{*p_i} \\ \downarrow & & \downarrow \\ J(\mathbb{Q})/\psi_{p_i}(B_{p_i}(\mathbb{Q})) & \xrightarrow{\partial^{D_{p_i}}} & \mathbb{Q}^*/\mathbb{Q}^{*p_i} \end{array} \tag{176}$$

where the right vertical map is given by $[r_1, r_2] \mapsto [r_1 r_2]$.

We can find birational models for μ_{p_i}-covers of J given a Steinitz class. For our case we will look at the Steinitz class of $D_{p_i} = D_{p_i,0} + D_{p_i,1}$. The distinguished μ_{p_i}-cover for this Steinitz class is the cover $B_{p_i} \to J$. Let this μ_{p_i}-cover correspond with the data $(\mathcal{L}_{p_i}, \eta_{p_i})$. By Lemma 3.7 we have that $f(0_J)$ is a p_i-th power in $\mathbb{Q}^*$ where $f = \eta^{-1} \in \mathbb{Q}(J)$. For any point $P \in J(\mathbb{Q})/\psi_{p_i}(B_{p_i}(\mathbb{Q}))$ we have that $\partial^{D_{p_i}}(P) = r_{p_i,P} = f(P+Q)/f(Q)$ using Lemma 3.6. Taking $Q = 0_J$ we can rewrite this equation to get

$$f(P) = f(P + 0_J) = f(0_J) r_{p_i,P} = 1. \tag{177}$$

since $f(0_J)$ is a p_i-th power and $r_{p_i,P} = 1$ because the cover $B_{p_i} \to J$ is isomorphic to $(\mathcal{L}_{p_i}, \eta_{p_i})$. Because $p_i D_{p_i} = \operatorname{div}(x(x - e_1))$, it follows from Lemma 3.8 that $1 = f(P) = [x(x - e_1)](P)$. Since P can be written in the form $\sum_{j=1}^{g}(x_j, y_j) - g\cdot\infty$ we finally get the equation

$$z^{p_i} = \prod_{j=1}^{g} x_j(x_j - e_1). \tag{178}$$

where the variable z^{p_i} comes from lifting the equation out of $\mathbb{Q}^*/\mathbb{Q}^{*p_i}$. Together with the birational model for J given by the equations

$$y_j^n = x_j(x_j - e_1)(x_j - e_2). \tag{179}$$

for $1 \leq j \leq g$, we get a birational model for B_{p_i}.

Finally for $r \in \mathbb{Q}^*$, the μ_{p_i}-cover $(\mathcal{L}_{p_i}, r\eta_{p_i})$ is described by the equations

$$y_j^n = x_j(x_j - e_1)(x_j - e_2). \tag{180}$$

for $1 \leq j \leq g$, together with the additional equation

$$rz^{p_i} = \prod_{j=1}^{g} x_j(x_j - e_1). \tag{181}$$

which is twisted by r.

7.3 Computing $\#J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q)))$

Similarly to the case where $n = p$, we will specialize the curve (145) and look at the curve $C_{u,v}$ given by the affine model:

$$C = C_{u,v} : y^n = x(x - 3u)(x - 9v). \tag{182}$$

Here u, v are integers not divisible by 3 and $n = p_1 \dots p_t$ a product of distinct primes $p_1, \dots, p_t$. Let J be the Jacobian of C and let A and B be the μ_n-covers from the previous section and let A_{p_i} and B_{p_i} be the μ_{p_i}-covers from the previous section for all $1 \leq i \leq t$.

We can determine the size of $J(\mathbb{Q}_q/\phi(A(\mathbb{Q}_q)))$ for certain primes q similar to Lemma 5.1:

Lemma 7.9. *Let q be a prime such that $q \equiv 1 \pmod n$. Then we have that $\#J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q))) = n^2 \cdot \prod_{i=1}^{t} c_q(J)/c_q(A_{p_i})$.*

Proof. The congruence condition on q implies that $\mathbb{Q}_q^*$ contains the n-th roots of unity. Consequently, this means that $\mathbb{Q}_q^*$ also contains the p_i-th roots of unity, since p_i divides n for all $1 \leq i \leq t$. Let ζ_k denote a primitive k-th root of unity where $k \in \{n, p_1, \dots, p_t\}$.

Since $\mathbb{Q}_q$ contains ζ_k, we get an autotomorphism $(x, y) \mapsto (x, \zeta_k y)$ on C. If we interpret (x, y) as a divisor on C, then we can define the pushforward $\zeta_{k*} : \text{div}(C) \to \text{div}(C)$ as $\zeta_{k*}(x, y) = (x, \zeta_k y)$. We can extend this map $\mathbb{Z}$-linearly to all divisors of C and acquire a homomorphism $\zeta_{k*} : J \to J$ sending $[D] \mapsto [\zeta_{k*}D]$ by [25, Proposition II.3.6]. This gives us a ring embedding $\iota : \mathbb{Z}[\zeta_k] \hookrightarrow \text{End}(J)$ which is described in the following way: For an element $m\zeta_k^i$ in $\mathbb{Z}[\zeta_k]$ with $m \in \mathbb{Z}$ and $0 \leq i \leq k-1$, the element $\iota(m\zeta_k^i)$ acts on a divisor class $[D]$ in J by $\iota(m\zeta_k^i)[D] = [m \cdot (\zeta_{k*}D)]$. Note that $\mathbb{Q}(\zeta_k) \simeq \mathbb{Z}[\zeta_k] \otimes \mathbb{Q}$ forms a $\mathbb{Q}$-subalgebra under this embedding. By [15, Proposition V.10.23] we have that $\deg(\iota(\alpha)) = \text{Nm}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\alpha)^{\frac{2g}{f}}$ where g is the genus of J and $f = [\mathbb{Q}(\zeta_k) : \mathbb{Q}] = \varphi(k)$.

Let us assume that $k = p_i$ for some $1 \leq i \leq t$. The kernel of $\widehat{\phi_{p_i}} : J \to \widehat{A_{p_i}}$ is given by $\langle D_{p_i,0}, D_{p_i,1} \rangle$. The kernel of the endomorphism $1 - \iota(\zeta_{p_i})$ is given by all points P in J such that $P \sim \iota(\zeta_{p_i})(P)$. In particular, a point P of the form $[(x, y)]$ satifies the relation if $y = 0$. So it follows that

$$\ker(\widehat{\phi_{p_i}}) = \langle D_{p_i,0}, D_{p_i,1} \rangle \subset \ker(1 - \iota(\zeta_{p_i})). \tag{183}$$

In contrast to Lemma 5.1, the kernels of $1 - \iota(\zeta_{p_i})$ and $\widehat{\phi_{p_i}}$ do not coincide since the size of $\ker(1 - \iota(\zeta_{p_i}))$ is equal to $\text{Nm}_{\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}}(1 - \zeta)^{\frac{2g}{p_i - 1}} = p_i^{\frac{2g}{p_i - 1}}$, which is strictly larger than the size of $\ker(\widehat{\phi_{p_i}})$.

Let $\phi_{p_i}^{(q)} : A_{p_i}(\mathbb{Q}_q) \to J(\mathbb{Q}_q)$ denote the induced homomorphism on $\mathbb{Q}_q$. The local Selmer ratio is defined as

$$c_q(\phi_{p_i}) = \frac{\#\text{coker}\phi_{p_i}^{(q)}}{\#\text{ker}\phi_{p_i}^{(q)}} = \frac{\#J(\mathbb{Q}_q)/\phi_{p_i}^{(q)}(A_{p_i}(\mathbb{Q}_q))}{\#A_{p_i}(\mathbb{Q}_q)[\phi_{p_i}^{(q)}]}. \tag{184}$$

By [23, Corollary 3.2] we have that

$$c_q(\phi_{p_i}) = c_q(J)/c_q(A_{p_i}), \tag{185}$$

where the right hand side is the ratio of the Tamagawa numbers at q.

Let us now examine $\phi^{(q)} : A(\mathbb{Q}_q) \to J(\mathbb{Q})$ the induced homomorphism of $\phi : A(\mathbb{Q}) \to J(\mathbb{Q})$. Similar to $\phi_{p_i}^{(q)}$ we define the local Selmer ratio as

$$c_q(\phi) = \frac{\#\text{coker}\phi^{(q)}}{\#\text{ker}\phi^{(q)}} = \frac{\#J(\mathbb{Q}_q)/\phi^{(q)}(A(\mathbb{Q}_q))}{\#A(\mathbb{Q}_q)[\phi^{(q)}]}. \tag{186}$$

The result of [23, Corollary 3.2] only applies to isogenies with degree equal to a power of a prime, so we will take a different approach to show that $c_q(\phi) = c_q(J)/c_q(A)$.

Recall that equation (138) tells us that $\ker(\phi) \simeq \prod_{i=1}^t \ker(\phi_{p_i})$, so we find that $\#\text{ker}\phi^{(q)} = \prod_{i=1}^t \#\text{ker}\phi_{p_i}^{(q)}$. For $\#\text{coker}\phi^{(q)}$ we can find a similar by looking at the dual of the cokernel. For the dual of the cokernel we have that

$$\text{coker}\phi = \widehat{\ker\phi} = \widehat{\ker\widehat{\widehat{\phi}}} = \ker\widehat{\phi}, \tag{187}$$

since ϕ is isomorphic to $\widehat{\widehat{\phi}}$ by Corollary 2.22 and because the cokernel of ϕ is equal to the dual of $\ker\phi$. Since $\ker\widehat{\phi} = \langle D_0, D_1\rangle \simeq \prod_{i=1}^t \langle D_{p_i,0}, D_{p_i,1}\rangle = \prod_{i=1}^t \ker\widehat{\phi_{p_i}}$ we find that

$$\#\text{coker}\phi^{(q)} = \#\ker\widehat{\phi^{(q)}} = \prod_{i=1}^t \#\ker\widehat{\phi_{p_i}^{(q)}} = \prod_{i=1}^t \#\text{coker}\phi_{p_i}^{(q)}. \tag{188}$$

Combining this with (185) and (186) we find that

$$c_q(\phi) = \frac{\#\text{coker}\phi^{(q)}}{\#\text{ker}\phi^{(q)}} = \prod_{i=1}^t \frac{\#\text{coker}\phi_{p_i}^{(q)}}{\#\text{ker}\phi_{p_i}^{(q)}} = \prod_{i=1}^t c_q(\phi_{p_i}) = \prod_{i=1}^t c_q(J)/c_q(A_{p_i}). \tag{189}$$

Since the kernel of ϕ is isomorphic to μ_n it follows that $\#A(\mathbb{Q}_q)[\phi^{(q)}] = n^2$. So we get that

$$\#J(\mathbb{Q}_q)/\phi^{(q)}(A(\mathbb{Q}_q)) = \#A(\mathbb{Q}_q)[\phi^{(q)}] \cdot \prod_{i=1}^t c_q(J)/c_q(A_{p_i}) = n^2 \cdot \prod_{i=1}^t c_q(J)/c_q(A_{p_i}). \tag{190}$$

□

We find that $\#J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q))) = n^2 \cdot \prod_{i=1}^t c_q(J)/c_q(A_{p_i})$ which makes us run into some trouble. The proof of Proposition 5.2 relies on the fact that the two elements $\partial^H([(0,0)-\infty])$ and $\partial^H([(3uk,0)-\infty])$ are linearly independent. Since in the setting of Proposition 5.2 we have that $\#J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q))) = p^2$, these elements generate all of $J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q)))$. In the above proof the genus of A makes it not possible to find an isomorphism between J and A or A_{p_i} over $\mathbb{Q}_q$. So we need to directly calculate the Tamagawa numbers or find a different method. Unfortunately, my experience with measure theory is not sufficient to see this through.

One observation we can make is that we acquire A_{p_i} by taking the quotient of A with a finite set, as seen from the diagram (137) and its dual diagram (136). This could mean that the Tamagawa numbers of A and A_{p_i} are equal. In that scenario we get that $\#J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q))) = n^2 \cdot (c_q(J)/c_q(A))^t$, so we would only need to calculate the Tamagawa numbers $c_q(J)$ and $c_q(A)$ in this scenario.

8 Lemmermeyer and Mollin in the language of μ_2-covers

In this section we will look at the paper "On Tate-Shafarevich groups of $y^2 = x(x^2-k^2)$" by F. Lemmermeyer and R. Mollin [13] and look at their results through the lens of μ_2-covers. We will see how our methods are applicable and compare our results with their findings.

We will consider an elliptic curve E_k over $\mathbb{Q}$ with affine model

$$y^2 = x(x^2-k^2) = x(x-k)(x+k), \tag{191}$$

where $k \geq 1$ is some integer. This affine model is smooth and we denote the point at infinity with ∞ to stay consistent with previous notation. Since E_k is an elliptic curve its genus is equal to 1.

Let $J_k = \mathrm{Pic}^0(E_k)$ be the Jacobian of E_k. Note that the morphism $P \mapsto [P-\infty]$ from E_k to $\mathrm{Pic}^0(E_k)$ is an isomorphism, so we can always think of J_k as the elliptic curve E_k. It is well known that the 2-torsion points of an elliptic curve are given by $E_k[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$ [25, Corollary III.6.4.] and in our case the 2-torsion points are given by $E_k[2] = \{\infty, (0,0), (k,0), (-k,0)\}$. We will denote these points by $D_0 = (0,0)$, $D_1 = (k,0)$ and $D_2 = (-k,0)$. We have an equality of divisors $D_0 + D_1 + D_2 = \mathrm{div}(y)$, so in J_k we have that $D_0 + D_1 + D_2 = 0$. We let $H = \langle D_0, D_2\rangle$ and define the abelian variety

$$\widehat{A_k} = J_k/H. \tag{192}$$

Likewise for $D = D_0 + D_2$, we define the variety

$$\widehat{B_k} = J_k/\langle D\rangle, \tag{193}$$

This gives us the quotient isogenies $\widehat{\phi} : J_k \to \widehat{A_k}$ and $\widehat{\psi} : J_k \to \widehat{B_k}$, and their corresponding dual isogenies $\phi : A_k \to J_k$ and $\psi : B_k \to J_k$. In a similar way we define the varieties $A_{k,D_i} = J_k/\langle D_i\rangle$ with isogenies $\psi_i : A_{k,D_i} \to J_k$ for $i \in \{0,1,2\}$. Note that we have an isomorphism $B_k \simeq A_{k,D_1}$, as $D = -D_1$ in J_k.

We can define the map

$$\begin{aligned} \partial^H : J_k(\mathbb{Q})/\phi(A_k(\mathbb{Q})) &\to \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} && (194)\\ [(x,y)-\infty] &\mapsto (x, x+k) && (195)\end{aligned}$$

as described in the Lemmas 3.6, 3.8 and 3.9. Because E_k has $\mathbb{Q}$-rational points, by [21, Proposition 2.7] the divisor class $[(x,y)-\infty]$ is $\mathbb{Q}$-rational. By [10, VI §4 Lemma 3] every class in $J_k(\mathbb{Q})/\phi(A_k(\mathbb{Q}))$ can be represented by a divisor, such that x and $x-k$ are non-zero. So the map ∂^H is well-defined.

We can construct similar homomorphisms for the other varieties we have defined:

$$\begin{aligned} \partial^{D_i} :& J_k(\mathbb{Q})/\psi_i(A_{k,D_i}(\mathbb{Q})) \to \mathbb{Q}^*/\mathbb{Q}^{*2} && (196)\\ & [(x,y)-\infty] \mapsto x - e_i, && (197)\end{aligned}$$

where $e_i = \begin{cases} 0, & \text{if } i = 0\\ k, & \text{if } i = 1\\ -k, & \text{if } i = 2\end{cases}$, for A_{k,D_i} whenever $i \in \{0,1,2\}$. We can use the identity (94) to describe the maps ∂^{D_i} on classes that evaluate to 0. In particular, we can give a more general description of $\partial^H(e_k)$ for $k \in \{0,1,2\}$, because we can divide squares out in $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Lemma 8.1. *Let $H = \langle D_i, D_j\rangle$. We introduce the following notation $\partial^{D_i}(e_k) := \partial^{D_i}([(e_k,0)-\infty])$ and $\partial^H(e_k) := \partial^H([(e_k,0)-\infty])$. We have the following expression for ∂^H:*

$$\partial^H(e_k) = \begin{cases} [\partial^{D_i}(e_k), \partial^{D_j}(e_k)], & \text{if } k \neq i,j,\\ [\prod_{l\neq k}\partial^{D_l}(e_k), \partial^{D_j}(e_k)], & \text{if } k = i,\\ [\partial^{D_i}(e_k), \prod_{l\neq k}\partial^{D_l}(e_k)], & \text{if } k = j.\end{cases} \tag{198}$$

Proof. We consider $\partial^{D_i}(e_k)$. If $k \neq i$ then we can evaluate $\partial^{D_i}(e_k)$ as it is. If $k = i$ then we can use the identity (94) and find that

$$\partial^{D_i}(e_k) = \prod_{l\neq k}\partial^{D_l}(e_k)^{-1} = \prod_{l\neq k}\partial^{D_l}(e_k).$$

The expression of ∂^H follows from these observations. □

Lastly, for B_k we have the homomorphism

$$\partial^D : J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})) \to \mathbb{Q}^*/\mathbb{Q}^{*2}, \tag{199}$$
$$[(x,y)-\infty] \mapsto x(x-k). \tag{200}$$

This gives us the following commutative diagram which we will use in the next section

$$\begin{array}{ccc} J_k(\mathbb{Q})/\phi(A_k(\mathbb{Q})) & \xrightarrow{\partial^H} & \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} \\ \downarrow & & \downarrow \\ J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})) & \xrightarrow{\partial^D} & \mathbb{Q}^*/\mathbb{Q}^{*2} \end{array} \tag{201}$$

where the right vertical map is given by $[r_1, r_2] \mapsto [r_1 r_2]$. We can apply this map on the results of Lemma 8.1 to get the following results:

Corollary 8.2. *The element $\partial^H(e_k)$ gets mapped to*

$$\partial^H(e_k) \mapsto \begin{cases} \partial^{D_i}(e_k)\partial^{D_j}(e_k), & \text{if } k \neq i,j, \\ \partial^{D_l}(e_k), & \text{otherwise}, \end{cases} \tag{202}$$

under the right vertical map of diagram (201) *where $l \neq i,j$.*

We will construct birational models of J_k for a μ_n-cover with Steinitz class $D = D_0 + D_1$. The distinguished μ_2-cover for this Steinitz class is the cover $B_k \to J_k$. Let this μ_2-cover correspond with the data $(\mathcal{L}, \eta)$. By Lemma 3.7 we have that $f(0_J)$ is a square in $\mathbb{Q}^*$ where $f = \eta^{-1} \in \mathbb{Q}(J_k)$. For any point $P \in J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q}))$ we have that $\partial^D(P) = r_P = f(P+Q)/f(Q)$ using Lemma 3.6. Taking $Q = 0_{J_k}$ we can rewrite this equation to get

$$f(P) = f(P + 0_{J_k}) = f(0_{J_k})r_P = 1, \tag{203}$$

since $f(0_{J_k})$ is a square and because the cover $B_k \to J_k$ is isomorphic to $(\mathcal{L}, \eta)$, so $r_P = 1$. Because $nD = \mathrm{div}(x(x-k))$, it follows from Lemma 3.8 that $1 = f(P) = [x(x-k)](P)$. Since P can be written in the form $(x,y) - \infty$ we finally get the equation

$$z^2 = x(x-k), \tag{204}$$

where the variable z^2 comes from lifting the equation out of $\mathbb{Q}^*/\mathbb{Q}^{*2}$. Together with the birational model for J_k given by the equation

$$y^2 = x(x-k)(x+k) \tag{205}$$

we get a birational model for B_k.

Finally for $r \in \mathbb{Q}^*$, the μ_p-cover $(\mathcal{L}, r\eta)$ is described by the equation

$$y^2 = x(x-k)(x+k), \tag{206}$$

together with the additional equation

$$rz^2 = x(x-k). \tag{207}$$

which is twisted by r.

8.1 Finding elements of the Selmer group

In Section 5 we specialized the curve $C : y^p = x(x-e_1)(x-e_2)$ to be of the form $C_k : y^p = x(x-3uk)(x-9vk)$, where $p > 3$ is a prime and $u, v \in \mathbb{Z}$ are not divisible by 3. However, we are now working with curves of a specific form, namely $y^2 = x(x-k)(x+k)$, so we cannot make a specialization of this form and we will have to see which of our previous results can be applied and which have to be modified. The first lemma we encountered, Lemma 5.1, is still applicable and can be worded more strongly.

Lemma 8.3. *For all odd primes q, we have that $\#J_k(\mathbb{Q}_q)/\phi(A_k(\mathbb{Q}_q)) = 2^2$.*

Proof. The proof is the same as the proof of Lemma 5.1, with all instances of p replaced with 2. □

When we look at the analogue of Proposition 5.2 we run into some complications. The first problem we face is that previously the integer 3 in the curve C_k played a crucial role in proving Proposition 5.2, since the images of $\partial^H([(0,0)-\infty])$ and $\partial^H([(3uk,0)-\infty])$ contained powers of 3 across the localizations $\mathbb{Q}_{p_i}^*\mathbb{Q}_{p_i}^{*p} \times \mathbb{Q}_{p_i}^*/\mathbb{Q}_{p_i}^{*p}$ for all p_i. This allowed 3 to act as a global prime over all localizations and carry across information between the localizations. Secondly, the localizations $\mathbb{Q}_l^*/\mathbb{Q}_l^{*2}$ contain less structure than $\mathbb{Q}_l^*/\mathbb{Q}_l^{*p}$. Lemma 8.3 tells us that $J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q))$ is generated by 2 elements of order 2, which limits our options for finding certain congruences. Lastly, we need to consider which set of conditions our primes need to satisfy as in the paper [13] and as in Proposition 5.2. Considering these complications we might consider a different choice of divisor D, and consequently a different subspace H.

We will proceeed in proving analogue of Proposition 5.2 in the following way. We consider the elliptic curve $E_k : y^2 = x(x^2 - k^2)$ where $k = p_1 \dots p_m$ is a product of odd primes. Let J_k be the Jacobian of this elliptic curve. We let $\psi : B_k \to J_k$ denote the dual isogeny acquired by modding out the divisor $D = D_i + D_j$ for some $0 \le i < j \le 2$ and subsequently $\phi : A_k \to J_k$ denotes the dual isogeny of modding out the subspace $H = \langle D_i, D_j \rangle$. We will first show that p_i lies in the Selmer group B_k for all i and all choices of D. We define the Selemer group of B_k as the subgroup $\mathrm{Sel}(B_k) \subseteq \mathbb{Q}^*/\mathbb{Q}^{*2}$ of classes r with the property that for every prime $l \le \infty$, the class of r in $\mathbb{Q}_l^*/\mathbb{Q}_l^{*2}$ is in the image of $\partial^D : J(\mathbb{Q}_l)/\psi(B_k(\mathbb{Q}_l)) \to \mathbb{Q}_l^*/\mathbb{Q}_l^{*2}$. We can now state the first part of our analogue:

Proposition 8.4. *Let $k = p_1 \dots p_m$ be a product of distinct odd primes satisfying $(p_i/p_j) = 1$ for all $i \neq j$ in $\{1, \dots, m\}$. Then for all i we have that $p_i \in \mathit{Sel}(B_k)$.*

Proof. We fix an index $1 \le i \le m$. We would like to show that $p_i \in \mathrm{Sel}(B_k)$. For this we show that p_i lies in $\partial^D(J_k(\mathbb{Q}_l)/\psi(B_k(\mathbb{Q}_l)))$ for all choices of D and all primes l.

Let us first assume that l is of the form p_j where j is distinct from the index i. By our assumptions on k, p_i is a square in $\mathbb{Q}_{p_j}^*$. So p_i is equal to the image of the identity under ∂^D for any choice of D. The same argument holds for $l = 2$, as all odd primes are squares modulo 2. If l is not equal to p_j for all j or 2, then p_i lies in the image ∂^D by Proposition 3.11 because the discriminant of E_k is only divisible by 2 and the primes p_i.

Lastly for $l = p_i$, we can directly find elements of $J_k(\mathbb{Q}_l)/\psi(B_k(\mathbb{Q}_l))$ that get mapped to p_i. If $D = D_0 + D_1$, then $\partial^D([(0,0) - \infty]) = -1 \cdot -k = k$. Note that p_j is a square in $\mathbb{Q}_{p_i}$ for j distinct from i and thus k is equal to p_i in $\mathbb{Q}_{p_i}$. In the case where $D = D_0 + D_2$, we have that $\partial^D(0) = -k$. So the case where $D = D_0 + D_2$ is only applicable whenever the primes p_i are equivalent to $1 \pmod 4$, since -1 is a square then. Lastly if $D = D_1 + D_2$, then $\partial^D(k) = 2 \cdot 2k = k$ so by the previous argument it is equal to p_i. ☐

Now we will examine if we can prove that p_i does not lie in $\partial^D(J_k(\mathbb{Q}))$ for certain choices of D, using the methods employed in Proposition 5.2. We will continue with the notation introduced in Lemma 8.1. Before we get started with the proposition we will first prove the following lemma.

Lemma 8.5. *Let $k = p_1 \dots p_m$ be a product of distinct primes satisfying $(p_i/p_j) = 1$ and $(-1/p_i) = -1$ for all $i \neq j$ in $\{1, \dots, m\}$. Let $D = D_i + D_j$ where $0 \le i < j \le 2$ and $H = \langle D_i, D_j \rangle$. We can find $0 \le k < k' \le 2$ such that $\partial^H(e_k)$ and $\partial^H(e'_k)$ are linearly independent in $\mathbb{Q}_{p_l}^*/\mathbb{Q}_{p_l}^{*2} \times \mathbb{Q}_{p_l}^*/\mathbb{Q}_{p_l}^{*2}$ for all possible pairs of D and all primes p_l. Furthermore, these two elements will generate all of $\partial^H(J_k(\mathbb{Q}_{p_l})/\phi(A_k(\mathbb{Q}_{p_l}))$.*

Proof. By the conditions on the primes the element k is equal to p_l in $\mathbb{Q}_{p_l}^*/\mathbb{Q}_{p_l}^{*2} \times \mathbb{Q}_{p_l}^*/\mathbb{Q}_{p_l}^{*2}$.

Let $D = D_0 + D_1$. By Lemma 8.1 we find that $\partial^H(0) = [-1, -p_l]$, $\partial^H(k) = [p_l, 2]$ and $\partial^H(-k) = [-p_l, -2p_l]$ in $\mathbb{Q}_{p_l}^*/\mathbb{Q}_{p_l}^{*2} \times \mathbb{Q}_{p_l}^*/\mathbb{Q}_{p_l}^{*2}$. We can interpret elements of $\mathbb{Q}_{p_l}^*/\mathbb{Q}_{p_l}^{*2} \times \mathbb{Q}_{p_l}^*/\mathbb{Q}_{p_l}^{*2}$ as squarefree elements. So if we want to check if two elements are linearly independent, it is sufficient to check that their product is not equal to $[1,1]$. With this in mind it is easy to see that these elements are all pairwise linearly independent.

Similarly, for $D = D_0 + D_2$ the elements $\partial^H(0) = [-1, k]$, $\partial^H(k) = [k, 2k]$ and $\partial^H(-k) = [-k, 2]$ are pairwise linearly independent. Lastly, for $D = D_1 + D_2$ we have that the elements $\partial^H(0) = [-k, k]$, $\partial^H(k) = [2, 2k]$ and $\partial^H(-k) = [-2k, 2]$ are pairwise linearly independent.

By Lemma 8.3 these two elements will generate all of $\partial^H(J_k(\mathbb{Q}_{p_i})/\phi(A_k(\mathbb{Q}_{p_i}))$. ☐

We can now prove the proposition.

Proposition 8.6. *Let $k = p_1 \dots p_m$ be a product of distinct primes satisfying $(p_i/p_j) = 1$ and $(-1/p_i) = -1$ for all $i \neq j$ in $\{1, \dots, m\}$. Then p_i does not lie in $\partial^D(J_k(\mathbb{Q}))$ for $D = D_0 + D_2$. More generally, if $q = \prod_{i \in I} p_i$ where $I \subset \{1, \dots, m\}$ is a non-empty proper subset, then q does not lie in $\partial^D(J_k(\mathbb{Q}))$ for $D = D_0 + D_2$.*

Proof. We fix a prime p_l for $1 \leq l \leq m$. Let $D = D_i + D_j$ where $0 \leq i < j \leq 2$ and $H = \langle D_i, D_j \rangle$. From Lemma 8.1 we find that.

$$\partial^H(e_k) = \begin{cases} [\partial^{D_i}(e_k), \partial^{D_j}(e_k)], & \text{if } k \neq i, j, \\ [\prod_{l \neq k} \partial^{D_l}(e_k), \partial^{D_j}(e_k)], & \text{if } k = i, \\ [\partial^{D_i}(e_k), \prod_{l \neq k} \partial^{D_l}(e_k)], & \text{if } k = j. \end{cases} \tag{208}$$

And by Lemma 8.5 we have that $\partial^H(e_k)$ and $\partial^H(e_{k'})$ are linearly independent for every choice of $0 \leq k < k' \leq 2$ in $\mathbb{Q}_l^*/\mathbb{Q}_l^{*2} \times \mathbb{Q}_l^*/\mathbb{Q}_l^{*2}$ and generate all of $\partial^H(J_k(\mathbb{Q}_{p_l})/\phi(A_k(\mathbb{Q}_{p_l}))$.

Similar to the proof of Proposition 5.2, we consider an element $[r_1, r_2]$ in $\partial^H(J_k(\mathbb{Q})/\phi(A_k(\mathbb{Q})))$ and we will show that r_1r_2 cannot be of the form $q = \prod_{i \in I} p_i$ where $I \subset \{1, \dots, m\}$ is a non-empty proper subset. By Proposition 3.11 the integers are only divisible by the primes in $\{p_1, \dots, p_m, 2\}$. If there is no l such that p_l divides both r_1 and r_2 to the same power, then all the p_l divide r_1r_2. So r_1r_2 cannot be of the form q as described above.

Now assume p_l divides r_1 and r_2 to the same power. We know that the pair of $\partial^H(e_k)$ and $\partial^H(e_{k'})$ generate all of $\partial^H(J_k(\mathbb{Q}_{p_l})/\phi(A_k(\mathbb{Q}_{p_l})))$, so $[r_1, r_2] = \partial^H(e_k)$ for some $0 \leq k \leq 2$ or $[1, 1]$. We will apply the mapping $[r_1, r_2] \mapsto r_1r_2$ from diagram (201) to $\partial^H(e_k)$ for every choice of k. This allows us to check for which choices of k the product r_1r_2 is divisible by p_l. The elements -1 and 2 will act as global primes in this proof similar to the element 3 in Proposition 5.2. We will use these global primes to check what the representatives of $[r_1, r_2]$ are in $\partial^H(J_k(\mathbb{Q}_{p_{l'}})/\phi(A_k(\mathbb{Q}_{p_{l'}})))$ for l' an index different from l. We want to show that r_1r_2 are not divisible by $p_{l'}$ then and conclude that r_1r_2 is not of the form $q = \prod_{i \in I} p_i$ where $I \subset \{1, \dots, m\}$ is a non-empty proper subset. We will do this for all choices of $D = D_i + D_j$.

The case $D = D_0 + D_1$:
Let $D = D_0 + D_1$. Because of the condition on our primes, in $\partial^H(J_k(\mathbb{Q}_{p_l})/\phi(A_k(\mathbb{Q}_{p_l})))$ we get the elements $\partial^H(0) = [-1, -p_l]$, $\partial^H(k) = [p_l, 2]$ and $\partial^H(-k) = [-p_l, -2p_l]$. Under the mapping $[r_1, r_2] \mapsto r_1r_2$ it follows that $\partial^H(0) \mapsto p_l$, $\partial^H(k) \mapsto 2p_l$ and $\partial^H(-k) \mapsto 2$. Since r_1r_2 is not divisible by p_l, it follows that $[r_1, r_2]$ is equal to $[1, 1]$ or $\partial^H(-k)$. In the former case r_1r_2 is not divisible by 2 and in the latter case it is divisible by 2.

Now we will determine what the representative of $[r_1, r_2]$ is in $\partial^H(J_k(\mathbb{Q}_{p_{l'}})/\phi(A_k(\mathbb{Q}_{p_{l'}})))$. Similar to above, applying the mapping $[r_1, r_2] \mapsto r_1r_2$ to $\partial^H(e_k)$ we see that $\partial^H(0) \mapsto p_{l'}$, $\partial^H(k) \mapsto 2p_{l'}$ and $\partial^H(-k) \mapsto 2$. So $[r_1, r_2]$ is equal to $[1, 1]$ or $\partial^H(0)$ if r_1r_2 is not divisible by 2 and it is equal to $\partial^H(k)$ or $\partial^H(-k)$ otherwise. In both cases there exists a representative for $[r_1, r_2]$ such that r_1r_2 is divisible by $p_{l'}$. Thus we conclude that r_1 and r_2 are not necessarily divisible by $p_{l'}$ to the same power if $D = D_0 + D_1$.

The case $D = D_1 + D_2$:
Let $D = D_1 + D_2$. In $\partial^H(J_k(\mathbb{Q}_{p_l})/\phi(A_k(\mathbb{Q}_{p_l})))$ we now have that $\partial^H(0) = [-p_l, p_l]$, $\partial^H(k) = [2, 2p_l]$ and $\partial^H(-k) = [-2p_l, 2]$. Under the mapping $[r_1, r_2] \mapsto r_1r_2$ it follows that $\partial^H(0) \mapsto -1$, $\partial^H(k) \mapsto p_l$ and $\partial^H(-k) \mapsto -p_l$. Since r_1r_2 is not divisible by p_l, it follows that $[r_1, r_2]$ is equal to $[1, 1]$ or $\partial^H(0)$. In the former case r_1r_2 is not divisible by -1 and in the latter case it is divisible by -1.

Now we will determine what the representative of $[r_1, r_2]$ is in $\partial^H(J_k(\mathbb{Q}_{p_{l'}})/\phi(A_k(\mathbb{Q}_{p_{l'}})))$. Similar to above, applying the mapping $[r_1, r_2] \mapsto r_1r_2$ to $\partial^H(e_k)$ we see that $\partial^H(0) \mapsto -1$, $\partial^H(k) \mapsto p_{l'}$ and $\partial^H(-k) \mapsto -p_{l'}$. So $[r_1, r_2]$ is equal to $(1, 1)$ or $\partial^H(k)$ if r_1r_2 is not divisible by -1 and it is equal to $\partial^H(0)$ or $\partial^H(-k)$ otherwise. In both cases there exists a representative for $[r_1, r_2]$ such that r_1r_2 is divisible by $p_{l'}$. Thus we conclude that r_1 and r_2 are not necessarily divisible by $p_{l'}$ to the same power if $D = D_1 + D_2$.

The case $D = D_0 + D_2$:
Let $D = D_0 + D_2$. In $\partial^H(J_k(\mathbb{Q}_{p_l})/\phi(A_k(\mathbb{Q}_{p_l})))$ we now have that $\partial^H(0) = [-1, p_l]$, $\partial^H(k) = [p_l, 2p_l]$ and $\partial^H(-k) = [-p_l, 2]$. Under the mapping $[r_1, r_2] \mapsto r_1r_2$ it follows that $\partial^H(0) \mapsto -p_l$, $\partial^H(k) \mapsto 2$ and $\partial^H(-k) \mapsto -2p_l$. Since r_1r_2 is not divisible by p_l, it follows that $[r_1, r_2]$ is equal to $(1, 1)$ or $\partial^H(k)$. In the former case r_1r_2 is not divisible by 2 and in the latter case it is divisible by 2. Note that in both cases r_1r_2 is not divisible by -1.

Now we will determine what the representative of $[r_1, r_2]$ is in $\partial^H(J_k(\mathbb{Q}_{p_{l'}})/\phi(A_k(\mathbb{Q}_{p_{l'}})))$. Similar to above, applying the mapping $[r_1, r_2] \mapsto r_1r_2$ to $\partial^H(e_k)$ we see that $\partial^H(0) \mapsto -p_{l'}$, $\partial^H(k) \mapsto 2$ and $\partial^H(-k) \mapsto -2p_{l'}$. Since r_1r_2 is not divisible by -1 it follows that $[r_1, r_2]$ is equal to $(1, 1)$ if r_1r_2 is divisible by 2 or $\partial^H(k)$ otherwise. In both cases r_1r_2 is not divisible by $p_{l'}$. So we can conclude that r_1 and r_2 are divisible by $p_{l'}$ to the same power if $D = D_0 + D_2$.

Since this holds for all choices of l' different from l it follows that r_1r_2 is not of the form $q = \prod_{i \in I} p_i$ where $I \subset \{1, \dots, m\}$ is a non-empty proper subset. Since $\partial^H(J_k(\mathbb{Q})/\phi(A_k(\mathbb{Q})))$ maps surjectively onto the group $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})))$, it follows that elements of the form q do not lie in $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})))$. So the proposition holds for $D = D_0 + D_2$.

□

In the proof of Proposition 8.6 we see that we need a different choice of D to acquire the results of Proposition 5.2. Furthermore, we have the two different elements 2 and -1 in Proposition 8.6 that can serve the role of the prime 3 in Proposition 5.2. For $D = D_0 + D_1$ and $D = D_1 + D_2$ it is not possible to find the desired results. In the former case we see that we only need 2 to act as a global prime, while in the latter case we only need the element -1 to act as a global prime. In the case where $D = D_0 + D_2$ it is important that -1 is not a square modulo p_i, but 2 being a square does not impact our results. There is a certain asymmetry in the way the elements of $\partial^H(J_k)$ are represented in $\mathbb{Q}_{p_i}^*/\mathbb{Q}_{p_i}^{*2} \times \mathbb{Q}_{p_i}^*/\mathbb{Q}_{p_i}^{*2}$ in this case that allows us to get our results.

We can now prove the analogue of Corollary 5.3 and we will see that the proof is simpler now that we are working in a characteristic 2 setting.

Corollary 8.7. *Let E_k be the same as in Proposition 8.6. Then $\#\text{Ш}(B_k)[p] \geq 2^{m-1}$.*

Proof. From Proposition 3.10 we have the exact sequence

$$0 \to J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})) \to \mathrm{Sel}(B_k) \to \text{Ш}(B_k)[\psi] \to 0. \tag{209}$$

The products of the form $\prod_{i\in I} p_i$ as described in Proposition 5.2 lie in $\mathrm{Sel}(B_k)$, but these products do not lie in the subgroup $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})))$ of $\mathrm{Sel}(B_k)$. From the exact sequence it follows that these products do not lie in the kernel of $\text{Ш}(B_k)[\psi]$ and are non-trivial elements of $\text{Ш}(B_k/\mathbb{Q})[\psi]$. In particular, we can look at the single primes p_i and look at the intersection of $\partial^D(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})))$ with the subgroup of $\mathrm{Sel}(B_k)$ generated by $\{p_1, \dots, p_m\}$. This subgroup contains at most the element $p_1 \dots p_m = k$ and thus has a dimension of at most 1 as an $\mathbb{F}_2$-vector space.

By looking at the exact sequence we can see that the image of $\langle p_1, \dots, p_m\rangle$ in $\text{Ш}(B_k)[\psi]$, denoted by $\overline{\langle p_1, \dots, p_m\rangle}$, has dimension at least $m-1$. We have that $\deg(\psi) = 2$, since $\deg(\psi) = \deg(\widehat{\psi}) = \#\ker(\widehat{\psi}) = \#\langle D\rangle$, so $\text{Ш}(B_k)[\psi] \subset \text{Ш}(B_k)[2]$. We can conclude that $\#\text{Ш}(B_k)[2] = 2^{\dim_{\mathbb{F}_2}(\text{Ш}(B_k)[2])} \geq 2^{\dim_{\mathbb{F}_2}(\overline{\langle p_1,\dots,p_m\rangle})} \geq 2^{m-1}$. □

This corollary implies that the Tate-Shafarevich group can be arbitrarily large depending on the number of primes in the product k. Unfortunately, it is impossible to find more than 1 prime satisfying the conditions of Proposition 8.6. By the law of quadratic reciprocity we have for primes p and q that $(p/q)(q/p) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. Since the conditions of Proposition 8.6 imply that $p, q \equiv 3 \pmod 4$, we have that $\frac{p-1}{2}\cdot\frac{q-1}{2} = \frac{2+4m}{2}\cdot\frac{2+4n}{2} = 1 + 2(m+n+2mn)$ for some integers $m, n \in \mathbb{Z}$. Because this number is odd it follows that $(p/q)(q/p) = -1$, so if we would assume that $k = p_1p_2$ then only one of $(p_1/p_2) = 1$ or $(p_2/p_1) = 1$ can satisfy the conditions of Proposition 8.6.

8.2 A proof of Proposition 10

The paper of Lemmermeyer and Mollin concludes with the following proposition:

Proposition 8.8. *[13, Proposition 10] Let $k = p_1 \dots p_m$ be a product of primes $p_i \equiv 5 \pmod 8$ such that $(p_i/p_j) = +1$ whenever $i \neq j$. Then $\#\text{Ш}(\widehat{E}/\mathbb{Q}) \geq 2^{m-1}$ if m is odd and $\#\text{Ш}(\widehat{E}/\mathbb{Q}) \geq 2^{m-2}$ if m is even.*

The paper does not give a proof for this statement, so we will provide one here for completeness. To prove this proposition we have the following exact sequence

$$0 \to W(\widehat{E}/\mathbb{Q}) \to S^{(\psi)}(\widehat{E}/\mathbb{Q}) \to \text{Ш}(\widehat{E}/\mathbb{Q})[\psi] \to 0. \tag{210}$$

Here ψ is the dual isogeny of the 2-isogeny $\phi : E \to \widehat{E}$ associated with a rational point of order 2. In the sequence $W(\widehat{E}/\mathbb{Q})$ is the Weil-Chatelet group of $\widehat{E}$, $S^{(\psi)}(\widehat{E}/\mathbb{Q})$ is the Selmer group associated to ψ and $\text{Ш}(\widehat{E}/\mathbb{Q})[\psi]$ the Tate-Shafarevich group of ψ.

Additionally, we require a theorem and lemma from the paper. The proofs of these statements can be found the paper. We need the following lemma:

Lemma 8.9. *[13, Lemma 3.] Let $k = p_1 \dots p_m$ be a product of distinct odd primes p_i and write $k = b_1 c_1$ for some squarefree $b_1 > 0$. Then $b_1 \in Sel^{(\psi)}(\widehat{E}/\mathbb{Q})$ if and only if the following conditions are satisfied:*

1. $(c_1/p) = 1$ *or* $(-c_1/p) = 1$ *for all primes* $p \mid b_1$.
2. $(b_1/p) = 1$ *or* $(-b_1/p) = 1$ *for all primes* $p \mid c_1$.
3. $b_1 \equiv \pm 1 \pmod 8$ *or* $c_1 \equiv \pm 1 \pmod 8$.

And we need the theorem:

Theorem 8.10. *[13, Theorem 7.] Assume that $k = p_1 \dots p_m$ is a product of distinct odd primes $p_i \equiv \pm 3 \pmod 8$ such that $(p_i/p_j) = 1$ whenever $i \neq j$. Additionally, assume that there is at most one index i such that $p_i \equiv +3 \pmod 8$. Then $W(\widehat{E}/\mathbb{Q}) = \langle -1, k \rangle$.*

We can now proceed to the proof of the proposition.

Proof of Proposition 10: We can approximate $\#Ш(\widehat{E}/\mathbb{Q})$ using the sequence (210). From this we find that $\#Ш(\widehat{E}/\mathbb{Q})[\psi] = \#S^{(\psi)}(\widehat{E}/\mathbb{Q})/\#W(\widehat{E}/\mathbb{Q})$. So we will need to determine the sizes of $S^{(\psi)}(\widehat{E}/\mathbb{Q})$ and $W(\widehat{E}/\mathbb{Q})$, and use the inclusion $\#Ш(\widehat{E}/\mathbb{Q}) \supseteq Ш(\widehat{E}/\mathbb{Q})[\psi]$ to get the desired approximation.

Let $k = p_1 \dots p_m$ be a product of primes with $p_i \equiv 5 \equiv -3 \pmod 8$ such that $(p_i/p_j) = +1$ whenever $i \neq j$. In particular, this means that none of them are equivalent to $3 \pmod 8$. So we can apply Theorem 8.10 and find that $W(\widehat{E}/\mathbb{Q}) = \langle -1, k \rangle$.

To determine the size of the Selmer group we use Lemma 8.9. By the construction of k we automatically satisfy conditions 1. and 2. from the lemma for any choice of non-zero c_1. An even product of p_i's is congruent to $1 \pmod 8$, so either b_1 or c_1 must be a product of such distinct pairs to satisfy condition 3..

In the case that m is odd this means that b_1 is equal to a sole prime p_i or a product of the form p_i with pairs of the form $p_j p_k$ where i, j and k are distinct integers. Thus we have that $\langle p_i \mid 1 \leq i \leq m \rangle \subseteq S^{(\psi)}(\widehat{E}/\mathbb{Q})$. Since $-1 \in W(\widehat{E}/\mathbb{Q})$ we can further conclude that $\langle -1, p_i \mid 1 \leq i \leq m \rangle \subseteq S^{(\psi)}(\widehat{E}/\mathbb{Q})$. Note that this subset contains all of the squarefree divisor that satisfy the conditions of Lemma 8.9, so we can conclude that it is equal to the Selmer group. Thus we get that $\#Ш(\widehat{E}/\mathbb{Q}) \geq \#Ш(\widehat{E}/\mathbb{Q})[\psi] = \#S^{(\psi)}(\widehat{E}/\mathbb{Q})/\#W(\widehat{E}/\mathbb{Q}) = 2^{m+1}/2^2 = 2^{m-1}$.

The case where m is even follows in a similar way except here b_1 is a product of pairs $p_i p_j$ where i and j are distinct integers. From this it follows that $S^{(\psi)}(\widehat{E}/\mathbb{Q}) = \langle -1, p_i p_j \mid 1 \leq i < j \leq m \rangle$, so $\#S^{(\psi)}(\widehat{E}/\mathbb{Q}) = 2^m$ and we conclude that $\#Ш(\widehat{E}/\mathbb{Q}) \geq 2^{m-2}$. □

What is particular about this case is that the lower bound of the Tate-Shafarevich group depends on the number of primes in the product k, since the exponent depends on whether m is even or odd. This distinction is not there when we are working with μ_2-covers or in the other case mentioned in the paper of Lemmermeyer and Mollin [13, Corollary 8].

9 Conclusion

In this thesis we showed that we can generalize the results of the paper of Flynn and Shnidman to μ_n-covers where n is a product of distinct primes $p_1 \ldots p_t$. In this setting it is possible to decompose the μ_n-cover $(\mathcal{L}, \eta)$ uniquely into μ_{p_i}-covers $(\mathcal{L}_{p_i}, \eta_{p_i})$. We could not fully translate the results of Flynn and Shnidman. In particular, for Lemma 7.9 we find the result $J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q))) = n^2 \cdot \prod_{i=1}^{t} c_q(J)/c_q(A_{p_i})$ and we find an extra factor $\prod_{i=1}^{t} c_q(J)/c_q(A_{p_i})$ which we do not have in the case of $n = p$. Further research into the Tamagawa numbers of the μ_{p_i}-covers of μ_n-covers could shed more light on this situation.

We also applied the theory of μ_p-covers to the work of Lemmermeyer and Mollin and it showed that the theory is also applicable to elliptic curves. We saw that we got similar results to Lemmermeyer and Mollin with regards to the size of the Tate-Shafarevich group of the elliptic curve defined by $y^2 = x(x^2 - k^2)$ and we also have arbitrarily large 2-torsion for this curve. However, this number depends on the number of primes in $k = p_1 \ldots p_m$ and due to the conditions that we put on our primes and the global prime -1, the only possibility is when k is equal to a single prime. This method using μ_2-covers can be an alternative approach to computing the size of the Tate-Shafarevich group of elliptic curves as opposed to conventional methods like using p-descent for a prime p, but you need to be careful with choosing proper global primes.

References

[1] A. Arsiea and A. Vistoli, *Stacks of cyclic covers of projective spaces*, Compos. Math, **140**, (2004), 647-666.

[2] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, in *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, Thompson, Washington, D.C., (1967), 94-115.

[3] J.W.S. Cassels, Arithmetic on curves of genus 1, VI, *The Tate-Shafarevich group can be arbitrarily large*, J. Reine Angew. Math. **214/215**, (1964), 65-70.

[4] E.V. Flynn, *Arbitrarily large 2-torsion in Tate-Shafarevich groups of abelian varieties*, Acta Arith, **191**, (2019), 101-114.

[5] E.V. Flynn and A. Shnidman, *Arbitrarily large p-torsion in Tate-Shafarevich groups*, arXiv e-prints 2209.08088 (2022).

[6] M. Fried and M. Jarden, *Field arithmetic*, Revised by Moshe Jarden 3rd revised ed. 11., (2008), 10.1007/978-3-540-77270-5.

[7] R. Hartshorne,*Algebraic Geometry*, Springer-Verlag, New York, (1977).

[8] F. Hazama, *Hodge cycles on the jacobian variety of the Catalan curve*, Compositio Mathematica, **107(3)**, (1997), 339-353.

[9] T. Jedrezak, *On the torsion of the Jacobians of superelliptic curves $y^q = x^p + a$*, Journal of Number Theory, **145**, (2014), 402-425.

[10] S. Lang, *Abelian Varieties*, Springer New York, (1983).

[11] S. Lang, *Algebra*, Springer New York, (2002).

[12] S. Lang and J. Tate, *Principal Homogeneous Spaces Over Abelian Varieties*, American Journal of Mathematics 80, no. 3 (1958): 659–84. https://doi.org/10.2307/2372778.

[13] F. Lemmermeyer and R. Mollin, *On Tate-Shafarevich groups of $y^2 = x(x^2 - k^2)$*, Acta Mathematica Universitatis Comenianae. New Series, (2003).

[14] D.W. Masser, *Specialization of endomorphism rings of abelian varieties*, Bulletin de la Société Mathématique de France, **124**, (1996), 457-476.

[15] J.S. Milne, *Abelian Varieties (v. 2.00)*, (2008), Available at `www.jmilne.org/math/`.

[16] D. Mumford, *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, 5, Published for the Tata Institute of Fundamental Research, Bombay by Oxford University Press, London, (1970).

[17] Jürgen Neukirch, *Algebraic Number Theory*, Translated by Norbert Schappacher, Springer-Verlag, Berlin Heidelberg New York, (1999).

[18] P. Stevenhagen and H.W. Lenstra, Jr., *Chebotarëv and his Density Theorem*, The Mathematical Intelligencer, 18.2, (1996), 26–37.

[19] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Translated by Rachel Rowen, Pure and Applied Mathematics, 139, Academic Press, (1994).

[20] F. Poma, M. Talpo and F. Tonini, *Stacks of uniform cyclic covers of curves and their Picard groups*, Journal: Algebraic Geometry, (2015), ISSN: 2214-2584.

[21] E. F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Mathematische Annalen, 310, (1998), 447-471.

[22] E.S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Mathematica, 85, (1951), 203-362.

[23] A. Shnidman, *Quadratic Twists of Abelian Varieties With Real Multiplication*, International Mathematics Research Notices, Volume 2021, Issue 5, 2021, 3267–3298.

[24] L. C. J. Smith, *The Kontsevich Space of Rational Curves on Cyclic Covers of* $\mathbb{P}^n$, Stony Brook University, (2014).

[25] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106, Springer Verlag, (2009).

[26] C. Towse, *Weierstrass points on cyclic covers of the projective line*, Trans. Amer. Math. Soc. 348, (1996), 3355-3378.

[27] A. Weil, *Adèles and algebraic groups*, Institute for Advanced Study, Princeton, (1961).