rijksuniversiteit
groningen

On the p-rank of the class group of quadratic number fields

Masteronderzoek Wiskunde

Augustus 2014

Student: P.A. Helminck

Eerste Begeleider: Prof. dr. J. Top

Tweede Begeleider: Dr. A.E. Sterk

ON THE P-RANK OF THE CLASS GROUP OF QUADRATIC NUMBER FIELDS

PAUL HELMINCK

Abstract. The main goal of this thesis is to obtain quadratic number fields such that the p-rank of the class group is high. This is done by geometric means, more specifically: elliptic curves with p-torsion will be used. To obtain a high p-rank, we will use Jacobians that decompose into at least two elliptic curves, each of which having an isogeny of degree p to it. Several constructions of such Jacobians are given. Also, the influence of the rank of an elliptic curve on the p-rank of the class group will be shown.

Contents

1. Introduction

In this thesis we will be interested in the class group of quadratic number fields. One of the first to actively study class groups was Kummer, who was examining obstructions in a possible proof for Fermat's Last Theorem. It has ever since become an important part of number theory. We will try to find a way of tackling certain issues regarding the class group by using geometry. To do this, we will use *class field theory*.

The foundations of class field theory were laid in the beginning of the 20th century. It yielded a strong connection between more general class groups and abelian extensions of number fields. Using this theory it becomes fairly simple to put geometry in the picture: any point on a geometric object has coordinates, and one can add those coordinates to a base field to obtain extensions.

For our purposes though, it is necessary to have some extra structure on our geometric objects. In this thesis we take elliptic curves and add coordinates of points on those curves to our base field. One of the many advantages of working with elliptic curves is that the extensions made are almost everywhere unramified. This makes it easier to make extensions that are *everywhere unramified*. By class field theory, these unramified extensions yield subgroups of the class group.

We would like to have more than one extension on an elliptic curve though. This would gives us possibly two or more extensions, which corresponds to two or more subgroups of the class group. This is what will gives us a high p-rank. To obtain multiple extensions,

we will find Jacobians of curves that split into many elliptic curves with certain isogenies. This will most likely yield a nontrivial image in the following map

$$J(C)(K) \longrightarrow E_1'/\phi(E_1(K)) \times E_2'/\psi(E_2(K))$$

where the groups on the right hand side classify all extensions made with coordinates in K. In this thesis we will give many methods of finding such Jacobians. Most of these are constructions by Mestre. We have also included some generalizations. A quick summary:

(1) Section 4 contains the general construction of extensions for abelian varieties, plus a connection to the rank.
(2) Section 6 contains a proof on the impossibility of certain isogeny graphs on abelian varieties.
(3) Section 7 contains geometric information about certain fibre products of elliptic curves.
(4) Section 8 contains Mestre's "automorphism" method, which is generalized in that section.
(5) Section 9 contains more about fibre products of elliptic curves, where in this case there is more emphasis on fibering the isogeny pair.
(6) Section 10 contains some explicit examples of obtaining extensions.

2. Preliminaries

In this section we will give a short (but not self-contained) introduction to the concepts used in this thesis. This includes: abelian varieties, class field theory and Galois cohomology. Appropriate references will be given when needed.

2.1. **Abelian varieties.** Here we will quickly discuss abelian varieties and some useful theorems concerning them. More explicitly, we will study criteria for Jacobians of curves to *split* and we will obtain some results on the torsion of an abelian variety. Most of the material will be done in scheme-theoretic language, but one can think of the projective version given in [1]. A good reference for abelian varieties is [4]. Throughout this section, we will work over a field of characteristic 0. We will denote a field by the letters k, K or L. Also, for a given field k the notation $\bar{k}$ will denote an algebraic closure. All of the fields in this thesis will be of characteristic 0 unless mentioned otherwise.

2.1.1. *Definitions.* We will first define a group variety. Let V be an algebraic variety, i.e. a geometrically integral separated scheme of finite type over a field k[1].

Definition 2.1. A **group variety** is a variety V with morphisms

$$\begin{aligned} m: \quad & V \times V \longrightarrow V \\ inv: \quad & V \longrightarrow V \end{aligned}$$

and an element $e \in V(k)$ such that $V(\bar{k})$ becomes a group with m, inv and e.

Remark 2.1. Note that the group operation is not necessarily abelian. One can find many non-abelian group varieties, an example of which being $\mathrm{GL}_n(k)$.

We shall however mostly be concerned with so-called **abelian varieties**, which we define now.

Definition 2.2. An abelian variety is a complete group variety.

The way we defined them, abelian varieties do not automatically have a commutative group law. Luckily however, we have the following lemma

Lemma 1. *The group law on an abelian variety is commutative.*

Proof. The proof follows by using the so-called *Rigidity lemma*. The details are in [4]. □

Now that we have our definition for abelian varieties, we can give an important example.

Example 2.1. Every elliptic curve over k is an abelian variety. In fact, they are the only abelian varieties of dimension 1.

Let A and B be abelian varieties. We now come to the concept that allows us to create number fields with high p-rank: **isogenies**. By definition, an isogeny is a surjective homomorphism $A \longrightarrow B$ with finite kernel. We have the following theorem:

[1]Note that geometrically integral implies that the variety is also geometrically reduced and irreducible. In other words, the variety stays irreducible over any algebraic closure and its structure sheaf has no nilpotents.

Theorem 2.1. *For any homomorphism $\phi : A \longrightarrow B$, the following are equivalent:*

(1) *ϕ is an isogeny*
(2) *$dim(A) = dim(B)$ and ϕ is surjective*
(3) *$dim(A) = dim(B)$ and $Ker(\phi)$ is finite.*
(4) *ϕ is finite, flat and surjective.*

Proof. See [4] for the proof. □

2.1.2. *Torsion and Isogenies on Abelian Varieties.* In the theory of elliptic curves, one of the most important tools that was used, was the **dual isogeny**. For any isogeny ϕ, one was able to create a dual isogeny $\hat{\phi}$ with the property that $\phi \circ \hat{\phi} = [\deg \phi]$ (multiplication by $\deg \phi$ on E). There is a similar theory for abelian varieties, which we quickly present right now.
Most of the theory relies on the following lemma:

Lemma 2. *Let $[n] : A \longrightarrow A$ be the multiplication by n map on A. Then $[n]$ is a finite map of degree n^{2g}, where g is the dimension of A. That is, the corresponding map on function fields $k(A) \longrightarrow k(A)$ is of degree n^{2g}.*

Proof. See [4] for the details. □

Definition 2.3. Let A be an abelian variety. For any $n \geq 1$, we define

$$A[n](\bar{k}) = \{P \in A(\bar{k}) : [n]P = e\}$$

Corollary 2.1. $A[n](\bar{k}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$

Proof. This follows by the structure theorem for f.g. abelian groups and the fact that $\#(A[m]) = m^{2g}$ for any m dividing n. □

Now suppose that we have an isogeny $\phi : A \longrightarrow A'$. By definition, the kernel is finite. So let that order be n. Then we have $\ker(\phi) \subseteq \ker[n]$. Identifying A' with $A/\ker(\phi)$, we have a second map $\hat{\phi}$, the **dual isogeny**, that is just the quotient map $A/\ker(\phi) \longrightarrow (A/\ker(\phi))/(\ker[n]/\ker(\phi)) \simeq A/\ker[n]$. By definition, this map $\hat{\phi}$ has the property $\hat{\phi} \circ \phi = [n] = \phi \circ \hat{\phi}$.

2.2. **Jacobians.** Here we introduce the concept of a Jacobian of a curve C over any field of characteristic 0. By definition, a curve is a smooth 1-dimensional variety. For elliptic curves, one could obtain a canonical bijection between the points on the elliptic curve E and the **divisor class group** $\mathrm{Pic}^0(E)$. This automatically made E a group variety. On the other hand, it gave the abstract group $\mathrm{Pic}^0(E)$ the structure of a variety. One could try to give $\mathrm{Pic}^0(C)$ the structure of a variety for any curve C. The result is the **Jacobian** of C.

2.2.1. *Definition.* Consider the functor $P_C : (Var) \longrightarrow (Sets)$ defined by

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

where q is the projection map $C \times T \longrightarrow T$. We have the following theorem

Theorem 2.2. *If $C(k) \neq \emptyset$ then P_C is representable.*

Proof. See [4] for a proof. □

Definition 2.4. The object that represents the functor P_C is the **Jacobian** of C. It will be denoted by $J(C)$.

Using the universal property, one can show that the Jacobian is in fact a group variety. We refer to [2] or [4] for the details. There is one property of this Jacobian that we would like to put extra emphasis on:

Lemma 3. *There exists an isomorphism $H^1(C, \mathcal{O}_C) \longrightarrow T_e(J(C))$. Here $T_e(J(C))$ is the tangent space of the Jacobian of C at the identity element.*

Proof. See [2] or [4]. □

Remark 2.2. Recall also that Serre Duality gives an isomorphism $H^1(C, \mathcal{O}_C) \longrightarrow H^0(C, \omega_C)$, the last space being the space of holomorphic differentials. In particular, we have that the tangent space of $J(C)$ at e has dimension g (the genus of C). Thus we also have that the dimension of the Jacobian variety is g (since any abelian variety is smooth).

Lemma 4. *There is an isomorphism $H^0(J(C), \Omega) \longrightarrow H^0(C, \Omega)$.*

Proof. See [4] □

We will use these lemmas and the additional remarks to split certain Jacobian varieties. We will introduce this concept now.

2.2.2. *Simple Abelian varieties.* Suppose that we have an isogeny ϕ between abelian varieties A and B. As noted before, this also implies that we have an isogeny $\hat{\phi} : B \longrightarrow A$. Thus, we actually have an equivalence relation. We shall denote it by $A \sim B$.

Definition 2.5. An abelian variety A is **simple** if there does not exist an abelian variety $B \subset A$ other than $B = (0)$ or $B = A$.

We have an important theorem similar to Maschke's theorem in representation theory.

Theorem 2.3. *(Poincaré Reducibility) For every abelian variety A there exist simple abelian varieties A_i such that there is an isogeny*

$$A_1 \times A_2 \times ... \times A_n \longrightarrow A$$

Proof. A proof can be found in [4]. □

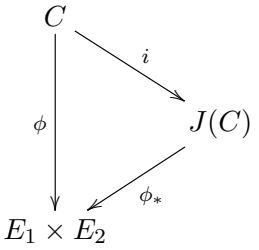
Thus we have that the simple abelian varieties are in fact the "building blocks" of abelian varieties. Our goal will be to find C such that its Jacobian contains "many" copies of an elliptic curve in the above sense. To find these, we need some way to detect whether a Jacobian splits. The scenario we will usually find ourselves in is as follows. We usually have a curve C and two (or more) maps $\phi_i : C \longrightarrow E_i$. Here C is a curve of genus g and the E_i are elliptic curves (over k). We have the following useful criterion:

Lemma 5. *Let C be a curve of a field k with a point P defined over k. Let E_i be a finite collection of elliptic curves (indexed by $I = \{1, 2, ..., n\}$, say) with invariant differentials ω_i. Suppose that we have maps $\phi_i : C \longrightarrow E_i$ such that the pullbacks $\phi_i^*(\omega_i)$ are independent over k (in the finite dimensional vector space $H^0(C, \Omega)$). Then there is an isogeny $(\prod E_i) \times B \longrightarrow J(C)$ for some abelian variety B.*

Proof. We will give the proof for *two* elliptic curves, the full proof is completely analogous. So suppose that we have two maps $\phi_1 : C \longrightarrow E_1$ and $\phi_2 : C \longrightarrow E_2$. We can combine them to create a map $\phi = (\phi_1, \phi_2) : C \longrightarrow E_1 \times E_2$. This induces a map

$$H^0(E_1, \Omega_1) \times H^0(E_2, \Omega_2) \longrightarrow H^0(C, \Omega_C)$$

(pull back of differentials) which is injective by assumption.
We also have a canonical morphism $i : C \longrightarrow J(C)$ which maps a point Q to the divisor class of $(Q) - (P)$, also denoted by $[Q - P]$. From the Jacobian, we have a map induced by ϕ (which is known as ϕ_* in [1]) which sends a point $[Q - P]$ to the divisor class $([\phi_1(Q) - \phi_1(P)], [\phi_2(Q) - \phi_2(P)])$. Naturally identifying E_i with $\mathrm{Pic}^0(E_i)$ (using the map $Q \longmapsto$ (divisor class of $(Q) - (\phi(P))$)), we have that the following diagram commutes



But this means that the image of the pull back of the differentials on $E_1 \times E_2$ to $J(C)$ must be two-dimensional. Thus we have an induced two-dimensional subspace of $H^0(J(C), \Omega_J)$. Dualizing, we have that $T_P(J(C)) \twoheadrightarrow T_{\phi_1(P)}(E_1) \times T_{\phi_2(P)}(E_2)$. Thus the image of $J(C)$ under the map ϕ_* is two-dimensional (since the image on tangent spaces is two-dimensional and everything is smooth). We can thus view $E_1 \times E_2$ as a two-dimensional subvariety of $J(C)$ using the map $\hat{\phi}_*$ (up to isogeny of course). Using the Poincaré lemma, the result follows. □

2.3. **Galois Cohomology.** In this section we shall quickly introduce infinite Galois groups and Galois cohomology groups. We will also give some background on inertia groups, since they make it somewhat easier to state "this extension is unramified at $\mathfrak{p}$" etc. As a side note, we won't be needing the full infinite version of the Galois correspondence because

all of the extensions we will encounter are in fact finite. Nevertheless, it is a convenient language, so we will use it here.

2.3.1. *Infinite Galois Theory.* Let K be a perfect field. Let $\bar{K}$ be the algebraic closure of K. One can give $\bar{K}$ the discrete topology and then consider the product topology on $Y := \bar{K}^{\bar{K}}$ (cartesian product of $\bar{K}$ over the index set $\bar{K}$). The space Y can naturally be identified with $\mathrm{Hom}(\bar{K}, \bar{K})$. The subspace we want to consider is $\mathrm{Aut}_K(\bar{K})$, the space of field automorphisms fixing K. With the corresponding subspace topology (also known as the **Krull topology**), we have that this group is in fact a topological group.
As in the finite case, we have a so-called **Galois Correspondence**. The theorem is as follows:

Theorem 2.4. *Let $\mathcal{D} = \{L : K \subset L \subset \bar{K},\ L$ a field$\}$ and let $\mathcal{C}$ be the collection of compact subgroups of $Aut_K(\bar{K})$. There is an inclusion-reversing bijection*

$$\begin{aligned} \psi : \quad & \mathcal{D} \longrightarrow \mathcal{C} \\ & L \longmapsto Aut_L(\bar{K}) \end{aligned}$$

where the inverse is given by $\phi(G) = \bar{K}^G$, the field of invariants under G. The field extensions $K \subset L$ that are finite correspond to subgroups of finite index.

One can find a proof in [10]. For a field L such that $K \subset L \subset \bar{K}$, we shall denote the corresponding compact subgroup by G_L. Thus we also adopt the notation G_K for $\mathrm{Aut}_K(\bar{K})$.

2.3.2. *Decomposition and Inertia groups.* We will now specialize to K a number field. At first, we will construct decomposition groups and inertia groups only for finite primes, since this is the most transparent case (in terms of number theory). Afterwards we will also create them for infinite primes, since this is needed for class field theory. Note that the construction used for infinite primes could have been used for finite primes as well, but we chose to include both.
Consider the ring of integers $\mathcal{O}_{\bar{K}}$. Given a prime $\mathfrak{p}$ of K, choose any prime $\bar{\mathfrak{p}}$ lying above $\mathfrak{p}$, i.e.: $\mathfrak{p} \subset \bar{\mathfrak{p}}$. We can look at the **decomposition group**

$$D_{\bar{\mathfrak{p}}} = \{\sigma \in G_K : \sigma(\bar{\mathfrak{p}}) = \bar{\mathfrak{p}}\}$$

For a different extension of $\mathfrak{p}$ to $\mathcal{O}_{\bar{K}}$, we obtain a conjugated subgroup. At any rate, we have that this subgroup of G_K naturally acts on the residue field $\mathcal{O}_{\bar{K}}/\bar{\mathfrak{p}} = \overline{\mathbb{F}}_p$. In fact, we have that the map

$$D_{\bar{\mathfrak{p}}} \longrightarrow \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$$

is in fact surjective. We define the kernel of this map to be the **inertia group** at $\mathfrak{p}$. We shall denote it by $I_{\mathfrak{p}}$. We have the following useful corollary

Corollary 2.2. Let $H = I_{\mathfrak{p}}$ for some prime $\mathfrak{p}$. Let L be any field such that $K \subset L \subset \bar{K}$. We have that $K \subset L$ is unramified at $\mathfrak{p}$ *if and only if* $L \subset \bar{K}^H$. That is, L is unramified at $\mathfrak{p}$ if and only if $I_{\mathfrak{p}}$ acts trivially on L.

For the infinite versions, we refer to [5] or [6].

2.3.3. *Galois Cohomology.* Let G_K be the absolute Galois group as in the previous sections. We can consider so-called G_K-modules: abelian groups M with a map

$$\begin{aligned} G_K \times M &\longrightarrow M \\ (\sigma, m) &\longmapsto m^\sigma \end{aligned}$$

that is continuous for the discrete topology on M and such that the following hold:

$$\begin{aligned} m^1 &= m \\ (m+n)^\sigma &= m^\sigma + n^\sigma \\ m^{\sigma\tau} &= (m^\sigma)^\tau \end{aligned}$$

The requirement that the action is continuous w.r.t. discrete topology on M implies (and is equivalent to) the fact that the *stabilizer*

$$\mathrm{Stab}(m) := \{\sigma \in G_K : m^\sigma = m\}$$

is an open subgroup. As it is also closed, we have that it is of finite index. Thus m "lives" in a finite extension of K, i.e. it is invariant under G_L for a finite extension $K \subset L$.

Caveat 2.1. Not every open subgroup of G_K is of finite index. One can find a good example in Milne's Field Theory. Thus the continuity condition is really needed.

Now suppose that we have two G_K-modules M, N. A morphism between these two is a homomorphism $\phi : M \longrightarrow N$ such that $\phi(m^\sigma) = \phi(m)^\sigma$. This relation implies for instance that

$$\mathrm{Stab}(m) \subseteq \mathrm{Stab}(\phi(m))$$

(which can be translated to the statement that under G_K-morphisms extensions become smaller).
The idea of Galois cohomology is as follows. One starts with an exact sequence of G_K-modules

$$0 \longrightarrow P \longrightarrow M \longrightarrow N \longrightarrow 0$$

In our case, we usually have points of an abelian variety over an algebraically closed field as modules. We are then interested in points that actually live in K for instance: they have to be invariant under G_K. Thus we are led to invariants, the zeroth cohomology groups:

$$H^0(G_K, M) := H^0(M) := \{m : m^\sigma = m \text{ for all } \sigma\}$$

This leads to the following exact sequence

$$0 \longrightarrow H^0(P) \longrightarrow H^0(M) \longrightarrow H^0(N)$$

where the last map is not necessarily surjective anymore. Cohomology makes the sequence exact by adding some extra groups. We will only need the first cohomology groups for our purposes.

Definition 2.6 (Cocycles, Coboundaries and H^1)**.** A 1-cocycle on M is a continuous map $\xi : G_K \longrightarrow M$ such that

$$\xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau)$$

A 1-coboundary is a continuous map $\xi : G_K \longrightarrow M$ of the form $\xi(\sigma) = m^\sigma - m$ for some $m \in M$. The group of all 1-cocycles is denoted by $Z^1(G_K, M)$. The group of all 1-coboundaries is denoted by $B^1(G_K, M)$. We have that $B^1(G_K, M) \subseteq Z^1(G_K, M)$. We define the **first cohomology group** as follows:

$$H^1(M) := H^1(G_K, M) := Z^1(G_K, M)/B^1(G_K, M)$$

These cohomology groups extend our exact sequence as follows

Corollary 2.3. For every exact sequence of G_K-modules

$$0 \longrightarrow P \longrightarrow M \longrightarrow N \longrightarrow 0$$

there is the following *long exact sequence* of G_K-modules

$$0 \longrightarrow H^0(P) \longrightarrow H^0(M) \longrightarrow H^0(N) \longrightarrow H^1(P) \longrightarrow H^1(M) \longrightarrow H^1(N)$$

Remark 2.3. One can in fact define higher cohomology groups to extend the current exact sequence. This will not be needed.

2.4. **Class Field Theory.** Here we will describe some basic facts about class field theory which are needed for the rest of the thesis. The idea is as follows: for a number field K, every abelian extension $L \supseteq K$ that is unramified at *every* place corresponds to an element of the class group C_K of $\mathcal{O}_K$. The more general correspondence is the main theorem of **Class Field Theory**. This classifies all abelian extensions of a number field K in terms of the "arithmetic" of K. We shall make this clear using the ring of *adèles* and group of *idèles*.

2.4.1. *Adèles and Idèles.* Let K be a number field. Let v be a valuation of K (in terms of [11]). Then we can complete K using the metric induced by v. This completion is denoted by K_v. The valuation naturally extends to this completion. For every non-archimedean valuation, we have that there is a valuation ring $A_v \subseteq K_v$ consisting of all elements having positive valuation. For infinite primes we define $A_v = K_v$.

Definition 2.7. The ring of **adèles**, $\mathbb{A}_K$ is the ring

$$\mathbb{A}_K := \prod_v{}' K_v = \{(x_v)_v \in \prod_v K_v : x_v \in A_v \text{ for all but finitely many } v\}$$

also known as a **restricted product** of the K_v with respect to the subrings A_v.

We give this ring the following topology: the open sets are generated by sets of the form

$$\prod_{v \in S} O_v \times \prod_{v \notin S} A_v$$

where S is a finite set of valuations and O_v is an open set of K_v.
Defining a similar product with respect to K_v^* and A_v^* (the group of units) gives us the **idèles**.

Definition 2.8. The **idèle** group is the group

$$J_K = \prod_v{}' K_v = \{(x_v)_v \in \prod_v K_v^* : x_v \in A_v^* \text{ for almost all } v\}$$

We give this group the topology generated by the sets:

$$\prod_{v\in S} O_v \times \prod_{v\notin S} A_v^*$$

where S is again a finite set of valuations and O_v is open in K_v^* (with respect to the induced topology).

Caveat 2.2. The topology on the idèles is not the same as the induced topology of J_K in $\mathbb{A}_K$! See [5] for an example.

We now come to the concept which will give us our class field correspondence. We can naturally embed K^* in J_K by canonically embedding an element in every completion.

Definition 2.9. The **idèle class group**, C_K is the group J_K/K^*.

In other words: idèles modulo principal idèles.

2.4.2. *Open subgroups of J_K.* Here we would like to state some results about open subgroups of J_K, which are needed to formulate class field theory. We will first introduce cycles.

Definition 2.10. A **cycle** is a formal product $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ where the products runs over all primes of K (also the infinite ones) such that

(1) $n(\mathfrak{p})$ is a non-negative integer for all $\mathfrak{p}$ and $n(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$.
(2) $n(\mathfrak{p}) \in \{0, 1\}$ if $\mathfrak{p}$ is real and $n(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is complex.

Definition 2.11. Let $\mathfrak{p}$ be a prime of K. An element $x \in K^*$ is said to be multiplicatively congruent to 1 modulo $\mathfrak{p}^n$, (notation $x \equiv 1 \mod \mathfrak{p}^n$) if one of the following is satisfied:

(1) $n = 0$
(2) $\mathfrak{p}$ is real, and x is positive under the embedding $\mathfrak{p} : K^* \longrightarrow \mathbb{R}^*$.
(3) $\mathfrak{p}$ is finite, and $x \in 1 + \mathfrak{p}^n \subset A_{\mathfrak{p}}$.

For any cycle $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$, we write $x \equiv 1 \mod \mathfrak{f}$ if $x \equiv 1 \mod \mathfrak{p}^{n(\mathfrak{p})}$ for all $\mathfrak{p}$.

We will now create open subgroups of the idèle group. For any finite prime $\mathfrak{p}$, we have a basis of $1 \in {K_{\mathfrak{p}}}^*$, consisting of

$$U_{\mathfrak{p}}^n = 1 + \mathfrak{p}^n$$

for $n \geq 1$ and $U_{\mathfrak{p}^0} = A_{\mathfrak{p}}^*$. For $\mathfrak{p}$ real, we have that

$$U_{\mathfrak{p}}^{(0)} = K_{\mathfrak{p}}^* \text{ and } U_{\mathfrak{p}}^{(1)} = K_{\mathfrak{p},>0}$$

(the positive part of $\mathbb{R}^*$). For $\mathfrak{p}$ complex, we only have $U_p^{(0)} = K_{\mathfrak{p}}^*$.
For every cycle $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$, we have a subgroup of J_K defined as follows

$$W_{\mathfrak{p}} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{n(\mathfrak{p})} \subset J_K$$

Proposition 2.1. A subgroup of the idèle group J is open if and only if it contains $W_{\mathfrak{f}}$ for some cycle $\mathfrak{f}$.

Corollary 2.4. A subgroup N of the idèle class group C_K is open if and only if it contains the homomorphic image D_f of some subgroup $W_f \subseteq J_K$.

This classifies open subgroups by local properties. Its usefulness will become apparent in the next section.

Lemma 6. *Taking $f = (1)$, we have that $C_K/D_{(1)} \simeq Cl_K$, the original class group of K.*

Proof. See [11] for a proof. □

Thus the original class group is expressed as a quotient of the idèle class group, which will be useful in the correspondence in the next section.

2.4.3. *Class Field Correspondence.* Using the language of adèles and idèles, we can give the following version of the main theorem of class field theory:

Theorem 2.5 (**Main Theorem of Class Field Theory**). *Let K be a number field. Let Σ_K be the set of finite abelian extensions contained in some fixed algebraic closure, and $\mathcal{D}$ the set of open subgroups of the idèle class group C of K. Then there exists an inclusion reversing bijection*

$$\Sigma_K \rightleftarrows \mathcal{D}$$

such that for an extension L/K corresponding to the subgroup D of C the following holds

1. $D = N_{L/K}C_L$
2. *There is a global Artin isomorphism $\psi_{L/K} : C/D \simeq Gal(L/K)$ such that the image of the completion $K^*_{\mathfrak{p}}$ in C is mapped onto the decomposition group $D_{\mathfrak{p}}$ of $\mathfrak{p}$ in $Gal(L/K)$.*
3. *For an open subgroup of the form $D_{\mathfrak{f}}$, we have that the corresponding extension is unramified outside $\mathfrak{f}$.*
4. *This correspondence is functorial (see [Stevenhagen]).*

Definition 2.12. Let H be the extension corresponding to the open subgroup defined by the cycle $f = (1)$. H is called the **Hilbert class field** of K. It is the maximal unramified abelian extension.

Corollary 2.5. $\mathrm{Gal}(H/K) \simeq Cl_K$

Proof. Follows from identifying Cl_K with $C/D_{(1)}$ and the Main Theorem. □

The fact that the correspondence is functorial also gives us the following. If we have any unramified abelian extension $L \supseteq K$, then it corresponds to a subgroup of the class group of K. Furthermore, two different extension give two different subgroups of the class group. Thus instead of looking for subgroups (or elements) of the class group directly, we will make extensions that are everywhere unramified.

3. Moduli problems

In this section we will discuss certain moduli problems related to torsion points on an elliptic curve. To be exact, we will give families of elliptic curves that have a certain torsion subgroup. These families will be used in the subsequent sections. Also, some background on $X_1(N)$ and $Y_1(N)$ is given to motivate our later choices for N. Most of the details concerning proofs etc. will be skipped since they are ubiquitous in the literature on the subject. The appropriate references will be given as needed.

3.1. **Background on $Y_1(N)$ and $X_1(N)$ for various N.** Consider the following functor (or moduli problem) $F : (\mathrm{Sch}/\mathbb{Z}[1/N]) \longrightarrow (\mathrm{Sets})$ given by:

$$F(S) = \{(E, P) : E/S \text{ an elliptic curve, } P \in E(S) \text{ of order } N \text{ in all geom. fibers}\}/\sim$$

where two pairs (E, P) and (E', P') are equivalent if there exists an isomorphism $\phi : E \longrightarrow E'$ (over S) such that $\phi(P) = \phi(P')$. We have the following theorem concerning this functor:

Theorem 3.1. *Let $N \geq 4$. The functor F is representable: there is an object $Y \in (Sch/\mathbb{Z}[1/N])$ and a natural isomorphism $F \longrightarrow Hom(-, Y)$.*

See [3] for a proof. The representing scheme shall be denoted by $Y_1(N)/\mathbb{Z}[1/N]$ or $Y_1(N)$. Our interest lies in $Y_1(N)(\mathrm{Spec}(K))$ (or: $Y_1(N)(K)$) for various fields $K \supseteq \mathbb{Q}$. These sets are in a one-to-one correspondence with elliptic curves over K having a point P (defined over K) of order N. One can also view these points of $Y_1(N)(K))$ as isogenies $E \longrightarrow E'$ over K of degree N with kernel generated by a rational element $P \in E(K)$. This is the viewpoint that we will use most of the time.

Remark 3.1. One of the cases which shall be of most interest to us is $N = 3$. For $N \geq 2$, we only have a so-called *coarse moduli space*. We won't explain this term here. For us it is sufficient to know that we can find plenty of elliptic curves with 3 torsion over $\mathbb{Q}$.

At some point we want to specify a certain N. But not all N are suitable: it might happen that $Y_1(N)(\mathbb{Q})$ is empty or finite for instance. We can use geometric methods to study this problem. The varieties where one can take advantage of these methods the most are the **proper** ones. However, $Y_1(N)$ turns out to be non-proper. One can *compactify* $Y_1(N)$ to obtain $X_1(N)$. This is a scheme over $\mathbb{Z}[1/N]$ which represents a similar functor as before on the category of *generalized elliptic curves*. We will not need this viewpoint. One can also view $X_1(N)$ as $Y_1(N)$ with some extra added **cusps**. This viewpoint is most evident in the complex case: one takes the upper half complex plane $\mathcal{H}$ with some added points at infinity, the cusps, and then one takes a quotient under the natural group action of $\mathrm{SL}_2(\mathbb{Z})$.

At any rate, for these compactified curves $X_1(N)$ we can look at the generic fiber. This is a variety over $\mathbb{Q}$. We have a classification of such proper curves based on the genus. As an example, $X_1(N)$ has genus 0 for $N = 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$. Since all these curves have a rational point on them, we have infinitely many points. Thus there are infinitely

many curves having a point of order $2, 3, 4, 5, 6, 7, 8, 9, 10$ or 12. This motivates our choice below for certain N.

3.2. **Explicit families.** Instead of actually giving $Y_1(N)(K)$, we will find a variety V such that $V(K) \twoheadrightarrow Y_1(N)(K)$ for every field $K \supseteq \mathbb{Q}$. In other words: we will parametrize the elliptic curves having a point of order N, not worrying about possibly "hitting" a particular elliptic curve twice. The following families were given in [6], but we shall reproduce them here.
In the table below the E_p will indicate a family of elliptic curves (given that the discriminant is nonzero) with an element $P = (0, 0)$ of order p. The curve is given by a Weierstrass equation (as per usual). Also, E'_p will indicate the quotient curve $E_p/ < P >$. To be clear: any choice of parameters such that the corresponding discriminant is nonzero will give an elliptic curve E_p and a point $P = (0, 0)$ of order p.

Elliptic Curve	Weierstrass Equation
E_3	$y^2 + wxy + vy = x^3$
E'_3	$y^2 + wxy + vy = x^3 - 5wvx - v(w^3 + 7v)$
E_5	$y^2 + (d+1)xy + dy = x^3 + dx^2$
E'_5	$y^2 + (d+1)xy + dy = x^3 + dx^2 + f_5(d)x + g_5(d)$
E_7	$y^2 + (1+d-d^2)xy + (d^2-d^3)y = x^3 + (d^2-d^3)x^2$
E'_7	$y^2 + (1+d-d^2)xy + (d^2-d^3)y = x^3 + (d^2-d^3)x^2 + f_7(d)x + g_7(d)$

The polynomials alluded to in the table are as follows:

$f_5(d)$	$5d(d^2 - 2d - 1)$
$g_5(d)$	$d(d^4 - 10d^3 - 5d^2 - 15d - 1)$
$f_7(d)$	$-5d(d-1)(d^2 - d + 1)(d^3 + 2d^2 - 5d + 1)$
$g_7(d)$	$-d(d-1)(d^9 + 9d^8 - 37d^7 + 70d^6 - 132d^5 + 211d^4 - 182d^3 + 76d^2 - 18d + 1)$

3.3. **Elliptic Curves with $\mathbb{Z}/6\mathbb{Z}$-torsion.** The previous tables were explained in [6]. For lack of reference, we would like to expand slightly on these tables by adding a family of curves with **6-torsion**. The idea is exactly the same, but we will put it as a theorem here:

Theorem 3.2. *Every elliptic curve E/K with a point P of order 6 defined over K can be put in the following form*

$$y^2 + wxy + vy = x^3 + vx^2$$

where $v = -w^2 + 3w - 2$ and $P = (0, 0)$. Conversely, every value of w such that the discriminant is nonzero gives an elliptic curve with a point of order 6: $P = (0, 0)$.

Proof. We will follow [6]. Given such a P, one can translate P to $(0, 0)$. Assuming that P is not of order 2 or 3 this yields the following equation (see [6]):

$$y^2 + wxy + vy = x^3 + vx^2$$

We now calculate $[3]P = (1-w, w-v-1)$. We also have that $[-3]P = (1-w, -(w-v-1)-w(1-w)-v) = (1-w, w^2-2w+1)$. In order for P to have order 6, it is necessary and sufficient that $[3]P = [-3]P$. We obtain

$$\begin{aligned} w-v-1 &= w^2-2w+1 \\ \iff v &= -w^2+3w-2 \end{aligned}$$

as desired. Also, a computation reveals that any such curve with $v = -w^2+3w-2$ and nonzero discriminant has $P = (0,0)$ of order 6 (with order 2,3 excluded as explained in [6]). This yields the desired conclusion. □

Lemma 7. *Let E be as above. Then $Q = (-v, 0)$ has order 3. The quotient curve $E/ <Q>$ satisfies the following equation:*

$$y^2 + wxy + vy = x^3 + vx^2 + f_1(w)x + f_2(w)$$

where $f_1 = -40 + 130w - 155w^2 + 80w^3 - 15w^4$ and $f_2 = -76 + 368w - 739w^2 + 787w^3 - 468w^4 + 147w^5 - 19w^6$.

Proof. This is a routine check using a computer algebra package. Alternatively one can use Vélu's formulas. □

3.4. **Elliptic Curves with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ torsion.** In this section we will expand upon the 6-torsion curves by adding an additional 2-torsion point. The result is as follows:

Theorem 3.3. *Every elliptic curve with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ torsion can be brought in the following form:*

$$y^2 + wxy + vy = x^3 + vx^2$$

where $v = -w^2+3w-2$ and $w = (10/9 - 2t^2)/(1-t^2)$.

Proof. We first start with a model for elliptic curves with $\mathbb{Z}/6\mathbb{Z}$ torsion

$$E : y^2 + wxy + vy = x^3 + vx^2$$

We can transform this to

$$y^2 = (x + 9w^2 - 12)(h(x))$$

where

$$h(x) = x^2 + (-9w^2+12)x - 162w^4 + 1296w^3 - 3456w^2 + 3888w - 1584.$$

Its discriminant is given by

$$\Delta(h) = (729)(w-2)^3(w-10/9)$$

E will have an additional 2-torsion point, if and only if this discriminant is a square (because this means that $h(x)$ has a rational zero). Equating $\Delta(h) = z^2$, we set

$$z' = z/(3^3(w-2))$$

and obtain

$$z'^2 = (w-2)(w-10/9)$$

This is a conic with a nonsingular rational point on it. Thus we can parametrize it. The result is (with $z = t(w-2)$):

$$w = \frac{10/9 - 2t^2}{1 - t^2}$$

which can easily be checked. □

3.5. **Elliptic Curves with $\mathbb{Z}/10\mathbb{Z}$-torsion.** The same result for 10-torsion is stated in [12]. We shall repeat the statement here:

Theorem 3.4. *Every elliptic curve E over K with a point P of order 10 is isomorphic to an elliptic curve defined by*

$$y^2 = (x^2 - u(u^2+u-1))(8xu^2 + (u^2+1)(u^4 - 2u^3 - 6u^2 + 2u + 1))$$

Furthermore, take $Q = [2]P$. The quotient curve $E/ < Q >$ then has the equation

$$y^2 = (x^2 - u(u^2+u-1))h_u(x)$$

where $h_u(x) = 8(u^2+u-1)^2x + (u^2+1)(u^4 + 22u^3 - 6u^2 - 22u + 1)$.

3.6. **Short Weierstrass form for certain curves.** Most of the curves that we obtained were of the form

$$y^2 + wxy + vy = x^3 + vx^2 + f_1(w)x + f_2(w)$$

For the upcoming sections we will need the short Weierstrass form of these equations. We will state them here for convenience in the following Lemma:

Lemma 8. *Let E be an elliptic curve in the above form. Then one can transform it to an elliptic curve of the form:*

$$y^2 = x^3 + \rho_1 x + \rho_2$$

where

$$\begin{aligned}
\rho_1 &= (-1/48)w^4 - (1/6)vw^2 - (1/3)v^2 + (1/2)vw + f_1 \\
\rho_2 &= (1/864)w^6 + (1/72)vw^4 + (1/18)v^2w^2 - (1/24)vw^3 + (2/27)v^3 \\
&\quad -(1/6)v^2w - (1/12)f_1w^2 - (1/3)f_1v + (1/4)v^2 + f_2
\end{aligned}$$

The transformation linking the first one to the second one is given by:

$$(x, y) \longmapsto (x + (v + w^2/4)/3, y + wx/2 + v/2)$$

Proof. One can obtain this form by completing the square twice and then removing the x^2 term, as is done in [1]. We leave the details to the reader. □

4. Abelian extensions of number fields using abelian varieties

In this section, we would like to discuss a method of creating abelian extensions of a number field k using abelian varieties over that field (or the ring of integers in that field or a completion of the ring of integers with respect to a certain absolute value) and torsion subgroups in those abelian varieties. This will be done in the language of Galois cohomology. The action of the various inertia groups will then relate the extensions made in the above manner to global class field theory.

4.1. **Preliminaries.** Let A be an abelian variety over k. Let K denote a field extension of k (contained in $\bar{k}$). For any scheme S over k we can consider the group:

$$A(S) := Hom_{(Sch,k)}(S, A) \tag{1}$$

The case of most interest to us is $S = \text{Spec}(\bar{k})$ or $S = \text{Spec}(K)$.We shall use an easier notation for $A(\text{Spec}(K))$, namely: $A(K)$. At any rate, we have that $A(K)$ is the group of K-valued points.
Let us now consider $A(\bar{k})$. The group $A(\bar{k})$ is equipped with a natural G_k-action, i.e. a continuous map

$$G_k \times A(\bar{k}) \longrightarrow A(\bar{k}) \tag{2}$$

where G_k has the Krull topology and we give $A(\bar{k})$ the discrete topology. This turns the abelian variety into a G_k-module.

4.2. **Abelian varieties with K-torsion.** Suppose now that $A(\bar{k})$ has a K- point P. This means that the stabilizer of P

$$\text{Stab}(P) := \{\sigma \in G_k : \sigma(P) = P\}$$

is equal to G_K for some finite extension K of k. This latter group is the closed (and open) subgroup of $G_{\bar{k}}$ corresponding to the field K under the infinite Galois correspondence. This group G_K acts trivially on P by definition.
Suppose now that this point P is actually a torsion point. This means that there is an integer $m > 0$ such that $m \cdot P = \mathcal{O}$, where $\mathcal{O}$ is the identity element of the abelian variety A. There is also a corresponding quotient variety $A' := A/ < P >$ (defined over K) and a morphism $\phi : A \longrightarrow A'$ defined over K. We can consider the following short exact sequence (over $\bar{k}$!) arising from this torsion point P:

$$0 \longrightarrow < P > \longrightarrow A(\bar{k}) \longrightarrow A(\bar{k})/ < P > \longrightarrow 0$$

Taking G_K cohomology yields the following long exact sequence of G_K-modules:

$$0 \longrightarrow < P > \longrightarrow A(K) \longrightarrow A'(K) \longrightarrow H^1(G_K, < P >) \longrightarrow H^1(G_K, A(\bar{k})) \longrightarrow H^1(G_K, A'(\bar{k}))$$

Since $< P >$ is naturally isomorphic to $\mathbb{Z}/m\mathbb{Z}$ as a G_K module, we replace the corresponding terms and by the connecting homomorphism, we obtain an injection:

$$\delta : A'(K)/\phi(A(K)) \hookrightarrow H^1(G_K, \mathbb{Z}/m\mathbb{Z})$$

In other words: for every point Q in $A'(K)$ we get an abelian extension $K \subseteq L$ with $\text{Gal}(L|K) = \mathbb{Z}/m\mathbb{Z}$ or a quotient of $\mathbb{Z}/m\mathbb{Z}$. Indeed, for every continuous homomorphism

$\rho : G_K \longrightarrow \mathbb{Z}/m\mathbb{Z}$ we have that the kernel is a closed subgroup of finite index, thus belonging to a field extension $K \subseteq L$ with Galois group $\mathrm{Im}(\rho)$ according to the Galois correspondence.
Thus field extensions are created in the Galois cohomology group. Let us run through the definition of the connecting homomorphism again and see where the field extension comes from. The homomorphism is created as follows: one takes a point $P \in A'(K)$. Now take any point $Q \in \bar{K}$ such that $\phi(Q) = P$. One can create the following element of the cohomology group $H^1(G_K, \mathbb{Z}/m\mathbb{Z})$ using this point:

$$\sigma \longrightarrow Q^\sigma - Q$$

where the exponential notation is for the action of G_k on $A(\bar{k})$. The kernel of this map is

$$\{\sigma : Q^\sigma = Q\} = G_K$$

so we see where our field extensions come from. As a side note, we also have that every abelian extension of K with Galois group $\mathbb{Z}/m\mathbb{Z}$ (or a quotient thereof) is obtained by an element of $H^1(G_K, \mathbb{Z}/m\mathbb{Z})$. Thus our field extensions coming from abelian varieties are nicely put into one framework.

4.3. **Local considerations.** Given an element ρ of $H^1(G_K, \mathbb{Z}/m\mathbb{Z})$, we can restrict it to subgroups of G_K. For instance, for every absolute value v of the number field K we have an inertia group I_v. Restricting our homomorphism to this subgroup we get a homomorphism:

$$I_v \to \mathbb{Z}/m\mathbb{Z}$$

which is in $H^1(I_v, \mathbb{Z}/m\mathbb{Z})$. Embedding the maximal unramfied extension above v into $\bar{K}$, we obtain a map

$$H^1(G_K, \mathbb{Z}/m\mathbb{Z}) \to H^1(I_v, \mathbb{Z}/m\mathbb{Z})$$

The kernel consists of the cohomology classes that are unramified above v. That is to say, the extensions corresponding to elements of the kernel are unramified above v.

For simplicity I will now assume that m is a prime number. I will denote it by p. The group $H^1(G_K, \mathbb{Z}/p\mathbb{Z})$ naturally has the structure of an $\mathbb{F}_p$-vector space. This makes $A'(K)/\phi(A(K))$ a subspace. This subspace is finite by a version of the Weak Mordell-Weil theorem. Of course, this also means that $A'(K)/\phi(A(K))$ has finite dimension as an $\mathbb{F}_p$ vector space.
Given this extra structure, we look at the subspace that is unramified everywhere.That is, consider the following map

$$f : H_1(G_K, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \prod H^1(I_v, \mathbb{Z}/p\mathbb{Z})$$

where v runs over all places of K and the I_v are the inertia subgroups. The kernel H of this map is equal to the **unramified cohomology classes**. It is again an $\mathbb{F}_p$-subspace of $H_1(G_K, \mathbb{F}_p)$. Let h_p be the p-rank of the class group of K. We now combine all of our previous results into one theorem which will guide us throughout the rest of the thesis.

Theorem 4.1. *The* **dimension** *of the subspace of* **unramified cohomology classes** *is equal to the p-rank of the class group of K.*

Proof. This follows from class field theory, which will be discussed in the next section. □

Corollary 4.1. Let H be the subspace of unramified cohomology classes. Let $V := H \bigcap (A'(K)/\phi(A(K)))$. Then

$$h_p \geq \dim(V)$$

The goal of this thesis will be to make $\dim(V)$ as large as possible. This yields a large p-rank by the previous corollary.

4.4. **Bounds and a connection to the rank.** In the last section we saw that the subspace $V := H \bigcap (A'(K)/\phi(A(K)))$ is of most interest to us. We will now give a lower bound on the dimension of this group in terms of the local parts. This is similar to the computation done in [8].
Let K be a number field. Let K_v be the completion of K at a valuation v. Let L_v be the maximal unramified abelian extension. As before, one can consider the groups $A'(K_v)/\phi(A(K_v))$ and $A'(L_v)/\phi(A(L_v))$. They are (finite) $\mathbb{F}_p$-vector spaces, so it makes sense to talk about their dimensions. If a class $Q \mod \phi(A(K))$ lands in either of them, then the corresponding extension will be unramified. The lower bound will be given by considering the image of $A'(K)/\phi(A(K))$ in $A'(K_v)/\phi(A(K_v))$ and then pulling it back.

Theorem 4.2. *For every v, let*

$$\delta_v = \min\{\dim(A'(K_v)/\phi(A(K_v)), \dim(A'(L_v)/\phi(A(L_v)))\}$$

Let $\delta = \sum_v \delta_v$. *Then the subgroup* $V = H \bigcap (A'(K)/\phi(A(K)))$ *is of codimension at most* δ. *In other words,* $\dim(V) \geq \dim(A'(K)/\phi(A(K))) - \delta$.

Proof. We will prove the theorem first for two places v_1 and v_2. The general proof follows in the same way.
Consider the following exact sequence for any place v:

$$0 \longrightarrow \ker(r_v) \longrightarrow A'(K)/\phi(A(K)) \xrightarrow{r_v} A'(K_v)/\phi(A(K_v))$$

where r_v is the natural map induced by the embedding of $A'(K)$ into $A'(K_v)$. Since these are all finite dimensional vector spaces, we can find a section for the last map. We can thus write

$$A'(K)/\phi(A(K)) = \mathrm{Im}(r_v) \bigoplus \mathrm{Ker}(r_v)$$

We will identify $\mathrm{Im}(r_v)$ with a vector subspace of $A'(K)/\phi(A(K))$. Consider the vector subspace

$$W = \mathrm{Im}(r_{v_1}) + \mathrm{Im}(r_{v_2})$$

We have

$$V = W + \ker(r_{v_1}) \cap \ker(r_{v_2})$$

Thus we have

$$\dim(V) \leq \dim(W) + \dim(\ker(r_{v_1}) \cap \ker(r_{v_2}))$$

and similarly

$$\dim(V) \leq \dim(A'(K_{v_1})/\phi(A(K_{v_1}))) + \dim(A'(K_{v_1})/\phi(A(K_{v_1}))) + \dim(\ker(r_{v_1}) \cap \ker(r_{v_2}))$$

which gives

$$\dim(V) \leq \delta + \dim(\ker(r_{v_1}) \cap \ker(r_{v_2}))$$

as desired. □

The rank of $A'(K)$ is connected to $\dim(A'(K)/\phi(A(K)))$ as follows.

Lemma 9. *Suppose that $A'(K)$ has no torsion over K. Then*

$$\textit{rank}(A'(K)) = \dim(A'(K)/\phi(A(K)))$$

At any rate, we have that $\operatorname{rank}(A'(K)) \leq \dim(A'(K)/\phi(A(K)))$. Combining this and our previous theorem, we obtain

Corollary 4.2. Suppose that $A'(K)$ has no torsion over K. Then

$$h_p \geq \dim(H \bigcap (A'(K)/\phi(A(K)))) \geq \operatorname{rank}\ A'(K) - \delta$$

5. Local ramification

In this section we will discuss ramification in our extensions. The fact that we are using elliptic curves naturally means that our extensions are unramified almost everywhere. That is to say, at the places of good reduction we have that there is no ramification. The same holds for the infinite primes. We can also bypass the places of bad reduction v that do not lie above the degree, p, of the isogeny. To make the extension unramified above p, one has to work with the explicit isogeny equation. This will be done later on.

5.1. **Places of good reduction.** Let us recall the setup. We had an isogeny

$$E \longrightarrow E'$$

of degree p over K. Suppose that E has good reduction at a prime v (this automatically implies that E' also has good reduction at v). We will reproduce the calculation in [Silverman, p333].

Theorem 5.1. *Let ξ be a cocycle in $E'(K)/\phi(E(K))$. Then ξ is unramified at v.*

Proof. Let $Q \in E'(K)$ and $\sigma \in I_v$. Take any P such that $\phi(P) = Q$. Consider the point $R := P^\sigma - P$ for any σ. Then the reduction is $\tilde{R} = \tilde{P^\sigma} - \tilde{P} = \mathcal{O}$ (because the inertia group acts trivially on $\mathbb{F}_q$). So R is in the kernel of the reduction map. But R is also in the kernel of ϕ. Since the kernel of ϕ injects into $\tilde{E}(\mathbb{F}_q)$, we have that $R = 0$, or $P^\sigma = P$. Thus P is invariant under the inertia group I_v and thus the extension $K(P) \supseteq K$ is unramified at v (which is equivalent to the cocycle being unramified). □

5.2. **Places of bad reduction.** At the places of bad reduction we will show that if we take our point in $E_0(K)$, then it will still be unramified. More explicitly, we will show the following

Theorem 5.2. *Let K_v be the completion of K at v. Let L_v be the maximal unramified extension. Then*

$$E'_0(L_v)/\phi(E_0(L_v)) = (0)$$

Proof. We will follow [8],[1] and [6]. There is an exact sequence ([1], formal groups])

$$0 \longrightarrow E_1(L_v) \longrightarrow E_0(L_v) \longrightarrow \tilde{E}(\bar{\mathbb{F}}_q) \longrightarrow 0$$

E' of course also has this exact sequence:

$$0 \longrightarrow E'_1(L_v) \longrightarrow E'_0(L_v) \longrightarrow \tilde{E'}(\bar{\mathbb{F}}_q) \longrightarrow 0$$

We would like to construct a map between the two of these. To do that, we need some lemmas to ensure that the proposed maps are indeed well-defined.

Lemma 10. *Let ϕ denote the restricted morphism $E_1(L_v) \longrightarrow E'(L_v)$. Then the image of ϕ is in $E'_1(L_v)$. If v does not divide p, then the co-kernel is in fact zero:*

$$E_1(L_v) \simeq E'_1(L_v)$$

Proof. See [6]. □

Lemma 11. $\phi(\tilde{E}_{ns}(\bar{\mathbb{F}}_q)) \subseteq \tilde{E}'_{ns}(\bar{\mathbb{F}}_q)$

Proof. See [6]. □

Corollary 5.1. $\phi(E_0(L_v)) \subseteq E'_0(L_v)$

Putting the last three results together gives us the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(L_v) & \longrightarrow & E_0(L_v) & \longrightarrow & \tilde{E}(\bar{\mathbb{F}}_q) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E'_1(L_v) & \longrightarrow & E'_0(L_v) & \longrightarrow & \tilde{E}'(\bar{\mathbb{F}}_q) & \longrightarrow & 0 \end{array}$$

We can now use the **Snake Lemma** to obtain the following exact sequence

$$0 \longrightarrow E'_1(L_v)/\phi(E_1(L_v)) \longrightarrow E'_0(L_v)/\phi(E_0(L_v)) \longrightarrow \tilde{E}'(\bar{\mathbb{F}}_q)/\tilde{\phi}(\tilde{E}(\bar{\mathbb{F}}_q)) \longrightarrow 0$$

The first group is (0), so we only have to show that the last group is indeed (0). We will give a slight generalization of the argument in [8]. Let $\hat{\phi}$ be the dual isogeny. We thus have $\phi \circ \hat{\phi} = [p]$. In [8] it is shown that the map $\tilde{E}_{ns}(\bar{\mathbb{F}}_q) \longrightarrow \tilde{E}_{ns}(\bar{\mathbb{F}}_q)$ is surjective. Note that both $\tilde{\phi}$ and $\tilde{\hat{\phi}}$ are both morphisms of varieties (over an algebraically closed field). Thus they are either surjective or constant. If $\tilde{\phi}$ were constant, then the composed map would also be constant. This is a contradiction and thus $\tilde{\phi}$ is surjective. This gives the desired theorem. □

6. Isogeny Constructions

In this section we will study certain isogeny constructions, also known as *Isogeny graphs*. At first we will only consider elliptic curves, but later on we will generalize to principally polarized abelian varieties.

6.1. **Elliptic curves and multiple isogenies.** Let E, E', E'' be elliptic curves over a number field K. Our construction of quadratic number fields with high p-rank shows that it is desirable to have as many isogenies $\phi : E' \longrightarrow E$ to *one* elliptic curve. Here any point in the kernel of ϕ has to be G_K rational: every point in the kernel has to have coordinates in K. One may wonder whether it is possible to have *multiple* arrows to one elliptic curve. Thus we are looking for pairs of different isogenies (ϕ, ψ) that fit in the following diagram:

$$E' \longrightarrow E \longleftarrow E''$$

We will prove the following theorem:

Theorem 6.1. *Let K be a number field such there is no torsion of the form $(\mathbb{Z}/p\mathbb{Z})^2$. Then there are no diagrams of the form*

$$E' \longrightarrow E \longleftarrow E''$$

Proof. We will start with some easy preliminaries. To fix notation, let E, E', E'' and (ϕ, ψ) be as above. Let $\{P_1, P_2\}$ be a basis for $E'[p]$ such that $< P_1 >= \ker(\phi)$ and let $\{P_1', P_2'\}$ be a basis for $E''[p]$ such that $< P_1' >= \ker(\psi)$. Define $Q := \phi(P_2)$ and $Q' := \psi(P_2')$.

Lemma 12. *Let $H :=< Q >$ with the above notation. Then H is G_K-invariant.*

Proof. The lemma will be proven once we show that $< Q >= \ker(\hat{\phi})$. Indeed, the kernel of any isogeny defined over K is invariant because $\mathcal{O} = \sigma(\hat{\phi}(P)) = \hat{\phi}(\sigma(P))$.
Now recall that $Q := \phi(P_2)$. Since the identity $\hat{\phi} \circ \phi = [p]$ holds, we have that $\hat{\phi}(Q) = \hat{\phi}(\phi(P_2)) = [p](P_2) = \mathcal{O}$. Thus $< Q >\subseteq \ker(\hat{\phi})$. But since Q is non-trivial, we actually have an equality. Thus the lemma is proved. □

The above lemma also holds verbatim for Q' and ψ of course. We now prove the following

Lemma 13. $< Q >\neq< Q' >$

Proof. This will follow with the identification $< Q >= \ker(\hat{\phi})$ and $< Q' >= \ker(\hat{\psi})$. Let $D_1 = \ker(\hat{\phi})$ and $D_2 = \ker(\hat{\psi})$. Suppose that we have $D_1 = D_2$. Viewing D_1 as the automorphism group of $\bar{K}(E) \supseteq \hat{\phi}^*(\bar{K}(E'))$ and D_2 as the automorphism group of $\bar{K}(E) \supseteq \hat{\psi}^*(\bar{K}(E''))$, we have that

$$\hat{\psi}^*(K(E'')) = \hat{\phi}^*(K(E'))$$

(since they are the invariant fields of D_1 and D_2). Putting this back in variety language, we have an isomorphism

$$\lambda : E' \longrightarrow E''$$

such that $\hat{\phi}^*\lambda^* = \hat{\psi}^*$ or put differently:

$$\lambda \circ \hat{\phi} = \hat{\psi}$$

Thus these isogenies differ by an isomorphism $E' \longrightarrow E''$. If we identify E' with E'', then this just says that $\hat{\psi} = \hat{\phi}$. Applying the dual map, we have that $\psi = \phi$. But this is in contradiction with what we assumed, so we obtain $<Q> \neq <Q'>$. □

One more lemma will give us all we need to prove our theorem. Let $R = \hat{\phi}(Q')$. Note that $R \neq \mathcal{O}$.

Lemma 14. *R is a K-rational point on E'.*

Proof. We have that $R \in \ker(\phi)$. Indeed, $\phi(R) = \phi(\hat{\phi}(Q')) = [p](Q') = \mathcal{O}$. Since $\ker\phi =< P_1 >$, the lemma follows. □

We now finish the proof of our theorem. Instead of using $\hat{\phi}$ we will use the notation mod $< Q >$. Since R is rational we have that $\sigma(Q') \equiv Q' \mod < Q >$. Thus $\sigma(Q') = Q' + k_\sigma Q$. But note also that $< Q' >$ is invariant. Thus $k_\sigma = 0$. We have therefore proved that Q' is a K-rational torsion point. The same reasoning (but with ϕ replaced by ψ) gives us that Q is a K-rational point. Thus $E[p] = \mathbb{F}_p^2$. But this contradicts what we assumed, so the theorem follows. □

6.2. **Isogeny graphs for abelian varieties.** For abelian varieties, we have that $A[p] = (\mathbb{Z}/p\mathbb{Z})^{2g}$, where g is the dimension of A. As in the elliptic curve case, there is the notion of a dual isogeny, and we can reproduce most of the proofs given above. So let us assume that we again have a graph of the form

$$A' \xrightarrow{\phi} A \xleftarrow{\psi} A''$$

where the isogenies are again of degree p and the isogenies are distinct. Our result is as follows:

Theorem 6.2. *Let $L = K(A[p])$. Suppose that the p does not divide the order of the Galois group $Gal(L|K)$ and that there exists no torsion of the form $(\mathbb{Z}/p\mathbb{Z})^2$ in A over K. Then there are no diagrams of the above form.*

Proof. We will first fix some notation. Let $\{P_1, P_2, ..., P_{2g}\}$ be a basis of $A'[p]$ as before such that $< P_1 >= \ker(\phi)$. Similarly, let $\{Q_1, Q_2, ..., Q_{2g}\}$ be the counterpart for A'' and ψ. We now fix two important subspaces:

$$\begin{aligned} H_1 &= \phi(\mathrm{Span}\{P_2, ..., P_{2g}\}) \\ H_2 &= \psi(\mathrm{Span}\{Q_2, ..., Q_{2g}\}) \end{aligned}$$

As in the previous proof, we have that these two subspaces are invariant, since they are the kernels of the dual isogenies. Now let $W = H_1 \bigcap H_2$. Note that W is an invariant subspace.

Lemma 15. *$dim(W) = 2g - 2$*

Proof. We have that $H_1 + H_2 = A'[p]$. For if not, then the isogenies would have the same kernel and therefore would be the same. We can now use a little lemma from Linear Algebra (Inclusion/Exclusion) which is as follows:

Lemma 16. *For any two vector subspaces V_1 and V_2 of a vector space V, we have that*

$$dim(V_1 + V_2) = dim(V_1) + dim(V_2) - dim(V_1 \cap V_2)$$

Using the lemma, we obtain

$$\dim(W) = (2g-1) + (2g-1) - (2g) = 2g - 2$$

as desired. □

We can now return to our original proof. By using **Maschke's Theorem** (this is where the assumption on the Galois group is used!), we can decompose H_1 as $H_1 = W \bigoplus W'$, where W' is again invariant. W' is 1-dimensional, so we have that $W' =< R >$ for some R. Now let $R' = \hat{\psi}(R)$.

Lemma 17. *R' is K-rational.*

Proof. We have that $R' \in \ker(\psi)$. Since ψ is assumed to have rational kernel, the result follows. □

We thus have that $\sigma(R') = R' + h_{2,\sigma}$ where $h_{2,\sigma} \in H_2$. But note also that $< R' >$ is assumed to be invariant. So $h_{2,\sigma} = 0$. The same reasoning yields that H_2 contains a rational p-torsion point, which yield different subspaces by construction. The theorem follows. □

7. Fibre products of elliptic curves

In this section we will discuss the geometry of the curve C obtained when one takes the fibre product of a number of elliptic curves over a specific cover of $\mathbb{P}^1$. To be more precise, we will find the genus of such C and we will find out whether they are hyperelliptic or not.

7.1. **Fibre product of two elliptic curves with specific 2-torsion.** Certain results from other papers will be used in this section. First of all, let us set some notation. Suppose that we have two elliptic curves E_1 and E_2 given by the following two equations:

$$y_1^2 = f_1(x_1)$$
$$y_2^2 = f_2(x_2)$$

where f_1 and f_2 are polynomials in one variable of degree 3. The two affine equations define a two-dimensional variety $V \subseteq \mathbb{A}^4$. We shall however be concerned with the closure in $\mathbb{P}^4$, but it will be denoted by the same equations. Also, several blow-ups are needed to obtain a non-singular model, but since we are only interested in the birational equivalence class we will denote it by the same equations.
For both elliptic curves we have a natural map $E_i \longrightarrow \mathbb{P}^1$ given in the above affine chart by $(x_i, y_i) \longmapsto x_i$. Fibering over this morphism we get the curve $C := E_1 \times_{\mathbb{P}^1} E_2$. In down-to-earth terms, this just means that we take the above equations and identify the x-coordinates. Thus we have the equations:

$$y_1^2 = f_1(x)$$
$$y_2^2 = f_2(x)$$

The genus of the curve C is given by the following the Lemma (see [9]):

Lemma 18. *The genus of the curve C is given by*

$$Genus(C) = \lfloor \frac{9 - 2 \cdot deg(h)}{2} \rfloor$$

where $h(x) := gcd(f_1(x), f_2(x))$.

The four possibilities left by this Lemma are as follows:

- $\deg(h) = 0$ gives $g(C) = 4$
- $\deg(h) = 1$ gives $g(C) = 3$
- $\deg(h) = 2$ gives $g(C) = 2$

Since all curves of genus 2 are hyperelliptic, we will focus on the case $\deg(h) = 2$. For the case $\deg(h) = 1$ (and thus $g(C) = 3$) we have the following theorem however:

Theorem 7.1. *Let C be given as above by the two equations*

$$y_1^2 = (x - a) \cdot (f_1(x))$$
$$y_2^2 = (x - a) \cdot (f_2(x))$$

where $gcd(f_1(x), f_2(x)) = 1$, *and* $f_i(x) = x^2 + a_i x + b_i$ *for* $a_i, b_i \in k$ *and* $b_1 \neq b_2$. *Then the curve* C *is* **not hyperelliptic**. *That is: there is no degree 2 morphism* $\phi : C \longrightarrow \mathbb{P}^1$.

Proof. We can translate the curve such that it is of the form

$$y_1^2 = x(f_1(x))$$
$$y_2^2 = x(f_2(x))$$

We will assume that C is in the above form. We have the following three holomorphic differentials on C:

$$\frac{dx}{y_1}, \frac{dx}{y_2}, \frac{y_1}{y_2 f_1} \cdot dx$$

These can be calculated by pulling back divisors along the covers $C \longrightarrow E_i$ for instance. They give the canonical embedding

$$(x, y_1, y_2) \longrightarrow (\frac{y_1}{y_2}, \frac{x}{y_2})$$

This corresponds to the following map of function fields

$$k(\frac{y_1}{y_2}, \frac{x}{y_2}) \longrightarrow k(x, y_1, y_2) = k(\frac{x}{y_2}, \frac{y_1}{y_2}, y_2)$$

Note that we have an involution τ on C given by

$$\tau(x, y_1, y_2) = (x, -y_1, -y_2)$$

Taking invariants under this automorphism we have the diagram of function fields

$$\begin{array}{ccc} k(\frac{y_1}{y_2}, \frac{x}{y_2}) & \longrightarrow & k(\frac{x}{y_2}, \frac{y_1}{y_2}, y_2) \\ \uparrow & & \uparrow \\ k(\frac{y_1}{y_2}, \frac{f_2}{x}, \frac{f_1}{x}) & \longrightarrow & k(x, \frac{y_1}{y_2}) \end{array}$$

where the vertical maps have degree 2. The fields on the bottom are the invariants of the ones on the top under the involution τ. Now, if we show that

$$k(\frac{f_1}{x}, \frac{f_2}{x}) \neq k(\frac{f_i}{x})$$

then it follows that

$$k(x) = k(f_1/x, f_2/x)$$

(because the degree $[k(x) : k(f_1/x)] = 2$ is prime) and thus we have that $k(\frac{y_1}{y_2}, \frac{f_2}{x}, \frac{f_1}{x}) = k(x, \frac{y_1}{y_2})$. This also implies that

$$k(\frac{y_1}{y_2}, \frac{x}{y_2}) = k(\frac{x}{y_2}, \frac{y_1}{y_2}, y_2)$$

Thus the canonical map is an embedding and thus the curve is not hyperelliptic (see [2]).

Lemma 19. $k(\frac{f_1}{x}, \frac{f_2}{x}) \neq k(\frac{f_i}{x})$

Proof. Let σ_i be the automorphism of $\mathbb{P}^1$ defined by

$$x \longmapsto \frac{b_i}{x}.$$

It has order two and its fixed field is $k(f_i/x)$. Thus to show $k(\frac{f_1}{x}, \frac{f_2}{x}) \neq k(\frac{f_1}{x})$, it suffices to show that $\sigma_1(f_2/x) \neq f_2/x$. First, write $f_2/x = x + a_2 + b_2/x$. We now compute

$$\sigma_1(f_2/x) = b_1/x + a_2 + xb_2/b_1$$

Suppose that $\sigma_1(f_2/x) = f_2/x$. Then

$$0 = \sigma_1(f_2/x) - f_2/x = (b_1 - b_2)1/x + x(b_2/b_1 - 1)$$

This can only hold if $b_1 = b_2$, which is not true by assumption. Thus the lemma follows. □

As mentioned before, this lemma gives us the theorem.

Remark 7.1. We have two canonical maps to elliptic curves:

$$(x, y_1, y_2) \longmapsto (x, y_i)$$

which gives us two differentials

$$\frac{dx}{y_1}, \frac{dx}{y_2}$$

which are independent. Thus by section 2, lemma 5, we have that $J(C) \sim E_1 \times E_2 \times E_3$, where E_1 and E_2 are as above. The third factor has to be a curve of genus 1 by counting dimensions.

□

7.2. **Hyperelliptic involution for $C = E_1 \times E_2$.** Thus from now on we will only focus on curves given by

$$y_1^2 = (x - a_1) \cdot (f(x))$$
$$y_2^2 = (x - a_2) \cdot (f(x))$$

where $a_1 \neq a_2$. These curves have genus 2 and are thus hyperelliptic. The hyperelliptic cover can be obtained as follows. Consider the following equality in the function field of C:

$$(y_1/y_2)^2 = (x - a_1)/(x - a_2)$$

The righthand side can be viewed as a Möbius transformation on $\mathbb{P}^1$. Indeed, the corresponding matrix is

$$\begin{pmatrix} 1 & -a_1 \\ 1 & -a_2 \end{pmatrix}$$

which has determinant $a_1 - a_2$ which is assumed to be nonzero. Thus it is an invertible matrix.
Now consider the curve C' given by the equation:

$$(x - a_2)z^2 = x - a_1$$

Its function field is generated by z: using the inverse matrix of the Möbius transformation we can express x in terms of z^2. Thus the curve C has genus 0. Note also that we have a morphism $C \longrightarrow C'$ given locally by $(x, y_1, y_2) \longrightarrow (x, y_1/y_2)$. This morphism is of degree 2 and thus we have obtained our hyperelliptic cover.

7.3. **Hyperelliptic involution for $C = E_1 \times E_2 \times E_3$.** Instead of taking two elliptic curves, we can try to glue together three elliptic curves with prescribed two-torsion as above. That is, we take a curve C of the form

$$\begin{aligned} y_1^2 &= (x - a_1)(f(x)) \\ y_2^2 &= (x - a_2)(f(x)) \\ y_3^2 &= (x - a_3)(f(x)) \end{aligned}$$

where $f(x)$ has degree 2. Let us assume that all a_i are different. We will again produce a degree 2 map to $\mathbb{P}^1_k$.
We will work in the function field of C. Let

$$\begin{aligned} z &= \frac{y_1}{y_2} \\ w &= \frac{y_1}{y_3} \end{aligned}$$

We then have

$$\begin{aligned} z^2 &= \frac{x - a_1}{x - a_2} =: \sigma(x) \\ w^2 &= \frac{x - a_1}{x - a_3} =: \tau(x) \end{aligned}$$

Here σ and τ are again invertible Möbius transformations. Using the inverse of σ for instance, we can express x as a function of z^2:

$$x = \frac{a_2 z^2 - a_1}{z^2 - 1}$$

Plugging this into the equation for w^2, we get

$$(\frac{a_2 z^2 - a_1}{z^2 - 1} - a_3)w^2 = \frac{a_2 z^2 - a_1}{z^2 - 1} - a_1$$

Clearing the denominators, we obtain

$$((a_2 - a_3)z^2 + (a_3 - a_1))w^2 = (a_2 - a_1)z^2$$

Letting $w' = z/w$ (or equivalently: blowing up the singularity), we arrive at our desired quadratic form

$$(a_2 - a_3)z^2 + (a_3 - a_1) = (a_2 - a_1)(w')^2$$

Let V be the corresponding variety. Note that under our assumptions this is a nonsingular model. Also, we have a rational point $P := (1, 1)$ on V for all a_i. Thus V is isomorphic to $\mathbb{P}^1_k$. The end result is as follows:

Theorem 7.2. *The curve C has a degree 2 map to $\mathbb{P}^1_k$ for all a_i such that $\prod_{1\leq i<j\leq 3}(a_i - a_j) \neq 0$. The map is given (locally) by:*

$$(x, y_1, y_2, y_3) \longrightarrow \frac{y_3 - y_2}{y_1 - y_2}$$

Proof. Let $w' = t(z - 1) + 1$ or equivalently $t = \dfrac{w' - 1}{z - 1} = \dfrac{z - w}{w(z - 1)}$ where $w' = \dfrac{z}{w}$. Then t generates the function field of V. Recalling our definition of z and w in terms of the y_i and rewriting the above expression for t, we arrive at our map. □

Remark 7.2. For future reference, it will be convenient to express all our intermediate variables in terms t. The end result is:

$$\begin{aligned}
z &= \frac{t^2(a_1 - a_2) + 2t(a_2 - a_1) - (a_3 - a_2)}{a_1t^2 - a_2t^2 + a_2 - a_3} \\
w &= \frac{-a_1t^2 + a_2t^2 - 2a_2t + 2a_3t + a_2 - a_3}{a_1t^2 - a_2t^2 + a_2 - a_3} \\
x &= \frac{h_1}{h_2} \\
h_1 &= (a_1^2 - 2a_1a_2 + a_2^2)t^4 + (4a_1a_2 - 4a_2^2)t^3 + (-2a_1a_2 + 6a_2^2 - 2a_1a_3 - 2a_2a_3)t^2 \\
&\quad +(-4a_2^2 + 4a_2a_3)t + a_2^2 - 2a_2a_3 + a_3^2 \\
h_2 &= 4a_1t^3 - 4a_2t^3 - 4a_1t^2 + 8a_2t^2 - 4a_3t^2 - 4a_2t + 4a_3t
\end{aligned}$$

7.4. **Bi-elliptic involution for $C = \prod_{i=1}^4(E_i)$.** For four elliptic curves, the above method doesn't give a hyperelliptic involution, but a *bi-elliptic involution*. That is, there is a degree 2 map $\phi : C \longrightarrow E$ to some elliptic curve E. We will show this now.
As before, let C be the curve given by the equations

$$y_i^2 = (x - a_i)(f(x))$$

for $1 \leq i \leq 4$. As before, let

$$\begin{aligned}
z &= \frac{y_1}{y_2} \\
w &= \frac{y_1}{y_3} \\
v &= \frac{y_1}{y_4}
\end{aligned}$$

Similar to the previous case, we obtain

$$z^2 = \frac{x-a_1}{x-a_2} =: \sigma_2(x)$$
$$w^2 = \frac{x-a_1}{x-a_3} =: \sigma_3(x)$$
$$v^2 = \frac{x-a_1}{x-a_4} =: \sigma_4(x)$$

Last time we obtained *one* quadratic form, but this time we will obtain two quadratic forms. Since a nonsingular intersection of two quadratic forms has genus 1 (see [2]), the result follows.
As before, we can express x as a function of z^2:

$$x = \frac{a_2z^2 - a_1}{z^2 - 1}$$

Plugging this expression into the equation for w^2, we obtain

$$(\frac{a_2z^2 - a_1 - a_3(z^2-1)}{z^2-1})w^2 = \frac{(a_2-a_1)z^2}{z^2-1}$$

Cancelling the $z^2 - 1$ terms and replacing w by $w' = z/w$, we have the following equation

$$(a_2 - a_3)z^2 + (a_3 - a_2) = (a_2 - a_1)w'^2$$

Repeating the same procedure for v, we obtain another quadratic form

$$(a_2 - a_4)z^2 + (a_4 - a_2) = (a_2 - a_1)v'^2$$

Note that $z = 1, w' = 0, v' = 0$ give a rational point on the curve. Thus it is an elliptic curve.

7.5. **Involution for $C = \prod_{i=1}^{n}(E_i)$.** We will now generalize to products of n elliptic curves (still with prescribed 2-torsion!). Thus we are given a curve C given by

$$y_i^2 = (x - a_i)f(x)$$

where $f(x)$ is again of degree 2. Introduce the following variables:

$$z_i = \frac{y_1}{y_{i+1}}$$

so that

$${z_i}^2 = \frac{x-a_1}{x-a_{i+1}} =: \sigma_{i+1}(x)$$

We can start by expressing x as a function of z_1:

$$x = \frac{a_2{z_1}^2 - a_1}{{z_1}^2 - 1}$$

Plugging x into the other equations for z_i^2 and replacing z_i by z_1/z_i, we have

$$(a_2 - a_i)z_1^2 + (a_i - a_1) = (a_2 - a_1)z_i^2$$

We thus have the following theorem

Theorem 7.3. *There exists a degree 2 map from the curve C to the curve D given by the equations*

$$(a_2 - a_i)z_1^2 + (a_i - a_1) = (a_2 - a_1)z_i^2$$

Proof. This was proved above. □

Remark 7.3. As before, this curve has every elliptic curve E_i as a factor in its Jacobian by section 2, lemma 5.

8. Automorphisms and split Jacobians

In this section we will describe a different method of obtaining Jacobians with multiple elliptic curves. The idea is as follows. One constructs a hyperelliptic curve C with a specific automorphism σ. One also has to provide an elliptic curve such that there is a map $\phi : C \longrightarrow E$. Having done this, the following diagram is obtained:

$$\begin{array}{ccc} C & \xrightarrow{\sigma} & C \\ & \searrow^{\phi} \quad \swarrow_{\phi} & \\ & E & \end{array}$$

Note that this diagram is not required to commute. Our desire in this diagram is for the invariant differential on E to pull back to two independent differentials on C using the map ϕ on the one hand, and the map $\phi_2 := \phi \circ \sigma$ on the other. Thus we would obtain two independent differentials $\phi_2^*(\omega)$ and $\phi^*(\omega)$. This implies that the Jacobian of C contains two copies of the elliptic curve E.
Automorphisms on any curve C are very hard to find however. A construction of Mestre gives explicit curves C with an automorphism of order 2 and a map ϕ to an elliptic curve E. This was reproduced and re-examined in [7]. We shall follow that exposition. Also, we will expand upon that construction by creating automorphisms of C that are an extensions of automorphisms on $\mathbb{P}^1$.

8.1. **Mestre's construction.** Suppose we have an elliptic curve E of the form

$$y^2 = x^3 + ax + b$$

where $ab \neq 0$ (this excludes the cases of elliptic curves with j-invariant 1728 and 0). The idea is as follows. One first gives a specific rational function $\phi(u) \in k(u)$. One considers the curve defined by $y^2 = f(\phi(u))$. Of course this doesn't define a curve in the ordinary sense, but one can remove the denominators to obtain a right equation (one could just say that we're working in the function field $k(C)$ at all times, or one could work with localizations). There is a map

$$\phi : (u, v) \longmapsto (\phi(u), v)$$

This will be our map $C \longrightarrow E$. One next tries to choose ϕ such that the curve C has an extra automorphism. We will first follow Mestre and then slowly generalize.
So first take

$$\phi = \frac{-b}{a} \cdot \frac{u^4 + u^2 + 1}{u^2(u^2 + 1)}$$

To see a later generalization, we can also write this as

$$\phi = \frac{-b}{a} \cdot \frac{u^6 - 1}{u^2(u^4 - 1)}$$

We have the following relation

$$u^2\phi(u) = \phi(u^{-1})$$

From the definition, we can rearrange some terms to obtain

$$u^6(a\phi(u)+b) = a\phi(u)+b$$

These two relations will give us our automorphism. To that end, we compute

$$\begin{aligned} f(\phi(u^{-1})) = f(u^2\phi(u)) &= u^6\phi(u)^3 + au^2\phi(u) + b \\ &= u^6(\phi(u)^3 + a\phi(u) + b) = u^6 f(\phi(u)) \end{aligned}$$

Thus we see that the map

$$\sigma(u,v) := (\frac{1}{u}, u^3 v)$$

defines an automorphism of C of order 2 (because σ is its own inverse).

8.2. **Extending Mestre's construction I.** We will now slightly extend this construction by taking other ϕ's. Recall that ϕ was defined by

$$\phi = \frac{-b}{a} \cdot \frac{u^6-1}{u^2(u^4-1)}$$

Notice that the polynomials involved are actually cyclotomic polynomials. Let us try a different cyclotomic polynomial. Take

$$\phi(u) = \frac{-b}{a}\frac{u^9-1}{u^3(u^6-1)}$$

We have the following two relations (obtained as before):

$$\begin{aligned} \phi(u^{-1}) &= u^3(\phi(u)) \\ u^9(a\phi(u)+b) &= a\phi(u)+b \end{aligned}$$

Consider the curve C defined by

$$v^3 = f(\phi(u))$$

Using the above relations, we find that

$$\begin{aligned} f(\phi(u^{-1})) = f(u^3\phi(u)) &= u^9\phi(u)^3 + au^3\phi(u) + b \\ &= u^9(\phi(u)^3 + a\phi(u) + b) \end{aligned}$$

Thus we can define an automorphism

$$\sigma(u,v) = (\frac{1}{u}, u^3 v)$$

Notice that the elliptic curve in question is $y^3 = x^3 + ax + b$, which automatically has j-invariant 0.

8.3. **Extending Mestre's construction II.** We will try our above construction for a more general class of ϕ. To that end, define

$$\phi(u) = \frac{-b}{a}\frac{u^{2k}-1}{u^2(u^{2k-2}-1)}$$

Also, let $f(x) = x^k + ax + b$ for some $k \geq 2$. We have the following two relations

$$\begin{aligned} \phi(u^{-1}) &= u^2(\phi(u)) \\ u^{2k}(a\phi(u)+b) &= a\phi(u)+b \end{aligned}$$

We can again compute

$$\begin{aligned} f(\phi(u^{-1})) = f(u^2\phi(u)) &= u^{2k}\phi(u)^k + au^2\phi(u) + b \\ &= u^{2k}(\phi(u)^k + a\phi(u) + b) = u^{2k}f(\phi(u)) \end{aligned}$$

Thus we can again define an automorphism of $C : v^2 = f(\phi(u))$ by

$$\sigma(u,v) := (u^{-1}, u^k v)$$

C automatically has a morphism to the curve D defined by the equations

$$y^2 = f(x) = x^k + ax + b$$

8.4. **Extending Automorphisms on $\mathbb{P}^1$.** The previous computations almost seemed like we were "in luck". We obtained a ϕ by copying the structure of our initial example. We can try to look at the problem more intrinsically as follows. Notice that the automorphism always was of the form $\sigma(u,v) = (u^{-1}, u^k v)$. This automorphism is actually an extension of an automorphism on $\mathbb{P}^1$:

$$x \longmapsto 1/x$$

These automorphisms are classified by the group $\mathrm{PGL}_2(k)$: every matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with non-zero determinant corresponds to an automorphism of the form $x \longmapsto \dfrac{ax+b}{cx+d}$(up to nonzero scaling of the matrix). We are thus looking for an extension of the following diagram of function fields

$$\begin{array}{ccc} k(C) & \dashrightarrow & k(C) \\ {\scriptstyle \phi^*}\uparrow & & {\scriptstyle \phi^*}\uparrow \\ k(\mathbb{P}^1) & \longrightarrow & k(\mathbb{P}^1) \end{array}$$

such that the entire diagram commutes. For example, we will construct a ϕ such that C has an automorphism of order 3 over $\mathbb{Q}$. Also, this C will have a map to an elliptic curve by construction.

8.4.1. *Construction of automorphisms over k.* Our construction relies on the following observation: suppose that we have a hyperelliptic curve C given by

$$v^2 = f(\phi(u))$$

where $\phi \in k(u)$ and f is a degree n polynomial with roots β_i. We would like to extend an automorphism from $\mathbb{P}^1$. So suppose we're given such an automorphism σ. We will extend σ by demanding that

$$\frac{f(\phi(\sigma(u)))}{f(\phi(u))} = h^2$$

holds for some $h \in k(u)$. This is actually also a necessary condition, as can be seen using a little bit of linear algebra.
We can rephrase this condition in terms of divisors:

$$\operatorname{div}(f(\phi(\sigma(u)))) - \operatorname{div}(f(\phi(u))) \equiv 0 \mod 2$$

Using the notation in [Silverman] for the pullback of divisors, we obtain the following:

$$\operatorname{div}(f(\phi(\sigma))) = \sigma^*(\phi^*(f^*((0)-(\infty)))) = \sum_{\alpha:\phi(\alpha)=\beta_i} (\sigma^{-1}(\alpha)) - n\sigma^*(\phi^*(\infty))$$

Recall that the β_i are the roots of the initial polynomial f. The corresponding expression for $\operatorname{div}(f(\phi(u)))$ is

$$\operatorname{div}(f(\phi)) = \phi^*(f^*((0)-(\infty))) = \sum_{\alpha:\phi(\alpha)=\beta_i} ((\alpha)) - n(\phi^*(\infty))$$

We will treat several examples to show the possibilities in obtaining $\operatorname{div}(f(\phi(\sigma(u)))) - \operatorname{div}(f(\phi(u))) \equiv 0 \mod 2$.

Example 8.1. If the poles of ϕ occur with double multiplicity, then we have the following equation

$$\sum_{\alpha:\phi(\alpha)=\beta_i} \sigma^{-1}(\alpha) - (\alpha) \equiv 0 \mod 2$$

In other words, we want the roots of the equations $\phi(x) = \beta_i$ to cancel out properly. One way to do this is to demand that the roots of these equations are actually *invariant* under σ.
Let us try this on an explicit example. Let us take $n = 3$ and $f = (x-1)(x-2)(x-3) = x^3 - 7x + 6$. Let us take $\sigma(x) = \dfrac{-x}{x+1}$. This is an element of order 2. Let us take ϕ of the form

$$\phi = \frac{a_2x^2 + a_1x + a_0}{(x+a)^2}$$

Define $\phi_1 = a_2x^2 + a_1x + a_0$ and $\phi_2 = (x+a)^2$ so that $\phi = \phi_1/\phi_2$. We are given the equations $\phi(x) = \beta_i$, or:

$$\phi(x) = 1$$
$$\phi(x) = 2$$
$$\phi(x) = -3$$

We can impose the condition that the roots of $g_1 = \phi_1 - \phi_2$ are mapped to $g_2 = \phi_1 - 2\phi_2$ (this can be done by saying that $\text{num}(g_1(\sigma(x))) = k_1 g_2(x)$ for some k_1). We can also impose the condition that the roots of $g_3(x) := \phi_1 + 3\phi_2$ are invariant (or: $\text{num}(g_3(\sigma(x))) = k_3 g_3$ for some k_3). Putting this together (and doing a Gröbner basis calculation) yields the following result:

Result 8.1. Let $\phi_1 = (\frac{73}{9}x^2 + 22x + 13)$ and $\phi_2 = (x+3)^2$. Let $\phi = \phi_1/\phi_2$. Let $f = x^3 - 7x + 6$. We have that

$$\frac{f(\phi(\sigma(x)))}{f(\phi(x))} = \frac{1}{8^2}\frac{(x+3)^6}{(x+3/2)^6}$$

Let $h = \frac{1}{8}\frac{(x+3)^3}{(x+3/2)^3}$. Let C be the curve given by

$$v^2 = f(\phi(u))$$

Then C has an automorphism of order 2 given by

$$\tilde{\sigma} : (u, v) \longmapsto (\sigma(u), h(x)v)$$

One can get a proper affine equation for C by multiplying both sides of the equation by $(u+3)^6$ and replacing v by $v(u+3)^3$. The resulting equation is

$$v^2 = \frac{352000}{729}x^6 + \frac{97600}{27}x^5 + \frac{274000}{27}x^4 + \frac{36800}{3}x^3 + \frac{12400}{3}x^2 - 2400x - 800$$

Our initial goal was for the Jacobian to split. The next lemma says this actually happens.

Lemma 20. *Let C be given by the above equation. Then $J(C) \sim E^2$, where E is given by $y^2 = (x-1)(x-2)(x+3)$.*

Proof. We can pull back the differential on E via two maps: ϕ and $\phi \circ \tilde{\sigma}$. Let $r_1 = \phi(\sigma)$ and $r_2 = \phi$. Then

$$dr_1 = \frac{-40(x+3)}{3(2x+3)^3}dx$$
$$dr_2 = \frac{40(2x+3)}{3(x+3)^3}dx$$

The invariant differential on E is given by dx/y. Pulling it back, we obtain

$$\phi^*(dx/y) = d(\phi(x))/y = \frac{40(2x+3)}{3(x+3)^3}\frac{dx}{y}$$

$$(\phi \circ \tilde{\sigma})^*(dx/y) = \frac{d(\phi(\sigma))}{h(x)y} = -40/3\frac{dx}{y(x+3)^2}$$

which are independent. Thus, the theorem follows by section 2, lemma 5. □

Remark 8.1. Note that the divisor equality only tells us that the roots occur as squares. It doesn't tell us that the constants occur as squares as well. However, must of the time the conditions imposed seem to imply squares in the constant terms as well.

Example 8.2. We will now give an example of a curve C with an automorphism of order 3, induced by $\mathbb{P}^1$. Let $\sigma(x) = \dfrac{-1}{1+x}$. Then σ has order 3. We will use the above technique to produce a curve with an induced automorphism.
The curve that we will obtain, will have the form

$$v^3 = f(\phi(u))$$

where $f = (x-1)(x-2)(x+3)$. This time, we want a cube, so we get the following equation

$$\sum_{\alpha:\phi(\alpha)=\beta_i} (\sigma^{-1}(\alpha) - (\alpha)) \equiv 0 \mod 3$$

We again obtain the equations

$$\phi(x) = \beta_i$$

To find an invariant solution to these, we construct an orbit in the equations. That is, we want the following

$$Z(\phi - 1) \longrightarrow^{\sigma} Z(\phi - 2) \longrightarrow^{\sigma} Z(\phi + 3)$$

and the last one will automatically map back to the first one. Trying various degrees for ϕ, we found the following solution

$$\phi = \frac{29/37x^4 + 82/37x^3 - 13/37x^2 + x + 1}{x^4 + 142/49x^3 + 1479/1813x^2 - 51/1813x + 1/37}$$

Let

$$h = 37 \cdot \frac{x^4 + 142/49x^3 + 1479/1813x^2 - 51/1813x + 1/37}{x^4 + 247/49x^3 + 1926/49x^2 - 1947/49x - 38}$$

We have that

$$f(\phi(\sigma(x)))/f(\phi(x)) = (h(x))^3$$

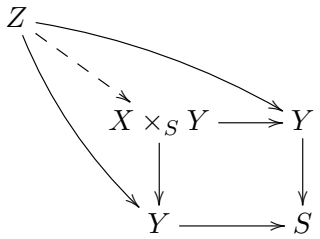
Thus the curve $C : v^3 = f(\phi(u))$ has an automorphism

$$\tilde{\sigma}(u, v) = (\sigma(u), h(u)v)$$

9. Fibre products of curves over $\mathbb{P}^1$

In section 7, we took the fibre product of two elliptic curves over a morphism to $\mathbb{P}^1$. The morphism in this case being the projection onto the x-axis. Of course, fibre products exists more generally. In this section we will exploit these fibre products to create more examples of Jacobians that decompose into elliptic curves. We will also use these fibre products to create multiple quadratic points on elliptic curves.

9.1. **Generalities about fibre products.** For any two schemes X, Y over another scheme S, there is the notion of a fibre product. To be exact, a fibre product of X and Y (denoted by $X \times_S Y$) is a scheme with morphisms $p_1 : X \times_S Y \longrightarrow X$ and $p_2 : X \times_S Y \longrightarrow Y$ such that for every scheme Z with morphisms $Z \longrightarrow X$ and $Z \longrightarrow Y$, there exists a unique morphism $Z \longrightarrow X \times_S Y$ such that the following diagram commutes:



In this section, we will take $S = \mathbb{P}^1$ and $X, Y \longrightarrow S$ two non-constant morphisms. We will work in affine charts usually.

Remark 9.1. It is important to note that most of these fibre products are not irreducible. They will have multiple components, most of which we can discard. To find the correct components, we first found the radical of the ideal, and then computed a primary decomposition to find the right components.

9.2. **Fibre product over the y-coordinate.** Suppose we are given an elliptic curve E in the form

$$y^2 = x^3 + ax + b$$

We will take two copies of this elliptic curve E with different coordinates. So let

$$y_i^2 = x_i^3 + ax_i + b$$

with $i \in \{1, 2\}$. Consider the morphism defined by $(x_i, y_i) \longrightarrow y_i$. We can now take the fibre product over these two morphisms. In other words, we obtain the following set of equations:

$$y^2 = x_i^3 + ax_i + b$$

where y is the common function $y = y_1 = y_2$. This curve has two components however. We can see this as follows. Subtracting both equations, we obtain

$$x_1^3 - x_2^3 + a(x_1 - x_2) = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 + a)$$

We take the component with $x_1^2 + x_1x_2 + x_2^2 + a = 0$. This is a quadratic form, so provided $a \neq 0$, we have that over an algebraic extension it is isomorphic to $\mathbb{P}^1$. The map sending (x_1, x_2, y) to (x_1, x_2) is thus a map $C \longrightarrow \mathbb{P}^1$ of degree 2 (again, once we find a point on the quadratic form).

Theorem 9.1. *C is a hyperelliptic curve of genus 3 over a finite extension of k for any value of $a \neq 0$.*

Proof. Consider the cover

$$C \longrightarrow E_1$$

given locally by

$$(x_1, x_2, y) \longmapsto (x_1, y)$$

In terms of function fields, it is just the quadratic extension of $\mathbb{Q}(x_1, y)$ given by

$$x_1^2 + x_1x_2 + x_2^2 + a = 0$$

As such, we can find the ramification points by calculating the discriminant of this quadratic polynomial. The resulting discriminant is

$$x_1^2 - 4(x_1^2 + a).$$

Setting this equal to zero, we obtain

$$-3x_1^2 = a$$

or

$$x_1 = \pm\sqrt{-a/3}$$

Note that we assumed $a \neq 0$, so we obtain two values of x_1. For each of these values of x_1, one obtains two values of y (one has to check that they do not give a point with $y = 0$) . Since the infinite points do not ramify, we have a total of 4 ramification points. Using the Hurwitz formula, we obtain

$$2g(C) - 2 = 0 + 4$$

and thus $g(C) = 3$, as desired. □

9.3. **Fibre products of elliptic curves with extra structure.** In this section we will take the fibre product of elliptic curves E' with an isogeny $E \longrightarrow E'$. The fibre product is exactly as in section 7. Let us recall the situation. We had two elliptic curves

$$y_i^2 = (x - a_i)f(x)$$

where $f(x)$ is of degree 2. We first have to find elliptic curves such that their Weierstrass form is as above. We will do this explicitly using the families in section 3.

9.3.1. *For elliptic curves with $\mathbb{Z}/6\mathbb{Z}$ torsion.* Suppose that we have an elliptic curve E with $\mathbb{Z}/6\mathbb{Z}$ torsion. Then according to Theorem 3.2, we have that E is of the following form

$$y^2 + wxy + vy = x^3 + vx^2$$

with $v = -w^2 + 3w - 2$. Modding out a point of order 3 gives us an isogenous curve E', which has the following equation

$$y^2 + wxy + vy = x^3 + vx^2 + f_1x + f_2$$

where

$$f_1 = -40 + 130w - 155w^2 + 80w^3 - 15w^4$$
$$f_2 = -76 + 368w - 739w^2 + 787w^3 - 468w^4 + 147w^5 - 19w^6$$

Using the short Weierstrass form given later in that section, we get that the curve E' is given by

$$y^2 = (x+9/4w^2-6w+11/3)(x^2+(-9/4w^2+6w-11/3)x-81/8w^4+54w^3-105w^2+89w-251/9)$$

For fibering purposes, we translate again to obtain the equation

$$y^2 = (x + 27/8w^2 - 9w + 11/2)(x^2 - 729/64w^4 + 243/4w^3 - 945/8w^2 + 100w - 125/4)$$

Consider the variety $\mathbb{P}^1$ with coordinate w. It has a morphism defined by

$$\rho(w) = -729/64w^4 + 243/4w^3 - 945/8w^2 + 100w - 125/4$$

Let us take two copies of $\mathbb{P}^1$ with coordinates w_1 and w_2, and consider the fiber product of this morphism. The fiber product is reducible. This can be seen by the following decomposition:

$$\begin{aligned}\rho(w_1) - \rho(w_2) &= (w_1 - w_2)(-729/64w_1^3 - 729/64w_1^2w_2 - 729/64w_1w_2^2 - 729/64w_2^3 + 243/4w_1^2 \\ &\quad +243/4w_1w_2 + 243/4w_2^2 - 945/8w_1 - 945/8w_2 + 100)\end{aligned}$$

Let us call this last polynomial $\tilde{\rho}$. It defines a curve of genus 0. It actually has the rational point $P = (10/9, 2)$ on it (which is nonsingular), so it is birational to $\mathbb{P}^1$. We will give the explicit parametrization below.

Theorem 9.2. *A parametrization for $Z(\tilde{\rho})$ is given by*

$$\begin{aligned}w_1 &= \frac{t^3 + 9/5t^2 + 9/5t + 9/5}{9/10t^3 + 9/10t^2 + 9/10t + 9/10} \\ w_2 &= \frac{9/5t^3 + 9/5t^2 + 9/5t + 1}{9/10t^3 + 9/10t^2 + 9/10t + 9/10}\end{aligned}$$

where the inverse is given by

$$t = (w_2 - 10/9)/(w_1 - 10/9)$$

Proof. One can check that these maps are inverse to each other. Since $k(t)$ is the function field of $\mathbb{P}^1$, we have that the completion of $Z(\tilde{\rho})$ is isomorphic to $\mathbb{P}^1$. □

We are now in the following scenario. For every value of t, we have a curve C_t of genus 2 such that there exist two maps $C_t \longrightarrow E_{1,t}$ and $C_t \longrightarrow E_{2,t}$. Furthermore, for every t we have that the Jacobian of C_t splits into those two elliptic curves. Recall that C_t was given by the following equations

$$y_1^2 = (x - a_1(t))f_t(x)$$
$$y_2^2 = (x - a_2(t))f_t(x)$$

We were able to express x as

$$x = \frac{a_2 z^2 - a_1}{z^2 - 1}$$

where $z = y_1/y_2$. This gave a hyperelliptic form for C_t. Thus, we are able to give C_t the following coordinates: (z, y, t). We can fiber two of these curves (or surfaces!) over the morphism given by

$$(z, y, t) \longmapsto (y)$$

The resulting set of equations is as follows

$$y^2 = f(z_1, t_1)$$
$$y^2 = f(z_2, t_2)$$

If we subtract these we obtain the following equation:

$$f(z_1, t_1) - f(z_2, t_2) = 0.$$

This defines a 3-dimensional reducible variety in $\mathbb{A}^4$. There are multiple components in this variety, one of them defined by the ideal $(z_1 - z_2, t_1 - t_2)$. If we can find rational points on the other components then we have **four** quadratic points on 4 (or less) elliptic curves. Also, these points are all defined over the same quadratic field $\mathbb{Q}(y_0)$. This would in principal give 4 extensions of $\mathbb{Q}(y_0)$. Finding a primary decomposition of this variety turned out to be to costly for a single computer, so we couldn't find a neat representation of all the components.

10. Examples

Here we will give some explicit examples of quadratic number fields with a certain 3-rank. For this, we shall use the constructions that were made in the last sections and the moduli spaces in section 3.

10.1. **Quadratic number field with 3-rank greater than or equal to 1.** Consider the family of curves

$$y^2 + wxy + vy = x^3$$

with 3-torsion point P. The isogenous curve $E/ < P >$ is given by

$$y^2 + wxy + vy = x^3 - 5wvx - v(w^3 + 7v)$$

The isogeny ϕ is given by

$$\phi : (x, y) \longmapsto (\frac{x^3 + wvx + v^2}{x^2}, \frac{x^3y - w^2vx^2 - wvxy - 2wv^2x - 2v^2y - v^3}{x^3})$$

As was shown in [6], the extension are created by the first rational function

$$\phi_1(x) := \frac{x^3 + wvx + v^2}{x^2}$$

We will give an explicit example of such an extension.

Example 10.1. Take $w = 5$ and $v = 3$. Then we have the elliptic curve E' given by

$$y^2 + 5xy + 3y = x^3 - 75x - 438$$

with discriminant

$$\Delta E' = 2^6 \cdot 3 \cdot 11^3$$

Note that this model is minimal, thus we can look at the reduction of E' modulo primes. The singular point on $E' \mod 2$ is given by $\tilde{P} = (1, 0)$. The singular point on $E' \mod 11$ is given by $\tilde{P} = (-1, 1)$. So if we impose that $x(P) \neq 1 \mod 2$ and $x(P) \neq -1 \mod 11$, then the corresponding extension will be unramified above 2 and 11. The only problem is $p = 3$. For that, we have to look at the explicit equation.
Recall that our isogeny is given by

$$\phi_1(x) = \frac{x^3 + 13x + 9}{x^2}$$

Suppose that we take $t \in \mathbb{Z}$. Then the corresponding extension is given by $\phi_1(x) = t$, or put differently:

$$x^3 - tx^2 + 13x + 9$$

If the extension

$$\mathbb{Q}_3 \subseteq \mathbb{Q}_3(\phi_1(x))$$

is **not** totally ramified, then the extension $\mathbb{Q}(y) \subseteq \mathbb{Q}(y, \phi_1(x))$ will be unramified (see [6] for this). One can use Newton polygons for this or any other method. Let us take $t = 4$. We can reduce $\phi_1(x) \mod 3$ to obtain

$$\tilde{\phi_1}(x) = (x + 2)x^2.$$

Thus the extension $\mathbb{Q}_3 \subseteq \mathbb{Q}_3(\phi_1)$ is not totally ramified, and we're done.

10.2. **Quadratic number field with 3-rank greater than or equal to 2.** We shall use the fibre product method. We will take two elliptic curves E_1' and E_2' with isogenies $E_i \longrightarrow E_i'$, and a 2-torsion point on both E_1' and E_2', and we will fibre them. This will yield a hyperelliptic curve of genus 2.

Example 10.2. Recall that in Short Weierstrass Form, any elliptic curve E' with an isogeny $E \longrightarrow E'$ of degree 3 (with kernel generated by a rational point) and a 2-torsion point could be given by

$$y^2 = x^3 + \rho_1 x + \rho_2$$

with

$$\begin{aligned}\rho_1 &= (-1/48)w^4 - (1/6)vw^2 - (1/3)v^2 + (1/2)vw + f_1\\ \rho_2 &= (1/864)w^6 + (1/72)vw^4 + (1/18)v^2w^2 - (1/24)vw^3 + (2/27)v^3\\ &\quad -(1/6)v^2w - (1/12)f_1w^2 - (1/3)f_1v + (1/4)v^2 + f_2\end{aligned}$$

and

$$\begin{aligned}f_1 &= -40 + 130w - 155w^2 + 80w^3 - 15w^4\\ f_2 &= -76 + 368w - 739w^2 + 787w^3 - 468w^4 + 147w^5 - 19w^6\end{aligned}$$

In fact, as we saw, we had

$$y^2 = (x + 27/8w^2 - 9w + 11/2)(x^2 - 729/64w^4 + 243/4w^3 - 945/8w^2 + 100w - 125/4)$$

We also were able to identify the quadratic terms. The result we had stated that we were able to parametrize them by

$$\begin{aligned}w_1 &= \frac{t^3 + 9/5t^2 + 9/5t + 9/5}{9/10t^3 + 9/10t^2 + 9/10t + 9/10}\\ w_2 &= \frac{9/5t^3 + 9/5t^2 + 9/5t + 1}{9/10t^3 + 9/10t^2 + 9/10t + 9/10}\end{aligned}$$

Note that these are indeed different rational functions. This allowed us to create quadratic points on the curve given by

$$\begin{aligned}y_1^2 &= (x - a_1)f(x)\\ y_2^2 &= (x - a_2)f(x)\end{aligned}$$

by means of

$$x = \frac{a_2z^2 - a_1}{z^2 - 1}$$

So take $z = 3$, $t = 10$. The minimal models are given by

$$\begin{aligned}y^2 + xy + y &= x^3 - x^2 - 448345574132x - 175198592120394769\\ y^2 + xy &= x^3 - x^2 - 2503284524685x + 1660475546421968925\end{aligned}$$

with points P_1 and P_2 such that

$$x(P_1) = 12762599/72$$
$$x(P_2) = -18747561/8$$

The minimal discriminants are

$$\begin{aligned}\Delta(E_1') &= -1 \cdot 2^3 \cdot 3^9 \cdot 5^3 \cdot 11^6 \cdot 37^3 \cdot 101^6 \cdot 1999^2 \\ \Delta(E_2') &= -1 \cdot 2^3 \cdot 3^9 \cdot 5^3 \cdot 11^6 \cdot 37^3 \cdot 97^2 \cdot 101^6 \cdot 103^2\end{aligned}$$

This gives a congruence condition at each prime $\neq 3$ for a point not to reduce singularly. After some translations, we find that the extensions are given by

$$\phi_1(x) = x^3 + 363085569x^2 + 20668672781856000x + 330533415127441152000000$$
$$\phi_2(x) = x^3 + 235701081x^2 + 11478000653856x + 917413636261402368$$

which have discriminants

$$\Delta(\phi_1(x)) = -1 \cdot 2^{17} \cdot 3^{14} \cdot 5^6 \cdot 11^6 \cdot 37 \cdot 787 \cdot 1999^4 \cdot 72740897$$
$$\Delta(\phi_2(x)) = -1 \cdot 2^{11} \cdot 3^{12} \cdot 11^6 \cdot 37 \cdot 97^4 \cdot 103^4 \cdot 787 \cdot 72740897$$

Note that simply reducing the polynomials doesn't show that the extension is not totally ramified. One can however consider the Newton polygon of these polynomials to obtain the desired result. Note also that the discriminants are **different**, and as such the extensions are different. To summarize our results: $\mathbb{Q}(\sqrt{-4236284359486})$ has 3-rank at least 2. Indeed, it has class group $\mathbb{Z}/101214\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which has 3-rank 2.

As in [6] and in [12], one should be able to show that there are infinitely many of these number fields with 3-rank at least 2 using these elliptic curves. We didn't explicitly give the congruence conditions, but it is quite easy to obtain them (see our first example in this section).

11. Conclusion

Our goal was to obtain quadratic number fields with high p-rank. To achieve this we set out to investigate certain geometric structures. In this thesis you will find many generalizations on geometric methods that were known. The method that seems to work the best right now is the method of fibering elliptic curves. We obtained quadratic number fields with 3-rank 2. We also saw the underlying possibilities of making this rank higher:

(1) There is a direct interplay between the rank of a curve and the p-rank of a number field, as shown in section 4.
(2) One can try to find quadratic points on the fibre product of more than four elliptic curves. However, as we saw during this thesis, this takes a lot of computing power.
(3) One can try to improve on the automorphism method by creating Galois extensions of certain varieties as is done in Serre's book *Topics in Galois Theory*. This can also yield quadratic number fields with certain p-ranks.

As a side note, one can consider representations of elliptic curves (not necessarily $p = 3$) such that the torsion point is defined over a quadratic extension. This might also give quadratic number fields with certain p-ranks for $p \geq 11$. We were bound by Mazur's Theorem till now, so we weren't able to go higher than 11. Another idea that might work is to put quadratic points on Jacobians directly. This seems like a hard task though.

12. Acknowledgements

I would like to thank my thesis supervisor, Prof. Jaap Top for his support and supervision during my thesis and the rest of my curriculum.

References

[1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2nd Edition, 2009.
[2] Robin Hartshorne, *Algebraic Geometry*, Springer, 1999.
[3] Nicholas M. Katz, Barry Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, 1985.
[4] J.S. Milne, *Abelian Varieties*, Online course notes, 2nd version, http://www.jmilne.org/math/
[5] Jürgen Neukirch, *Algebraic Number Theory*, Springer, 1999.
[6] Meinte Boersma, *Construction of infinite families of quadratic number fields with class number divisible by certain primes*, Master's thesis.
[7] René Pannekoek, *Topological aspects of rational points on K3 surfaces* Dissertation.
[8] Tim Dokchitser, *Deformations of p-divisible groups and p-descent on elliptic curves* Dissertation
[9] Muhammad Afzal Soomro, *Algebraic curves over finite fields*, Dissertation.
[10] P.Stevenhagen,*Algebra 3*, Online course notes, Available at http://websites.math.leidenuniv.nl/algebra/
[11] P.Stevenhagen,*Voortgezette getaltheorie*, Online course notes,
[12] Jean-François Mestre, *Corps quadratiques dont le 5-rang du groupe des classes est* ≥ 3, Arxiv, June 16th, 1992