university of groningen / faculty of science and engineering / mathematics and applied mathematics

Asymptotic integral solutions to $Aa^p + Bb^p = Cc^3$ over number fields

Master's Project Mathematics
July 2025
Student: S. Nomden
First supervisor: Dr. E. Özman
Second assessor: Dr. P. Kılıçer

Abstract

In this thesis we apply the modular method to show the non-existence of certain asymptotic solutions to the equation $Aa^p + Bb^p = Cc^3$ over the ring of integers of a number field K. The modular method uses the conjectured relation between modular forms and elliptic curves. To introduce these ideas we cover the necessary details of elliptic curves and Galois theory. The latter is studied, in great detail, using Galois representations. Finally, we specialize our number field K to imaginary quadratic extensions of $\mathbb{Q}$. This specialization requires a close study of S-units and S-unit equations over these fields.

Contents

Introduction

Fermat's Last Theorem is one of the most monumental results of twentieth-century mathematics. It states that $a^n + b^n = c^n$ has no non-trivial integer solutions for $n \geqslant 3$. This theorem was conjectured by Fermat in 1637 and the final step of the proof was completed by Wiles in 1995 [62, Theorem 0.4]. In his paper, Andrew Wiles proved that every semi-stable elliptic curve over $\mathbb{Q}$ is associated to some weight-two cuspidal modular form. Showing this turned out to be enough to prove Fermat's Last Theorem. This is due to the level lowering theorem proven by Ribet in 1990 [43, Theorem 1.1]. The relation between elliptic curves over $\mathbb{Q}$ and modular forms was already conjectured by Taniyama and Shimura in 1957. In 2001, the collaborative efforts of Breuil, Conrad, Diamond, and Taylor proved this conjecture in [7, Theorem A].

The ideas of exploiting the connection between modular forms and elliptic curves over $\mathbb{Q}$ to solve Diophantine equations over $\mathbb{Z}$ is not limited to this particular equation. In the years after the proof of Fermat's Last Theorem, number theorists were able to show non-existence of solutions to specific Diophantine equations over $\mathbb{Z}$. Due to the usage of the modularity of elliptic curves, this way of solving Diophantine equations is known as 'the modular method'.

There is a conjectured relation between modular forms and elliptic curves over numbers fields. This modularity can again be used to solve Diophantine equations, now over the ring of integers of a number field. Replacing $\mathbb{Q}$ by a more general object introduces many difficulties and complications. In this thesis we explore these hurdles and apply the modular method for a set of Diophantine equations over the ring of integers of a number field.

Often, it is stated that there is a fundamental connection between elliptic curves and modular forms but the bridge that connects these two objects is neglected: Galois representations. Galois representations are fundamental objects in number theory and the conjectures relating modular forms and elliptic curves are often stated in terms of these representations. In the third section of this thesis we explore, in quite some detail, Galois representations and how they relate to elliptic curves. To do this, we cover the necessary results in Galois theory and elliptic curves in the first two sections of this thesis. In the final section we use the developed theory in order to asymptotically show non-existence of solutions to a set of Diophantine equations of the form $Aa^p + Bb^p = Cc^3$. This means that we find some constant V depending only on the number field and the constants A, B and C such that whenever $p > V$, there are no solutions to $Aa^p + Bb^p = Cc^3$.

1 Algebraic number theory

In this section we fix some notation and state some results from algebraic number theory. In particular, we are interested in Galois theory of local fields and of number fields (global fields). In this section, and throughout the rest of this thesis, we usually state results in terms of local fields but we always do this with a view on global fields via embedding a number field into its completion at a prime. Thus the reader should always keep in mind that the local theory serves the global theory, despite the fact that most of the results are stated in terms of local fields.

1.1 Inverse limits

In this section we give a somewhat formal introduction to inverse limits. This formal introduction proves its usefulness as inverse limits show up in many different contexts throughout this thesis and they describe the structure of the absolute Galois group, one of the main object of study.

An *inverse system* of groups $(G_\alpha, \varphi_{\alpha\beta})_{\alpha\in I}$ consists of:

1. A partially ordered set $(I, \leqslant)$ such that for every $\alpha, \beta \in I$ there is some $\gamma \in I$ with $\alpha \leqslant \gamma$ and $\beta \leqslant \gamma$;
2. for every $\alpha \in I$ a group G_α;
3. for every $\alpha, \beta \in I$ such that $\alpha \leqslant \beta$ a group morphism $\varphi_{\alpha\beta}\colon G_\beta \to G_\alpha$ such that $\varphi_{\alpha\gamma} = \varphi_{\alpha\beta} \circ \varphi_{\beta\gamma}$ whenever $\alpha \leqslant \beta \leqslant \gamma$.

The *inverse limit* of an inverse system $(G_\alpha, \varphi_{\alpha\beta})_{\alpha\in I}$ is

$$\varprojlim_\alpha G_\alpha = \Big\{(g_\alpha)_\alpha \in \prod_{\alpha\in I} G_\alpha : \varphi_{\alpha\beta}(g_\beta) = g_\alpha \text{ for all } \alpha \leqslant \beta\Big\} \subset \prod_{\alpha\in I} G_\alpha.$$

When it is clear from the context that we are taking an inverse limit, we will often write $\lim_\alpha G_\alpha$ for the inverse limit of the system $(G_\alpha, \varphi_{\alpha\beta})_{\alpha\in I}$. The inverse limit $\lim_\alpha G_\alpha$ inherits a group structure from the product $\prod_\alpha G_\alpha$ and comes with natural projection morphisms $\varphi_\beta\colon \lim_\alpha G_\alpha \to G_\beta$ for all $\beta \in I$.

This construction is not restricted to groups only; we can replace the word 'group' with, for example, 'ring', 'topological space' or 'module'. It may be worth noting that the inverse limit construction is a particular case of limits in categories. In a general category these limits may not exist. For example, in the category of fields, arbitrary products do not exist so the above construction may fail. The study of arbitrary inverse limit's is often far too broad. We are mostly interested in groups of the following form.

Definition 1.1. A *profinite group* G is a group which is the inverse limit of a inverse system consisting of finite groups. ■

Example 1.2. 1. Every finite group is a profinite group. It is the inverse limit of the system $(G, \mathrm{id}_G)_{\alpha\in I}$ for any non-empty partially ordered set I satisfying condition 1.

2. Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\mathfrak{p}$ be a prime ideal in K. Then $(\mathcal{O}_K/\mathfrak{p}^n, \pi_n)_{n\in\mathbb{Z}_{\geqslant 0}}$ is an inverse system of rings where $\pi_n\colon \mathcal{O}_K/\mathfrak{p}^{n+1} \to \mathcal{O}_K/\mathfrak{p}^n$ is the natural projection for every $n \in \mathbb{Z}_{\geqslant 0}$. Its inverse limit is the ring of integers of a local field.

3. Let $(I, \leqslant) = (\mathbb{Z}_{>0}, \mid)$ where the ordering is divisibility (i.e. $n \leqslant m$ when $n \mid m$). Let $G_m = \mathbb{Z}/m\mathbb{Z}$ and for $m \mid n$, let $\varphi_{mn}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the natural projection. The inverse limit $\lim_n \mathbb{Z}/n\mathbb{Z}$ is denoted by $\hat{\mathbb{Z}}$ and is referred to as the *profinite integers*. ■

A profinite group $G = \lim_\alpha G_\alpha$ carries a topology in a natural way: endow the finite groups G_α with the discrete topology and let the topology on G be the smallest topology for which the projection morphisms $G \to G_\alpha$ are continuous. In this topology the group law $G \times G \to G$ is continuous. It then follows that the sets of the form $\ker(G \to G_\alpha)$ form a fundamental system around the identity $1 \in G$ and that

$$\{g \cdot \ker(G \to G_\alpha)\}_{g\in G, \alpha\in I}$$

forms a basis for the topology on G. This topology is called the *profinite topology* on G. The following standard result reveals the interplay between the group structure and the topology of a profinite group.

Proposition 1.3. Let G be a profinite group. Then a subgroup H of G is open in G if and only if H is closed and of finite index in G. ■

Let $(A_\alpha, \varphi_{\alpha\beta})_{\alpha\in I}$ and $(B_\alpha, \psi_{\alpha\beta})_{\alpha\in I}$ be inverse inverse systems of groups. We say that a set of group morphisms $(f_\alpha\colon A_\alpha \to B_\alpha)_\alpha$ is a morphism of inverse systems if for every $\alpha, \beta \in I$ such that $\alpha \leqslant \beta$ the square

$$\begin{array}{ccc} A_\beta & \xrightarrow{f_\beta} & B_\beta \\ {\scriptstyle\varphi_{\alpha\beta}}\downarrow & & \downarrow{\scriptstyle\psi_{\alpha\beta}} \\ A_\alpha & \xrightarrow[f_\alpha]{} & B_\alpha \end{array}$$

commutes. It is then readily verified that a morphism of inverse systems induces a morphism of groups $f\colon \lim_\alpha A_\alpha \to \lim_\alpha B_\alpha$ acting coordinate-wise. The next result is an abstract result regarding morphisms of inverse systems and exact sequences. It is used in Section 1.3.

Proposition 1.4. Let $(A_\alpha, \varphi_{\alpha\beta})_{\alpha\in I}$, $(B_\alpha, \psi_{\alpha\beta})_{\alpha\in I}$ and $(C_\alpha, \sigma_{\alpha\beta})_{\alpha\in I}$ be inverse systems of groups and let $(f_\alpha\colon A_\alpha \to B_\alpha)_{\alpha\in I}$ and $(g_\alpha\colon B_\alpha \to C_\alpha)_{\alpha\in I}$ be morphisms of inverse systems such that

$$1 \longrightarrow A_\alpha \xrightarrow{f_\alpha} B_\alpha \xrightarrow{g_\alpha} C_\alpha \longrightarrow 1$$

is exact. Suppose that I has a unique least element and that the transition maps $A_\beta \to A_\alpha$ are surjective for all $\alpha \leqslant \beta$. Then

$$1 \longrightarrow \lim_\alpha A_\alpha \xrightarrow{f} \lim_\alpha B_\alpha \xrightarrow{g} \lim_\alpha C_\alpha \longrightarrow 1$$

is exact. ■

Proof. It is generally true and fairly straightforward that

$$1 \longrightarrow \lim_\alpha A_\alpha \xrightarrow{f} \lim_\alpha B_\alpha \xrightarrow{g} \lim_\alpha C_\alpha$$

is exact. Thus all that remains to be shown is that $\lim_\alpha B_\alpha \to \lim_\alpha C_\alpha$ is surjective. Let $(c_\alpha)_{\alpha\in I} \in \lim_\alpha C_\alpha$ and suppose that $\alpha \leqslant \beta$. We have a commutative diagram with exact rows of the form

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A_\beta & \xrightarrow{f_\beta} & B_\beta & \xrightarrow{g_\beta} & C_\beta & \longrightarrow & 1 \\ & & {\scriptstyle\varphi_{\alpha\beta}}\downarrow & & {\scriptstyle\psi_{\alpha\beta}}\downarrow & & {\scriptstyle\sigma_{\alpha\beta}}\downarrow & & \\ 1 & \longrightarrow & A_\alpha & \xrightarrow{f_\alpha} & B_\alpha & \xrightarrow{g_\alpha} & C_\alpha & \longrightarrow & 1 \end{array}$$

Suppose we are given that $b_\alpha \in B_\alpha$ such that $g_\alpha(b_\alpha) = c_\alpha$. We construct $b_\beta \in B_\beta$ such that $\psi_{\alpha\beta}(b_\beta) = b_\alpha$ and such that $g_\beta(b_\beta) = c_\beta$. By exactness, g_β is surjective. Let $\tilde{b}_\beta$ be such that $g_\beta(\tilde{b}_\beta) = c_\beta$. Then

$$g_\alpha(\psi_{\alpha\beta}(\tilde{b}_\beta)b_\alpha^{-1}) = \sigma_{\alpha\beta}(g_\beta(\tilde{b}_\beta))g_\alpha(b_\alpha^{-1}) = c_\alpha c_\alpha^{-1} = 1$$

and hence $\psi_{\alpha\beta}(\tilde{b}_\beta)b_\alpha^{-1} \in \ker g_\alpha = \operatorname{im} f_\alpha$. Since $\varphi_{\beta\alpha}$ is surjective, there is some $a_\beta \in A_\beta$ such that

$$\psi_{\alpha\beta}(\tilde{b}_\beta)b_\alpha^{-1} = f_\alpha(\varphi_{\alpha\beta}(a_\beta)) = \psi_{\alpha\beta}(f_\beta(a_\beta)) \quad\Longleftrightarrow\quad \psi_{\alpha\beta}(f_\beta(a_\beta^{-1})\tilde{b}_\beta) = b_\alpha.$$

Further,

$$g_\beta(f_\beta(a_\beta^{-1})\tilde{b}_\beta) = g_\beta(f_\beta(a_\beta^{-1}))g_\beta(\tilde{b}_\beta) = 1 \cdot c_\beta = c_\beta.$$

Therefore, $b_\beta \coloneqq f_\beta(a_\beta^{-1})\tilde{b}_\beta$ satisfies the required properties. Let $i \in I$ be the unique least element and let $b_i \in B_i$ be such that $g_i(b_i) = c_i$. Then via the above construction we inductively construct an element $b = (b_\alpha)_{\alpha\in I} \in \lim_\alpha B_\alpha$ such that $g(b) = (c_\alpha)_{\alpha\in I}$. It follows that g is surjective. □

Remark 1.5. The conditions on $(A_\alpha, \varphi_{\alpha\beta})_{\alpha\in I}$ in Proposition 1.4 is a specific case of a Mittag-Leffler condition on a exact sequence of inverse systems. In the category of abelian groups or modules over a ring it is more generally true that whenever an exact sequence of inverse systems satisfies the Mittag-Leffler condition then the inverse limit of an exact sequence is exact (see [54, Tag 0594] or [5, Proposition 10.2]). In the non-abelian case, some more care is required, as we did here. ■

1.2 Finite Galois theory

In this section we briefly cover Galois theory of finite Galois extensions of local fields and of number fields. We do this with a view on Galois theory of extensions of possibly infinite degree.

Definition 1.6. A field K is *local* if it is complete with respect to some discrete non-Archimedean absolute value and if it has a finite residue field. ■

Let K be a local field which is complete with respect to the absolute value $|\cdot|$. Then since $|\cdot|$ is discrete and non-Archimedean, the *ring of integers* or *valuation ring*

$$\mathcal{O}_K = \{x \in K : |x| < 1\}$$

is a discrete valuation ring with finite residue field.

Example 1.7. Let K be a number field with ring of integers $\mathcal{O}_K$ and let $\mathfrak{p}$ be a prime of K. Then the completion of K with respect to the absolute value

$$\begin{aligned} |\cdot|_{\mathfrak{p}} \colon K &\to \mathbb{R}_{\geq 0} \\ x &\mapsto (\mathcal{O}_K : \mathfrak{p})^{-v_{\mathfrak{p}}(x)} \end{aligned}$$

where $v_{\mathfrak{p}} \colon x \mapsto \max\{n \in \mathbb{Z} : x \in (\mathfrak{p})^n\}$ is denoted by $K_{\mathfrak{p}}$ and is called the $\mathfrak{p}$-*adic completion of* K or the $\mathfrak{p}$-*adic numbers*. Its valuation ring $\mathcal{O}_{K_{\mathfrak{p}}}$ is isomorphic to the inverse limit as in Example 1.2. In the special case where $K = \mathbb{Q}$ and $\mathfrak{p} = (p)$ for some rational prime p we write $K_{\mathfrak{p}} = \mathbb{Q}_p$ and $\mathcal{O}_{K_{\mathfrak{p}}} = \mathbb{Z}_p$. ■

Let K be a local field and let L/K be a finite extension of degree n. Then there is a unique extension of the absolute value of K to L and L is local with respect to this absolute value. Let ℓ and k denote the residue field of L and K respectively. Then ℓ/k is an extension of degree $f \leqslant n$, this value is the *residue class degree*. Further, let $\mathfrak{P}$ and $\mathfrak{p}$ denote the maximal ideals of the valuation rings $\mathcal{O}_L$ and $\mathcal{O}_K$, respectively. Then there is some integer $e \leqslant n$ called the *ramification index* such that

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e.$$

We have $n = ef$. We call L/K *unramified* if $e = 1$, *totally ramified* if $e = n$, *tamely ramified* if $\operatorname{char} k \nmid e$ and *wildly ramified* if $\operatorname{char} k \mid e$.

Example 1.8. Let L/K be an extension of number fields and let $\mathfrak{P}$ be a prime in L lying above a prime $\mathfrak{p}$ in K. If f denotes the residue field degree of $\mathfrak{P}/\mathfrak{p}$ and e denotes the ramification index of $\mathfrak{P}/\mathfrak{p}$, then $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is a finite extension with residue field degree f and ramification index e. ■

Let L/K be a finite Galois extension of local fields with Galois group G. Let $|\cdot|$ denote the absolute value on L which extends the absolute value on K and let $\sigma \in G$. Define the absolute value $|\cdot|_\sigma \colon x \mapsto |\sigma(x)|$. Then, since σ fixes K, $|\cdot|_\sigma$ extends the absolute value on K. By uniqueness of this extension it follows that $|\cdot| = |\cdot|_\sigma$ and hence $|\sigma(x)| = |x|$ for all $x \in L$. It follows that G preserves the absolute value on L and in particular, G preserves

$$\mathcal{O}_L = \{x \in L : |x| \leqslant 1\} \quad \text{and} \quad \mathfrak{P} = \{x \in L : |x| < 1\}.$$

Let $\Pi \in \mathcal{O}_L$ be such that $\mathfrak{P} = \Pi\mathcal{O}_L$.

Definition 1.9. Let i be non-negative integer. The i^{th} *ramification* subgroup $G_i = G_i(L/K)$ is the subgroup of G defined by

$$G_i = \{\sigma \in G : |\sigma(\alpha) - \alpha| < |\Pi|^i \text{ for all } \alpha \in \mathcal{O}_L\}.$$

The group G_0 is called the *inertia group* and G_1 is called the *wild inertia group*. ■

We thus get a filtration $G \supset G_0 \supset G_1 \supset \ldots$ of subgroups. Let $\sigma \in G \setminus \{1\}$, then there is some $\alpha \in B$ such that $\sigma(\alpha) \neq \alpha$. It follows that for i large enough, $|\sigma(\alpha) - \alpha| \geqslant |\Pi|^i$ and hence $\sigma \notin G_i$. This shows the following.

Lemma 1.10. The filtration $G \supset G_0 \supset G_1 \supset \ldots$ terminates. ■

Proposition 1.11. The G_i are normal subgroups of G. Let k and ℓ be the residue fields of K and L, respectively. Then the fixed field of G_0 is the largest unramified extension K_0 of K in L and the fixed field of G_1 is the largest tamely ramified extension K^t of K in L. Further,

$$G/G_0 \cong \mathrm{Gal}(K_0/K) \cong \mathrm{Gal}(\ell/k). \qquad \blacksquare$$

Next we switch from the local situation to the global situation and connect the two.

Let L/K be a finite Galois extension of number fields and let G denote the Galois group of this extension. Let $\mathcal{O}_L$ and $\mathcal{O}_K$ denote the ring of integers of L and K, respectively. Let $\mathfrak{p}$ be a prime in K and let $\mathfrak{P}$ be a prime in L extending $\mathfrak{p}$. Let $\sigma \in G$, then $\sigma(\mathfrak{P})$ is again a prime extending $\mathfrak{p}$. Indeed, since σ fixes K, we find that $\mathfrak{p} \subset \sigma(\mathfrak{P})$ so $\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \mathfrak{p}$. Therefore, we have a well-defined group action of G on the set of primes in L which extend $\mathfrak{p}$. An application of the Chinese remainder theorem shows that this action is transitive. Since this action is transitive it follows that all primes above $\mathfrak{p}$ are isomorphic and hence their ramification indexes and residue class degrees are equal. Let e and f denote these common values, respectively. Then if g is the amount of primes above $\mathfrak{p}$, the fundamental formula shows

$$[L : K] = gef. \tag{1.1}$$

For a prime $\mathfrak{P}$ above $\mathfrak{p}$, we define the *decomposition subgroup* $D_{\mathfrak{P}} \subset G$ of $\mathfrak{P}$ over K as

$$D_{\mathfrak{P}} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

It follows from the orbit stabilizer theorem and (1.1) that $D_{\mathfrak{P}}$ has order ef. Since the elements of $D_{\mathfrak{P}}$ fix $\mathfrak{P}$ they define an action on $\mathcal{O}_L/\mathfrak{P}$ fixing $\mathcal{O}_K/\mathfrak{p}$. In this way we get a morphism of groups

$$\pi_{\mathfrak{P}} \colon D_{\mathfrak{P}} \to \mathrm{Gal}\big((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\big).$$

Another application of the Chinese remainder theorem shows that this map is surjective. The *inertia group* $I_{\mathfrak{P}}$ of $\mathfrak{P}$ over K is the kernel of $\pi_{\mathfrak{P}}$. Thus we have an exact sequence

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow D_{\mathfrak{P}} \xrightarrow{\pi_{\mathfrak{P}}} \mathrm{Gal}\big((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\big) \longrightarrow 1.$$

From this we see that $I_{\mathfrak{P}}$ has order e and hence $I_{\mathfrak{P}}$ is non-trivial if and only if $\mathfrak{P}$ is ramified over K. The Galois group $\mathrm{Gal}\big((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\big)$ is finite, cyclic of order f, and is generated by the Frobenius automorphism which sends $x \mapsto x^q$ with $q = [\mathcal{O}_K : \mathfrak{p}]$. Since $\pi_{\mathfrak{P}}$ is surjective, there is some element of $D_{\mathfrak{P}}$ which is mapped to the Frobenius automorphism under $\pi_{\mathfrak{P}}$. Such an element is called a *Frobenius element* for $\mathfrak{P}$. Such an element is unique if $I_{\mathfrak{P}}$ is trivial i.e. when $\mathfrak{p}$ is unramified. In this case we can speak of *the* Frobenius element.

The following proposition connects the global and local Galois theory and serves as a foundation for when we move to the infinite case.

Proposition 1.12. Let L/K be a finite Galois extension of number fields. Let $\mathfrak{p}$ be a prime in K and $\mathfrak{P}$ a prime in L extending $\mathfrak{p}$. Then the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois and the restriction morphism

$$\varphi \colon \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to D_{\mathfrak{P}}$$

is an isomorphism of groups. Furthermore, the restriction of φ to the inertia group $G_0 = G_0(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is an isomorphism $G_0 \to I_{\mathfrak{P}}$. $\blacksquare$

1.3 Infinite Galois theory

In this section we take a closer look at Galois extensions of possibly infinite degree. We then combine this with the theory of the previous sections to define decomposition groups, inertia groups and Frobenius elements for $\mathrm{Gal}(\overline{K}/K)$ where K is a number field. For the second part we draw great inspiration from [61, Section 1.2].

Let L/K be a (possibly infinite) Galois extension with Galois group $\mathrm{Gal}(L/K)$. The goal of this section is to get a slightly better grasp on $\mathrm{Gal}(L/K)$ and to define the objects of the previous section in the case

where K is a number field and L is the algebraic closure $\overline{K}$ of K.

To try and understand $\mathrm{Gal}(L/K)$ we may start by studying the finite Galois sub-extensions $L/M/K$. For two finite Galois extensions M/K and M'/K in L such that $M \subset M'$, we have a natural group morphism $\varphi_{MM'} \colon \mathrm{Gal}(M'/K) \to \mathrm{Gal}(M/K)$ defined by restriction. If we have three finite Galois extensions M, M', and M'' of K contained in L such that $M \subset M' \subset M''$, then the composition

$$\mathrm{Gal}(M''/K) \xrightarrow{\varphi_{M'M''}} \mathrm{Gal}(M'/K) \xrightarrow{\varphi_{MM'}} \mathrm{Gal}(M/K)$$

is equal to $\varphi_{MM''} \colon \mathrm{Gal}(M''/K) \to \mathrm{Gal}(M/K)$. Let I denote the set of fields M such that M/K is finite Galois and $M \subset L$. Then I is a partially ordered set with respect to inclusion. The partially ordered set $(I, \subset)$ satisfies condition 1 of Section 1.1. To see this, let M and M' be fields in I, then the compositum MM' in L is Galois and $M, M' \subset MM' \subset L$. It follows that $(\mathrm{Gal}(M/K), \varphi_{MM'})_{M \in I}$ is a inverse system. Let

$$G = \varprojlim_{\substack{K \subset M \subset L \\ \text{finite Galois}}} \mathrm{Gal}(M/K)$$

denote the inverse limit. For an element $\sigma \in \mathrm{Gal}(L/K)$ we can construct a well-defined element $(\sigma|_M)_M$ of G. This gives a group morphism $\mathrm{Gal}(L/K) \to G$. In this sense, G can be viewed as the group which contains all the data of elements of $\mathrm{Gal}(L/K)$ on every finite Galois sub-extension $L/M/K$. As it turns out, this perfectly describes $\mathrm{Gal}(L/K)$.

Proposition 1.13. Let L/K be a (possibly infinite) Galois extension. Then $\mathrm{Gal}(L/K)$ is a profinite group and

$$\mathrm{Gal}(L/K) \longrightarrow \varprojlim_{\substack{K \subset M \subset L \\ \text{finite Galois}}} \mathrm{Gal}(M/K)$$

sending $\sigma \mapsto (\sigma|_M)_M$is an isomorphism of groups. ■

Example 1.14. Let $\mathbb{F}_q$ be a finite field with q elements. Let $k/\mathbb{F}_q$ be a finite Galois extension of $\mathbb{F}_q$ of degree n. Then $\mathrm{Gal}(k/\mathbb{F}_q)$ is cyclic and generated by the Frobenius endomorphism $x \mapsto x^q$. It follows that $\mathrm{Gal}(k/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. Then by Proposition 1.13, $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \lim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$. ■

By the isomorphism in Proposition 1.13 it follows that there is a natural topology on $\mathrm{Gal}(L/K)$ induced from the profinite topology. By section 1.1, the topology is generated by the sets

$$\sigma \cdot \ker(\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K))$$

where M/K is a finite Galois extension of K in L and $\sigma \in \mathrm{Gal}(L/K)$. The Galois correspondence for finite extensions extends to infinite extensions but it takes into account the topology on $\mathrm{Gal}(L/K)$.

Theorem 1.15 (Galois correspondence)**.** Let L/K be a (possibly infinite) Galois extension with Galois group G. Then there is an inclusion reversing bijection

$$\left\{\begin{array}{r}\text{Intermediate} \\ \text{extensions} \\ K \subset M \subset L\end{array}\right\} \longleftrightarrow \left\{\begin{array}{r}\text{Closed} \\ \text{subgroups} \\ H \leqslant G\end{array}\right\}$$
$$M \longmapsto \mathrm{Gal}(L/M)$$
$$L^H \longmapsfrom H.$$

Further, an intermediate extension M/K is Galois if and only if $\mathrm{Gal}(L/M)$ is normal in G. In this case we have $\mathrm{Gal}(M/K) \cong G/\mathrm{Gal}(L/M)$. ■

For an arbitrary subgroup $H \leqslant G$, the proof of Theorem 1.15 shows that L^H corresponds to the closure $\overline{H}$ of H in G via the Galois correspondence.

Example 1.16. Let $\mathbb{F}_q$ be a finite field with q elements. The Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ has an element $\mathrm{Fr} \colon x \mapsto x^q$ called the *Frobenius automorphism*. For any finite Galois extension $k/\mathbb{F}_q$, $\mathrm{Fr}|_k$ generates $\mathrm{Gal}(k/\mathbb{F}_q)$. The element Fr has infinite order in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and hence $\langle \mathrm{Fr} \rangle \cong \mathbb{Z}$. We have

$$\overline{\mathbb{F}}_q^{\langle \mathrm{Fr} \rangle} = \{x \in \overline{\mathbb{F}}_q : x^q = x\} = \mathbb{F}_q = \overline{\mathbb{F}}_q^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}.$$

In Example 1.14 we saw that $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$. Thus $\mathbb{Z}$ and $\hat{\mathbb{Z}}$ have the same fixed field. This shows that $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$ and that the topology of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ indeed needs to be taken into account. ■

Let L/K be a possibly infinite extension of local fields in characteristic 0 and let k be the residue field of K. For every finite Galois extension M/K in L let $G_0(M/K) \subset \mathrm{Gal}(M/K)$ be the inertia subgroup and let $k(M)$ denote the residue field of M. Then, by Proposition 1.11, we have an exact sequence

$$1 \longrightarrow G_0(M/K) \longrightarrow \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(k(M)/k) \longrightarrow 1.$$

Now let M, N be finite Galois extensions of K in L such that $N \subset M$. Then we have a commutative diagram with exact rows of the form

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_0(M/K) & \longrightarrow & \mathrm{Gal}(M/K) & \longrightarrow & \mathrm{Gal}(k(M)/k) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & G_0(N/K) & \longrightarrow & \mathrm{Gal}(N/K) & \longrightarrow & \mathrm{Gal}(k(N)/k) & \longrightarrow & 1. \end{array} \tag{1.2}$$

By Proposition 1.4, we have that $\mathrm{Gal}(L/K)$ arises as the inverse limit over the finite Galois extensions of K in L. Define the *inertia group* $G_0(L/K) \subset \mathrm{Gal}(L/K)$ of L/K to be

$$G_0(L/K) = \varprojlim_{\substack{K \subset M \subset L \\ \text{finite Galois}}} G_0(M/K).$$

Let ℓ denote the residue field of L. Then $\mathrm{Gal}(\ell/k)$ is isomorphic to the inverse limit of the fields $\mathrm{Gal}(k(M)/k)$ where M is a finite Galois extension of K in L. Then by Proposition 1.4 and commutativity of (1.2) we get an exact sequence

$$1 \longrightarrow G_0(L/K) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(\ell/k) \longrightarrow 1.$$

By Proposition 1.11, for a finite extension M of K in L, we have that the fixed field $M^{G_0(M/K)}$ is the largest unramified extension of K in M. From this it follows that the fixed field $L^{G_0(L/K)}$ is the largest extension of K in L which is such that if $M \subset L^{G_0(L/K)}$ is a finite extension of K then M/K is unramified. We call the field $L^{G_0(L/K)}$ is the *largest unramified extension* of K in L.

In particular, in the case where $L = \overline{K}$ we get an exact sequence

$$1 \longrightarrow G_0(\overline{K}/K) \longrightarrow \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Gal}(\overline{k}/k) \longrightarrow 1. \tag{1.3}$$

We simply call the largest unramified extension $\bar{K}^{G_0(\bar{K}/K)}$ of K in $\overline{K}$ the *largest unramified extension of* K and we denote it by K^{nr}. Considering the exact sequence (1.3), we have proven the following.

Proposition 1.17. Let K be a local field of characteristic zero. Then the maximal unramified extension K^{nr} is a Galois extension of K. We have $G_0(\overline{K}/K) = \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}})$ and

$$\mathrm{Gal}(K^{\mathrm{nr}}/K) \cong \mathrm{Gal}(\overline{k}/k).$$ ■

Now we move to the global case. Let K be a number field and let $\mathfrak{p}$ be a prime in K. Let L/K be a finite Galois extension of K and let $\mathfrak{P}$ be a prime above $\mathfrak{p}$. By, Proposition 1.12 we have that the decomposition group $D_{\mathfrak{P}}$ is isomorphic to the Galois group $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. By taking the inverse limit, we see that $\mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ is, in a canonical way, a subgroup of $\mathrm{Gal}(\overline{K}/K)$. We define the *decomposition group* $D_{\mathfrak{p}} \subset \mathrm{Gal}(\overline{K}/K)$ of $\mathfrak{p}$ to be the subgroup isomorphic to $\mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ in this way. By abuse of language, we often say that $\mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ is the decomposition subgroup of $\mathfrak{p}$. The *inertia group* $I_{\mathfrak{p}}$ of $\mathfrak{p}$ is the group $G_0(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$. Let $k_{\mathfrak{p}}$ denote the residue field of K at $\mathfrak{p}$ (equivalently, the residue field of $K_{\mathfrak{p}}$). Thus we have an exact sequence

$$1 \longrightarrow I_{\mathfrak{p}} \longrightarrow \mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}}) \xrightarrow{\pi_{\mathfrak{p}}} \mathrm{Gal}(\overline{k_{\mathfrak{p}}}/k_{\mathfrak{p}}) \longrightarrow 1$$

A *Frobenius element* of $\mathfrak{p}$ is an element $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}} = \mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ which maps to the Frobenius automorphism of $\mathrm{Gal}(\overline{k}_{\mathfrak{p}}/k_{\mathfrak{p}})$ under $\pi_{\mathfrak{p}}$ (see example 1.16). We have the following theorem regarding the density of Frobenius elements due to Cheboratev.

Theorem 1.18. (Cheboratev) Let K be a number field and S a finite set of primes of K. Then the set of elements

$$\{\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(\overline{K}/K) : \mathfrak{p} \notin S\}.$$

Is dense in $\mathrm{Gal}(\overline{K}/K)$ with respect to the profinite topology. ■

1.4 Class field theory

To conclude this section, we cover some standard results from class field theory regarding unramified extensions of number fields. Further, we state a fundamental result in Kummer theory which is relevant in multiple occasions throughout this thesis.

Let K be a field. A *place* of K is an equivalence class of absolute values on K. If L/K is an extension of fields and v is a place of K then we say that a place w of L *extends* v if there is an absolute value in w which restricts to an absolute value which is in v. The following theorem classifies places of number fields.

Theorem 1.19. (Ostrowski) Let K be a number field. Then K has exactly one place for
(i) Every prime $\mathfrak{p}$ of K;
(ii) Every real embedding $K \hookrightarrow \mathbb{R}$;
(iii) Every conjugate pair of totally complex embeddings $\sigma\colon K \hookrightarrow \mathbb{C}$ (so $\sigma(K) \not\subset \mathbb{R}$). ■

Let K be a number field. A place of K is called a *finite place* (or *finite prime*) if it corresponds to a prime, otherwise it is called a *infinite place* (or *infinite prime*). If L/K is an extension of number fields and $\mathfrak{p}$ is a prime of K corresponding to the place $v_\mathfrak{p}$, then the places of L extending $v_\mathfrak{p}$ are precisely those places that correspond to primes of L extending $\mathfrak{p}$.

We call a finite place of K *ramified* if the corresponding prime ramifies in L/K. If v is an infinite prime of K which corresponds to a real embedding $\sigma\colon K \hookrightarrow \mathbb{R}$ then we call v *ramified* if σ extends to a conjugate pair of totally complex embeddings $\sigma\colon L \hookrightarrow \mathbb{C}$. We call v *unramified* if the extension of σ to L remains a real embedding or if σ is complex.

Proposition 1.20. Let K be a number field with class group $\mathrm{Cl}(K)$. Then there exists a finite maximal abelian extension L of K such that every finite and infinite place in K is unramified in L/K. The extension L/K has Galois group $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(K)$. ■

Example 1.21. The field $K = \mathbb{Q}(\sqrt{3})$ has class number 1 so it does not have a non-trivial extension which is unramified at every place. The extension $L = \mathbb{Q}(\sqrt{3}, i)$ is an abelian extension of K such that no prime of K is ramified in L/K. The infinite places do ramify in L/K since K has 2 real embeddings whilst L has 2 conjugate pairs of totally complex embeddings. ■

In Example 1.21 we see that the condition on the infinite places is strictly necessary. However, if we relax the condition on the infinite places, we still get something tangible in this case. This turns out to be more generally true.

Proposition 1.22. Let K be a number field. There exists a finite maximal abelian extension L of K such that every finite prime in K is unramified in L/K. ■

Definition 1.23. Let K be a number field and let L/K be the finite maximal abelian extension of K such that every finite prime is unramified. The *narrow class number* h_K^+ of K is the degree of L/K. ■

Example 1.24. Let L/K be as in Example 1.21. Then, h_K^+ is at least 2 since L/K is unramified outside of the infinite places. Using a description of the narrow class number in terms of the class group of K it can be shown that $h_K^+ = 2$. Hence, L/K is the largest abelian extension of K which is unramified at every prime in K. ■

Finally, we state without proof a fundamental result from Kummer Theory.

Proposition 1.25. Let K be a field such that $\zeta_n \in K$. If L/K is a Galois extension of K such that $\mathrm{Gal}(L/K) = \mathbb{Z}/n\mathbb{Z}$. Then $L = K(\alpha^{1/n})$ where $\alpha \in K$ is such that $\alpha^{1/d} \notin K$ for any proper divisor d of n. ■

2 Elliptic curves

The modular method makes heavy use of elliptic curves and the body of known results related to them. The first two parts of this section we recall and state the standard definitions and results which are relevant to us. The second part is about the reduction of elliptic curves over local fields. The last part of this section connects the local and global theory and defines the conductor of an elliptic curve.

2.1 Basic definitions

We briefly recall some definitions and results relating to elliptic curves. We are mostly working over a general field K but for the purposes of this thesis, K is usually a number field, a finite field or local field of characteristic 0. By a variety V over K we mean all the points in $\overline{K}$ satisfying the equations defining V and for an extension L/K we let $V(L)$ denote the L-points of V. By a curve we mean a variety of dimension 1.

Definition 2.1. Let K be a field. A non-singular projective curve E/K is called an elliptic curve if its genus is 1 and if E has a K-rational point. ■

We can construct an elliptic curve from a *Weierstrass equation* as follows. Given elements $a_1, \ldots, a_6 \in K$ we define a projective curve in $\mathbb{P}^2_K$ given by the Weierstrass equation

$$E\colon Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

This projective curve has a K-rational point $O = [0 : 1 : 0]$ and has no other points where $Z = 0$ so we often write a Weierstrass equation in the form

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Note that E has genus 1 so E is an elliptic curve if and only if it is non-singular. Define the quantities associated to E,

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.
\end{aligned}$$

The value Δ is called the *discriminant* of E and j is called the *j-invariant* of E.

Proposition 2.2. Let E be a curve given by a Weierstrass equation with discriminant Δ and c_4 as above. Then
(a) E is non-singular if $\Delta \neq 0$;
(b) E has a nodal singularity if and only if $\Delta = 0$ and $c_4 \neq 0$;
(c) E has a cuspidal singularity if and only if $\Delta = c_4 = 0$.
In any case, E has at most one singular point. ■

We see that a curve defined by a Weierstrass equation is an elliptic curve if and only if its discriminant $\Delta \neq 0$. In fact, the converse is also true, given an Elliptic curve E/K with K-rational point P then there exists a K-isomorphism from E to a curve defined by a Weierstrass equation which sends P to $O = [0 : 1 : 0]$.

Given a curve E/K defined by a Weierstrass equation with coefficients $a_1, \ldots, a_6 \in K$. By making a coordinate transformation $x = u^2X$ and $y = u^3Y$ for some $u \in K^\times$ we obtain a new Weierstrass equation with coefficients

$$\begin{aligned}
a_i' &= u^{-i}a_i \\
c_i' &= u^{-i}c_i \\
\Delta' &= u^{-12}\Delta \\
j' &= j.
\end{aligned}$$

Let E be a curve given by a Weierstrass equation and let E_{ns} denote all the non-singular points of E. By the paragraph above, if the discriminant Δ of E is non-zero then $E_{\text{ns}} = E$ and E is an elliptic curve, otherwise E_{ns} is E with a point removed. It is well known that E_{ns} has the structure of an abelian group, this can be seen from the fact that the embedding of E_{ns} into its Jacobian $\text{Pic}^0(E_{\text{ns}})$ via $P \mapsto [P - O]$ is surjective. Alternatively, the group law on E is given geometrically by rational equations over K, i.e. the group law $E_{\text{ns}} \times E_{\text{ns}} \to E_{\text{ns}}$ and inversion $E_{\text{ns}} \to E_{\text{ns}}$ are morphism over K. This turns E_{ns} into an abelian variety. If E has a singular point, then the structure of E_{ns} is quite simple.

Proposition 2.3. Let E/K be given by a Weierstrass equation and suppose that E has a singular point. Then if E has a nodal singularty we have an isomorphism $E_{\text{ns}} \cong \bar{K}^\times$ of abelian groups. If E has a cuspidal singularity then $E_{\text{ns}} \cong \bar{K}^+$ as abelian groups. ■

Let E/K be an elliptic curve, then E is not only an abelian group but also carries the structure of a $\text{Gal}(\overline{K}/K)$-module, that is, there is an action of $\text{Gal}(\overline{K}/K)$ on E which is compatible with the group law on E. Fix some Weierstrass coordinates for E, let $P = (x, y) \in E$ and let $\sigma \in \text{Gal}(\overline{K}/K)$. Then the action of σ on P is $P^\sigma = (\sigma(x), \sigma(y))$. This is well defined since E is defined over K and this is compatible with the group law on E since the group law is defined over K.

Definition 2.4. Let E_1/K and E_2/K be elliptic curves with distinguished K-rational points O_1 and O_2, an *isogeny* $E_1 \to E_2$ is a morphism $E_1 \to E_2$ sending O_1 to O_2. We say that two elliptic curves defined over K are *isogenous* if there exists and isogeny between them. An isogeny is a *K-rational isogeny* if it is an defined over K. ■

An isogeny $\varphi\colon E_1 \to E_2$ of elliptic curves induces a homomorphism between the Jacobians $\text{Pic}^0(E_1) \to \text{Pic}^0(E_2)$ compatible with the isomorphisms identifying E_1 and E_2 with their Jacobian. From this it follows that φ is a group homomorphism. We define the *degree* $\deg\varphi$ *of* φ to be the degree of the extension of function fields $K(E_1)/\varphi^*K(E_2)$. We say that φ is an m-isogeny if its degree is equal to m. If $\varphi\colon E_1 \to E_2$ is an m-isogeny, then

$$\varphi^{-1}(O_2) = \ker\varphi$$

has at most $\deg\varphi = m$ elements. If the extension $K(E_1)/\varphi^*K(E_2)$ is separable, then we say that φ is *separable*. In this case, $\ker\varphi$ has exactly m elements.

Example 2.5. 1. Let E/K be an elliptic curve. Let $m > 0$ be a positive integer and let $[m]\colon E \to E$ denote the morphism that takes a point $P \in E$ and sends it to P summed to itself m times. Define $[-m]$ to be the morphism which sends P to $[m](-P)$. Since the inversion and addition laws on E are defined over K, the map $[m]\colon E \to E$ is a K-rational isogeny for every $m \in \mathbb{Z}$ where we define $[0]$ to be the constant isogeny.

2. Let $\mathbb{F}_q$ be a finite field and let $E/\mathbb{F}_q$ be an elliptic curve. The $\mathbb{F}_q$-rational isogeny $\varphi\colon E \to E$ sending $(x, y) \mapsto (x^q, y^q)$ is called the Frobenius morphism and has degree q. The Frobenius morphism indeed maps to E since the coefficients of E are fixed under $x \mapsto x^q$. Since $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is topologically generated by $x \mapsto x^q$ (i.e. it generates a dense subgroup of $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$), a point $P \in E$ is defined over $\mathbb{F}_q$ if and only if $\varphi(P) = P$. ■

Every isogeny $\varphi\colon E_1 \to E_2$ of degree d has a dual isogeny $\hat{\varphi}\colon E_2 \to E_1$ such that $\varphi\hat{\varphi} = \hat{\varphi}\varphi = [d]$, this can be used to show that the isogeny $[m]\colon E \to E$ has degree m^2. If in addition $[m]$ is separable then $\#\ker[m] = m^2$. Note that $\ker[m]$ is simply the m-torsion of E which we denote by $E[m]$. For every d dividing m we have $\#E[d] = d^2$. Some group theory then shows that

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}. \tag{2.1}$$

The precise characterization of the kernel of $[m]$ is as follows.

Proposition 2.6. Let m be a positive integer and E/K an elliptic curve, if the characteristic of K is 0 or coprime to m then $[m]$ is separable and we have (2.1). If the characteristic of K is equal to $p > 0$, then $E[p^e]$ is equal to $\{O\}$ or isomorphic to $\mathbb{Z}/p^e\mathbb{Z}$ for all positive integers e. ■

For a positive integer m coprime to $\text{char}\, K$, it is tempting to think of $E[m]$ as the abstract group $(\mathbb{Z}/m\mathbb{Z})^2$, however, $E[m]$ carries the structure of a $\text{Gal}(\overline{K}/K)$-module. Indeed, for a point $P \in E[m]$ we have

$$[m](P^\sigma) = ([m]P)^\sigma = O^\sigma = O$$

so $\mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$. Let ℓ be a prime different from the characteristic of K and let n be a positive integer. We have a surjective homomorphism $[\ell]\colon E[\ell^{n+1}] \to E[\ell]$ which is compatible with the $\mathrm{Gal}(\overline{K}/K)$-action on $E[\ell^{n+1}]$ and $E[\ell^n]$. We have that

$$\begin{array}{ccc} E[\ell^{n+1}] & \xrightarrow{\sim} & (\mathbb{Z}/\ell^{n+1}\mathbb{Z})^2 \\ \downarrow{\scriptstyle [\ell]} & & \downarrow \\ E[\ell^n] & \xrightarrow{\sim} & (\mathbb{Z}/\ell^n\mathbb{Z})^2 \end{array}$$

commutes. Here, the horizontal maps are the isomorphisms in (2.1). Thus we have an inverse system

$$\ldots \longrightarrow E[\ell^3] \longrightarrow E[\ell^2] \longrightarrow E[\ell]$$

which is isomorphic to the inverse system defined by the $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. We call the inverse limit of this system the *Tate module* which we denote by $T_\ell(E)$. Since $E[\ell^n]$ has the structure of an $\mathbb{Z}/\ell^n\mathbb{Z}$-module for every n, it follows from Example 1.7 that the Tate module $T_\ell(E)$ has the structure of a $\mathbb{Z}_\ell$-module. We also obtain the isomorphism

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell \tag{2.2}$$

of $\mathbb{Z}_\ell$-modules. Since the action of $\mathrm{Gal}(\overline{K}/K)$ on $T_\ell(E)$ is compatible with the transition maps of the $E[\ell^n]$, the abelian group $T_\ell(E)$ is a $\mathrm{Gal}(\overline{K}/K)$-module.

Let E_1/K and E_2/K be elliptic curves over K and let $\varphi\colon E_1 \to E_2$ be an isogeny, since φ is a homomorphism of groups, we can restrict φ as $\varphi\colon E_1[m] \to E_2[m]$ for every $m \in \mathbb{Z}_{>0}$ from this it follows that for a prime ℓ, φ induces a $\mathbb{Z}_\ell$-module homomorphism $\varphi_\ell\colon T_\ell(E_1) \to T_\ell(E_2)$. In the special case where $E = E_1 = E_2$, we can take the trace and determinant of φ_ℓ. To get a proper grip on these quantities we need the Weil pairing (see Proposition 3.14). With such a gadget we get the following result.

Proposition 2.7. Let E/K be an elliptic curve, $\varphi\colon E \to E$ an isogeny and ℓ a prime distinct from the characteristic of K. The trace and determinant of the induced map $\varphi_\ell\colon T_\ell(E) \to T_\ell(E)$ on the Tate modules are given by

$$\det \varphi_\ell = \deg \varphi \quad \text{and} \quad \operatorname{Tr} \varphi_\ell = 1 + \deg \varphi - \deg(1 - \varphi).$$

In particular, the trace and determinant of φ_ℓ are independent of ℓ. ■

Example 2.8. Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field of characteristic p. Let $\varphi\colon E \to E$ be the Frobenius endomorphism. In Example 2.5 it is shown that φ has degree q and that a point $P \in E$ is defined over $\mathbb{F}_q$ if and only if $\varphi(P) = P$, this is equivalent to asking $P \in \ker(1 - \varphi)$. The map $1 - \varphi$ is separable and hence

$$\#\ker(1 - \varphi) = \deg(1 - \varphi) = \#E(\mathbb{F}_q).$$

Let ℓ be a prime distinct from p, then by the previous proposition,

$$\operatorname{Tr} \varphi_\ell = 1 + q - \#E(\mathbb{F}_q).$$

This quantity is called the *trace of Frobenius* and is of significance when studying the Galois representation associated to $T_\ell(E)$ as in Section 3.3. ■

We finish this section by explaining complex multiplication. Given two isogenies φ and ψ mapping $E \to E$, we can add φ and ψ to obtain a new isogeny $\varphi + \psi$ defined by sending $P \mapsto \varphi(P) + \psi(P)$. We can also compose isogenies $E \to E$ to obtain a new isogeny. Addition and composition gives a ring structure on the set of endomorphisms $\mathrm{End}(E)$ of E (i.e. the isogenies $E \to E$). The isogenies $[m]\colon E \to E$ with $m \in \mathbb{Z}$ are elements of $\mathrm{End}(E)$. These elements are such that they give an embedding $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ of rings. Very often this embedding is an isomorphism. In the cases where it is not we say that E has *complex multiplication*. The following is a way to detect when an elliptic curve does not have complex multiplication when K is a number field. This is useful when we are trying to apply, for example, Serre's irreducibility theorem. This theorem requires the elliptic curve it describes to not have complex multiplication. We use this result in Section 4.3.

Proposition 2.9. Let E/K be an elliptic curve over a number field with ring of integers $\mathcal{O}_K$, then if E has complex multiplication then the j-invariant of E is an element of $\mathcal{O}_K$. ■

2.2 Reduction of Elliptic curves

Let K be a local field of characteristic 0 with valuation v, valuation ring $\mathcal{O}_K$, residue field k and uniformizer π, i.e. $v(\pi) = 1$. Let E/K be an elliptic curve given by a Weierstrass equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with associated constants c_4, c_6 and Δ. By making a coordinate transformation

$$(x, y) \mapsto \big((\pi^k)^2x, (\pi^k)^3y\big)$$

the discriminant Δ changes as $\Delta \mapsto \pi^{-12k}\Delta$. We say that a Weierstrass equation for E is *minimal* if $a_i \in \mathcal{O}_K$ for all i and $v(\Delta)$ is minimized. Via coordinate transformations, $v(\Delta)$ can only be changed by multiples of 12, therefore, if the a_i are elements of $\mathcal{O}_K$ and $v(\Delta) < 12$, it follows that the equation is minimal. Similarly, if the a_i are elements of $\mathcal{O}_K$, it follows that the constants c_4 and c_6 are elements of $\mathcal{O}_K$. Similarly, under the coordinate transformation above, the associated quantities c_4 and c_6 change as $c_4 \mapsto \pi^{-4k}c_4$ and $c_6 \mapsto \pi^{-6k}c_6$. By a similar argument we get the following result.

Proposition 2.10. Let E/K be an elliptic curve given by a Weierstrass equation with coefficients $a_i \in K$. Then E is minimal if the a_i are elements of $\mathcal{O}_K$ and either $v(c_4) < 4$, $v(c_6) < 6$ or $v(\Delta) < 12$. Further, a minimal Weierstrass equation for E/K is unique up to isomorphism. ■

Given a minimal Weierstrass equation for E/K, we can reduce the coefficients of E to obtain a new curve $\tilde{E}/k$ given by a Weierstrass equation over k with associated quantities given by reducing the associated quantities of E. It follows from Proposition 2.2 that $\tilde{E}/k$ is an elliptic curve if and only if $v(\Delta) = 0$. Inspecting Proposition 2.2 and Proposition 2.3 we obtain the following.

Proposition 2.11. Let E/K be an elliptic curve with associated quantities Δ and c_4. Let $\tilde{E}/k$ denote the reduction of E.
(a) $\tilde{E}$ is an elliptic curve if and only if $v(\Delta) = 0$;
(b) $\tilde{E}$ has a nodal singularity if and only if $v(\Delta) > 0$ and $v(c_4) = 0$. In this case, we have

$$\tilde{E}_{\mathrm{ns}}(\bar{k}) \cong \bar{k}^{\times};$$

(c) $\tilde{E}$ has a cuspidal singularity if and only if $v(\Delta) > 0$ and $v(c_4) > 0$. In this case,

$$\tilde{E}_{\mathrm{ns}}(\bar{k}) \cong \bar{k}^{+}.$$ ■

In case (a), we say that E/K has *good reduction* and in case (b) and (c) we say that E has *bad reduction*. More specifically, in case (b) we say that E has *multiplicative reduction* and if, in addition, the slopes of E at the singularity of $\tilde{E}$ are in k we say that E has *split multiplicative reduction*. In case (c) we say that E has *additive reduction*.

Though less standard, in the case of multiplicative reduction, it can be read off from the coefficient c_6 whether or not the reduction is split or not.

Proposition 2.12. [11, Lemma 2.2] Let E/K be an elliptic curve with multiplicative reduction and suppose char $k \neq 2$. Then E/K has split multiplicative reduction if and only if $-c_6$ is a square in $K^{\times}$ (or, equivalently, the reduction of $-c_6$ in $k^{\times}$ is a square). ■

Example 2.13. 1. Let K be a local field with odd residue characteristic. The elliptic curve E_1/K given by Weierstrass equation

$$E_1\colon y^2 = x^3 + x^2 + a$$

with $a \in \mathcal{O}_K$ has multiplicative reduction if and only if $v(a) > 0$ and good reduction otherwise.

2. The elliptic curve E_2/K given by Weierstrass equation

$$E_2\colon y^2 = x^3 + \pi.$$

has has additive reduction. ■

Given an extension L/K of local fields, we can consider an elliptic curve E/K as an elliptic curve E/L. A natural question arises: how does the reduction of E/L relate to the reduction E/K?

Proposition 2.14. Let E/K be an elliptic curve and let L/K be a finite extension. Then
(a) If L/K is unramified then the reduction type of E/L is the same as that of E/K.
(b) If E/K has good or multiplicative reduction then so does E/L.
(c) There is a finite extension M/K of K such that E/K has either good or multiplicative reduction. ■

From Proposition 2.14 it follows that the reduction type an elliptic curve E/K can only change under field extensions if E/K has additive reduction. Moreover, if E/K has additive reduction then the reduction type is guaranteed to change under some field extension. If the reduction of E/K becomes good over some field extension we say that E/K has *potentially good reduction*. Similarly, if E/K attains multiplicative reduction over some extension of K we say that E/K has *potentially multiplicative reduction*.

Proposition 2.15. Let E/K be an elliptic curve with j-invariant j. Then E/K has potentially good reduction if and only if $v(j) \geqslant 0$. ■

Since E/K either has potential good or potentially multiplicative reduction, it follows immediately from Proposition 2.15 that E/K has potential multiplicative reduction if and only if $v(j) < 0$.

Example 2.16. Let E_2/K be as in example 2.13.2 and let $L = K(\sqrt[6]{\pi})$. Then E_2/L has good reduction. Indeed, the coordinate transformation

$$(x, y) \mapsto (\sqrt[3]{\pi}\, x, \sqrt{\pi}\, y)$$

gives a minimal Weierstrass equation for E_2/L with good reduction. Thus, E_2/K has potentially good reduction. ■

Due to the 'stable' nature of good and multiplicative reduction under field extensions, this type of reduction is referred to as *semi-stable reduction*.

Consider a point $P = (x : y : z) \in \mathbb{P}^2_K(K)$. There is a unique representative of P such that x, y and z are all elements of $\mathcal{O}_K$ and such that at least one of them is an element of $\mathcal{O}_K^\times$. Given such a representative $(x_0 : y_0 : z_0)$ of P, we can reduce x_0, y_0 and z_0 modulo π to get a point $\tilde{P} = (\tilde{x}_0 : \tilde{y}_0 : \tilde{z}_0)$ in $\mathbb{P}^2_k(k)$. In this way we get a map

$$\mathbb{P}^2_K(K) \to \mathbb{P}^2_k(k).$$

Let E/K be an elliptic curve given by a Weierstrass equation and suppose that $P \in E(K) \subset \mathbb{P}^2_K(K)$. Then the point $\tilde{P}$ satisfies the reduced Weierstrass equation of $\tilde{E}/k$ and hence $\tilde{P} \in \tilde{E}(k)$. We obtain a map

$$E(K) \to \tilde{E}(k). \tag{2.3}$$

If $\tilde{E}$ is non-singular then $\tilde{E}(k)$ is a group and the reduction map (2.3) is a group homomorphism. More generally, define

$$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{\text{ns}}(k)\}$$
$$E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{O}\}.$$

Then we have the following result.

Proposition 2.17. The sequence

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{\text{ns}}(k) \longrightarrow 0$$

is exact sequence of abelian groups. ■

The final result we cover is the criterion of Néron-Ogg-Shafarevich. Let $G_0(\overline{K}/K) = \text{Gal}(\overline{K}/K^{\text{nr}})$ be the inertia subgroup of $\text{Gal}(\overline{K}/K)$ and let Ω be a set on which $\text{Gal}(\overline{K}/K)$ acts. We say that Ω is *unramified* if $G_0(\overline{K}/K)$ acts trivially on Ω.

Theorem 2.18. (Criterion of Néron-Ogg-Shafarevich) Let E/K be an elliptic curve. The following are equivalent:
(a) E has good reduction;
(b) $E[m]$ is unramified for all integers $m \geqslant 1$ relatively prime to char k;
(c) The Tate module $T_\ell(E)$ is unramified for all primes $\ell \neq$ char k. ■

Let $m \geqslant 1$ be an integer and let $L = K(E[m])$ be the field obtained by adjoining all coordinates of points in $E[m]$ to K. Then L/K is Galois. Indeed, L/K is separable and L/K is normal. To see that L/K is normal note that this is equivalent to requiring that every field morphism $\sigma\colon L \to \overline{K}$ with $\sigma|_K = \mathrm{id}_K$ is such that $\sigma(K(E[m])) \subset K(E[m])$. This requirement is satisfied since $\mathrm{Gal}(\overline{K}/K)$ defines a group action on $E[m]$. Therefore L/K is Galois. The action of $\mathrm{Gal}(\overline{K}/K)$ on $E[m]$ factors through $\mathrm{Gal}(L/K)$ and hence the action of the inertia group $G_0(\overline{K}/K)$ factors through the inertia group $G_0(L/K)$. If E/K has good reduction then it follows from Proposition 2.18 that the action of $G_0(\overline{K}/K)$ on $E[m]$ is trivial. Therefore, the action of $G_0(L/K)$ is trivial on $E[m]$ and hence also on L/K. It follows that $G_0(L/K) = 1$ and L/K is unramified. Studying this extension L/K may seem artificial but this turns out to be a beneficial way to look at the reduction of an elliptic curve, even when there is bad reduction.

The study of elliptic curves and their reduction over local fields is mainly to study elliptic curves over global fields. The connection between the two is as follows. Let K be a number field (a global field in characteristic 0) and let E/K be an elliptic curve over K. For every prime $\mathfrak{p}$ of K we form the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$. Then via the inclusion $K \hookrightarrow K_\mathfrak{p}$ we can view E as an elliptic curve defined over $K_\mathfrak{p}$. The field $K_\mathfrak{p}$ is local so all the theory in this section applies. For any property that $E/K_\mathfrak{p}$ satisfies (good reduction, for example) we say that E/K satisfies this property *at* $\mathfrak{p}$ (good reduction at $\mathfrak{p}$, for example).

2.3 The conductor of an elliptic curve

Let K be a number field with ring of integers $\mathcal{O}_K$ and let E/K be an elliptic curve given by a Weierstrass equation with coefficients in $\mathcal{O}_K$. There are only finitely many primes $\mathfrak{p}$ of K such that $E/K_\mathfrak{p}$ has bad reduction. Indeed, by Proposition 2.11, if there is bad reduction at $\mathfrak{p}$ then $\mathfrak{p}$ necessarily divides the discriminant of E. It is often convenient to record the primes of bad reduction and which reduction type occurs at this prime. The conductor captures this idea. The following definition of the conductor often occurs in the literature.

'Definition' 2.19. Let E/K be an elliptic curve over a number field K. The *conductor* $\mathcal{N}_E$ *of* E is the ideal

$$\mathcal{N}_E = \prod_\mathfrak{p} \mathfrak{p}^{f(\mathfrak{p})}$$

where, if E/K does not have additive reduction at $\mathfrak{p}$ or if $\mathfrak{p}$ does not divide 2 or 3,

$$f(\mathfrak{p}) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } \mathfrak{p} \\ 1 & \text{if } E \text{ has multiplicative reduction at } \mathfrak{p} \\ 2 & \text{if } E \text{ has additive reduction at } \mathfrak{p} \end{cases}$$

and when $\mathfrak{p}$ lies above 2 or 3 and E has additive reduction, $f(\mathfrak{p})$ is some integer such that $2 \leqslant f(\mathfrak{p}) \leqslant 2 + 3v_\mathfrak{p}(3) + 6v_\mathfrak{p}(2)$. ■

This definition of the conductor does a good job of recording what kind of reduction occurs at the primes. However, when $\mathfrak{p}$ lies above 2 or 3, there is some mystery as to what power of $\mathfrak{p}$ occurs in $\mathcal{N}_E$. This allures to the idea that the conductor of an elliptic curve has some deeper meaning. In the next two sections we aim to explain this mystery, both in an arithmetic and geometric way, and we define the conductor of an elliptic curve properly.

2.3.1 Minimal proper regular model for curves

Let K be a number field with ring of integers $\mathcal{O}_K$ and let E/K be an elliptic curve. For any prime $\mathfrak{p}$ of K we can reduce E modulo $\mathfrak{p}$ to obtain a new curve over $\mathcal{O}_K/\mathfrak{p}$. A natural question arises: is there an object which stores the data of E and of all the reductions of E? A well-chosen equation of E with coefficients in $\mathcal{O}_K$ defines a scheme $\mathcal{E} \to \operatorname{Spec} \mathcal{O}_K$ over $\mathcal{O}_K$ such that its generic fiber is E/K and its special fibers are the reductions. There are many ways of choosing this scheme, we wish to have a 'minimal', or, 'canonical' choice of $\mathcal{E}$. In this section we aim to define such an object. As a result we obtain more insight on the reduction of an elliptic curve.

In this section we introduce the required technical definitions and we introduce this 'minimal' choice for curves over the field of fractions of a Dedekind domain. Finally we write down the classification done

by Kodaira and Néron of the special fiber of the minimal model of an elliptic curve. The abstract theory covered in this section comes back in Section 3.5 when discussing the Néron model of an elliptic curve.

A Noetherian scheme X over a ring A such that $X \to \operatorname{Spec} A$ is of finite type is *proper* if for every valuation ring R with field of fractions K and morphisms

$$\begin{array}{ccc} \operatorname{Spec} K & \longrightarrow & X \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \longrightarrow & \operatorname{Spec} A \end{array}$$

there exists a unique morphism $\operatorname{Spec} R \to X$ making the diagram commute. The notion of properness tries to capture completeness of a scheme X. In the definition we have a inclusion of a point $\operatorname{Spec} K \to X$ over A which is dense in the two point space $\operatorname{Spec} R$. Being proper then means that there is a unique way of extending $\operatorname{Spec} K \to X$ to a morphism $\operatorname{Spec} R \to X$.

Let X be a scheme and $x \in X$ be a point. Let $\mathcal{O}_{X,x}$ denote the local ring at x and $\mathfrak{m}_x$ the maximal ideal of $\mathcal{O}_{X,x}$. A scheme X is said to be *regular at* x if the dimension of $\mathfrak{m}_x/\mathfrak{m}_x^2$ as a $\mathcal{O}_{X,x}/\mathfrak{m}_x$-vector space is equal to the Krull dimension of the local ring $\mathcal{O}_{X,x}$. A scheme X is said to be *regular* if it is regular at every point $x \in X$. Considering [22, Theorem I.5.1], the notion of a scheme being regular at a point extends the idea of being non-singular at a point of a variety. An example of a regular scheme is the affine scheme $X = \operatorname{Spec} R$ where R is a Dedekind domain. Indeed, for closed points $\mathfrak{p}$ of X, the local rings $R_\mathfrak{p}$ are discrete valuation rings and hence have Krull dimension equal to 1. Further, if $\mathfrak{m}_\mathfrak{p} \subset R_\mathfrak{p}$ is the maximal ideal at $\mathfrak{p}$, then a characterization of being a discrete valuation ring is that the dimension of $\mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2$ is equal to 1 as an $R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$-vector space.

Let $\varphi\colon X \to S$ be a morphism of finite type, let $x \in X$ and set $s = \varphi(x) \in S$. The map φ is *smooth at a point* $x \in X$ if there are affine open neighborhoods

$$s \in \operatorname{Spec} R \subset S \quad \text{and} \quad x \in \operatorname{Spec} A \subset X$$

with $A = R[t_1, \dots, t_{n+r}]/(f_1, \dots, f_n)$ for some $f_i \in R[t_1, \dots, t_{n+r}]$ so that the $n \times n$ minors of the Jacobian $(\partial f_i/\partial t_j)$ generate the unit ideal in A. We say that φ is smooth if it is smooth at every point $x \in X$. The most important application of smooth morphism is the case where $S = \operatorname{Spec} R$. By considering the definition of a non-singular variety it follows that if $X \to \operatorname{Spec} R$ is smooth, then for any maximal ideal $\mathfrak{p} \in \operatorname{Spec} R$, the variety $X_\mathfrak{p}$ is non-singular.

The next definition is somewhat imprecise since the proper definition requires some technical definitions which would lead us too far astray from our purposes. The definition we give here is more than sufficient for what we wish to cover. For the full definition, we refer the reader to the very expansive source [35, Definition 8.3.14].

Definition 2.20. Let R be Dedekind domain with field of fractions K. An *arithmetic surface over* R is a scheme $\mathcal{C}$ over R satisfying a handful of technical conditions, whose generic fiber is a non-singular projective curve C/K and whose special fibers are unions of curves over the corresponding residue field. ■

An arithmetic surface $\mathcal{C}$ over a Dedekind domain R need not be smooth; it is not required that a special fiber of $\mathcal{C}$ is non-singular. In other words, for $\mathfrak{p} \in \operatorname{Spec} R$, there may be points of $\mathcal{C}_\mathfrak{p} \subset \mathcal{C}$ which are not smooth (i.e. non-singular).

Example 2.21. Define the arithmetic surface $\mathcal{C} \subset \mathbb{P}^2_\mathbb{Z}$ as the closed subscheme defined by the minimal Weierstrass equation

$$\mathcal{C}\colon y^2 + xy + y = x^3 - x^2 - x.$$

Then the generic fiber of $\mathcal{C}$ is the elliptic curve $E/\mathbb{Q}$ defined by the same equation and with discriminant $\Delta_E = 17$. By Proposition 2.11 it follows that the fibers $\mathcal{C}_p$ are non-singular and hence elliptic curves for primes $p \neq 17$. For the prime $p = 17$ we find that $\mathcal{C}_p$ is a curve with a nodal singular point. ■

The definition of an arithmetic surface ensures that, in general, an arithmetic surface only has finitely many points which are not regular. It follows that an arithmetic surface is regular in codimension one as in [22, Chapter II.6]. Therefore, we have a notion of Weil divisors on $\mathcal{C}$ and for every irreducible curve $F \subset \mathcal{C}$ with generic point η, we have that the local ring $\mathcal{O}_{\mathcal{C},\eta}$ is a discrete valuation ring with field of fractions equal to the function field of $\mathcal{C}$. We denote the corresponding normalized discrete valuation by ord_F.

Following [51, Section IV.4], let $\pi\colon \mathcal{C} \to \operatorname{Spec} R$ be an arithmetic surface over a Dedekind domain R. Let $\mathfrak{p} \in \operatorname{Spec} R$ be a maximal ideal and let $k_\mathfrak{p} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ denote the residue field. Then as seen in Example 2.21, the fiber $\mathcal{C}_\mathfrak{p}/k_\mathfrak{p}$ may be singular. We can write $\mathcal{C}_\mathfrak{p}$ as a union of irreducible curves and multiplicities. This is done as follows. Let $u \in R$ be such that $v_\mathfrak{p}(u) = 1$. Then $u \circ \pi$ is a rational function on $\mathcal{C}$ and

$$\mathcal{C}_\mathfrak{p} = \bigcup_{F \subset \mathcal{C}_\mathfrak{p}} \mathrm{ord}_F(u \circ \pi) F$$

where the union is taken over the irreducible curves $F \subset \mathcal{C}_\mathfrak{p}$.

Let K be the field of fractions of a Dedekind domain R. Given a curve C/K and an arithmetic surface $\mathcal{C}/R$ with generic fiber C/K. We want $\mathcal{C}/R$ to be large enough such that no information gets lost, i.e. we want the R-valued points of $\mathcal{C}$ to correspond to the K-valued points of C. More generally, if $\mathcal{C}^0 \subset \mathcal{C}$ is the largest subscheme of $\mathcal{C}$ such that $\mathcal{C}^0 \to \operatorname{Spec} R$ is smooth, then in some situations (as in Section 3.5, for example) we might want the R-valued points of $\mathcal{C}^0$ to be equal to the R-valued points of $\mathcal{C}$. The technical restrictions we have to put on $\mathcal{C}$ to ensure this are as follows.

Proposition 2.22. [51, Corollary IV.4.4] Let R be a Dedekind domain and let K be its field of fractions. Let $\mathcal{C}/R$ be an arithmetic surface with generic fiber C/K. If $\mathcal{C}$ is proper over R, then $C(K) = \mathcal{C}(R)$. If $\mathcal{C}$ is regular, then $\mathcal{C}(R) = \mathcal{C}^0(R)$ ■

Proof. Suppose that $\mathcal{C}$ is proper over R. Then by taking the fiber product we get an injective map $\mathcal{C}(R) \hookrightarrow C(K)$. This map is injective since if two maps agree on the dense subset $\operatorname{Spec} K \subset \operatorname{Spec} R$ then they agree on $\operatorname{Spec} R$. Suppose we are given a point $P \in C(K)$. Then for any maximal ideal $\mathfrak{p} \in \operatorname{Spec} R$ we get that $R_\mathfrak{p}$ is a discrete valuation ring. Using the projection $C \to \mathcal{C}$ we get a commutative diagram

$$\begin{array}{ccccc} \operatorname{Spec} K & \xrightarrow{P} & C & \longrightarrow & \mathcal{C} \\ \downarrow & & & & \downarrow \\ \operatorname{Spec} R_\mathfrak{p} & & \longrightarrow & & \operatorname{Spec} R. \end{array}$$

Since $\mathcal{C}$ is assumed to be proper over R, this gives a unique map $\sigma_{P,\mathfrak{p}}\colon \operatorname{Spec} R_\mathfrak{p} \to \mathcal{C}$. Gluing then gives a unique map $\operatorname{Spec} R \to \mathcal{C}$. It follows that the natural map $\mathcal{C}(R) \hookrightarrow C(K)$ is a bijection. Secondly, let $\mathcal{C}/R$ be regular. By Proposition IV.4.3 of [51], if $\mathcal{C}/R$ is regular and $P \in \mathcal{C}(R)$ then $\mathcal{C}_\mathfrak{p} \subset \mathcal{C}$ is non-singular at $P(\mathfrak{p})$ (note that P is a morphism over $\operatorname{Spec} R$ where $\operatorname{Spec} R \to \operatorname{Spec} R$ is understood to be the identity, so $P(\mathfrak{p})$ indeed lies in $\mathcal{C}_\mathfrak{p}$). This concludes the proof. □

Let R be a Dedekind domain with field of fractions K. The previous paragraph motivates the following result which states that for a given non-singular projective curve C/K there exists a arithmetic surface which is proper and regular whose generic fiber is equal to C/K. Further, there exists an optimal such arithmetic surface. Néron investigated this result for the specific case where the genus of C is equal to one in [39]. The higher genus cases were proven by Lichtenbaum and Shafarevich in [32] and [48]. Combining these results with the theory of resolutions of singularities developed by Abhyankar [1, 2] and Lipman [34, 33] gives the following result.

Theorem 2.23. [51, Theorem IV.4.5] Let R be a Dedekind domain with field of fractions K, and let C/K be a non-singular projective curve of genus g.
(a) There exists a regular arithmetic surface $\mathcal{C}/R$ which is proper over R and whose generic fiber is isomorphic to C/K. We call $\mathcal{C}$ a *proper regular model for* C/K
(b) Assume that $g \geqslant 1$. Then there exists a proper regular model $\mathcal{C}^{\min}/R$ for C/K which is minimal in the following sense: every R-birational morphism $\mathcal{C}^{\min} \to \mathcal{C}$ over R to another proper regular model $\mathcal{C}/R$ is an R-isomorphism. We call $\mathcal{C}^{\min}/R$ the *minimal proper regular model for* C/K. ■

Via the usual argument, $\mathcal{C}^{\min}$ is unique up to unique isomorphism over R. For the purpose of this thesis we use the minimal regular model to study the reduction of an elliptic curve more closely. To make this precise, let R be a discrete valuation ring with field of fractions K and residue field k. Let E/K be an elliptic curve over K. Let $\mathcal{C}/R$ be a minimal proper regular model for E/K. Then the special fiber $\mathcal{C}_\mathfrak{p}$ over $\overline{k}$ can be written as

$$\mathcal{C}_\mathfrak{p} = \bigcup_{i=1}^{n} n_i F_i$$

where the F_i are irreducible curves in $\mathcal{C}_\mathfrak{p}$ and the n_i are the multiplicities. All the possibilities for this decomposition of the special fiber over $\overline{k}$ are classified as follows by the work of Kodaira [27] and Néron [39].

Theorem 2.24. [51, Theorem IV.8.2] Let R be a discrete valuation ring with maximal ideal $\mathfrak{p}$, field of fractions K, and residue field k. Let E/K be an elliptic curve and let $\mathcal{C}/R$ be a minimal proper regular model for E/K. Then the special fiber $\mathcal{C}_\mathfrak{p}$ considered as a curve over $\overline{k}$ has one of the following forms.

Type I_0.	$\mathcal{C}_\mathfrak{p}$ is a non-singular curve of genus 1.
Type I_1.	$\mathcal{C}_\mathfrak{p}$ is a curve with a node.
Type I_n.	$\mathcal{C}_\mathfrak{p}$ consists of n non-singular curves arranged in the shape of an n-gon with $n \geqslant 2$.
Type II.	$\mathcal{C}_\mathfrak{p}$ is a curve with a cusp.
Type III.	$\mathcal{C}_\mathfrak{p}$ consists of two non-singular curves which intersect tangentially at a single point.
Type IV.	$\mathcal{C}_\mathfrak{p}$ consists of three non-singular curves which intersect at a single point.
Type I_0^*.	$\mathcal{C}_\mathfrak{p}$ is a non-singular curve of multiplicity 2 with four non-singular curves of multiplicity 1 attached.
Type I_n^*.	$\mathcal{C}_\mathfrak{p}$ consists of a chain of $n+1$ non-singular curves of multiplicity 2 with two non-singular curves of multiplicity 1 at either end.
Type IV^*.	$\mathcal{C}_\mathfrak{p}$ consists of seven non-singular curves.
Type III^*.	$\mathcal{C}_\mathfrak{p}$ consists of eight non-singular curves.
Type II^*.	$\mathcal{C}_\mathfrak{p}$ consists of nine non-singular curves.

■

The proof of Theorem 2.24 is proven in an exhaustive case-by-case fashion. It uses the theory of intersections on surfaces and the theory of blow-ups. The types IV^*, III^* and II^* require a picture to fully describe the multiplicities of the components and how these components intersect. For our purposes, only the amount of components are relevant but the interested reader is referred to [51, Figure IV.4.4].

Let K be a local field. Tate's algorithm [57] is a twelve step algorithm which takes an elliptic curve E/K and produces the reduction type from Theorem 2.24 along with the number of components of the special fiber over the residue field of K, the valuation of the minimal discriminant of E and one more quantity which we encounter in the next section. Additionally, Tate's algorithm finds the reduction type of E. It turns out that type I_0 corresponds to good reduction and type I_n (with $n \geqslant 1$) corresponds to multiplicative reduction. All the other types correspond to additive reduction. Tate's algorithm and a proof of its termination can be found in [51, Section IV.9].

2.3.2 The conductor

In this section we introduce the (proper) definition of the conductor of an elliptic curve over a local field and relate it to the reduction type. We then state Ogg's formula which relates the (exponent of the) conductor to the theory of the previous section.

Let K be a local field of characteristic 0 whose residue field k has characteristic ℓ. Let E/K be an elliptic curve. We define the conductor of E in two parts. Let p be a prime distinct from ℓ and $T_p(E)$ be the Tate module of E and let $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ be the *p-adic tate module*. The $\mathbb{Q}_p$-vector space $V_p(E)$ has dimension 2 by (2.2) and is a $\mathrm{Gal}(\overline{K}/K)$-module via the action of $\mathrm{Gal}(\overline{K}/K)$ on $T_p(E)$. Let $G_0(\overline{K}/K) \subset \mathrm{Gal}(\overline{K}/K)$ be the inertia subgroup and let $V_p(E)^{G_0(\overline{K}/K)}$ be the $\mathbb{Q}_p$-subspace of $V_p(E)$ which is fixed by the action of $G_0(\overline{K}/K)$ on $V_p(E)$. The *tame part of the conductor* $\varepsilon(E/K)$ *of* E is

$$\varepsilon(E/K) = \dim_{\mathbb{Q}_p}\left(V_p(E)/V_p(E)^{G_0(\overline{K}/K)}\right) = 2 - \dim_{\mathbb{Q}_p}\left(V_p(E)^{G_0(\overline{K}/K)}\right).$$

Let $L = K(E[p])$ be the Galois extension of K obtained by adjoining the coordinates of the elements of $E[p]$. Let G_i denote the ramification groups of L/K. The *wild part of the conductor* $\delta(E/K)$ *of* E/K is

$$\delta(E/K) = \sum_{i=1}^{\infty} \frac{1}{[G_0 : G_i]} \dim_{\mathbb{F}_p} \left(E[p]/E[p]^{G_i} \right).$$

Note that the sum defining $\delta(E/K)$ is finite by Lemma 1.10. The *exponent of the conductor* $f(E/K)$ is defined to be the sum of $\varepsilon(E/K)$ and $\delta(E/K)$.

Note that $\varepsilon(E/K)$ only takes three distinct values depending on how it is fixed by $G_0(\overline{K}/K)$. In what follows we aim to more precisely characterize which one of these three values are attained (following [51, Section IV.10]). Let K^{nr} be the maximal unramified extension of K. Then K^{nr} has residue field $\overline{k}$. Let $\tilde{E}_{\mathrm{ns}}(\overline{k})$ be the set of non-singular points of the reduction of $E(K^{\mathrm{nr}})$. Further, let $E_0(K^{\mathrm{nr}})$ and $E_1(K^{\mathrm{nr}})$ be the points of $E(K^{\mathrm{nr}})$ which reduce to non-singular points and the K^{nr}-points which reduce to the unit element of $\tilde{E}_{\mathrm{ns}}(\overline{k})$, respectively. We have exact sequences of $\mathrm{Gal}(\overline{K}/K)$-modules

$$\begin{aligned} 0 &\longrightarrow E_0(K^{\mathrm{nr}}) \longrightarrow E(K^{\mathrm{nr}}) \longrightarrow E(K^{\mathrm{nr}})/E_0(K^{\mathrm{nr}}) \longrightarrow 0 \\ 0 &\longrightarrow E_1(K^{\mathrm{nr}}) \longrightarrow E_0(K^{\mathrm{nr}}) \longrightarrow \tilde{E}_{\mathrm{ns}}(\overline{k}) \longrightarrow 0 \end{aligned} \tag{2.4}$$

where the second sequence is exact by Proposition 2.17. For an abelian group A, let

$$T_p(A) = \varprojlim_n A[p^n] \tag{2.5}$$

and let $V_p(A) = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Since $p \neq \ell$, it follows from [52, Proposition VII.3.1] that $E_1(K^{\mathrm{nr}})$ has no p-torsion. It follows from [51, Corollary IV.9.2d] that $E(K^{\mathrm{nr}})/E_0(K^{\mathrm{nr}})$ is finite. And hence

$$T_p(E_1(K^{\mathrm{nr}})) = 0 \quad \text{and} \quad T_p(E(K^{\mathrm{nr}})/E_0(K^{\mathrm{nr}})) = 0.$$

By taking the inverse limits of (2.4) and then tensoring with the (flat) $\mathbb{Z}_\ell$-module $\mathbb{Q}_\ell$ it follows from Proposition 1.4 that we get exact sequences

$$0 \longrightarrow V_p(E_0(K^{\mathrm{nr}})) \longrightarrow V_p(E(K^{\mathrm{nr}})) \longrightarrow V_p(E(K^{\mathrm{nr}})/E_0(K^{\mathrm{nr}})) \longrightarrow 0$$

$$0 \longrightarrow V_p(E_1(K^{\mathrm{nr}})) \longrightarrow V_p(E_0(K^{\mathrm{nr}})) \longrightarrow V_p(\tilde{E}_{\mathrm{ns}}(\overline{k})) \longrightarrow 0.$$

And hence we get isomorphisms

$$V_p(E(K^{\mathrm{nr}})) \cong V_p(E_0(K^{\mathrm{nr}})) \cong V_p(\tilde{E}_{\mathrm{ns}}(\overline{k})).$$

By Proposition 1.17 and the Galois correspondence it follows that

$$V_p(E(K^{\mathrm{nr}})) = V_p(E(\overline{K}))^{\mathrm{Gal}(\overline{K}/K^{\mathrm{nr}})} = V_p(E(\overline{K}))^{G_0(\overline{K}/K)}.$$

By putting this all together, and by using Proposition 2.11, we get

$$V_p(E)^{G_0(\overline{K}/K)} = V_p(E(\overline{K}))^{G_0(\overline{K}/K)} \cong V_p(\tilde{E}_{\mathrm{ns}}(\overline{k})) = \begin{cases} V_p(\tilde{E}) & \text{if } E \text{ has good reduction} \\ V_p(\overline{k}^\times) & \text{if } E \text{ has multiplicative reduction} \\ V_p(\overline{k}^+) & \text{if } E \text{ has additive reduction.} \end{cases}$$

Since $p \neq \ell$, it follows from Proposition 2.6 that

$$\varepsilon(E/K) = 2 - \dim_{\mathbb{Q}_p} \left(V_p(E)^{G_0(\overline{K}/K)} \right) = \begin{cases} 0 & \text{if } E \text{ has good reduction} \\ 1 & \text{if } E \text{ has multiplicative reduction} \\ 2 & \text{if } E \text{ has additive reduction.} \end{cases}$$

If E has good reduction, then by the Criterion of Néron-Ogg-Shafarevich (Theorem 2.18) it follows that $L = K(E[p])$ is an unramified extension of K. It follows that $G_i(L/K) = 0$ for all $i \geqslant 0$. Therefore $\delta(E/K) = 0$ in this case. In [51, Section IV.10] it is shown using more advanced techniques that if E/K has multiplicative reduction or if $\ell \geqslant 5$ then $\delta(E/K) = 0$. Further, if the reduction of E/K is additive, then $\delta(E/K)$ is an integer. To summarize, we have the following.

Theorem 2.25. [51, Theorem IV.10.2] Let K be a local field whose residue field has characteristic p and let E/K be an elliptic curve. If $p \geqslant 5$, E/K has good reduction, or if E/K has multiplicative reduction, then

$$f(E/K) = \begin{cases} 0 & \text{if } E \text{ has good reduction} \\ 1 & \text{if } E \text{ has multiplicative reduction} \\ 2 & \text{if } E \text{ has additive reduction.} \end{cases}$$

In any case, the exponent of the conductor is an integer and independent of the choice of ℓ. ■

The description of $f(E/K)$ is rather simple when the characteristic of the residue field of K is not equal to 2 or 3 or if E/K does not have additive reduction. The only trouble which arises is when trying to calculate $f(E/K)$ when E/K has additive reduction and $p = 2$ or 3. Luckily a result by Lockhart, Rosen and Silverman shows that $f(E/K)$ does not get unreasonably large in this case.

Theorem 2.26. [36] Let K be a local field of characteristic 0 with normalized valuation v. Let E/K be an elliptic curve. Then

$$f(E/K) \leqslant 2 + 3v(3) + 6v(2).$$ ■

Theorem 2.26 only says something about local fields of characteristic 0. This is sufficient for our purposes. However, the same statement is true for Henselian fields with perfect residue field fields. A proof can be found in [8].

The conductor and the exponent $f(E/K)$ is often introduced and considered as in 'Definition' 2.19. In this sense, it is a quantity of an elliptic curve storing the arithmetic data of how it reduces. In the previous section we mostly considered the geometry of (elliptic) curves. Ogg's formula is the bridge that connects these two concepts.

Theorem 2.27. (Ogg's formula) [40, Theorem 2], [51, IV.11.1] Let K be a local field with normalized valuation v, valuation ring $\mathcal{O}_K$ and maximal ideal $\mathfrak{p}$. Let E/K be an elliptic curve with minimal discriminant Δ, let $\mathcal{C}/\mathcal{O}_K$ be a minimal proper regular model for E/K. Let $m(E/K)$ denote the amount of components of the fiber $\mathcal{C}_\mathfrak{p}$ (see Theorem 2.24). Then

$$v(\Delta) = f(E/K) + m(E/K) - 1.$$ ■

Tate's algorithm calculates the reduction type (see Theorem 2.24) of E/K rather easily. It is also fairly straightforward to compute the valuation of the minimal discriminant of E/K. Ogg's formula is therefore used in Tate's algorithm [57] to compute $f(E/K)$.

In the global case, the conductor is given by passing to the local case for every prime.

Definition 2.28. Let K be a number field and E/K an elliptic curve. The conductor $\mathcal{N}_E$ of E over K is the ideal

$$\mathcal{N}_E = \prod_{\mathfrak{p}} \mathfrak{p}^{f(E/K_\mathfrak{p})}$$

where the product runs over all the primes in K. ■

Note that $\mathcal{N}_E$ is well defined and the product in the definition can be replaced by a product which only runs over the primes $\mathfrak{p}$ dividing the discriminant of E/K by Proposition 2.11.

3 Galois representations

The absolute Galois group is a very mysterious and central object in number theory. Many problems in number theory are solved by studying this object and this thesis is no exception. A common way to study an object which is hard to grasp is to study how it acts on other objects. This is precisely the idea that Galois representations try to capture. In this section we introduce Galois representations, and in particular we study Galois representations that arise from elliptic curves and ramification of these. Finally, we relate representations to a certain type of group scheme.

3.1 Definitions

In this section we state some standard definitions and results relating to Galois representations. Throughout this section, let K be a field of characteristic 0.

Definition 3.1. Let R be a commutative topological ring. A *Galois representation* (or, *representation*) is a continuous homomorphism

$$\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(R)$$

where $\mathrm{GL}_n(R)$ denotes the group of n by n invertible matrices over R. Two Galois representations ρ_1 and ρ_2 are said to be equivalent if there is some $M \in \mathrm{GL}_n(R)$ such that $\rho_1 = M\rho_2 M^{-1}$. In this case we write $\rho_1 \sim \rho_2$. A representation ρ is said to be *trivial* if $\rho(\mathrm{Gal}(\overline{K}/K)) = \{1\}$. ■

More generally, one can define Galois representations to be a continuous homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(M)$ where M is some topological abelian group. In more general contexts we sometimes use this definition.

Barring a few cases, the Galois representations considered in this thesis will mostly be those which have $R = \mathbb{F}_\ell$ (with the discrete topology) for some prime ℓ and $n = 2$. Consider a Galois representation $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(R)$ where R is a ring with the discrete topology. Then the singleton $\{1\} \subset \mathrm{GL}_n(R)$ is open. Since ρ is continuous, it follows that $\ker\rho = \rho^{-1}(1)$ is open. By Proposition 1.3, $\ker\rho$ is closed in $\mathrm{Gal}(\overline{K}/K)$ and has finite index. By the Galois correspondence, the field $M = \overline{K}^{\ker\rho}$ is a Galois extension of K. Its Galois group $\mathrm{Gal}(M/K)$ is isomorphic to

$$\mathrm{Gal}(\overline{K}/K)/\ker\rho \cong \mathrm{im}\,\rho$$

which is a finite group. Therefore, the extension M/K is finite and ρ factors through $\mathrm{Gal}(M/K)$.

Example 3.2. 1. Let E/K be an elliptic curve and let m be a positive integer. In Section 2.1 we saw that $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Pick an ordered basis (P, Q) of $E[m]$ and let $\sigma \in \mathrm{Gal}(\overline{K}/K)$, then

$$P^\sigma = aP + bQ$$
$$Q^\sigma = cP + dQ$$

for some $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$. It follows that σ acts on $E[m]$ via the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

In this way we get a group homomorphism

$$\overline{\rho}_{E,m}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

To show that $\overline{\rho}_{E,m}$ is a Galois representation, we show that $\overline{\rho}_{E,m}$ is continuous. Since $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ has the discrete topology, it follows that it is sufficient to show that $\ker\rho = \rho^{-1}(1)$ is open. The subgroup $\ker\rho$ consists precisely of those automorphisms $\sigma \in \mathrm{Gal}(\overline{K}/K)$ such that σ acts trivially on $E[m]$ i.e. σ acts trivially on $K(E[m])$. It follows that

$$\ker\rho = \ker\left(\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K(E[m])/K)\right)$$

which is open in $\mathrm{Gal}(\overline{K}/K)$ as seen in Section 1.1. It follows that $\overline{\rho}_{E,m}$ is a representation. We call $\overline{\rho}_{E,m}$ the *mod-m Galois representation attached to E* (or simply *mod-m representation*). By the above and by the Galois correspondence it also follows that

$$\mathrm{Gal}(K(E[m])/K) = \mathrm{Gal}(\overline{K}/K)/\ker\rho \cong \mathrm{im}\,\rho \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

The construction of $\overline{\rho}_{E,m}$ is dependent of the basis we pick for $E[m]$. A different basis for $E[m]$ gives a representation equivalent to $\overline{\rho}_{E,m}$.

2. Let ℓ be a prime. In section 2.1 we saw that the Tate module $T_\ell(E)$ of an elliptic curve E/K is isomorphic to $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$. A similar construction to the above gives a homomorphism

$$\rho_{E,\ell} \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

By composing $\rho_{E,\ell}$ with the projection $\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ we retrieve the mod-ℓ^n representation $\overline{\rho}_{E,\ell^n}$. The homomorphism $\rho_{E,\ell}$ is continuous since

$$\mathrm{GL}_2(\mathbb{Z}_\ell) = \varprojlim_n \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$$

and $\rho_{E,\ell}$ is equal to $\overline{\rho}_{E,\ell^n}$ in every component, which is continuous. We call $\rho_{E,\ell}$ the *ℓ-adic representation associated to E*. ■

Definition 3.3. Let R be a commutative ring. A Galois representation $\rho \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(R)$ is *reducible* if there is some proper, nontrivial R-submodule M of R^n such that $\rho(\mathrm{Gal}(\overline{K}/K))(M) \subset M$. This occurs if and only if ρ is equivalent to a representation of the form

$$\begin{pmatrix} \rho_1 & * \\ 0 & \rho_2 \end{pmatrix}$$

for some representations ρ_1 and ρ_2. A representation is said to be *irreducible* if it is not reducible. ■

Proposition 3.4. Let E/K be an elliptic curve and let ℓ be a prime. If E admits to a K-rational ℓ-isgeony, then the mod-ℓ Galois representation $\overline{\rho}_{E,\ell}$ is reducible. ■

Proof. Let $\varphi \colon E \to E'$ be a K-rational ℓ-isogeny. Then $\#\ker\varphi = \ell$ and hence is cyclic. Let P be a generator of $\ker\varphi \subset E[\ell]$ and let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. An arbitrary element of $\ker\varphi$ has the form nP for some integer n. Then, since addition on E and φ are defined over K, we have,

$$\varphi((nP)^\sigma) = \varphi(nP^\sigma) = \varphi^\sigma(nP^\sigma) = n\varphi^\sigma(P^\sigma) = n(\varphi(P))^\sigma = O_E.$$

It follows that $(nP)^\sigma \in \ker\varphi$. Since σ and n were taken to be arbitrary, it follows that

$$\overline{\rho}_{E,\ell}(\mathrm{Gal}(\overline{K}/K))(\ker\varphi) \subset \ker\varphi.$$

This completes the proof. □

Definition 3.5. Let k be a field. A Galois representation $\rho \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(k)$ is *absolutely irreducible* if the composition

$$\mathrm{Gal}(\overline{K}/K) \xrightarrow{\ \rho\ } \mathrm{GL}_n(k) \hookrightarrow \mathrm{GL}_n(\overline{k})$$

is an irreducible representation. ■

Clearly, if a representation is absolutely irreducible, then it is irreducible. A sufficient condition for the converse is as follows.

Proposition 3.6. Let k be a field and let $\rho \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(k)$ be a Galois representation. If ρ is surjective, then ρ is absolutely irreducible. ■

Proof. Let $V \subset \bar{k}^n$ be a proper, non-trivial $\bar{k}$-subspace. Let $v \in V$ be non-zero. Since $V \subset \bar{k}^n$ is proper, there is an element $A \in \mathrm{GL}_n(k) \subset \mathrm{GL}_n(\bar{k})$ such that $Av \notin V$. By assumption, there is some $\sigma \in \mathrm{Gal}(\overline{K}/K)$ such that $\rho(\sigma) = A$. It follows that $\rho(\sigma)(V) \not\subset V$. □

Finally, we discuss the notion of ramification of Galois representations.

Definition 3.7. Suppose K is a local field with inertia group $G_0(\overline{K}/K) \subset \mathrm{Gal}(\overline{K}/K)$. Let R be a commutative ring, we say that a Galois representation $\rho \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(R)$ is *unramified* if $\rho(G_0(\overline{K}/K)) = \{1\}$. We say that ρ is *ramified* otherwise. ■

Example 3.8. 1. Let K be a local field with residue characteristic p. Let E/K be an elliptic curve. For an integer m coprime to p consider the Galois representation $\overline{\rho}_{E,m}$ attached to E. By the Criterion of Néron-Ogg-Shafaravich, the Galois representation $\overline{\rho}_{E,m}$ is unramified if E/K has good reduction. The converse is in general not true. That is, if $\overline{\rho}_{E,m}$ is unramified, then this does not imply that E/K has good reduction. This is more thoroughly explored in Section 3.3.

2. Let $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(R)$ be a representation and suppose that $\{1\}$ is open in $\mathrm{GL}_n(R)$. Then, the kernel of ρ corresponds to a finite Galois extension L/K with Galois group $\operatorname{im}\rho$. If K is a local field and $I_K = G_0(\overline{K}/K)$ then the inertia group of L/K is $\rho(I_K)$. Therefore, since L/K is unramified if and only if the inertia group is trivial. It follows that ρ is unramified if and only if L/K is unramified. ■

If K is a number field and $\mathfrak{p}$ is a prime in K. Consider the decomposition group

$$D_{\mathfrak{p}} = \mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}}) \subset \mathrm{Gal}(\overline{K}/K).$$

Given a Galois representation $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(R)$, we can consider the restriction

$$\rho|_{D_{\mathfrak{p}}} : \mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}}) \to \mathrm{GL}_n(R)$$

and ramification of $\rho|_{D_{\mathfrak{p}}}$. We say that ρ is *unramified at* $\mathfrak{p}$ if $\rho|_{D_{\mathfrak{p}}}$ is unramified. Otherwise we say that ρ is *ramified at* $\mathfrak{p}$.

Similarly to elliptic curves, we would like to define an invariant which stores the information of ramification at the primes. As we are mostly interested in Galois representations to $\mathrm{GL}_2(\mathbb{F}_\ell)$, we consider representations to $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ where $\overline{\mathbb{F}}_\ell$ has the discrete topology.

Let K be a local field of characteristic 0 and let $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be a representation. We saw that the fixed field $M = \bar{K}^{\ker\rho}$ is a finite Galois extension of K. Let $G_i = G_i(M/K)$ denote the higher ramification groups of M/K. Set $V = \overline{\mathbb{F}}_\ell^n$ considered with its $\mathrm{Gal}(\overline{K}/K)$ action. For a subgroup $H \leqslant \mathrm{Gal}(\overline{K}/K)$, let $V^H \subset V$ denote the subspace of V fixed by the action of H. Define

$$f(\rho/K) = \sum_{i \geqslant 0} \frac{1}{[G_0 : G_i]} \dim_{\overline{\mathbb{F}}_\ell}(V/V^{G_i}).$$

It follows immediately that if ρ is unramified, then $f(\rho/K) = 0$. Further, the value $f(\rho/K)$ is an integer by [46]. Now let K be a number field, and let $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be a representation which is ramified at only finitely many primes $\mathfrak{p}$ of K. The *Artin conductor* $\mathscr{N}$ of ρ is the ideal

$$\mathscr{N}_\rho = \prod_{\mathfrak{p}} \mathfrak{p}^{f(\rho/K_{\mathfrak{p}})}$$

where the product is over all primes in K. This product is finite since we assume that ρ is ramified at only finitely many primes, and so $f(\rho/K_{\mathfrak{p}})$ is non-zero for all but finitely many primes $\mathfrak{p}$. The representation $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ is often ramified at the primes above ℓ. Therefore, it makes sense to ignore these primes and only consider the prime-to-ℓ part of $\mathscr{N}_\rho$. The prime-to-ℓ part $\mathfrak{N}_\rho$ of the Artin conductor is called the *Serre conductor*. Thus, the Serre conductor $\mathfrak{N}_\rho$ is the ideal

$$\mathfrak{N}_\rho = \prod_{\mathfrak{p} \nmid \ell} \mathfrak{p}^{f(\rho/K_{\mathfrak{p}})}$$

where the product is over the primes in K not lying above ℓ.

Remark 3.9. The naming convention of the conductors in the literature is not consistent. For example, in [23] and [20] the naming of the conductors is the same as here. However, in, for example, [46] or [43] they call what we call the Serre conductor the Artin conductor. ■

Example 3.10. Let K be a number field and let E/K be an elliptic curve. Consider the representation $\overline{\rho}_{E,\ell}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{F}_\ell)$. If E/K has good reduction at a prime $\mathfrak{p} \nmid \ell$, then, as seen in Example 3.8.1, $\overline{\rho}_{E,\ell}$ is unramified at $\mathfrak{p}$. It follows that the Artin conductor $\mathscr{N}_E \coloneqq \mathscr{N}_{\overline{\rho}_{E,\ell}}$ is supported on the primes dividing the conductor $\mathcal{N}_E$ of E and the primes above ℓ. Even when ignoring the primes above ℓ in $\mathcal{N}_E$ and $\mathscr{N}_E$, the conductors $\mathcal{N}_E$ and $\mathscr{N}_E$ are, in general, not equal. To see this, we need the theory of the Tate curve. This is explored more in Section 3.3. In fact, the reason why the modular method works in the first place is due to the fact that these two ideals are not equal. ■

3.2 Galois characters

Galois characters are Galois representations which act on a ring. Despite characters being less general than representations, they still serve to reveal intrinsic properties of objects found in number theory. In this section we cover cyclotomic characters and quadratic characters. Throughout this section K is a field of characteristic 0.

Recall that a representation is a continuous homomorphism $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(R)$ where R is a topological ring. In the case where $n = 1$ we have an isomorphism $\mathrm{GL}_n(R) \cong R^\times$.

Definition 3.11. Let R be a ring. A *Galois character* (or, *character*) is a continuous homomorphism $\psi\colon \mathrm{Gal}(\overline{K}/K) \to R^\times$. A character ψ is called *trivial* if $\psi(\mathrm{Gal}(\overline{K}/K)) = \{1\}$ and *non-trivial* otherwise. ■

Thus, Galois characters are simply Galois representations with $n = 1$.

Example 3.12. 1. Let $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(R)$ be a representation then the composition

$$\mathrm{Gal}(\overline{K}/K) \xrightarrow{\quad\rho\quad} \mathrm{GL}_n(R) \xrightarrow{\quad\det\quad} R^\times$$

is a Galois character.

2. Let m be an integer and let $\zeta_m \in \overline{K}$ be a primitive m^{th} root of unity. Then, for $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have $\sigma(\zeta_m) = \zeta_m^n$ where $n \in \mathbb{Z}$ is coprime to m and determined uniquely modulo m. This defines a unique homomorphism

$$\chi_m\colon \mathrm{Gal}(\overline{K}/K) \to (\mathbb{Z}/m\mathbb{Z})^\times$$

such that $\sigma(\zeta_m) = \zeta_m^{\chi_m(\sigma)}$, independent of the choice of ζ_m. The kernel $\ker \chi_m$ consists precisely of the elements of $\mathrm{Gal}(\overline{K}/K)$ which fix ζ_m, i.e.

$$\ker \chi_m = \mathrm{Gal}(\overline{K}/K(\zeta_m)) = \ker(\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K(\zeta_m)/K)),$$

which is open in $\mathrm{Gal}(\overline{K}/K)$. It follows that χ_m is continuous and hence a Galois character. We call χ_m the *m^{th} cyclotomic character.*

3. For a positive integer m, let $\mu_m(\overline{K}) \cong \mathbb{Z}/m\mathbb{Z}$ denote the set of m^{th} roots of unity of m. There is a Galois action on $\mu_m(\overline{K})$ which gives rise to the representation of the previous example. Let ℓ be a prime, then, for positive integer n, the map $\mu_{\ell^{n+1}}(\overline{K}) \to \mu_{\ell^n}(\overline{K})$ sending $\zeta \mapsto \zeta^\ell$ is compatible with the Galois action and hence we get an inverse system

$$\ldots \longrightarrow \mu_{\ell^3}(\overline{K}) \longrightarrow \mu_{\ell^2}(\overline{K}) \longrightarrow \mu_\ell(\overline{K})$$

of $\mathrm{Gal}(\overline{K}/K)$-modules. The inverse limit of this system is called the *ℓ-adic Tate module of K* and is denoted by $T_\ell(\boldsymbol{\mu})$. The ℓ-adic Tate module is a $\mathbb{Z}_\ell$-module and a $\mathrm{Gal}(\overline{K}/K)$-module. Alternatively, one defines the ℓ-adic tate module of K via $T_\ell(\boldsymbol{\mu}) = T_\ell(\bar{K}^\times)$ as in (2.5). Since $\mu_{\ell^n}(\overline{K}) \cong \mathbb{Z}/\ell^n\mathbb{Z}$ as abelian groups, it follows that $T_\ell(\boldsymbol{\mu}) \cong \mathbb{Z}_\ell$. Via this isomorphism, the Galois action on $T_\ell(\boldsymbol{\mu})$ gives rise to a unique homomorphism

$$\chi_{\ell^\infty}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{Z}_\ell) \cong \mathbb{Z}_\ell^\times$$

such that

$$\begin{array}{ccc} \mathrm{Gal}(\overline{K}/K) & \xrightarrow{\chi_{\ell^\infty}} & \mathbb{Z}_\ell^\times \\ & \searrow^{\chi_{\ell^n}} & \downarrow \\ & & (\mathbb{Z}/\ell^n\mathbb{Z})^\times \end{array}$$

commutes for every positive integer n. The homomorphism χ_{ℓ^∞} is a representation since χ_{ℓ^∞} is continuous in every coordinate. We call χ_{ℓ^∞} the *ℓ-adic cyclotomic character.* ■

Let E/K be an elliptic curve. For every positive integer m we have a representation $\overline{\rho}_{E,m}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and by Example 3.12.1, a character $\det \overline{\rho}_{E,m}$. The Weil pairing (Proposition 3.14 below) gives us a precise description of this character.

Proposition 3.13. Let m be a positive integer and E/K an elliptic curve. Then $\det \overline{\rho}_{E,m} = \chi_m$ ■

To prove this we need to following well-known result.

Proposition 3.14. (Weil) There exists a bilinear, alternating, nondegenrate, Galois invariant pairing

$$e_m\colon E[m] \times E[m] \to \mu_m(\overline{K})$$ ■

Proof of Proposition 3.13. By Proposition 2.6, $E[m]$ is a $\mathbb{Z}/m\mathbb{Z}$-module of rank 2. Let P and Q be a basis of $E[m]$. Then, since e_m is non-degenerate, $e_m(P,Q)$ is a primitive m^{th} root of unity. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and suppose that

$$\begin{aligned} P^\sigma &= aP + bQ \\ Q^\sigma &= cP + dQ \end{aligned} \tag{3.1}$$

for some $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$. Then $\overline{\rho}_{E,m}(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and

$$\begin{aligned} e_m(P,Q)^{\chi_m(\sigma)} &= \sigma(e_m(P,Q)) && \text{definition of } \chi_m \\ &= e_m(P^\sigma, Q^\sigma) && e_m \text{ is Galois invariant} \\ &= e_m(aP+bQ, cP+dQ) && (3.1) \\ &= e_m(P,Q)^{ad} e_m(Q,P)^{bc} && e_m \text{ is bilinear} \\ &= e_m(P,Q)^{ad} e_m(P,Q)^{-bc} && e_m \text{ is alternating} \\ &= e_m(P,Q)^{ad-bc} \\ &= e_m(P,Q)^{\det \overline{\rho}_{E,m}(\sigma)} \end{aligned}$$

Since e_m is non-degenerate, it follows that $\det \overline{\rho}_{E,m}(\sigma) = \chi_m(\sigma)$. □

Corollary 3.15. Let ℓ be a prime and E/K an elliptic curve. Then $\det \rho_{E,\ell} = \chi_{\ell^\infty}$. ■

In the rest of this section we study quadratic characters. These characters are the simplest kind of characters aside from the trivial character and have a straightforward description. Further, we study quadratic twists of elliptic curves and how the corresponding representations relate.

Definition 3.16. A *quadratic character* is a non-trivial character $\psi\colon \mathrm{Gal}(\overline{K}/K) \to \{\pm 1\}$. ■

Let ψ be a quadratic character. Since ψ is non-trivial and its target is $\{\pm 1\}$, it follows that ψ is surjective. In Section 3.1 we saw that the fixed field $L \coloneqq \bar{K}^{\ker \psi}$ is a finite extension with Galois group isomorphic to $\operatorname{im} \psi = \{\pm 1\}$. It follows that $L = K(\sqrt{d})$ for some $d \in K^\times \setminus K^{\times 2}$. Then ψ factors as

$$\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Gal}(L/K) \xrightarrow{\sim} \{\pm 1\}$$

where the last isomorphism is given by

$$\begin{aligned} \mathrm{Gal}(L/K) &\to \{\pm 1\} \\ (\sqrt{d} \mapsto \sqrt{d}) &\mapsto 1 \\ (\sqrt{d} \mapsto -\sqrt{d}) &\mapsto -1. \end{aligned}$$

It follows that, for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$\psi(\sigma) = \begin{cases} 1 & \text{if } \sigma(\sqrt{d}) = \sqrt{d} \\ -1 & \text{if } \sigma(\sqrt{d}) = -\sqrt{d}. \end{cases} \tag{3.2}$$

Conversely, every quadratic extension L/K defines a quadratic character defined as in (3.2). We are interested in quadratic characters because of the following construction.

Definition 3.17. Let E/K be an elliptic curve given by a Weierstrass equation of the form

$$E\colon y^2 = x^3 + c_4x + c_6$$

(recall that $\operatorname{char} K = 0$). Let $d \in K^\times \setminus K^{\times 2}$, then the *quadratic twist by d of E* is the elliptic curve E^d given by the equation

$$E^d\colon dy^2 = x^3 + c_4x + c_6.$$ ■

Let E/K be an elliptic curve and let $d \in K^\times \setminus K^{\times 2}$. The elliptic curves E and E^d are not isomorphic over K but they are isomorphic over $L = K(\sqrt{d})$, indeed, the map

$$\begin{aligned} g\colon E^d &\to E \\ (x, y) &\mapsto (x, \sqrt{d}\cdot y) \\ O_{E^d} &\mapsto O_E \end{aligned}$$

is an isomorphism (of elliptic curves) defined over L. Let $\psi_d\colon \operatorname{Gal}(\overline{K}/K) \to \{\pm 1\}$ be the quadratic character defined by L/K. Let $P \in E$. Choose Weierstrass coordinates for E and write $P = (x, y)$. Then $-P = (x, -y)$. Let $\sigma \in \operatorname{Gal}(\overline{K}/K)$, then

$$g(P)^\sigma = (\sigma(x), \sigma(\sqrt{d}\cdot y)) = (\sigma(x), \psi_d(\sigma)\sqrt{d}\cdot\sigma(y)) = [\psi_d(\sigma)](\sigma(x), \sqrt{d}\cdot\sigma(y)) = [\psi_d(\sigma)]g(P^\sigma) \tag{3.3}$$

where $[m]$ (with $m \in \mathbb{Z}$) denotes the multiplication by m isogeny, i.e. $[\psi_d(\sigma)]$ is the identity or the inversion homomorphism $E \to E$. The isomorphism g restricts to a group isomorphism $E^d[m] \to E[m]$. From this and from (3.3) it follows that the mod-m representations attached to E and E^d are related via

$$\overline{\rho}_{E,m}(\sigma) \sim \psi_d(\sigma)\cdot\overline{\rho}_{E^d}(\sigma)$$

for every $\sigma \in \operatorname{Gal}(\overline{K}/K)$. Since $\psi_d(\sigma)^2 = 1$ it also follows that

$$\overline{\rho}_{E^d,m}(\sigma) \sim \psi_d(\sigma)\cdot\overline{\rho}_{E,m}(\sigma)$$

for every $\sigma \in \operatorname{Gal}(\overline{K}/K)$. For a representation ρ and a character ψ, let $\psi \otimes \rho$ denote the representation $\sigma \mapsto \psi(\sigma)\cdot\rho(\sigma)$. Then the above proves the following.

Proposition 3.18. Let E/K be an elliptic curve and let E^d/K denote the quadratic twist of E by $d \in K^\times \setminus K^{\times 2}$. Then for every positive integer m,

$$\overline{\rho}_{E^d,m} \sim \overline{\rho}_{E,m} \otimes \psi_d \quad \text{and} \quad \overline{\rho}_{E,m} \sim \overline{\rho}_{E^d,m} \otimes \psi_d$$

where ψ_d is the quadratic character associated to $K(\sqrt{d})/K$. ■

Let E/K be an elliptic curve and let ψ be a quadratic character. Let $d \in K^\times/K^{\times 2}$ be such that ψ is associated to $K(\sqrt{d})/K$. Then we also let $E \otimes \psi$ denote the quadratic twist E^d. In Section 3.3 we use the theory of the Tate curve to show that for an elliptic curve E with potential multiplicative reduction, there is some quadratic twist $E \otimes \psi$ of E such that $E \otimes \psi$ has split multiplicative reduction. Then Proposition 3.18 allows us to study representations attached to elliptic curves in the general case when there is potentially multiplicative reduction.

3.3 Galois representations from elliptic curves

In Section 3.1 we covered some general theory for Galois representations with as our main example the mod-m Galois representation $\overline{\rho}_{E,m}\colon \operatorname{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ associated to some elliptic curve E over a field K. In this section we examine more closely how the representation $\overline{\rho}_{E,m}$ relates to E, i.e. what properties of $\overline{\rho}_{E,m}$ can we deduce by only looking at E. A mayor tool in this study is the Tate curve; an analytic construction of an elliptic curve over a local field. It may seem counterintuitive that an analytic construction gives information about the inherently arithmetic object $\overline{\rho}_{E,m}$, however, the structure of the Tate curve as a Galois module bridges the gap and makes this theory crucial.

Let $E/\mathbb{C}$ be an elliptic curve over the complex numbers. Then there is some lattice $\Lambda \subset \mathbb{C}$ such that E is isomorphic to $\mathbb{C}/\Lambda$ as complex Lie groups. Further, there is a unique τ in the upper half complex plane such that Λ can be chosen to be the lattice $\tau\mathbb{Z} \oplus \mathbb{Z}$. Let $q = e^{2\pi i\tau}$ and

$$q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\}.$$

Then there is a complex Lie group isomorphism $\mathbb{C}/\Lambda \to \mathbb{C}^\times/q^{\mathbb{Z}}$ sending $z \mapsto e^{2\pi i z}$. Given a local field K, an analogous construction to $\mathbb{C}/\Lambda$ does not exists as the discrete subgroups of K are trivial. An analogous construction to $\mathbb{C}^\times/q^{\mathbb{Z}}$ does exist. This is known as the Tate curve.

Theorem 3.19. (Tate) Let K be a local field of characteristic 0 with absolute value $|\cdot|$. Let $q \in K^\times$ be such that $|q| < 1$, and let

$$s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n}, \quad a_4(q) = -5s_3(q) \quad a_6(q) = -\frac{5s_3(q)+7s_5(q)}{12}.$$

Then
(a) The series $a_4(q)$ and $a_6(q)$ converge in K and the *Tate curve*

$$E_q\colon y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

is an elliptic curve with j-invariant

$$j_{E_q} = \frac{1}{q} + 744 + 196884q + \dots$$

and discriminant

$$\Delta = q\prod_{n\geqslant 1}(1-q^n)^{24}.$$

(b) There is a surjective homomorphism of groups

$$\phi\colon \bar{K}^\times \to E_q(\overline{K})$$

with kernel $q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\}$.
(c) The map ϕ in (b) is a $\mathrm{Gal}(\overline{K}/K)$-module homomorphism in the sense that

$$\phi(\sigma(u)) = \phi(u)^\sigma \quad \text{for all } u \in \bar{K}^\times \text{ and } \sigma \in \mathrm{Gal}(\overline{K}/K).$$

In particular, for every algebraic extension L/K, there is an isomorphism $L^\times/q^{\mathbb{Z}} \cong E_q(L)$. ■

Proof. See [59] or [51, Section V] for full, in-depth proofs. □

Given an elliptic curve E over a local field K, one might wonder, as in the case of elliptic curves over $\mathbb{C}$, when is E isomorphic to E_q for some $q \in K^\times$ with $|q| < 1$? And over what field are E and E_q isomorphic? By Theorem 3.19, the j-invariant of E_q is equal to

$$j(q) = \frac{1}{q} + 744 + 19884q + \dots$$

If $|\cdot|$ denotes the absolute value on K, it follows that $|j(q)| = |q|^{-1} > 1$. Therefore, a necessary condition is that the j invariant of E absolute value > 1. This turns out to be sufficient to be isomorphic over $\overline{K}$ by Theorem 3.20 below. To state over which finite extension of K the curves E and E_q are isomorphic, choose a Weierstrass equation for E and let c_4 and c_6 be the associated quantities of E. Then define the class

$$\gamma(E/K) = -\frac{c_4}{c_6} \in K^\times/K^{\times 2}. \tag{3.4}$$

This choice is well defined since any other choice of Weierstrass equation for E replaces c_4 and c_6 by u^4c_4 and u^6c_6 for some $u \in K^\times$. Then

$$-\frac{u^4c_4}{u^6c_6} = -u^{-2}\frac{c_4}{c_6} \equiv -\frac{c_4}{c_6} \bmod K^{\times 2} = \gamma(E/K).$$

The statement is then as follows.

Theorem 3.20. (Tate) Let K be a local field with absolute value $|\cdot|$, let E/K be an elliptic curve with j-invariant j_E satisfying $|j_E| > 1$, and let $\gamma(E/K) \in K^\times/K^{\times 2}$ be as in (3.4). Then
(a) There is a unique $q \in K^\times$ with $|q| < 1$ such that E is isomorphic over $\overline{K}$ to the Tate curve E_q.
(b) Let q be as in (a). Then the following three conditions are equivalent:
(i) E is isomorphic to E_q over K.

(ii) $\gamma(E/K) = 1$.
(iii) E has split multiplicative reduction. ■

Proof. This is a straightforward computation and follows from Theorem 3.19. For the precise details, see [51, Theorem V.5.4] □

Let E/K be an elliptic curve with j-invariant j_E. Suppose that E/K has potentially multiplicative reduction i.e. $|j_E| > 1$ by Proposition 2.15. Consider the (possibly trivial) extension $L = K(\sqrt{\gamma(E/K)})$ of K. Then $\gamma(E/L) = 1$ and by Theorem 3.20, E/L has split multiplicative reduction. We have proven the following.

Corollary 3.21. Let K be a local field and let E/K be an elliptic curve with potentially multiplicative reduction. Then E attains split multiplicative reduction over an at most quadratic extension of K. ■

Let E be an elliptic curve over a local field K. Let $\overline{\rho}_{E,p}$ be the mod-ℓ Galois representation. From the criterion of Néron-Ogg-Shafaravich (Theorem 2.18) we know that if E has bad reduction, then $\overline{\rho}_{E,p}$ is possibly ramified. In the case where E/K has potentially multiplicative reduction, the Tate curve gives a better description of the image of the inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$ under $\overline{\rho}_{E,p}$. The proof we present here is essentially the same as in [51, Proposition V.6.1] and is repeated here to show the effectiveness of the Tate curve.

Proposition 3.22. Let E be an elliptic curve over a local field K with absolute value $|\cdot|$ and normalized valuation v. Let j_E be the j-invariant of E and suppose that $|j_E| > 1$. Let ℓ be an odd prime such that $\ell \nmid v(j_E)$. Then there is an element σ in the inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$ such that

$$\overline{\rho}_{E,\ell}(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

i.e. such that σ acts as a transvection on $E[\ell]$. ■

Proof. If L/K is a finite extension of degree prime to ℓ. Then if Proposition 3.22 holds for E/L then it holds for E/K. Indeed, if v_L is the normalized valuation of L, then $v_L(j_E) = e(L/K)v(j_E)$ where $e(L/K)$ is the ramification index which is coprime to ℓ, by assumption. If ℓ is coprime to $v(j_E)$ then it is coprime to $v_L(j(E))$ and hence there is an element σ in the inertia group $G_0(\overline{L}/L) \subset G_0(\overline{K}/K)$ which acts as a transvection on $E[\ell]$.
By Theorem 3.20, there is some $q \in K$ such that the E/K is isomorphic to E_q over at most a quadratic extension (by Corollary 3.21). Since ℓ is odd we may, by the previous paragraph, replace K by this quadratic extension and assume that $E = E_q$. Similarly, we may assume that K contains a primitive ℓ^{th} root of unity ζ_ℓ since $[K(\zeta_\ell) : K]$ is strictly less than ℓ and hence coprime to ℓ. Let $q^{1/\ell}$ be a ℓ^{th} root of q. Then since $v(q) = -v(j_E)$ is not divisible by ℓ, it follows that $K(q^{1/\ell})/K$ is an extension of degree ℓ. Further, $K(q^{1/\ell})/K$ is totally ramified and hence there is some $\sigma \in \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}}) = G_0(\overline{K}/K)$ such that $\sigma(q^{1/\ell}) = \zeta_\ell q^{1/\ell}$. We have

$$(\bar{K}^\times/q^{\mathbb{Z}})[\ell] = \langle q^{1/\ell} \rangle \times \langle \zeta_\ell \rangle.$$

And since $\phi\colon \bar{K}/q^{\mathbb{Z}} \to E(\overline{K})$ is an isomorphism of groups, it follows that $P = \phi(\zeta_\ell)$ and $Q = \phi(q^{1/\ell})$ form a basis for $E[m]$. Then, since ϕ is a $\mathrm{Gal}(\overline{K}/K)$-module homomorphism,

$$\begin{aligned} P^\sigma &= \phi(\zeta_\ell)^\sigma = \phi(\sigma(\zeta_\ell)) = \phi(\zeta_\ell) = P \\ Q^\sigma &= \phi(q^{1/\ell})^\sigma = \phi(\sigma(q^{1/\ell})) = \phi(\zeta_\ell q^{1/\ell}) = \phi(\zeta_\ell) + \phi(q^{1/\ell}) = P + Q \end{aligned}$$

which concludes the proof. □

Proposition 3.23. Let K be a local field and let E/K be an elliptic curve with split multiplicative reduction. Let ℓ be a prime, then there is an exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$1 \longrightarrow T_\ell(\boldsymbol{\mu}) \longrightarrow T_\ell(E) \longrightarrow \mathbb{Z}_\ell \longrightarrow 0$$

where $\mathrm{Gal}(\overline{K}/K)$ acts trivially on $\mathbb{Z}_\ell$. ■

Proof. Since E/K has split multiplicative reduction, we may assume that $E = E_q$ for some $q \in K^\times$ with $|q| < 1$. The isomorphism $\phi\colon \bar{K}^\times/q^{\mathbb{Z}} \to E_q(\overline{K})$ of $\mathrm{Gal}(\overline{K}/K)$-modules induces an inclusion $\mu_{\ell^n}(\overline{K}) \hookrightarrow E_q[\ell^n]$ of $\mathrm{Gal}(\overline{K}/K)$-modules for all positive integers n. Let $z \in (\bar{K}^\times/q^{\mathbb{Z}})[\ell^n] \cong E_q[\ell^n]$, then $z^{\ell^n} = q^m$

for some $m \in \mathbb{Z}$ which is uniquely determined modulo ℓ^n. Then $f\colon z \mapsto m$ is a surjective group homomorphism $(\bar{K}^\times/q^{\mathbb{Z}})[\ell^n] \to \mathbb{Z}/\ell^n\mathbb{Z}$. This is a $\mathrm{Gal}(\overline{K}/K)$-module homomorphism (with the action on $\mathbb{Z}/\ell^n\mathbb{Z}$ being trivial) since, for z as above and $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$\sigma(z)^{\ell^n} = \sigma(z^{\ell^n}) = \sigma(q^m) = q^m$$

so $f(z) = f(\sigma(z))$. Let $z \in \ker f$, then $z^{\ell^n} = q^{f(z)} = 1$ and hence $z \in \mu_{\ell^n}(\overline{K})$. Since $\phi\colon \bar{K}^\times/q^{\mathbb{Z}} \to E(\overline{K})$ is compatible with the Galois action, we get an exact sequence

$$1 \longrightarrow \mu_{\ell^n}(\overline{K}) \longrightarrow E[\ell^n] \xrightarrow{f} \mathbb{Z}/\ell^n\mathbb{Z} \longrightarrow 0$$

for every positive integer n. Taking the inverse limit and using Proposition 1.4 concludes the proof. □

Corollary 3.24. Let K be a local field with residue characteristic p, ℓ a prime and let E/K be an elliptic curve with split multiplicative reduction. Then

$$\rho_{E,\ell} \sim \begin{pmatrix} \chi_{\ell^\infty} & * \\ 0 & 1 \end{pmatrix}$$

where χ_{ℓ^∞} denotes the ℓ-adic cyclotomic character. ■

Proof. The action of $\mathrm{Gal}(\overline{K}/K)$ on $T_\ell(\boldsymbol{\mu})$ is given as χ_{ℓ^∞} on $T_\ell(\boldsymbol{\mu})$. By the exact sequence in Proposition 3.23, it follows that $T_\ell(E)/T_\ell(\boldsymbol{\mu}) \cong \mathbb{Z}_\ell$ with the trivial Galois action. Thus, a generator of $T_\ell(\boldsymbol{\mu})$ and $\mathbb{Z}_\ell$ as $\mathbb{Z}_\ell$-modules gives the desired representation equivalent to $\rho_{E,\ell}$. □

Remark 3.25. In [44, A.1.2], Serre proves that the exact sequence of Proposition 3.23 does not split. In other words, there is no $\sigma \in \mathrm{Gal}(\overline{K}/K)$, such that the the matrix $\rho_{E,\ell}(\sigma)$ is equivalent to a matrix as in Corollary 3.24 where the top-right entry is zero. ■

Let K be a number field. In Section 3.1 we defined the (Artin and Serre) conductor of a representation. In Example 3.10 we compared the conductor of $\overline{\rho}_{E,\ell}$ to the conductor of E and deduced that if E has good reduction at a prime in K not dividing ℓ, then $\overline{\rho}_{E,\ell}$ is unramified. The converse is in general not true. That is, it is possible for $\overline{\rho}_{E,\ell}$ to be unramified at a prime $\mathfrak{p} \nmid \ell$ whilst E has bad reduction at $\mathfrak{p}$. If E has potential multiplicative reduction at $\mathfrak{p}$, then the Tate curve allows us to classify the ramification behavior of $\overline{\rho}_{E,\ell}$. The proof presented here is an adaption of the sketch presented in [42, Proposition 3.4].

Proposition 3.26. Let ℓ be a prime, K a local field with normalized valuation v and residue characteristic p. Let E/K an elliptic curve with minimal discriminant Δ and let $\ell \neq p$ be a prime. Suppose that E/K has potential multiplicative reduction. Then the mod-ℓ representation $\overline{\rho}_{E,\ell}$ is unramified if and only if $v(\Delta) \equiv 0 \bmod \ell$. ■

Proof. Let $I_K = G_0(\overline{K}/K) = \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}})$ be the inertia group of $\overline{K}/K$. Then $\overline{\rho}_{E,\ell}$ is unramified if and only if I_K acts trivially on $E[\ell]$ i.e. if and only if all points of $E[\ell]$ are defined over K^{nr}. Since E has potentially multiplicative reduction, it follows from Proposition 2.15 that the j-invariant of E has absolute value > 1 and hence, by 3.20, there is some $q \in K^\times$ such that $E(\overline{K}) \cong \bar{K}/q^{\mathbb{Z}}$. From this it follows that

$$K(E[\ell]) = K(q^{1/\ell}, \zeta_\ell)$$

where ζ_ℓ is an ℓ^{th} root of unity. Since $\ell \neq p$ it follows that $\zeta_\ell \in K^{\mathrm{nr}}$. We have $q^{1/\ell} \in K^{\mathrm{nr}}$ if and only if $v(q)$ is a multiple of ℓ, i.e. if and only if $v(q) \equiv 0 \bmod \ell$. By Theorem 3.20, we have

$$v(\Delta) = v\Big(q \prod_{n \geqslant 1} (1-q^n)^{24}\Big) = v(q).$$

To conclude, we have that $K(E[\ell]) \subset K^{\mathrm{nr}}$ if an only if $v(\Delta) \equiv 0 \bmod \ell$. □

If an elliptic curve E over a local field has good reduction, then both of the results of Proposition 3.26 are satisfied according to Proposition 2.11 and Theorem 2.18. Thus we can enlarge the criteria of Proposition 3.26 and we obtain the following.

Corollary 3.27. Let ℓ be a prime, K a local field with normalized valuation v and residue characteristic p. Let E/K an elliptic curve with minimal discriminant Δ and let $\ell \neq p$ be a prime. Suppose that E/K has good or potentially multiplicative reduction. Then the mod-ℓ representation $\overline{\rho}_{E,\ell}$ is unramified if and only if $v(\Delta) \equiv 0 \bmod \ell$. ■

Corollary 3.27 covers a lot of scenarios, but we are still in the dark when there is additive reduction and no potential multiplicative reduction (i.e. potential good reduction) or if $\ell = p$. Luckily, we do not have to deal with the former case in this thesis. In the latter case, the representation is often ramified when $\ell = p$, unrelated to E. For this reason, the right question to ask is not whether the mod-p representation is unramified but rather: 'Does $\overline{\rho}_{E,p}$ arise from a finite flat group scheme?' It turns out that this idea of finite flatness is equivalent to the notion of being unramified at the primes which do not lie above p. In this sense, finite flatness extends the notion of $\overline{\rho}_{E,p}$ being unramified. We delve deeper into these concepts in Section 3.4 and Section 3.5.

We finish this section by proving two results which relate elliptic curves with their representations. These results do not directly involve the theory of the Tate curve but are stated here for lack of a better place.

Proposition 3.28. Let K be a local field with residue field k, p the characteristic of k, $\mathrm{Frob}_K \in \mathrm{Gal}(\overline{K}/K)$ a Frobenius element and $\ell \neq p$ a prime. Let E/K be an elliptic curve with good reduction. Then

$$\mathrm{Tr}(\rho_{E,\ell}(\mathrm{Frob}_K)) = 1 + \#k - \#\tilde{E}(k)$$

where $\tilde{E}$ is the reduction of E. In other words, $\mathrm{Tr}(\rho_{E,\ell}(\mathrm{Frob}_K))$ is equal to the trace of Frobenius (see example 2.8). ■

Proof. By Proposition 2.6, we have that $\tilde{E}[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank 2. By considering E as an elliptic curve over $K(E[\ell^n])$, it follows from Proposition 2.17 that there is an isomorphism $E[\ell^n] \to \tilde{E}[\ell^n]$ of $\mathrm{Gal}(\overline{K}/K)$-modules. Taking the inverse limit, gives an isomorphism

$$T_\ell(E) \cong T_\ell(\tilde{E}) \tag{3.5}$$

of $\mathrm{Gal}(\overline{K}/K)$-modules. Let $\psi\colon \tilde{E} \to \tilde{E}$ denote the Frobenius endomorphism. Then the action of the Frobenius element Frob_K on $\tilde{E}[\ell^n]$ acts as ψ for all n. Take a matrix representation of the induced morphism $\psi_\ell\colon T_\ell(\tilde{E}) \to T_\ell(\tilde{E})$. Then, via the isomorphism (3.5), we see that the matrix representing ψ_ℓ is equivalent to $\rho_{E,\ell}(\mathrm{Frob}_K)$. Taking traces and using Example 2.8 concludes the proof. □

Remark 3.29. From the proof of Proposition 3.28, Proposition 2.7 and Corollary 3.15 we see that

$$\chi_\ell(\mathrm{Frob}_K) = \det(\rho_{E,\ell}(\mathrm{Frob}_K)) = \det(\psi_\ell) = \deg(\psi) = \#k.$$

This fact is not needed in this thesis, but does appear often in the study of Galois representations. ■

Proposition 3.30. Let E be an elliptic curve over a local field and suppose that E has potential multiplicative reduction. Then there is a quadratic twist E^d/K of E such that E^d/K has split multiplicative reduction. ■

Proof. Suppose we are given a short Weierstrass equation with associated coefficients c_4 and c_6 for E. For any $d \in K^\times \setminus K^{\times 2}$ the quadratic twist E^d of E by d is given by

$$E^d\colon dy^2 = x^3 + c_4x + c_6.$$

Via the coordinate transformation $X = dx$ and $Y = d^{-2}y$ we obtain the equation

$$E^d\colon Y^2 = X^3 + d^2c_4X + d^3c_6 \tag{3.6}$$

for E^d. Consider the quantity $\gamma(E/K) \in \bar{K}^\times/\bar{K}^{\times 2}$ as in (3.4). By Theorem 3.20, if $\gamma(E/K) = 1$ then E/K has split multiplicative reduction and we are done. If $\gamma(E/K) \neq 1$, then the quadratic twist E^d of E by $d \in \bar{K}^\times \setminus \bar{K}^{\times 2}$ has associated coefficients d^2c_4 and d^3c_6 according to (3.6). Since E and E^d are isomorphic over $K(\sqrt{d})$ they have the same j-invariant and hence E^d has potentially multiplicative reduction, too. Then

$$\gamma(E^d/K) = -\frac{d^2c_4}{d^3c_6} \bmod K^{\times 2} = d^{-1}\gamma(E/K).$$

Choose d as $\gamma(E/K)^{-1}$. For this choice of d, it follows from Theorem 3.20 that E^d has split multiplicative reduction. □

3.4 Group schemes

In the previous section it was alluded to that the idea of ramification of the mod-p Galois representation $\overline{\rho}_{E,p}$ over a local field K of residue characteristic p is often independent of a properties of the elliptic curve E/K. A Galois representation being finite flat extends the notion of being unramified and gives us something meaningful to say about what happens at the primes above p. To introduce what it means for a Galois representation to be finite flat we require the language of group schemes. In this section we introduce group schemes and introduce what it means to be finite flat. In the next section we relate properties of E to the finite flatness of $\overline{\rho}_{E,p}$.

In the category Sch of schemes, every scheme X represents a contravariant functor $\mathsf{Sch}^{\mathrm{op}} \to \mathsf{Set}$ sending $T \mapsto X(T) \coloneqq \mathrm{Hom}_{\mathsf{Sch}}(T, X)$. For example, the scheme $\operatorname{Spec} \mathbb{Z}[Y, Y^{-1}]$ represents the covariant functor

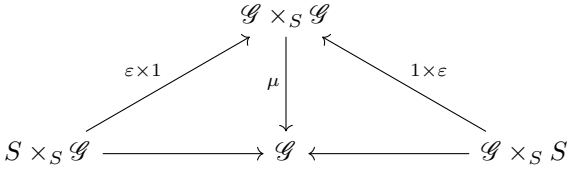
$$T \mapsto \mathrm{Hom}_{\mathsf{Sch}}(T, \operatorname{Spec} \mathbb{Z}[Y, Y^{-1}]) \cong \mathrm{Hom}_{\mathsf{Ring}}(\mathbb{Z}[Y, Y^{-1}], \mathcal{O}_T(T)) \cong \mathcal{O}_T(T)^\times,$$

where $\mathcal{O}_T$ denotes the structure sheaf of T. We consider the functor represented by $\operatorname{Spec} \mathbb{Z}[Y, Y^{-1}]$ as a functor to Set. However, for a given scheme T, the set $\mathcal{O}_T(T)^\times$ has additional structure, namely, that of a group. We would like to harness this group structure so we need to restrict our study to a certain type of scheme. These schemes are precisely group schemes; those objects of Sch that represent functors from $\mathsf{Sch}^{\mathrm{op}}$ to the category Grp of groups.

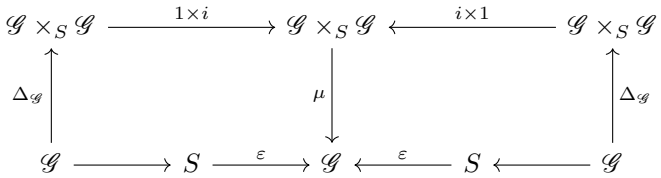
Definition 3.31. Let S be a scheme. *A group scheme over S* is an S-scheme $\mathscr{G} \to S$ along with morphisms

$$\varepsilon \colon S \to \mathscr{G}, \qquad i \colon \mathscr{G} \to \mathscr{G} \qquad \text{and} \qquad \mu \colon \mathscr{G} \times_S \mathscr{G} \to \mathscr{G}$$

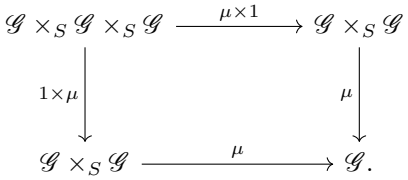
such that the following diagrams commute.
(i) (identity)



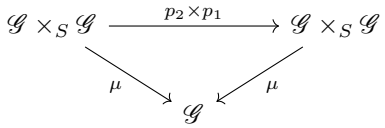
(ii) (inverse)



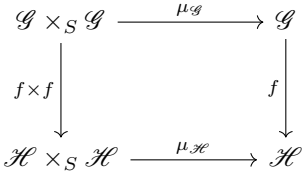
where $\Delta_{\mathscr{G}} \colon \mathscr{G} \to \mathscr{G} \times_S \mathscr{G}$ is the diagonal map.
(iii) (assocativity)



We call $\mathscr{G}$ a *commutative group scheme over S* if in addition to (i)-(iii), the diagram (iv) (commutativity)



commutes. A *morphism $f \colon \mathscr{G} \to \mathscr{H}$ of S-group schemes* is an S-scheme morphism such that



commutes. Here, $\mu_{\mathscr{G}}$ and $\mu_{\mathscr{H}}$ denote the multiplications on $\mathscr{G}$ and $\mathscr{H}$ respectively. ■

Example 3.32. 1. The affine scheme $\operatorname{Spec}\mathbb{Z}[Y,Y^{-1}]$ is a group scheme over $\mathbb{Z}$. The associated morphisms $\varepsilon\colon \operatorname{Spec}\mathbb{Z} \to \operatorname{Spec}\mathbb{Z}[Y,Y^{-1}]$ and $i\colon \operatorname{Spec}\mathbb{Z}[Y,Y^{-1}] \to \operatorname{Spec}\mathbb{Z}[Y,Y^{-1}]$ are induced by ring morphisms

$$\begin{aligned} \tilde{\varepsilon}\colon \mathbb{Z}[Y,Y^{-1}] &\to \mathbb{Z} \\ Y &\mapsto 1 \\ \text{and} \quad \tilde{i}\colon \mathbb{Z}[Y,Y^{-1}] &\to \mathbb{Z}[Y,Y^{-1}] \\ Y &\mapsto Y^{-1}. \end{aligned}$$

For the multiplication morphism μ, we have

$$\operatorname{Spec}\mathbb{Z}[Y,Y^{-1}] \times_{\mathbb{Z}} \operatorname{Spec}\mathbb{Z}[Y,Y^{-1}] \cong \operatorname{Spec}\left(\mathbb{Z}[Y,Y^{-1}] \otimes_{\mathbb{Z}} \mathbb{Z}[Y,Y^{-1}]\right) \cong \operatorname{Spec}\mathbb{Z}[Y_1,Y_1^{-1},Y_2,Y_2^{-1}].$$

The morphism μ is then induced by the ring morphism $\tilde{\mu}\colon \mathbb{Z}[Y,Y^{-1}] \to \mathbb{Z}[Y_1,Y_1^{-1},Y_2,Y_2^{-1}]$ sending $Y \mapsto Y_1Y_2$. Commutativity of the diagrams in Definition 3.31 can be checked in the category of commutative rings. The group scheme $\operatorname{Spec}\mathbb{Z}[T,T^{-1}]$ is denoted by $\mathbb{G}_m$. For a scheme S, the scheme $\mathbb{G}_{m,S} = \mathbb{G}_m \times_{\mathbb{Z}} S$ is a group scheme over S.

2. Let n be a positive integer and let μ_n denote the affine scheme $\operatorname{Spec}\mathbb{Z}[X]/(X^n-1)$. The scheme μ_n is a closed subscheme of $\mathbb{G}_m$ and it turns out that μ_n inherits the group structure from $\mathbb{G}_m$. This can be verified directly or can be seen from Example 3.35. The group scheme μ_n represents the functor $T \mapsto \mu_n(\mathcal{O}_T(T))$ where, for a ring R, $\mu_n(R)$ denotes the n^{th} roots of unity of R. For a scheme S, let $\mu_{n,S}$ denote the base change $\mu_n \times_{\mathbb{Z}} S$

3. Let G be a group. Consider the scheme

$$G_{\mathbb{Z}} = \coprod_{g\in G} \operatorname{Spec}\mathbb{Z}.$$

Define a multiplication $\mu\colon G_{\mathbb{Z}} \times_{\mathbb{Z}} G_{\mathbb{Z}} \to G_{\mathbb{Z}}$ via sending the component corresponding to (g,h) to the component corresponding to gh. Similarly define an inversion and identity on $G_{\mathbb{Z}}$. In this way $G_{\mathbb{Z}}$ defines a group scheme over $\mathbb{Z}$. For an arbitrary scheme S, let G_S denote the group scheme $G_{\mathbb{Z}} \times_{\mathbb{Z}} S$ over S. The scheme G_S represents the functor sending a scheme T over S to the set of locally constant functions $T \to G$ where G has the discrete topology. In particular, if T is non-empty and connected, $G_S(T) \cong G$. In the literature, G_S is sometimes denoted by $\underline{G}$.

4. Let E/K be an elliptic curve over a field (or more generally, let E/K be an abelian variety). Then the group law on E defines a group scheme structure on E. The morphism $\operatorname{Spec}K \to E$ sending the generic point of $\operatorname{Spec}K$ to the distinguished K-rational point of E that serves as the identity is the identity morphism ε. In this way, E defines a group scheme over K. The group scheme E represents the functor sending a scheme T over K to $E(T)$ in such a way that if $T = \operatorname{Spec}L$ with L/K an algebraic extension, the group $E(T)$ is the group of L-rational points of E. ■

It is apparent that the group schemes in Example 3.32 represent functors $\mathsf{Sch}^{\mathrm{op}} \to \mathsf{Grp}$. It is not clear that an arbitrary group scheme $\mathscr{G}$ over a fixed base scheme S represents such a functor. Let T be a scheme over S and, if Sch_S denotes the category of S-schemes, let $\mathscr{G}(T) \coloneqq \operatorname{Hom}_{\mathsf{Sch}_S}(T,\mathscr{G})$. For two elements φ and ψ of $\mathscr{G}(T)$, define the element $\varphi \star \psi \in \mathscr{G}(T)$ as the map making

$$\begin{array}{ccc} T \times_S T & \xrightarrow{\varphi\times\psi} & \mathscr{G} \times_S \mathscr{G} \\ {\scriptstyle \Delta_T}\uparrow & & \downarrow{\scriptstyle \mu} \\ T & \xrightarrow{\varphi\star\psi} & \mathscr{G} \end{array}$$

commute. This assignment $\mathscr{G}(T) \times \mathscr{G}(T) \to \mathscr{G}(T)$, $(\varphi,\psi) \mapsto \varphi \star \psi$ defines a group structure on $\mathscr{G}(T)$ where the identity is the morphism $T \to S \xrightarrow{\varepsilon} \mathscr{G}$. In fact, it defines a group structure on $\mathscr{G}(T)$ compatible with the morphisms in Sch_S.

Proposition 3.33. [51, Proposition 3.2] Let $\mathscr{G}$ be a group scheme over S. Let T be an S-scheme. Then $\mathscr{G}(T)$ is group where the composition is defined by $\star$. Further, if $f\colon T \to T'$ is a morphism of S-schemes, then f induces a group homomorphism $f^*\colon \mathscr{G}(T') \to \mathscr{G}(T')$ sending $\varphi \mapsto \varphi \circ f$. ■

If $\mathscr{G}$ is a commutative group scheme over S, then $\mathscr{G}(T)$ is an abelian group. Indeed, for arbitrary $\varphi, \psi \in \mathscr{G}(T)$,

$$\varphi \star \psi = \mu(\varphi \times \psi)\Delta_T = \mu(p_2 \times p_1)(\varphi \times \psi)\Delta_T = \mu(\psi \times \varphi)\Delta_T = \psi \star \varphi.$$

We now have that group schemes represent functors $\mathsf{Sch}^{\mathrm{op}} \to \mathsf{Grp}$. Tate shows in [58, Section 1.6] that the converse is also true. That is, if an S-scheme $\mathscr{G}$ such that $\mathscr{G}(T)$ is a group for every S-scheme T and such that any S-morphism $f\colon T \to T'$ induces a group homomorphism $f^*\colon \mathscr{G}(T') \to \mathscr{G}(T)$, then there there is a unique way of making $\mathscr{G}$ a group scheme. With this equivalence, group schemes not only induce representable functors $\mathsf{Sch}^{\mathrm{op}} \to \mathsf{Grp}$ but are precisely such functors.

Example 3.34. 1. The S-scheme S is trivially a group scheme over S. Further, since S is a terminal object in Sch_S, it follows that S represents the functor sending $T \mapsto \{1\}$, the trivial group.

2. Let $f\colon \mathscr{G} \to \mathscr{H}$ be a moprhism of group schemes over a base scheme S. We aim to define the kernel of f. Following [12, Section III.2] we can define the kernel as the fibered product $\ker f \coloneqq \mathscr{G} \times_{\mathscr{H}} S$ fitting in the pull-back diagram

$$\begin{array}{ccc} \mathscr{G} \times_{\mathscr{H}} S & \xrightarrow{p_2} & S \\ \downarrow & & \downarrow{\scriptstyle \varepsilon_{\mathscr{H}}} \\ \mathscr{G} & \xrightarrow{f} & \mathscr{H} \end{array}$$

Then $\ker f$ is again a group scheme over S with $p_2\colon \ker f \to S$. The inverse and multiplication on $\ker f$ are induced from $\mathscr{G}$. The group scheme $\ker f$ represents the functor $T \mapsto \ker(\mathscr{G}(T) \xrightarrow{f_*} \mathscr{H}(T))$ where $f_*\colon \sigma \mapsto f\sigma$. Indeed, $(\ker f)(T)$ is the fibred product $\mathscr{G}(T) \times_{\mathscr{H}(T)} \{1\}$ in Grp. According to the preceding paragraph, defining $\ker f$ to be the scheme representing this functor would be sufficient. The construction above shows that such a representing object exists in Sch_S.

3. More generally, if $\mathscr{G}$ is a group scheme over S and $T \to S$ is a morphism. Then $\mathscr{G} \times_S T$ is a group scheme. ■

Example 3.34.3 shows that a group scheme over S is a collection of group schemes over fields; for every element $s \in S$ we get a group scheme $\mathscr{G}_s$ over the residue field at s. This interpretation is used as a foundation in [51, Chapter IV].

Let $\mathscr{G}$ be a group scheme over a scheme S and let m be a positive integer. Define the *multiplication by* $[m]$ recursively as

$$[1] = \mathrm{id}_{\mathscr{G}} \quad \text{and} \quad [m] = \mu(\mathrm{id}_{\mathscr{G}} \times_S [m-1]).$$

Let $\mathscr{G}[m]$ denote $\ker[m]$.

Example 3.35. Let $\mathbb{G}_m$ be as in Example 3.32 and let n be a positive integer. Then the multiplication by n morphism $[n]\colon \mathbb{G}_m \to \mathbb{G}_m$ is induced from the ring morphism $\mathbb{Z}[Y, Y^{-1}] \to \mathbb{Z}[Y, Y^{-1}]$ sending $Y \mapsto Y^n$. The kernel of $[n]$ is μ_n. Indeed, $\mathbb{G}_m[n]$ is the group scheme representing the functor sending a scheme T to the n-torsion of $\mathcal{O}_T(T)^\times$, which is precisely the functor representing μ_n and hence they are equal, by Yoneda's lemma. ■

Let R be a Dedekind domain with field of fractions K, a perfect field. Further, and let $\mathscr{G} \to \operatorname{Spec} R$ be a commutative group scheme. Then by Proposition 3.33 the set $\mathscr{G}(\overline{K})$ forms an abelian group. In fact, it carries the structure of a $\mathrm{Gal}(\overline{K}/K)$-module in the following sense. Let $\varphi \in \mathscr{G}(\overline{K})$ be a $\overline{K}$-valued point and let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then σ induces a morphism $\operatorname{Spec} \overline{K} \to \operatorname{Spec} \overline{K}$ over K. Then let the action of σ on φ be

$$\varphi^\sigma = \varphi \circ \sigma$$

This is again a morphism over R and it is compatible with the group law on $\mathscr{G}$.

So far we covered some general theory of group schemes. Our main reason for the study of group schemes is to study the mod-m representations $\overline{\rho}_{E,m}$ associated to an elliptic curve. These representations act on a finite $\mathrm{Gal}(\overline{K}/K)$-module. Thus we need to subject the group schemes we study to some finiteness condition. This condition is as follows.

Definition 3.36. Let $f\colon X \to S$ be a morphism of X to a locally Noetherian scheme S and let $\mathcal{O}_X$ and $\mathcal{O}_S$ denote the structure sheaves. We say that f is *finite flat* if there is a covering of open affine subsets U of S such that the morphisms $f^{-1}(U) \to U$ are of the form $\operatorname{Spec} A \to \operatorname{Spec} R$ where A is a free R-module of finite rank. If X is a scheme over S then we say that X is *finite flat* if the structure morphism $X \to S$ is. ■

For Definition 3.36 we require the existence of an open cover of the base scheme with the given property, however, this condition is equivalent to asking that this property holds for every open affine of the base (see [54, Tag 01wg] and [54, Tag 01U2]). If X is a finite flat scheme over a locally Noetherian base S, then the rank of $X \to S$ is a locally constant function. If X is connected then we call this value the *order* of X (over S).

Example 3.37. 1. The group scheme $\mu_n = \operatorname{Spec} \mathbb{Z}[X]/(X^n - 1)$ over $\mathbb{Z}$ is a finite flat group scheme over $\mathbb{Z}$. Its order is n.

2. Given a group G, the group scheme $G_{\mathbb{Z}}$ over $\mathbb{Z}$ is a finite flat group scheme if and only if the group G is finite. In this case, the order of $G_{\mathbb{Z}}$ is $\#G$.

3. The group scheme $\mathbb{G}_m = \operatorname{Spec} \mathbb{Z}[Y, Y^{-1}]$ over $\mathbb{Z}$ is not finite flat. Indeed, $\mathbb{Z}[Y, Y^{-1}]$ is free as a $\mathbb{Z}$-module, but not of finite rank. ■

The next proposition gives some idea to why Definition 3.36 is the 'correct' finiteness condition.

Proposition 3.38. Let R be a Dedekind domain and let K be its field of fractions. Let $X \to \operatorname{Spec} R$ be a finite flat scheme over R of order n. Suppose that K has characteristic 0 and let L/K be an algebraic extension. Then $X(L)$ is finite of order at most n with equality if $L = \overline{K}$ and if X is reduced. ■

Proof. Since $\operatorname{Spec} R$ is affine and $X \to \operatorname{Spec} R$ is finite flat, it follows that $X = \operatorname{Spec} A$ for some R-algebra A which is of finite rank as an R-module. Let $A \to L$ correspond to an L valued point of X. Then $A \to L$ factors as

$$A \longrightarrow A \otimes_R K \longrightarrow L$$

Let $A_K = A \otimes_R K$. Then A_K is a K-algebra of dimension n. A well known fact is that finite dimensional K-algebra's are Artinian and hence, by the structure theorem of Artinian rings,

$$A_K = \prod_{i=1}^{r} A_i$$

with A_i an Artinian local ring. Note that $n = \sum_{i=1}^{r} \dim_K A_i$. What remains to be shown is that there are only finitely many K-algebra morphisms $A_i \to L$ for all i. Let $\mathfrak{m}_i$ denote the maximal ideal of A_i. Then $\mathfrak{m}_i$ is the set of nilpotent elements of A_i and hence the morphism $A_i \to L$ factors through $A_i/\mathfrak{m}_i \to L$. Since L is an algebraic extension of K, the amount of morphisms $A_i/\mathfrak{m}_i \to L$ does not exceed $[A_i/\mathfrak{m}_i : K]$. Therefore, there are only finitely many of such morphisms which proves the first assertion. For the second assertion, if A is reduced, then the $\mathfrak{m}_i$ are trivial and hence A_i/K are finite extensions such that $n = \sum_{i=1}^{r} [A_i : K]$. If $L = \overline{K}$, then the number of morphisms $A_i \to L$ equals $[A_i : K]$. □

Finally, we connect the theory of finite flat commutative group schemes to Galois representations.

Definition 3.39. Let K be a local field of characteristic 0 with valuation ring $\mathcal{O}_K$. Let M be a finite module and let $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(M)$ be a Galois representation. We say that ρ is *finite flat (over $\mathcal{O}_K$)* if there exists a finite flat group scheme $\mathscr{G}$ over $\mathcal{O}_K$ such that $\mathscr{G}(\overline{K})$ is isomorphic to M as an $\mathrm{Gal}(\overline{K}/K)$-module (where the $\mathrm{Gal}(\overline{K}/K)$-action on M is defined by ρ). ■

Let $\mathscr{G}$ be a finite commutative group scheme over a valuation ring $\mathcal{O}_K$ of a local field K. Then any $\overline{K}$-point of $\mathscr{G}$ over $\mathcal{O}_K$ gives a $\overline{K}$-valued point over $\mathcal{O}_K$ and vice versa. Therefore, for a representation ρ acting on a finite module M to be finite flat is equivalent to asking that M is isomorphic to the $\overline{K}$-valued points of the generic fiber of a commutative group scheme over $\mathcal{O}_K$.

Example 3.40. 1. Let n be an integer and let K be a local field with ring of intgers $\mathcal{O}_K$. Then the n^{th} cyclotomic character $\chi_n\colon \mathrm{Gal}(\overline{K}/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is finite flat. Indeed, $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to the $\mathrm{Gal}(\overline{K}/K)$-module attached to $\mu_{n,\mathcal{O}_K}$.

2. Let G be a finite abelian group and let $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(G)$ be the trivial representation. Then ρ is finite flat and is associated to the finite flat group scheme $G_{\mathcal{O}_K}$.

3. Let $\rho_1\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(M)$ and $\rho_2\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(N)$ be two finite flat Galois representations. Then the Galois representation $\rho_1 \oplus \rho_2\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(M \oplus N)$ given by sending

$$\sigma \mapsto \big((m,n) \mapsto (\rho_1(\sigma)(m), \rho_2(\sigma)(n)\big)$$

is finite flat. Indeed, if ρ_1 and ρ_2 arise as the finite flat group schemes $\mathscr{G}_1$ and $\mathscr{G}_2$, respectively. Then $\rho_1 \oplus \rho_2$ arises as the finite flat group scheme $\mathscr{G}_1 \times_{\mathcal{O}_K} \mathscr{G}_2$. ■

The abelian group we are most interested in is of course the m-torsion of an elliptic curve. Finite flatness of such groups is a deep question and is explored in the next section.

3.5 Finite flatness of m-torsion

Let E/K be an elliptic curve over a local field of characteristic 0 and let m be a positive integer. In this section we write down some sufficient conditions on E/K which allows us to deduce that $\overline{\rho}_{E,m}$ is finite flat. In order to do this we need the theory of the Néron model of an elliptic curve. We open this section by introducing this model. We do this by following some results in [51, Section IV].

We have already seen minimal models for curves over the field of fractions of a Dedekind domain in Section 2.3.1. We applied this theory to say something about the special fiber of a minimal model of an elliptic curve. This study was completely geometric and nothing was said about how the group law extended from an elliptic curve to its minimal model. We would like to have a model $\mathcal{C}$ for an elliptic curve such that the group law extends to $\mathcal{C}$ in such a way that $\mathcal{C}$ is a group scheme. The following result gives some idea of what we must require of such a model.

Proposition 3.41. [51, Theorem IV.5.3] Let K be a local field and let $\mathcal{O}_K$ be its valuation ring. Let E/K be an elliptic curve and choose a minimal Weierstrass equation for E. This equation defines a scheme $\mathcal{E} \subset \mathbb{P}^2_{\mathcal{O}_K}$. Let $\mathcal{E}^0$ denote the largest sub-scheme of $\mathcal{E}$ such that $\mathcal{E}^0 \to \operatorname{Spec} \mathcal{O}_K$ is smooth. Then the addition and negation of E extend to $\mathcal{O}_K$-morphisms

$$\mathcal{E}^0 \times_{\mathcal{O}_K} \mathcal{E}^0 \longrightarrow \mathcal{E}^0 \qquad \text{and} \qquad \mathcal{E}^0 \longrightarrow \mathcal{E}^0$$

which define a group scheme structure on $\mathcal{E}^0$. ■

This result implies that we require some smoothness property for our model. We also do not want our model $\mathcal{C}/\mathcal{O}_K$ of an elliptic curve E/K to be 'too large' compared to E. 'Not too large' in this case means that we require the condition that $E(K) = \mathcal{C}(R)$. It turns out that the following definition captures this idea perfectly.

Definition 3.42. Let R be a Dedekind domain with fraction field R and let E/K be an elliptic curve. A *Néron model* for E/K is a smooth group scheme $\mathscr{E}/R$ whose generic fiber is E/K and for every smooth scheme $\mathcal{X}$ over R with generic fiber X/K we have

$$\mathrm{Hom}_K(X, E) = \mathrm{Hom}_R(\mathcal{X}, \mathscr{E}).$$ ■

Via the standard argument, a Néron model is unique up to unique isomorphism. Recall from Proposition 2.22 that for an elliptic curve E/K and its minimal proper regular model $\mathcal{C}/\mathcal{O}_K$ we have that

$$\mathcal{C}^0(\mathcal{O}_K) = \mathcal{C}(\mathcal{O}_K) = E(K)$$

where $\mathcal{C}^0$ is the largest subscheme of $\mathcal{C}$ such that $\mathcal{C}^0 \to \operatorname{Spec} \mathcal{O}_K$ is smooth. Thus $\mathcal{C}^0$ satisfies the property of a model which is 'not too large'. In view of this intuition and of Proposition 3.41 the following Theorem should make sense.

Theorem 3.43. [12, Chapter VIII][51, Theorem IV.6] Let R be Dedekind domain and let K be its field of fractions. Let E/K be an elliptic curve and let $\mathcal{C}/R$ be its minimal regular proper model. Let $\mathcal{C}^0/R$ be the largest subscheme of $\mathcal{C}$ which is smooth over R. Then $\mathcal{C}^0/R$ is a Néron model for E/K. ■

Though motivated by intuition, the proof of Theorem 3.43 is not at all trivial and requires heaps of abstract algebraic geometry. It turns out that, over a local field, if E has good reduction then a minimal Weierstrass equation for E defines a Néron model [51, Corollary IV.6.3]. If an elliptic curve E does not have good reduction, then it is far less obvious what the Néron model for E looks like. For example, the special fiber of such a model can consist of several components as is evident by Theorem 2.24.

The Néron model of an elliptic curve gives us the following result. The proof we present here is adapted from [10, Theorem 1.2].

Proposition 3.44. Let K be a local field of characteristic 0 with valuation ring $\mathcal{O}_K$. Let E/K be an elliptic curve with good reduction and let $\mathscr{E}/\mathcal{O}_K$ be the Néron model for E/K. Then, for any positive integer m, the group scheme $\mathscr{E}[m]$ is finite flat over $\mathcal{O}_K$. ■

Proof. We show that the multiplication by m map $[m]\colon \mathscr{E} \to \mathscr{E}$ is finite and flat. Then since these properties are preserved under base extension, it then follows that $\ker[m] = \mathscr{E}[m]$ is finite flat over $\mathcal{O}_K$. Since E/K has good reduction, the special fiber of $\mathscr{E} \to \operatorname{Spec} \mathcal{O}_K$ is geometrically connected, hence $\mathscr{E}$ has geometrically connected fibers. From this fact and from some deep results in algebraic geometry (see [10, Theorem 1.2] for details) it follows that $[m]$ is finite and flat. □

From this result we would like to deduce that $\overline{\rho}_{E,m}$ is finite flat when E/K has good reduction. However, it is not at all clear what the structure of $\mathscr{E}[m]$ is, let alone of $\mathscr{E}[m](\overline{K})$. We will show that $\overline{\rho}_{E,m}$ arises from the generic fiber of $\mathscr{E}[m]$. For this we need an intermediate result about group schemes.

Let R be a Dedekind domain with field of fractions K. Given group schemes $\mathscr{G}$ and $\mathscr{H}$ over R and a morphism of group schemes $f\colon \mathscr{G} \to \mathscr{H}$. Let η denote the generic fiber of $\operatorname{Spec} R$. For a scheme X over R, let the base change $X \times_R \operatorname{Spec} K$ be denoted by X_η. Then we have an induced morphism of group schemes

$$f_\eta\colon \mathscr{G}_\eta \to \mathscr{H}_\eta$$

defined to be $f \times_R 1$. We have the following result.

Proposition 3.45. Let R be a Dedekind domain with field of fractions K. Let $f\colon \mathscr{G} \to \mathscr{H}$ be a group scheme morphism. Then $\ker(f)_\eta = \ker(f_\eta)$. ■

Proof. We have

$$\ker(f)_\eta = (\mathscr{G} \times_{\mathscr{H}} \operatorname{Spec} R) \times_R \operatorname{Spec} K.$$

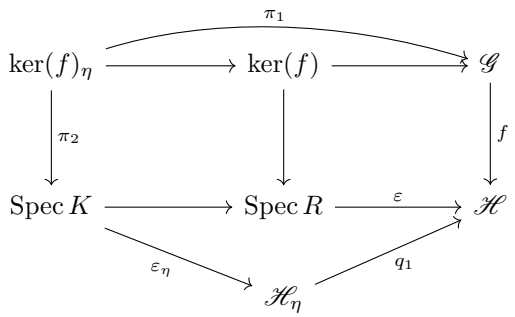
We show that $\ker(f)_\eta$ satisfies the universal property of

$$\ker(f_\eta) = (\mathscr{G} \times_R \operatorname{Spec} K) \times_{\mathscr{H}_\eta} \operatorname{Spec} K.$$

Denote the projections maps

$$\begin{aligned} q_1&\colon \mathscr{H}_\eta \to \mathscr{H} \\ p_1&\colon \mathscr{G}_\eta \to \mathscr{G} \\ \pi_1&\colon \ker(f)_\eta \to \ker(f) \to \mathscr{G} \\ \pi_2&\colon \ker(f)_\eta \to \operatorname{Spec} K. \end{aligned}$$

Further, if $\varepsilon\colon \operatorname{Spec} R \to \mathscr{H}$ is the identity, then denote $\varepsilon_\eta\colon \operatorname{Spec} K \to \mathscr{H}_\eta$ the induced identity which is such that $q_1\varepsilon_\eta$ is equal to the inclusion $\operatorname{Spec} K \to \operatorname{Spec} R$ followed by ε. For additional clarity, some of the maps and their relations are recorded in the following commutative diagram



(3.7)

Let $\psi\colon \ker(f)_\eta \to \mathscr{G} \times_R \operatorname{Spec} K$ be the morphism induced by π_1 and π_2. So ψ satisfies $p_1\psi = \pi_1$. Then we have a commutative diagram

$$\begin{array}{ccc} \ker(f)_\eta & \xrightarrow{\pi_2} & \operatorname{Spec} K \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varepsilon_\eta} \\ \mathscr{G}_\eta & \xrightarrow{f_\eta} & \mathscr{H}_\eta. \end{array} \tag{3.8}$$

To see this, first note that the morphisms p_1 and q_1 are monomorphisms in the category of schemes. To see this, note that p_1 is a base change of the inclusion $\operatorname{Spec} K \to \operatorname{Spec} R$ and according to [54, Tag 01L1], monomorphisms are stable under base-change. The map $\operatorname{Spec} K \to \operatorname{Spec} R$ is a monomorphism since it is injective on points and the induced local morphism at η is the identity and in particular, surjective (see [54, Tag 01L1]). Similarly, q_1 is a monomorphism. We have

$$q_1 f_\eta \psi = f p_1 \psi = f\pi_1 = q_1 \varepsilon_\eta \pi_2$$

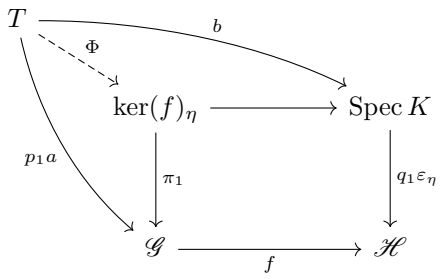
where the third equality follows from commutativity of (3.7). Since q_1 is a monomorphism, commutativity of (3.8) follows. We show that (3.8) is a pull-back diagram, from uniqueness it then follows that $\ker(f)_\eta = \ker(f_\eta)$. Let T be a scheme and let $a\colon T \to \mathscr{G}_\eta$ and $b\colon T \to \operatorname{Spec} K$ be morphisms such that $f_\eta a = \varepsilon_\eta \pi_2$. We aim to show that there is a unique morphism $\Phi\colon T \to \ker(f)_\eta$ such that $\pi_2\Phi = b$ and $\psi\Phi = a$. We have

$$\ker(f)_\eta = (\mathscr{G} \times_{\mathscr{H}} \operatorname{Spec} R) \times_R \operatorname{Spec} K = \mathscr{G} \times_{\mathscr{H}} \operatorname{Spec} K$$

Therefore, giving a map $T \to \ker(f)_\eta$ is the same as giving maps $T \to \mathscr{G}$ and $T \to \operatorname{Spec} K$ such that the appropriate diagram commutes (i.e. the outermost square of (3.9)). We have a map $p_1 a\colon T \to \mathscr{G}$ and we have

$$q_1 \varepsilon_\eta b = q_1 f_\eta a = f p_1 a$$

so we get a unique $\Phi\colon T \to \ker(f)_\eta$ such that



(3.9)

commutes. Since (3.9) commutes, it follows that

$$p_1\psi\Phi = \pi_1\Phi = p_1 a \quad \text{and} \quad \pi_2\Phi = b$$

and since p_1 is a monomorphism, $\psi\Phi = a$. It follows that (3.8) is a pull-back diagram. □

Proposition 3.46. Let K be a local field and let E/K be an elliptic curve with good reduction. Then for every positive integer m, the Galois representation $\overline{\rho}_{E,m}$ is finite flat. ■

Proof. Let $\mathcal{O}_K$ be the valuation ring of K and let $\mathscr{E}/\mathcal{O}_K$ be the Néron model of E/K. Then by Proposition 3.44 $\mathscr{E}[m]$ is finite flat for all positive integers m. Let η denote the generic fiber of $\operatorname{Spec} \mathcal{O}_K$, then $\mathscr{E}_\eta = E$ and by Proposition 3.45,

$$\mathscr{E}[m]_\eta = \mathscr{E}_\eta[m] = E[m].$$

The Galois structure of $E[m]$ is (by definition) given by $\overline{\rho}_{E,m}$ and hence it follows that $\overline{\rho}_{E,m}$ is finite flat. □

If we go by the idea that finite flatness of a representation extends the idea of being unramified, then, by the criterion of Néron-Ogg-Shavarevich, one should expect Proposition 3.46 to hold. Except, we get something more here, namely, finite flatness of $E[m]$ at integers m which are not co-prime to the residue characteristic of K. In this sense, finite-flatness extends the idea of being unramified at good reduction.

It can occur that for some integer m the representation $\overline{\rho}_{E,m}$ is not finite flat whilst E has bad reduction. To see this, suppose that K is a local field with residue characteristic p and that E/K has potentially multiplicative reduction. By Proposition 3.30 there is a trivial or quadratic twist $E \otimes \eta$ of E by a Galois character η such that $E \otimes \eta$ has split multiplicative reduction. By Theorem 3.20, there is some $q \in K$ such that $E \otimes \eta$ is K-isomorphic to the Tate curve E_q. Suppose that E is such that q is a p^{th} power. The p-torsion of E_q is generated by $q^{1/p}$ and ζ_p where ζ_p is a primitive p^{th} root of unity. Then, since q is a p^{th} power, $q^{1/p} \in K$ and

$$\overline{\rho}_{E_q,p} \sim \begin{pmatrix} \chi_p & 0 \\ 0 & 1 \end{pmatrix}.$$

It follows that $\overline{\rho}_{E,p}$ arises as a finite flat group scheme, namely as

$$\mu_{p,\mathcal{O}_K} \times_{\mathcal{O}_K} (\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_K}$$

where $\mathcal{O}_K$ is the valuation ring of K. Since E_q and $E \otimes \eta$ are isomorphic over K, it follows that $\overline{\rho}_{E_q,p} \sim \overline{\rho}_{E\otimes\eta,p}$ and from Proposition 3.18 it follows that

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \chi_p \cdot \eta & 0 \\ 0 & \eta \end{pmatrix}.$$

The character η is unramified. If η is trivial then this fact is clear. If η is non-trivial, then E/K does not have split multiplicative reduction. Let $d \in K^\times \setminus K^{\times 2}$ be such that η corresponds to $K(\sqrt{d})$. Then E/K not having split multiplicative reduction is equivalent to d not being a square in the residue field of K. If k denotes the residue field, then $k(\sqrt{d})/k$ is a degree 2 extension and hence $K(\sqrt{d})/K$ is unramified. Thus, if I_K denotees the inertia group $G_0(\overline{K}/K)$ of K. Then

$$\overline{\rho}_{E,p}|_{I_K} = \overline{\rho}_{E_q,p}|_{I_K}$$

which means that $\overline{\rho}_{E,p}|_{I_K}$ arises as the finite flat group scheme

$$\mu_{p,\mathcal{O}_{K^{\text{nr}}}} \times_{\mathcal{O}_{K^{\text{nr}}}} (\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_{K^{\text{nr}}}}.$$

According to [16, Proposition 8.2] (note that this proof is for the special case $K = \mathbb{Q}_p$ but relies on [41, Corollaire 2.2.3] which holds for general local fields), this is enough for $\overline{\rho}_{E,p}$ to arise as a finite flat group scheme over $\mathcal{O}_K$. The above example is in the particular case that q is a p^{th} power. If Δ denotes the discriminant of E and v the normalized valuation of K, then a necessary condition for q to be a p^{th} power is that

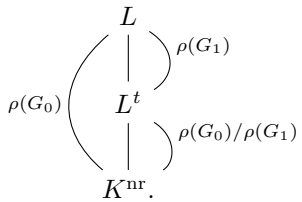
$$v(\Delta) = v(q) \equiv 0 \bmod p.$$

Though not trivial, this is also a sufficient condition in a specific case which we introduce next.

Let K be a local field with residue characteristic p and let $k/\mathbb{F}_p$ be a finite field. Suppose that $\rho\colon \text{Gal}(\overline{K}/K) \to \text{GL}_2(k)$ is a Galois representation (where k has the discrete topology) of the form

$$\rho \sim \begin{pmatrix} \chi_p\varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix}$$

where ε_1 and ε_2 are unramified Galois characters $\text{Gal}(\overline{K}/K) \to k^\times$ and χ_p is the p^{th} cyclotomic character which we consider as a character to $k^\times$ via the embedding $\mathbb{F}_p \hookrightarrow k$. Let K^{nr} be the largest unramified extension of K. Let $G_0 = G_0(\overline{K}/K)$ and $G_1 = G_1(\overline{K}/K)$ be the inertia group and wild inertia group, respectively. Then there is a finite, totally ramified, extension L/K^{nr} with Galois group $\rho(G_0)$. Let L^t be the maximal tamely ramified extension of K^{nr} in L, then $\text{Gal}(L/L^t) = \rho(G_1)$. The situation is summarized in the following diagram



Since ε_1 and ε_2 are unramified, it follows that

$$\rho|_{G_0} \sim \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho|_{G_1} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}. \tag{3.10}$$

From (3.10) it follows that $L^t = K^{\mathrm{nr}}(\zeta_p)$ where ζ_p is a primitive p^{th} root of unity. Since $\rho(G_1)$ has the form as in (3.10), it follows that every element in $\rho(G_1)$ has order p, so $\rho(G_1)$ is a finite product of copies of $\mathbb{Z}/p\mathbb{Z}$. Then by Proposition 1.25,

$$L = L^t(x_1^{1/p}, x_2^{1/p}, \ldots, x_m^{1/p})$$

where $x_i \in (K^{\mathrm{nr}})^\times \setminus (K^{\mathrm{nr}})^{\times p}$ and m is such that $[L : L^t] = p^m$. If the x_i can be chosen such that they are units in the valuation ring of K^{nr}, then we say that ρ is *un peu ramifiée*. If v is the normalized valuation of K^{nr}, then ρ is un peu ramifiée if and only if $v(x_i) \equiv 0 \bmod p$ for all i.

Remark 3.47. The term 'un peu ramifiée' is introduced in [46] by Serre which is written in French. In other literature written in English ([16], for example) the term is adopted. The above paragraph is essentially a translation (with additional details) of Serre's paper [46]. ■

We have the following result due to Edixhoven which he proves for the special case where $K = \mathbb{Q}_p$ but his proof extends to arbitrary local fields.

Proposition 3.48. [16, Proposition 8.2] Let K be a local field with residue characteristic p, let $k/\mathbb{F}_p$ be a finite extension and let $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(k)$ be a Galois representation of the form

$$\rho \sim \begin{pmatrix} \chi_p\varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix}$$

where ε_1 and ε_2 are unramified. Then ρ is finite flat if and only if ρ is un peu ramifiée. ■

Corollary 3.49. Let K be a local field with residue characteristic p and normalized discrete valuation v. Let E/K be an elliptic curve with potentially multiplicative reduction. Then the mod-p Galois representation $\overline{\rho}_{E,p}$ is finite flat if and only if $v(\Delta) \equiv 0 \bmod p$. ■

Proof. As deduced above, it follows from Proposition 3.20 and Proposition 3.18 that there is some unramified quadratic character η such that

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \chi_p\eta & * \\ 0 & \eta \end{pmatrix}.$$

Further, let K^{nr} be the maximal unramified extension of K and let L be the finite extension of K^{nr} with Galois group $\overline{\rho}_{E,p}(G_0)$ (with G_0 the inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$). Then, as seen above, $L = K^{\mathrm{nr}}(\zeta_p, q^{1/p})$ for some $q \in K$ which satisfies $v(q) = v(\Delta)$. Thus, $\overline{\rho}_{E,p}$ is un peu ramifiée if and only if $v(\Delta) \equiv 0 \bmod p$. The result then follows from Proposition 3.48. □

The condition that $v(\Delta) \equiv 0 \bmod p$ is easy to check but the geometric intuition is lacking as to why this should imply finite flatness. However, Ogg's formula gives us some idea as to what is happening. Let E/K be an elliptic curve over a local field of residue characteristic p and let Δ denote the minimal discriminant of E. Let $\mathscr{E}$ be a Néron model of E and let $\tilde{\mathscr{E}}$ denote its reduction (i.e. the special fiber of $\mathscr{E} \to \mathrm{Spec}\, \mathcal{O}_K$). If E/K has split multiplicative reduction, then Tate's algorithm (see [51, Section IV.9]) shows that

$$\tilde{\mathscr{E}} \cong \mathbb{G}_{m,\mathcal{O}_K} \times_{\mathcal{O}_K} (\mathbb{Z}/n\mathbb{Z})_{\mathcal{O}_K}$$

where n is the number of components of $\tilde{\mathscr{E}}$. From this and Example 3.35 we see that the p-torsion

$$\tilde{\mathscr{E}}[p] \cong \begin{cases} \mu_{p,\mathcal{O}_K} \times_{\mathcal{O}_K} (\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_K} & \text{if } p \mid n \\ \mu_{p,\mathcal{O}_K} & \text{if } p \nmid n. \end{cases}$$

So in the case where $p \mid n$, we have that there is 'enough room' for the p-torsion of $\mathscr{E}$ to reduce, making it 'unramified' in a sense (i.e. finite flat). Whilst when $p \nmid n$ we get no such room. According to Ogg's formula (Theorem 2.27) we find that n is equal to the valuation of the discriminant Δ (since $f(E/K) = 1$). Therefore, if the valuation of Δ is congruent to 0 modulo p we have 'enough room' for reduction and hence finite flatness. Of course, this reasoning is mere intuition and by no means a proof but this does give some geometric meaning as to where this divisibility condition comes from.

3.6 Modular forms and modularity conjectures

In this section we very briefly cover some theory of modular forms and how they are conjecturally correlated to Galois representations. The coverage done here is by no means a full introduction to the theory of modular forms but merely serves as glossary of notation for the remainder of this thesis. For this section we follow [64, Section 2] but we do not cover as much detail.

Let K be a number field with signature (r,s), let $\mathcal{O}_K$ denote its ring of integers and let $\mathfrak{N}$ be an ideal of $\mathcal{O}_K$. There is an adelic locally symmetric space

$$Y_0(\mathfrak{N}) = \mathrm{GL}_2(K)\backslash\left(\left(\mathrm{GL}_2(\mathbb{A}_K^f)/U_0(\mathfrak{N})\right)\times Y\right).$$

For $i\in\{0,\dots,2r+3s\}$ and a prime $\mathfrak{q}$ of K coprime to $\mathfrak{N}$, there exists a linear endomorphism $T_\mathfrak{q}$ of the i^{th} cohomology group $H^i(Y_0(\mathfrak{N}),\mathbb{C})$ called a *Hecke operator*. The collection of all of these Hecke operators generate a commutative $\mathbb{Z}$-algebra denoted by $\mathbb{T}^i_{\mathbb{C}}(\mathfrak{N})$ called the *Hecke algebra*. A *weight 2 complex eigenform* $\mathfrak{f}$ *over* K *of level* $\mathfrak{N}$ *and degree* i (or simply *complex eigenform*) is a ring homomorphism $\mathfrak{f}\colon \mathbb{T}^i_{\mathbb{C}}(\mathfrak{N})\to\mathbb{C}$. The hecke operators $T_\mathfrak{q}$ are such that $\mathfrak{f}(T_\mathfrak{q})$ are algebraic integers and the collection of these generate a number field denoted by $\mathbb{Q}_\mathfrak{f}$. We say that a complex eigenform is *trivial* if $f(T_\mathfrak{q}) = \mathrm{Norm}(\mathfrak{q})+1$ for all primes $\mathfrak{q}\nmid\mathfrak{N}$. We say that two complex eigenforms $\mathfrak{f}$ and $\mathfrak{g}$ (of possibly different degree and level) are *equivalent* if $\mathfrak{f}(T_\mathfrak{q}) = \mathfrak{g}(T_\mathfrak{q})$ for almost all primes $\mathfrak{q}$. A complex eigenform is *new* if it is not equivalent to a complex eigenform of lower level.

Let p be a prime coprime to $\mathfrak{N}$. Then, similarly to the complex case, for every prime $\mathfrak{q}\nmid\mathfrak{N}$ in K there exists linear endomorphisms $T_\mathfrak{q}$ of $H^i(Y_0(\mathfrak{N}),\overline{\mathbb{F}}_p)$ called Hecke operators. These generate the Hecke algebra $\mathbb{T}^i_{\overline{\mathbb{F}}_p}(\mathfrak{N})$ which is a commutative $\mathbb{Z}$-algebra. A *weight 2 mod* p *eigenform* θ *over* K *of level* $\mathfrak{N}$ *and degree* i (or simply a *mod* p *eigenform*) is a ring homomorphism $\theta\colon \mathbb{T}^i_{\overline{\mathbb{F}}_p}(\mathfrak{N})\to\overline{\mathbb{F}}_p$. We say that a mod p eigenform θ *lifts to a complex eigenform* if there is a complex eigenform $\mathfrak{f}$ of the same level and degree as θ such that

$$\mathfrak{f}(T_\mathfrak{q}) \bmod \mathfrak{p} = \theta(T_\mathfrak{q})$$

for every prime $\mathfrak{q}\nmid p\mathfrak{N}$ in K and every prime $\mathfrak{p}$ in $\mathbb{Q}_\mathfrak{f}$ extending p.

Let K be a number field and let ρ be a Galois representation of $\mathrm{Gal}(\overline{K}/K)$. For every embedding $\sigma\colon K\hookrightarrow\mathbb{R}$ and extension $\tau\colon\overline{K}\hookrightarrow\mathbb{C}$ we obtain a *complex conjugation* $\tau^{-1}\circ\bar{\cdot}\circ\tau\in\mathrm{Gal}(\overline{K}/K)$ where $\bar{\cdot}$ denotes usual complex conjugation of $\mathbb{C}$. We say that ρ is *odd* if K is totally complex or if the determinant of $\rho(c)$ is -1 for every complex conjugation $c\in\mathrm{Gal}(\overline{K}/K)$.

Example 3.50. Let K be a number field such that $\zeta_p\notin K$. Then $\chi_p\colon\mathrm{Gal}(\overline{K}/K)\to\mathbb{F}_p^\times$ is odd. Indeed, if $c\in\mathrm{Gal}(\overline{K}/K)$ is a complex conjugation and ζ_p a primitive p^{th} root of unity. Then $c(\zeta_p)=\zeta_p^{-1}$, which, by definition, implies that $\chi_p(c)=-1$. Thus

$$\det\chi_p(c) = \det(-1) = -1$$ ■

The following is a special case of Serre's modularity conjecture over number fields and concerns modularity of mod-p Galois representations.

Conjecture 1. [19, Conjecture 4.1][64, Conjecture 3.1] Let $\overline{\rho}\colon\mathrm{Gal}(\overline{K}/K)\to\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be and odd and irreducible, representation with Serre conductor $\mathfrak{N}$ such that $\det(\overline{\rho})=\chi_p$ is the mod-p cyclotomic character. Assume that p is unramified in K and that $\overline{\rho}|_{\mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p})}$ is finite flat for every prime $\mathfrak{p}|p$. Then there is weight 2, mod p eigenform θ over K of level $\mathfrak{N}$ such that, for all primes $\mathfrak{q}$ coprime to $p\mathfrak{N}$, we have

$$\mathrm{Tr}(\overline{\rho}(\mathrm{Frob}_\mathfrak{q})) = \theta(T_\mathfrak{q}),$$

where $T_\mathfrak{q}$ denotes the Hecke operator at $\mathfrak{q}$. ■

Next we discuss a second conjecture related to the Langlands program. To do this we first introduce some terminology. A simple abelian surface A over a number field K whose K-endomorphism algebra $\mathrm{End}_K(A)\otimes_\mathbb{Z}\mathbb{Q}$ is an indefinite division quaternion algebra $\mathbb{Q}$ is called a *fake elliptic curve*. Fake elliptic curves are merely part of the conjecture and will not appear prominently in what follows.

Conjecture 2. [64, Conjecture 4.1] Let $\mathfrak{f}$ be a weight 2 complex eigenform over K of level $\mathfrak{N}$ that is nontrivial and new. If K has some real place, then there exists an elliptic curve $E_{\mathfrak{f}}/K$ of conductor $\mathfrak{N}$ such that

$$\#E_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{q}) = 1 + \mathrm{Norm}(\mathfrak{q}) - \mathfrak{f}(T_{\mathfrak{q}}) \quad \text{for all} \quad \mathfrak{q} \nmid \mathfrak{N}. \tag{3.11}$$

If K is totally complex, then there exists either an elliptic curve $E_{\mathfrak{f}}$ of conductor $\mathfrak{N}$ satisfying (3.11) or a fake elliptic curve $A_{\mathfrak{f}}/K$, of conductor $\mathfrak{N}^2$, such that

$$\#A_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{q}) = (1 + \mathrm{Norm}(\mathfrak{q}) - \mathfrak{f}(T_{\mathfrak{q}}))^2 \quad \text{for all } \mathfrak{q} \nmid \mathfrak{N}. \qquad \blacksquare$$

4 The modular method

Fermat's Last Theorem is one of the most monumental results of twentieth-century mathematics. It states that $a^n + b^n = c^n$ has no nontrivial integer solutions for $n \geqslant 3$. The final step in the proof was done by Wiles in 1995 in his paper [62]. Wiles stood on the shoulders of giants and the culmination of the proof of Fermat's last theorem started with an idea of the German mathematician Frey. In his paper [21], he assumed existence of a non-trivial solution to $a^n + b^n = c^n$ and constructed an elliptic curve $E/\mathbb{Q}$ which depends on a, b and c and has bad reduction at all the primes dividing a, b and c. The conductor of the Galois representation attached to $E/\mathbb{Q}$ is a priori supported on the primes dividing a, b and c. In 1990, Ribet [43] proved a 'level lowering' theorem [43, Theorem 1.1] which states that if a representation ρ is modular of level N, then ρ is modular of level N/p for some prime $p \mid\mid N$ (under some technical conditions). In his paper, Ribet also shows that his level lowering result, along with the conjecture that every elliptic curve over $\mathbb{Q}$ is modular, implies that the representation attached to E is modular of level 2. This is a contradiction since there are no non-zero cusp forms of weight 2 and level 2. Wiles' proof in [62] showed the assumed conjecture in the case of semi-stable elliptic curves. This turned out to be enough to prove the 350-year-old conjecture.

Though a neat lesson in history, the above outlines a more general strategy for solving Diophantine equations over a number field K which have a similar form. Namely equations which are of the form

$$Aa^p + Bb^q = Cc^r,$$

with A, B and C elements of the ring of integers $\mathcal{O}_K$ of K. We say that the equation above is a signature (p, q, r) equation. Suppose we have a signature (p, q, r) equation over K which we aim to show has no solutions, proceed in the following three steps.

1. Construct an elliptic curve E/K associated to a putative solution $P \in \mathcal{O}_K^3$ to the Diophantine equation, named the Frey curve. The conductor of the Frey curve E depends on the putative solution P of the Diophantine equation
2. Lower the level of E: construct an object related to E in some way with a 'level' which does not depend on the solution P. In the case of Fermat's last theorem this was the level lowering done by Ribet where he obtained a Galois representation of level 2.
3. Use the object in 2 to get a contradiction.

This recipe proved effective for Darmon and Merel who proved in [13] that the equations

$$a^n + b^n = 2c^n, \quad a^k + b^k = c^2 \quad \text{and} \quad a^n + b^n = c^3$$

have no non-trivial primitive solutions over $\mathbb{Z}$ (primitive meaning that a, b and c are coprime) when $n \geqslant 3$ and $k \geqslant 4$. Some more general results for the non-existence of solutions to signature $(n, n, 3)$ equations over $\mathbb{Q}$ are given in [6]. A good introduction to solving Diophantine equations over $\mathbb{Q}$ is given by Siksek in [50]. For general number fields, this method is employed for several signature (p, p, p) equations in [15], [19] and [25]. In [64] and [65, 66] these equations are specifically studied over imaginary quadratic number fields. A great survey article that gives a general idea of the methods employed to solve signature (p, p, p) equations over number fields is [63]. In addition to a signature (p, p, p), [30] uses the method above to show non-existence of solutions to a $(p, p, 2)$ equation over totally real number fields. In [24] the same problem is tackled over general number fields. Finally, in [23], [29] and [37] non-existence of solutions to signature $(p, p, 3)$ equations is shown, the latter two only over totally real number fields. These last three sources serve as an inspiration for this section. There is a body of literature on equations with signature (r, r, p), where r is fixed and p varies. This is not the type of equation we study in this thesis, but a great introductory source for solving these equations is [18].

Let K be a number field and let

$$Aa^p + Bb^p = Cc^3 \tag{4.1}$$

be an equation of signature only depending on p defined over the ring of integers of K. The case for general number fields is special in the sense that we can always find a solution to (4.1) by taking K large enough. The question then becomes: if we fix K, how large should the exponent p be for there to be no solutions? Does such a size of p always exist? However, what if we want to say something about a whole class of number fields K? In this case we must restrict K in some way. In this section we investigate the following question: what restriction do we have to put on K for there to exist a positive constant

V, depending only on K, A, B and C, such that for every $p > V$ there is no solution to (4.1)? We do this by following the three steps in the previous paragraph: 'the modular method'. We start out quite general for the first two steps of the method. In Section 4.3 and 4.4 we put different restrictions on K and perform step 3 in two different ways, to get two types of asymptotic results.

4.1 Frey curve

The first step of the modular method is to construct a Frey curve. In this section we construct the Frey curve, classify its reduction at primes and look at some properties of its Galois representation.

Let K be a number field with ring of integers $\mathcal{O}_K$. Let $A, B, C \in \mathcal{O}_K$ be non-zero and let $p \geqslant 5$ be a prime number. Suppose that (a, b, c) is a non-trivial, primitive solution to

$$Aa^p + Bb^p = Cc^3 \tag{4.2}$$

such that $\mathfrak{P} \mid abc$ for every prime $\mathfrak{P}$ above 3 in K. Primitive here means that the ideal generated by a, b and c is the unit ideal in $\mathcal{O}_K$. Define the Frey curve $E = E(a, b, c)/K$ via a Weierstrass equation

$$E\colon y^2 + 3Ccxy + C^2Bb^py = x^3. \tag{4.3}$$

A swift calculation shows that its associated quantities are

$$\begin{aligned} c_4 &= 3^2C^3c(3^2Aa^p + Bb^p) \\ c_6 &= -3^3C^4(3^3C^2c^6 - 2^23^2Cc^3Bb^p + 2^3B^2b^{2p}) \\ \Delta &= 3^3C^8AB^3(abc^3)^p \\ \text{and} \quad j &= 3^3\frac{Cc^3(3^2Aa^p + Bb^p)^3}{AB^3(abc^3)^p}. \end{aligned}$$

In particular, since the solution (a, b, c) was assumed to be non-trivial, it follows that $\Delta \neq 0$ and hence, by Proposition 2.2, E defines an elliptic curve. Define

$$T_K = \{\mathfrak{P} : \mathfrak{P} \text{ is a prime in } K \text{ and } \mathfrak{P} \mid 3ABC\}$$

and for $R \in \mathcal{O}_K$ the ideals

$$\mathrm{Rad}_3(R) = \prod_{\substack{\mathfrak{p} \mid R \\ \mathfrak{p} \nmid 3}} \mathfrak{p} \quad \text{and} \quad \mathrm{Rad}_{2,3}(R) = \prod_{\substack{\mathfrak{p} \mid R \\ \mathfrak{p} \nmid 6}} \mathfrak{p}$$

where the products run over prime ideals. The following proposition gives some data that regarding the reduction of E.

Proposition 4.1. Suppose that $p > v_{\mathfrak{P}}(C)$ for all primes $\mathfrak{P}$ in K above 3. Let E/K be as in (4.3). Then E/K has semistable reduction outside of T_K. If, in addition, we assume that (Aa, Bb, Cc) is primitive and $p > \max_{\mathfrak{P}\mid 3}\{v_{\mathfrak{P}}(C), 3v_{\mathfrak{P}}(3)\}$. Then the conductor $\mathcal{N}_E$ of E is given by

$$\mathcal{N}_E = \mathrm{Rad}_3(AaBb)\mathrm{Rad}_{2,3}(C)^2 \left(\prod_{\mathfrak{p}\mid 2 \text{ and } \mathfrak{p}\mid C} \mathfrak{p}^{\varepsilon_{\mathfrak{p}}} \right) \left(\prod_{\mathfrak{P}\mid 3} \mathfrak{P}^{\delta_{\mathfrak{P}}} \right)$$

where $\varepsilon_{\mathfrak{p}} \geqslant 2$ for all primes $\mathfrak{p}$ above 2 dividing C. Here, for every prime $\mathfrak{P}$ above 3, $\delta_{\mathfrak{P}} = 1$, if $\mathfrak{P} \mid Aa$, $v_{\mathfrak{P}}(3) \geqslant 2$, and $v_{\mathfrak{P}}(3)$ is even or if $\mathfrak{P} \mid Bb$. Otherwise $2 \leqslant \delta_{\mathfrak{P}} \leqslant 2 + 3v_{\mathfrak{P}}(3)$. ∎

Proof. Let $\mathfrak{P} \notin T_K$. If $\mathfrak{P} \nmid \Delta$ then by Proposition 2.11 it follows that E has good reduction at $\mathfrak{P}$. If $\mathfrak{P} \mid \Delta$, then, since $\mathfrak{P} \notin T_K$, $\mathfrak{P} \mid abc$. If $\mathfrak{P} \mid a$ and $\mathfrak{P} \mid b$ then $\mathfrak{P}^p \mid Aa^p + Bb^p = Cc^3$ and since $p > v_{\mathfrak{P}}(C)$ we must have $\mathfrak{P} \mid c$. We also have that $\mathfrak{P} \mid a$ and $\mathfrak{P} \mid b$ so this is a contradiction with the fact that (a, b, c) is primitive. It follows that either $\mathfrak{P} \mid a$ or $\mathfrak{P} \mid b$. From this fact and the fact that $\mathfrak{P} \notin T_K$, it follows that $\mathfrak{P}$ does not divide $c_4 = 3^2C^3c(3^2Aa^p + Bb^p)$. Therefore, $v_{\mathfrak{P}}(c_4) = 0$ which shows that the equation for $E/K_{\mathfrak{P}}$ is minimal and that E has multiplicative reduction at $\mathfrak{P}$ by Proposition 2.11.

Now suppose that, in addition, we assume that (Aa, Bb, Cc) is primitive and that $p > \max_{\mathfrak{P}|3}\{v_{\mathfrak{P}}(C), 3v_{\mathfrak{P}}(3)\}$. If $\mathfrak{P} \nmid \Delta$ then E has good reduction at $\mathfrak{P}$. If $\mathfrak{P} \mid \Delta$, we distinguish a few cases.
If $\mathfrak{P} \mid Aa$ and $\mathfrak{P} \nmid 3$, then since (Aa, Bb, Cc) is primitive, $\mathfrak{P} \nmid BbCc$. We have

$$v_{\mathfrak{P}}(c_4) = 0 \quad \text{and} \quad v_{\mathfrak{P}}(\Delta) > 0$$

It follows that the equation of E is minimal and has multiplicative reduction. A similar argument shows that if $\mathfrak{P} \mid Bb$ and $\mathfrak{P} \nmid 3$, then there is multiplicative reduction at $\mathfrak{P}$.
Suppose that $\mathfrak{P} \mid C$ and $\mathfrak{P} \nmid 3$. By absorbing any cubes dividing C into c, we may assume that C is cube-free. Thus $v_{\mathfrak{P}}(C) \in \{1, 2\}$. We have

$$\begin{aligned} v_{\mathfrak{P}}(c_4) &= 3v_{\mathfrak{P}}(C) + v_{\mathfrak{P}}(c) \\ v_{\mathfrak{P}}(c_6) &= 4v_{\mathfrak{P}}(C) \\ v_{\mathfrak{P}}(\Delta) &= 8v_{\mathfrak{P}}(C) \end{aligned}$$

If $v_{\mathfrak{P}}(C) = 1$, then the equation for $E/K_{\mathfrak{P}}$ is minimal at $\mathfrak{P}$ and $v_{\mathfrak{P}}(c_4) > 0$ so we have additive reduction at $\mathfrak{P}$. If $v_{\mathfrak{P}}(C) = 2$ then the equation is not minimal. Let $\pi_{\mathfrak{P}}$ be a uniformizer of $K_{\mathfrak{P}}$, then the coordinate transformation

$$(X, Y) = (\pi_{\mathfrak{P}}^2 x, \pi_{\mathfrak{P}}^3 y)$$

gives a minimal Weierstrass equation for $E/K_{\mathfrak{P}}$ with coefficients c_4' and Δ' such that $v_{\mathfrak{P}}(c_4) > 0$ and $v_{\mathfrak{P}}(\Delta) > 0$ and hence we obtain additive reduction at $\mathfrak{P}$.
Finally, suppose that $\mathfrak{P} \mid 3$, then, by assumption, either $\mathfrak{P} \mid a$ or $\mathfrak{P} \mid b$. If $\mathfrak{P} \mid a$, then since (Aa, Bb, Cc) is primitive, it follows that $\mathfrak{P} \nmid BbCc$. Then

$$\begin{aligned} v_{\mathfrak{P}}(c_4) &= 2v_{\mathfrak{P}}(3) \\ v_{\mathfrak{P}}(c_6) &= 3v_{\mathfrak{P}}(3) \\ v_{\mathfrak{P}}(\Delta) &= 3v_{\mathfrak{P}}(3) + v_{\mathfrak{P}}(Aa^p) \end{aligned}$$

Suppose that $v_{\mathfrak{P}}(3)$ is even and let $\pi_{\mathfrak{P}}$ be a uniformizer of $K_{\mathfrak{P}}$. The coordinate transformation

$$(x, y) = \left(\left(\pi_{\mathfrak{P}}^{v_{\mathfrak{P}}(3)/2}\right)^2 X, \left(\pi_{\mathfrak{P}}^{v_{\mathfrak{P}}(3)/2}\right)^3 Y\right)$$

gives a Weierstrass equation for E over $K_{\mathfrak{P}}$ with associated coefficients c_4', c_6' and Δ' with

$$\begin{aligned} v_{\mathfrak{P}}(c_4') &= 2v_{\mathfrak{P}}(3) - v_{\mathfrak{P}}(\pi_{\mathfrak{P}}^{2v_{\mathfrak{P}}(3)}) = 0 \\ v_{\mathfrak{P}}(c_6') &= 3v_{\mathfrak{P}}(3) - v_{\mathfrak{P}}(\pi_{\mathfrak{P}}^{3v_{\mathfrak{P}}(3)}) = 0 \\ v_{\mathfrak{P}}(\Delta') &= 3v_{\mathfrak{P}}(3) + v_{\mathfrak{P}}(Aa^p) - v_{\mathfrak{P}}(\pi_{\mathfrak{P}}^{6v_{\mathfrak{P}}(3)}) = v_{\mathfrak{P}}(Aa^p) - 3v_{\mathfrak{P}}(3). \end{aligned}$$

Since $p > 3v_{\mathfrak{P}}(3)$ it follows that $v_{\mathfrak{P}}(\Delta') > 0$ and hence the equation for $E/K_{\mathfrak{P}}$ is minimal and has multiplicative reduction. If $v_{\mathfrak{P}}(3)$ is odd then similarly to the even case, the coordinate transformation $(X, Y) = (\pi_{\mathfrak{P}}^{2k} x, \pi_{\mathfrak{P}}^{3k} y)$ makes $E/K_{\mathfrak{P}}$ minimal, where k is such that $v_{\mathfrak{P}}(3) = 2k + 1$. The associated coefficients c_4' and Δ' of $E/K_{\mathfrak{P}}$ satisfy $v_{\mathfrak{P}}(c_4') = 1$ and $v_{\mathfrak{P}}(Aa^p) > 0$ and hence we have additive reduction in this case.
Suppose instead that $\mathfrak{P} \mid b$. Then, since $p > 3v_{\mathfrak{P}}(3)$,

$$\begin{aligned} v_{\mathfrak{P}}(c_4) &= 2v_{\mathfrak{P}}(3) + \min\{2v_{\mathfrak{P}}(3), v_{\mathfrak{P}}(Bb^p)\} && = 4v_{\mathfrak{P}}(3) \\ v_{\mathfrak{P}}(c_6) &= 3v_{\mathfrak{P}}(3) + \min\{3v_{\mathfrak{P}}(3), 2v_{\mathfrak{P}}(3) + v_{\mathfrak{P}}(Bb^p), 2v_{\mathfrak{P}}(Bb^p)\} && = 6v_{\mathfrak{P}}(3) \\ v_{\mathfrak{P}}(\Delta) &= 3v_{\mathfrak{P}}(3) + 3v_{\mathfrak{P}}(Bb^p) && > 12v_{\mathfrak{P}}(3). \end{aligned}$$

The coordinate transformation $(x, y) = (\pi_{\mathfrak{P}}^{2v_{\mathfrak{P}}(3)} X, \pi_{\mathfrak{P}}^{3v_{\mathfrak{P}}(3)} Y)$, makes $E/K_{\mathfrak{P}}$ minimal with $v_{\mathfrak{P}}(c_4') = 0$ and $v_{\mathfrak{P}}(\Delta') > 0$ and hence we have multiplicative reduction at $\mathfrak{P}$ in this case.
Considering the reduction types of E at the different primes dividing Δ, the exponents in the conductor $\mathcal{N}_E$ are determined by Theorem 2.25. For the primes $\mathfrak{P}$ above 3 we have that the exponent of the conductor $\delta_{\mathfrak{P}}$ is bounded by $2 + 3v_{\mathfrak{P}}(3)$ by Theorem 2.26. □

Remark 4.2. A closer inspection and usage of Tate's algorithm can give the precise reduction type of $E/K_{\mathfrak{P}}$ in the sense of Theorem 2.24. In the case $K = \mathbb{Q}$ this has been done in [6, Section 2]. This could have been done in its full generality here, too. However, this would be needlessly complex and is not necessary for our purposes. ■

Let $\mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K and let $\overline{\rho}_{E,p}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{F}_p)$ be the mod-p Galois representation associated to E/K as in Example 3.2.1.

Corollary 4.3. Let E/K be as in (4.3). Then E has a K-rational point of order 3. The Serre conductor $\mathfrak{N}_E$ of $\overline{\rho}_{E,p}$ is supported on the primes in T_K. In particular, there is a finite amount of possible values for $\mathfrak{N}_E$. ■

Proof. The K-rational point of order 3 on E is $(0,0)$. A priori the Serre conductor of $\overline{\rho}_{E,p}$ is supported on the primes dividing $3ABCab$ by the previous Proposition and Example 3.10. Suppose that $\mathfrak{P}$ divides ab and $\mathfrak{P} \nmid 3$, then $p \mid v_{\mathfrak{P}}(\Delta)$. Since there is multiplicative reduction at $\mathfrak{P}$ (by Proposition 4.1), it follows from Proposition 3.26 that $\overline{\rho}_{E,p}$ is unramified at $\mathfrak{P}$ and hence $\mathfrak{P} \nmid \mathfrak{N}_E$. Therefore $\mathfrak{N}_E$ is supported on the primes in T_K. The Serre conductor $\mathfrak{N}_E$ divides the Artin conductor $\mathscr{N}_{\overline{\rho}_{E,p}}$ which divides $\mathcal{N}_E$. By Theorem 2.26, for every prime $\mathfrak{P} \in T_K$ we get

$$v_{\mathfrak{P}}(\mathfrak{N}_E) \leqslant v_{\mathfrak{P}}(\mathcal{N}_E) \leqslant 2 + 3v_{\mathfrak{P}}(3) + 6v_{\mathfrak{P}}(2)$$

and hence $\mathfrak{N}_E$ belongs to a finite set. □

At some point we want to invoke Conjecture 1 on the Galois representation $\overline{\rho}_{E,p}$. To do this, we have to check whether $\overline{\rho}_{E,p}$ satisfies the conditions of the conjecture. Most of the conditions are verified in the next proposition.

Proposition 4.4. Let E/K be as in (4.3) and let $\overline{\rho}_{E,p}$ be its associated Galois representation. Let p be large enough such that K does not contain a p^{th} root of unity. Then $\det \overline{\rho}_{E,p} = \chi_p$ and $\overline{\rho}_{E,p}$ is odd. Further, if we take p to be large enough such that p is unramified in K and such that no prime above p in K divides $3ABC$. Then, for every prime $\mathfrak{p}$ above p in K we have that $\overline{\rho}_{E,p}|_{\mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})}$ is finite flat. ■

Proof. The first assertion follows from Proposition 3.13 and Example 3.50. For the second assertion, suppose that $\mathfrak{p}$ is a prime in K above p and suppose that $\mathfrak{p} \nmid \Delta$. Then E/K has good reduction at $\mathfrak{p}$ (i.e. $E/K_{\mathfrak{p}}$ has good reduction) and it follows from Proposition 3.46 that $\overline{\rho}_{E,p}|_{\mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})}$ is finite flat. Conversely, suppose that $\mathfrak{p} \mid \Delta$, then, by assumption, we have that $\mathfrak{p} \nmid 3ABC$ so we must have $\mathfrak{p} \mid ab$. According to Proposition 4.1, the curve E/K has multiplicative reduction at $\mathfrak{p}$. We also have that $p \mid v_{\mathfrak{p}}(\Delta)$ so by Corollary 3.49 it follows that $\overline{\rho}_{E,p}|_{\mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})}$ is finite flat. In either case, the Galois representation $\overline{\rho}_{E,p}|_{\mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})}$ is finite flat. □

For a prime $\mathfrak{q}$ of K, let $I_{\mathfrak{q}}$ denote the inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$ as in Section 1.3. The following is our main tool to detect when an elliptic curve has potentially multiplicative reduction. This Lemma is often used when solving Diophantine equations using the modular method (e.g. [20, Lemma 3.4] or [23, Lemma 2.5]), so we include a short proof.

Lemma 4.5. Let E/K be an elliptic curve with j-invariant j_E. Let $p \geqslant 5$ be a rational prime and $\mathfrak{q} \nmid p$ a prime of K. Then $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$ if and only if $p \nmid v_{\mathfrak{q}}(j_E)$ and E has potentially multiplicative reduction at $\mathfrak{q}$. ■

Proof. If $p \nmid v_{\mathfrak{q}}(j_E)$ and E has potentially multiplicative reduction at $\mathfrak{q}$ then by Proposition 3.22, $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \in \overline{\rho}_{E,p}(I_{\mathfrak{q}})$. This element has order p in $\mathrm{GL}_2(\mathbb{F}_p)$ which shows that $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$.
For the converse statement, we prove the contrapositive. Suppose that E does not have potentially multiplicative reduction. Then E has potential good reduction at $\mathfrak{q}$. By restriction, we may assume that $\overline{\rho}_{E,p}$ is a representation over the decomposition subgroup $\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}})$ of $\mathrm{Gal}(\overline{K}/K)$. By Proposition 1.17 we have that $I_{\mathfrak{q}} = \mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}}^{\mathrm{nr}})$. Since E has potentially good reduction, it follows from Proposition 2.14 that there is a finite extension L of $K_{\mathfrak{q}}$ such that E attains good reduction over L. Suppose L is the smallest such extension. Then by Example 3.8.1, the inertia group $I_L = \mathrm{Gal}(\overline{L}/L^{\mathrm{nr}})$ acts trivially on $E[p]$. It follows that

$$\overline{\rho}_{E,p}(I_{\mathfrak{q}}) = \overline{\rho}_{E,p}(\mathrm{Gal}(LK_{\mathfrak{q}}^{\mathrm{nr}}/K_{\mathfrak{q}}^{\mathrm{nr}})).$$

By [47, Theorem 2] it follows that $\mathrm{Gal}(L/K_{\mathfrak{q}}^{\mathrm{nr}})$ is a subgroup of the automorphism group of the reduced curve $\tilde{E}/\overline{k}_L$ where k_L is the residue field of L. Then one can read off via the reduction of the minimal regular proper model of E [39, Section 17] that the order of $\mathrm{Gal}(LK_{\mathfrak{q}}^{\mathrm{nr}}/K_{\mathfrak{q}}^{\mathrm{nr}})$ is $2, 3, 4$ or 6 (see also [45, Section 5.6] and [28, Proposition 1]). It follows that $p \nmid \#\overline{\rho}_{E,p}(\mathrm{Gal}(LK_{\mathfrak{q}}^{\mathrm{nr}}/K_{\mathfrak{q}}^{\mathrm{nr}}))$. □

Define

$$S_K = \{\mathfrak{q} : \mathfrak{q} \text{ is a prime in } K \text{ and } \mathfrak{q} \mid 3\}.$$

The Frey curve E/K in (4.3) has bad reduction at the primes in S_K. The following lemma uses Lemma 4.5 to give a condition on p that allows us to constrain the structure of $\overline{\rho}_{E,p}(I_\mathfrak{q})$ for $\mathfrak{q} \in S_K$.

Lemma 4.6. Let E/K be the Frey curve in (4.3). Suppose that

$$p > \max_{\mathfrak{q} \in S_K} \{v_\mathfrak{q}(3^2 A), v_\mathfrak{q}(B), v_\mathfrak{q}(C), |v_\mathfrak{q}(3) + v_\mathfrak{q}(BA^{-1})|, |3v_\mathfrak{q}(3) + v_\mathfrak{q}(AB^{-1})|\}.$$

Then for every $\mathfrak{q} \in S_K$, we have $p \mid \#\overline{\rho}_{E,p}(I_\mathfrak{q})$. ■

Proof. Rewrite the j-invariant of E as

$$j = 3^3 \frac{Cc^3(3^2 Aa^p + Bb^p)^3}{AB^3(ab^3)^p} = 3^3 \frac{(Aa^p + Bb^p)(3^2 Aa^p + Bb^p)^3}{AB^3(ab^3)^p}.$$

We aim to apply Lemma 4.5. Let $\mathfrak{q}$ be a prime in S_K. As in the proof of Proposition 4.1, we have that $p > v_\mathfrak{q}(C)$ implies that either $\mathfrak{q} \mid a$ or $\mathfrak{q} \mid b$. Suppose that $\mathfrak{q} \mid a$. Then $\mathfrak{q} \nmid b$ and, since $p > v_\mathfrak{q}(B)$,

$$\begin{aligned} v_\mathfrak{q}(j) &= 3v_\mathfrak{q}(3) + v_\mathfrak{q}(B) + 3v_\mathfrak{q}(B) - v_\mathfrak{q}(AB^3) - pv_\mathfrak{q}(a) \\ &= 3v_\mathfrak{q}(3) + v_\mathfrak{q}(BA^{-1}) - pv_\mathfrak{q}(a). \end{aligned}$$

Since $p > |3v_\mathfrak{q}(3) + v_\mathfrak{q}(BA^{-1})|$ it follows that $v_\mathfrak{q}(j) < 0$ and $p \nmid v_\mathfrak{q}(j)$.
If $\mathfrak{q} \mid b$, then $\mathfrak{q} \nmid a$ and, since $p > v_\mathfrak{q}(3^2 A)$,

$$\begin{aligned} v_\mathfrak{q}(j) &= 3v_\mathfrak{q}(3) + v_\mathfrak{q}(A) + 6v_\mathfrak{q}(3) + 3v_\mathfrak{q}(A) - v_\mathfrak{q}(AB^3) - 3pv_\mathfrak{q}(b) \\ &= 3\big(3v_\mathfrak{q}(3) + v_\mathfrak{q}(AB^{-1}) - pv_\mathfrak{q}(b)\big) \end{aligned}$$

and since $p > |3v_\mathfrak{q}(3) + v_\mathfrak{q}(AB^{-1})|$ it follows that $v_\mathfrak{q}(j) < 0$ and $p \nmid v_\mathfrak{q}(j)$. In both cases we have that $v_\mathfrak{q}(j) < 0$ and hence by Proposition 2.15 the elliptic curve E/K has potentially multiplicative reduction at $\mathfrak{q}$. In both cases we also have $p \nmid v_\mathfrak{q}(j)$ and hence it follows from Lemma 4.5 that $p \mid \#\overline{\rho}_{E,p}(I_\mathfrak{q})$. □

The only condition of Conjecture 1 that remains to be checked is whether the composition

$$\mathrm{Gal}(\overline{K}/K) \xrightarrow{\overline{\rho}_{E,p}} \mathrm{GL}_2(\mathbb{F}_p) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

is irreducible. In other words, we have to check whether $\overline{\rho}_{E,p}$ is absolutely irreducible. According to Proposition 3.6 it is sufficient to show that $\overline{\rho}_{E,p}$ is surjective. The following is Proposition 6.1 from [64] and is used to prove the desired surjectivity of $\overline{\rho}_{E,p}$.

Proposition 4.7. Let L be a Galois number field, and let $\mathfrak{Q}$ be a prime of L. There is a constant $B_{L,\mathfrak{Q}}$ such that the following is true. Let $p > B_{L,\mathfrak{Q}}$ be a rational prime. Let E/L be an elliptic curve that is semistable at all $\mathfrak{p} \mid p$ and having potentially multiplicative reduction at $\mathfrak{Q}$. Then $\overline{\rho}_{E,p}$ is irreducible. ■

Corollary 4.8. There is a constant $D = D(K, A, B, C)$ depending only on K, A, B and C such that the following holds. If E is the Frey curve (4.3) corresponding to a solution $(a, b, c) \in W_K$ with exponent $p > D$. Then the mod-p Galois representation $\overline{\rho}_{E,p}$ is surjective. ■

Proof. By Proposition 4.1, E is semistable outside of T_K by Proposition 4.1. Let L be the Galois closure of K and let $\mathrm{Gal}(\overline{L}/L)$ be the absolute Galois group of L. Let $\mathfrak{Q}$ in be a prime in L above any prime in S_K, say, $\mathfrak{q}$. Let $B_{L,\mathfrak{Q}}$ be the constant from Proposition 4.7. If we let p be large enough such that no prime in T_K lies above p, say, $p > c = c(K, A, B, C)$, then by Proposition 4.1, E is semistable at the primes above p. Additionally, since E has potentially multiplicative reduction at $\mathfrak{q}$, it will have potentially multiplicative reduction at $\mathfrak{Q}$ by Proposition 2.14. If we enlarge p further such that $p > B_{L,\mathfrak{Q}}$, it follows from 4.7 that

$$\overline{\rho}_{E,p}(\mathrm{Gal}(\overline{L}/L)) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

is irreducible. There are only finitely many primes $\mathfrak{Q}$ in L above $\mathfrak{q}$ and L depends only on K. So taking

$$D = \max_{\mathfrak{Q} \mid \mathfrak{q}} \{B_{L,\mathfrak{Q}}, c\}$$

gives us that $\overline{\rho}_{E,p}\colon \mathrm{Gal}(\overline{L}/L) \to \mathrm{GL}_2(\mathbb{F}_p)$ is irreducible whenever $p > D$. Since $\mathrm{Gal}(\overline{L}/L)$ is a subgroup of $\mathrm{Gal}(\overline{K}/K)$, it follows that $\overline{\rho}_{E,p}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{F}_p)$ is irreducible whenever, $p > D$. If necessary, enlarge D so that, by Lemma 4.6, we have that $p \mid \#\overline{\rho}_{E,p}(\mathrm{Gal}(\overline{K}/K))$. For such p, there is some element of order p in $\overline{\rho}_{E,p}(\mathrm{Gal}(\overline{K}/K))$. By [17, Propositions 2.3 and 2.6], it follows that $\overline{\rho}_{E,p}(\mathrm{Gal}(\overline{K}/K))$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. It now follows that $\overline{\rho}_{E,p}$ is surjective when $\det \overline{\rho}_{E,p}$ is surjective. From Corollary 3.15 we have that $\det \overline{\rho}_{E,p} = \chi_p$ which can be ensured to be surjective by taking D large enough so that $\zeta_p \notin K$. □

Remark 4.9. Corollary 4.8 is very similar to Serre's open image Theorem [45, Théorème 4.2.2] which states that for almost all primes ℓ, the Galois representation $\overline{\rho}_{E,\ell}$ is surjective. By using this theorem to get a constant D as in Corollary 4.8 is not quite what we want as this constant would depend on E (and hence on the solution (a, b, c)). The constant D we obtained does not depend on E, merely on A, B, C and K. ■

4.2 Level lowering

The second step of the modular method is to find an object with 'lower level'. In our case, this object is another elliptic curve. This section uses conjectures 1 and 2 to construct the elliptic curve with 'lower level'. The 'level', here, is represented by the conductor of the elliptic curve. This approach closely follows [23] and [64]. The Theorem below describes the elliptic curve with its 'lowered' conductor in terms of its reduction and its relation to E.

Theorem 4.10. Let K be a number field satisfying Conjectures 1 and 2. Then there is a constant $V = V(K, A, B, C)$ depending only on K, A, B and C such that the following holds. Let (a, b, c) be a non-trivial, primitive solution to (4.2) with prime exponent $p > V$ such that $\mathfrak{P} \mid ab$ for all primes $\mathfrak{P}$ in K above 3. Let E/K be the associated Frey curve (4.3). Then there is an elliptic curve E'/K such that the following statements hold:
(i) E' has good reduction away from T_K;
(ii) E' has a K-rational point of order 3;
(iii) $\overline{\rho}_{E',p} \sim \overline{\rho}_{E,p}$;
(iv) E' has potentially multiplicative reduction for all primes $\mathfrak{q} \in S_K$. ■

Theorem 4.10 is proven in a few steps. The first step is to associate a modular form to the Galois representation $\overline{\rho}_{E,p}$ where E/K is the Frey curve of Section 4.1.

The following results are very technical results relating eigenforms to elliptic curves. Not everything is known about this connection (over general number fields) so this is where the conjectures come in. The following Proposition is Proposition 2.1 from [64]. This result follows as a corollary from the lifting lemmas of Ash and Stevens [4, Section 1.2] which state that every mod p eigenform of degree i lifts to a complex one when $H^{i+1}(Y_0(\mathfrak{N}), \mathbb{Z})$ has no p-torsion (for some ideal $\mathfrak{N} \subset \mathcal{O}_K$).

Proposition 4.11. Let $\mathfrak{N}$ be an ideal in $\mathcal{O}_K$ There is an integer $B(\mathfrak{N})$ depending only on $\mathfrak{N}$, such that, for any prime $p > B(\mathfrak{N})$, every weight-two, mod p eigenform of level $\mathfrak{N}$ lifts to a complex one. ■

Proposition 4.11 allows us to prove the following result which plays a major role in the proof of Theorem 4.10.

Lemma 4.12. There is a constant $V = V(K, A, B, C)$ depending only on K, A, B and C such that whenever $p > V$, the following holds. There is a nontrivial, new, weight-two complex eigenform $\mathfrak{f}$ which has an associated elliptic curve $E' = E_{\mathfrak{f}}$ of conductor $\mathfrak{N}'$ dividing $\mathfrak{N}_E$ and $\overline{\rho}_{E',p} \sim \overline{\rho}_{E,p}$. ■

Proof. If we take p large enough (depending only on K, A, B and C), then by Corollary 4.8, $\overline{\rho}_{E,p}$ is surjective and hence absolutely irreducible by Proposition 3.6. Take p even larger, if necessary, such that p is unramified in K and such that, by Proposition 4.4, the Galois representation $\overline{\rho}_{E,p}$ is odd, satisfies $\det \overline{\rho}_{E,p} = \chi_p$ and is finite flat at every prime $\mathfrak{p} \mid p$ in K. Thus, $\overline{\rho}_{E,p}$ satisfies every condition of Conjecture 1. Applying Conjecture 1 gives a weight-two mod p eigenform θ over K of level $\mathfrak{N}_E$ (the Serre conductor of $\overline{\rho}_{E,p}$), such that for all primes $\mathfrak{q}$ coprime to $p\mathfrak{N}_E$, we have

$$\mathrm{Tr}(\overline{\rho}_{E,p}(\mathrm{Frob}_{\mathfrak{q}})) = \theta(T_{\mathfrak{q}}). \tag{4.4}$$

From Proposition 4.1, we know that there is only a finite amount of values of $\mathfrak{N}_E$ possible. Therefore, by Proposition 4.11 we know that we can take p large enough so that for any of the possible values of

$\mathfrak{N}_E$ there is weight-two complex eigenform $\mathfrak{f}$ with level $\mathfrak{N}_E$ that is a lift of θ. There are only finitely many such eigenforms $\mathfrak{f}$ and they depend only on K, A, B and C, so any constant depending on $\mathfrak{f}$ also only depends on these invariants.

Next, we aim to apply Conjecture 2. We have that $\overline{\rho}_{E,p}$ is absolutely irreducible irreducible. It then follows from (4.4) that $\mathfrak{f}$ is nontrivial. If $\mathfrak{f}$ is not new then we can replace $\mathfrak{f}$ with an equivalent new eigenform of level $\mathfrak{N}'$ dividing $\mathfrak{N}_E$. Therefore we may assume that $\mathfrak{f}$ is new of level $\mathfrak{N}'|\mathfrak{N}_E$. By applying Conjecture 2 we obtain that $\mathfrak{f}$ is either associated to an elliptic curve $E_{\mathfrak{f}}/K$ of conductor $\mathfrak{N}'$, or has an associated fake elliptic curve $A_{\mathfrak{f}}/K$ of conductor $\mathfrak{N}'^2$. By [64, Lemma 7.3], we can assume that we are in the former case by taking p sufficiently large ($p > 24$, in fact). Denote $E' = E_{\mathfrak{f}}$, then we have $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$. To see this, from Conjecture 2, we have that for all primes $\mathfrak{q} \nmid \mathfrak{N}'$,

$$\mathfrak{f}(T_{\mathfrak{q}}) = 1 + \mathrm{Norm}(\mathfrak{q}) - \#E'(\mathcal{O}_K/\mathfrak{q}).$$

Reducing this mod p and using Proposition 3.28, we find

$$\mathrm{Tr}(\overline{\rho}_{E',p}(\mathrm{Frob}_{\mathfrak{q}})) = \theta(T_{\mathfrak{q}}) \overset{(4.4)}{=} \mathrm{Tr}(\overline{\rho}_{E,p}(\mathrm{Frob}_{\mathfrak{q}})).$$

Since the set of elements of the form $\mathrm{Frob}_{\mathfrak{q}}$ with $\mathfrak{q} \nmid p\mathfrak{N}_E$ are a dense subset of $\mathrm{Gal}(\overline{K}/K)$ by Theorem 1.18, it follows that $\mathrm{Tr}(\overline{\rho}_{E,p}) = \mathrm{Tr}(\overline{\rho}_{E',p})$ and since also $\det \overline{\rho}_{E',p} = \chi_p = \det \overline{\rho}_{E,p}$, it follows that $\overline{\rho}_{E',p} \sim \overline{\rho}_{E,p}$. □

The following Lemma will allow us to take p large enough so that E' has a K-rational point of order 3.

Lemma 4.13. [23, Lemma 3.6] If E' as in Lemma 4.12 does not have a nontrivial K-rational point of order 3 and is not isogenous to an elliptic curve with a nontrivial K-rational point of order 3, then $p < C_{E'}$ where $C_{E'}$ is a constant depending only on E'. ■

Proof. By [26, Theorem 2], there are infinitely many primes $\mathfrak{P}$ such that $\#E'(\mathcal{O}_K/\mathfrak{P}) \not\equiv 0 \bmod 3$. Fix such a prime $\mathfrak{P} \notin T_K$. The conductor of E' is supported on the primes in T_K by Proposition 4.1 and Lemma 4.12. Therefore, E' has good reduction at $\mathfrak{P}$. By Proposition 4.1, E has semistable reduction at $\mathfrak{P}$. Suppose that E has good reduction at $\mathfrak{P}$. Then, $\mathfrak{P} \nmid \mathfrak{N}'$, we have $\mathrm{Tr}(\overline{\rho}_{E,p}(\mathrm{Frob}_{\mathfrak{P}})) = \mathrm{Tr}(\overline{\rho}_{E',p}(\mathrm{Frob}_{\mathfrak{P}}))$, or equivalently (by Proposition 3.28), $\#E(\mathcal{O}_K/\mathfrak{P}) \equiv \#E'(\mathcal{O}_K/\mathfrak{P}) \bmod p$. Since $3 \mid \#E(\mathcal{O}_K/\mathfrak{P})$, the difference is nonzero. Since the difference is divisible by p, it belongs to a finite set. This gives a bound on p. If E has multiplicative reduction at $\mathfrak{P}$, then we have

$$\pm(\mathrm{Norm}(\mathfrak{P}) + 1) \equiv a_{\mathfrak{P}}(E') \bmod p.$$

By comparing the traces of Frobenius, we get that the difference belongs to a bounded set which gives a bound on p. □

With all the ingredients gathered, we can now prove Theorem 4.10.

Proof of Theorem 4.10. By assuring that p is large enough, we invoke Lemma 4.12 to get an elliptic curve $E' = E_{\mathfrak{f}}$. It remains to show that E' satisfies *(i)-(iv)*. The elliptic curve E' has conductor $\mathfrak{N}'$ dividing $\mathfrak{N}_E$, which is supported on the primes in T_K. Thus, E' has good reduction outside of T_K giving *(i)*. Suppose that E' does not have a K-rational point of order 3 and is not 3-isogenous to an elliptic curve with a K-rational point of order 3. Then by Lemma 4.13, $p < C_{E'}$. Therefore, by taking p large enough and replacing V by $\max\{V, C_{E'}\}$ it follows that either E' has a K-rational point of order 3 or E' is 3-isogenous to an elliptic curve E'' with a K-rational point of order 3. In the latter case, we have that for every prime $\ell \neq 3$, the isogeny induces an isomorphism $E'[\ell] \cong E''[\ell]$ so $\overline{\rho}_{E',p} \sim \overline{\rho}_{E'',p}$ and since $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ we obtain *(ii)* and *(iii)* after possibly replacing E' by E''. To show that *(iv)* holds, let $\mathfrak{q} \in S_K$. As we have $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$, we have that $\#\overline{\rho}_{E,p}(I_{\mathfrak{q}}) = \#\overline{\rho}_{E',p}(I_{\mathfrak{q}})$ and from Lemma 4.6 it follows that $p \mid \#\overline{\rho}_{E',p}(I_{\mathfrak{q}})$ and by Lemma 4.5 it follows that $v_{\mathfrak{q}}(j(E')) < 0$ and hence E' has potentially multiplicative reduction at $\mathfrak{q}$ by Proposition 2.15. This gives *(iv)* and concludes the proof. □

4.3 Non-existence of the lowered curve

In this section we carry out step 3 of the modular method. To do this we look at a certain class of number fields K and show that for this class of number fields, the curve E' does not exist. In this section

we make use of class field theory and is greatly inspired by [19].

For a number field K with ring of integers $\mathcal{O}_K$. Let W_K be the set of non-trivial primitive solutions $(a, b, c) \in \mathcal{O}_K$ to

$$a^p + b^p = c^3 \tag{4.5}$$

such that every prime in K above 3 divides b. So this is the situation of Section 4.1 and 4.2 with $A = B = C = 1$ and $S_K = T_K$. The following result is essentially the same as [23, Theorem 1.1] except the condition on the narrow class number of K is more relaxed.

Theorem 4.14. (Nomden) Let K be a number field satisfying conjecture 1 and 2. Suppose that there is a unique prime λ in K above 3, that K contains a third root of unity ζ_3 and that $2 \nmid h_K^+$. Let W_K be as above. Then there is some $V = V(K)$ depending only on K such that for $p > V$, the equation (4.5) has no solutions in W_K. ■

4.3.1 ℓ-extensions and ℓ-groups

Let ℓ be a (rational) prime. We say that a group G is an *ℓ-group* if it is finite and its order is a power of ℓ. We say an extension of fields L/K is an *ℓ-extension* if it is a finite Galois extensions and $[L : K]$ is a power of ℓ. Hence if L/K is an ℓ-extension, then $\mathrm{Gal}(L/K)$ is a ℓ-group. The following result is non-trivial but a standard result from group theory. A proof can be found as a Corollary of [56, Theorem 2.1.6].

Lemma 4.15. Let G be an ℓ-group. Then every maximal subgroup of G is normal of index ℓ. ■

The following Lemma is heavily inspired by [19, Theorem 9.b]

Lemma 4.16. Let ℓ be an odd prime. Further, let K be a number field containing ζ_ℓ. Let L/K be an ℓ-extension. Then for any prime λ in K above ℓ, λ is totally ramified in L. ■

Proof. Write $G = \mathrm{Gal}(L/K)$ and let Λ be a prime in L above λ. Let $I = I_{\Lambda/\lambda}$ denote the inertia subgroup of Λ over K. We show that $I = G$. Suppose for a contradiction that I is a proper subgroup of G. Then by Lemma 4.15 there is some normal subgroup H of G, containing I and of index ℓ in G. Then the extension L^H/K is Galois of degree ℓ with Galois group G/H. We have that the image of I under the natural map $G \to G/H$ is $I_{\mathfrak{q}/\lambda}$ for some prime $\mathfrak{q}$ in L^H extending λ and which is a restriction of Λ. Since I is contained in H, its image vanishes under $G \to G/H$ so $I_{\mathfrak{q}/\lambda} = 0$ and $\mathfrak{q}/\lambda$ is unramified in L^H/K. Since L^H/K is Galois it follows that all primes above λ are unramified. On the other hand, since ζ_ℓ is in K, it follows from Proposition 1.25 that $L^H = K(\sqrt[\ell]{a})$ for some $a \in K^\times \setminus K^{\times \ell}$. This extension is always ramified above the primes above ℓ (here we use the fact that ℓ is odd) so we get a contradiction. It follows that $I = G$ which implies that λ is totally ramified in L. □

4.3.2 Non-existence of elliptic curves with specific reduction

The following theorem is the same as in [19, Theorem 1] except condition (iii) is a more relaxed condition on the narrow class number of K. The proof of the theorem is also similar to that of [19] except we use Lemma 4.16 instead of [19, Theorem 9b].

Theorem 4.17. (Nomden) Let ℓ be a rational odd prime and let K be a number field such that
(i) $\zeta_\ell \in K$;
(ii) K has a unique prime λ above ℓ;
(iii) $\gcd(h_K^+, \ell - 1) = 1$, where h_K^+ is the narrow class number of K.
There is no elliptic curve E/K with a K-rational ℓ-isogeny, good reduction outside of λ and potentially multiplicative reduction at λ. ■

The proof of Theorem 4.17 starts with a lemma, this lemma is proven analogously to the proof in [19, Section 3] except we fill in some more details for additional clarity. In what follows we say that a Galois representation $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{F}_p)$ is unramified (resp. ramified) at the infinite places if the corresponding extension $\bar{K}^{\ker \rho}/K$ is unramified (resp. ramified) at the infinite places.

Lemma 4.18. Let K be a number field as in Theorem 4.17. Let E/K be an elliptic curve with a K-rational ℓ-isogney, good reduction outside of λ and potentially multiplicative reduction at λ. Then there is a quadratic twist F/K of E such that $K(F[\ell^n])/K$ is an ℓ-extension for all $n \geqslant 1$ and F has split multiplicative reduction at λ. ■

Proof. Since E has a K-rational ℓ isogeny, the mod-ℓ representation is reducible by Proposition 3.4. So

$$\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \varphi & * \\ 0 & \psi \end{pmatrix} \tag{4.6}$$

where $\varphi, \psi \colon \mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_\ell^\times$ are characters mod ℓ. By Theorem 2.18 and Example 3.8.2, the characters φ and ψ are unramified outside of λ and the infinite places. On the other hand, by assumption, E/K_λ has potentially multiplicative reduction. By Proposition 3.30, there is some trivial or quadratic character $\eta \colon \mathrm{Gal}(\overline{K}_\lambda/K_\lambda) \to \{\pm 1\}$ such that the quadratic twist $E \otimes \eta/K_\lambda$ has split multiplicative reduction. It follows from Corollary 3.24 and Proposition 3.18 that

$$\overline{\rho}_{E,p}|_{\mathrm{Gal}(\overline{K}_\lambda/K_\lambda)} \sim \overline{\rho}_{E\otimes\eta,p}|_{\mathrm{Gal}(\overline{K}_\lambda/K_\lambda)} \otimes \eta \sim \begin{pmatrix} \chi_\ell & * \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix} = \begin{pmatrix} \chi_\ell \cdot \eta & * \\ 0 & \eta \end{pmatrix} \tag{4.7}$$

where $\chi_\ell \colon \mathrm{Gal}(\overline{K}_\lambda/K_\lambda) \to \mathbb{F}_\ell^\times$ is the ℓ^{th} cyclotomic character. By assumption we have $\zeta_\ell \in K$ so χ_ℓ is trivial. Let $I_\lambda \subset \mathrm{Gal}(\overline{K}_\lambda/K_\lambda)$ denote the inertia subgroup. Comparing (4.6) and (4.7) it follows that

$$\varphi|_{I_\lambda} = \psi|_{I_\lambda} = \eta|_{I_\lambda}.$$

Since η is quadratic or trivial, it follows that

$$\frac{\varphi}{\psi}\Big|_{I_\lambda} = 1 \quad \text{and} \quad \varphi^2|_{I_\lambda} = 1.$$

Therefore, φ/ψ and φ^2 are characters which are unramified away from the infinite places. Then by Example 3.8.2, φ/ψ and φ^2 correspond to abelian extensions of K which are unramified away from the infinite places and have degree $\#\mathrm{im}\,(\varphi/\psi)$ and $\#\mathrm{im}\,(\varphi^2)$, respectively. Since φ/ψ and φ^2 map to $\mathbb{F}_\ell^\times$, these degrees divide $\ell - 1$. By assumption, h_K^+ is coprime to $\ell - 1$. The quantity h_K^+ is the degree of the maximal abelian extension of K which is unramified away from the infinite primes (see Section 1.4). It follows that $\varphi/\psi = 1$ and $\varphi^2 = 1$ are trivial. And hence $\varphi = \psi$ are quadratic or trivial characters of $\mathrm{Gal}(\overline{K}/K)$. Let F/K be the quadratic twist $E \otimes \varphi/K$ of E, then F/K has split multiplicative reduction at λ and good reduction outside λ. Further, according to Proposition 3.18, the Galois representation $\overline{\rho}_{F,\ell} \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ of F/K is given by

$$\overline{\rho}_{F,\ell} = \overline{\rho}_{E,\ell} \otimes \varphi = \begin{pmatrix} \varphi & * \\ 0 & \varphi \end{pmatrix} \cdot \begin{pmatrix} \varphi & 0 \\ 0 & \varphi \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

and hence $\overline{\rho}_{E,\ell}(\mathrm{Gal}(\overline{K}/K))$ has order 1 or ℓ and is therefore an ℓ-group. Finally, we show that the image of the mod-ℓ^n representation $\overline{\rho}_{E,\ell^n}(\mathrm{Gal}(\overline{K}/K))$ is an ℓ-group for all $n \geqslant 1$. We have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\overline{K}/K) & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \\ & \searrow & \downarrow \pi \\ & & \mathrm{GL}_2(\mathbb{F}_\ell) \end{array}$$

where π is the projection. From this we obtain an exact sequence

$$1 \longrightarrow \overline{\rho}_{F,\ell^n}(\mathrm{Gal}(\overline{K}/K)) \cap \ker \pi \longrightarrow \overline{\rho}_{F,\ell^n}(\mathrm{Gal}(\overline{K}/K)) \longrightarrow \overline{\rho}_{F,\ell}(\mathrm{Gal}(\overline{K}/K)) \longrightarrow 1$$

Since $\overline{\rho}_{F,\ell}(\mathrm{Gal}(\overline{K}/K))$ is an ℓ-group, it follows that $\overline{\rho}_{F,\ell^n}(\mathrm{Gal}(\overline{K}/K))$ is an ℓ-group whenever $\ker \pi$ is. Indeed,

$$\ker \pi = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) : a \equiv d \equiv 1 \text{ and } b \equiv c \equiv 0 \bmod \ell \right\}$$

has order ℓ^{4^n-4}. By Example 3.2.1, the Galois extension $K(F[\ell^n])/K$ has Galois group $\overline{\rho}_{F,\ell^n}(\mathrm{Gal}(\overline{K}/K))$ so $K(F[\ell^n])/K$ is an ℓ-extension for all $n \geqslant 1$. □

Theorem 4.17 now follows from the previous lemma along with a famous result from Serre.

Proof of Theorem 4.17. Let E/K be an elliptic curve with a K-rational ℓ-isogeny, good reduction outside λ and potentially multiplicative reduction at λ. By Lemma 4.18, it follows that there is some quadratic twist F/K of E such that $K(F[\ell^n]/K)$ is an ℓ-extension and such that F has multiplicative reduction at λ. It follows from Proposition 2.15 that $v_\lambda(j(F)) < 0$, where $j(F)$ is the j-invariant of F. It then follows from Proposition 2.9 that F/K has no complex multiplication. By Serre's irreducibility theorem [44, Theorem 2.1], it follows that the ℓ-adic representation $\rho_{F,\ell}\colon \mathrm{Gal}(\overline{K}/K) \to T_\ell(E)$ is irreducible. On the other hand, we have that $\zeta_\ell \in K$ and $K(F[\ell^n])$ is an ℓ-extension and λ a prime above ℓ, it follows from Lemma 4.16 that λ is totally ramified in $K(F[\ell^n])$. The inertia group of λ in the extension $K(F[\ell^n])/K$ is equal to $\overline{\rho}_{F,\ell^n}(I_\lambda)$ and since λ is totally ramified, it follows that

$$\overline{\rho}_{F,\ell^n}(\mathrm{Gal}(\overline{K}/K)) = \overline{\rho}_{F,\ell^n}(I_\lambda).$$

Taking the inverse limit it follows that $\rho_{F,\ell}(\mathrm{Gal}(\overline{K}/K)) = \rho_{F,\ell}(I_\lambda)$. Since F has has split multiplicative reduction at λ, it follows from Corollary 3.24 that $\rho_{F,\ell}(I_\lambda)$ is reducible, a contradiction. □

4.3.3 Elimination

We are now ready to prove Theorem 4.14. Most of the work has already been done; the result follows from Theorem 4.10 and Theorem 4.17.

Proof of Theorem 4.14. Let K be a number field which satisfies conjectures 1 and 2 with narrow class number h_K^+ which is coprime to 2, a unique prime λ above 3 and which contains a primitive 3^{rd} root of unity. Let $(a,b,c) \in W_K$ be a solution to (4.5). Then $\lambda \mid b$ and hence it follows from Theorem 4.10 that there is an elliptic curve E'/K such that E' has good reduction away from λ, E' has a K-rational point of order 3 and E' has potentially multiplicative reduction at λ. Let $P \in E(K)$ be a K-rational point of order 3, then $E \to E/\langle P\rangle$ is a K-rational 3-isogeny. This is a contradiction with Theorem 4.17 for $\ell = 3$. □

4.4 S-unit equations and elliptic curves

In this section we give a different method to carry out step 3 of the modular method. To do this we ask K to satisfy another condition in terms of S-units. This condition in combination with the reduction properties of E' will give a contradiction. This section introduces S-units, proves an asymptotic result and delves deeper in the case where K is a quadratic imaginary number field. Our results are very comparable to [37] and [29].

4.4.1 S-units and S-unit equations

The notion of an S-unit generalizes the idea of a unit and the idea of localization at elements.

Definition 4.19. Let K be a number field and let S a finite set of primes in K. The ring of *S-integers* is defined to be

$$\mathcal{O}_S = \{x \in K : v_\mathfrak{p}(x) \geqslant 0 \notin S \text{ for all } \mathfrak{p} \notin S\}.$$

The unit group $\mathcal{O}_S^\times$ is called the *S-units* and is characterized as

$$\mathcal{O}_S^\times = \{x \in K : v_\mathfrak{p}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}.$$ ■

Example 4.20. 1. If $S = \varnothing$, then every $x \in \mathcal{O}_S$ satisfies $v_\mathfrak{p}(x) \geqslant 0$ for every prime $\mathfrak{p}$ in K and hence $\mathcal{O}_S \subset \mathcal{O}_K$. The converse inclusion $\mathcal{O}_K \subset \mathcal{O}_S$ is always true so it follows that $\mathcal{O}_K = \mathcal{O}_S$ and $\mathcal{O}_K^\times = \mathcal{O}_S^\times$.

2. Let $\mathcal{O}_K$ be the ring of integers of K and suppose that K has class number 1. A finite set of primes S can be considered as a finite set of prime elements of $\mathcal{O}_K$. Write $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ where we view the $\mathfrak{p}_i$ as elements of $\mathcal{O}_K$. Then

$$\mathcal{O}_S = \mathcal{O}_K[\tfrac{1}{\mathfrak{p}_1}, \ldots, \tfrac{1}{\mathfrak{p}_k}].$$

The ring on the right hand side is the localization of $\mathcal{O}_K$ at $\{\mathfrak{p}_i^n : i = 1, \ldots, k \text{ and } n \in \mathbb{Z}\}$. Via this point of view, S-integers generalize the idea of localization at elements. The S-units are given by $\mathcal{O}_S^\times = \mathcal{O}_K^\times \times \langle \mathfrak{p}_1\rangle \times \ldots \times \langle \mathfrak{p}_k\rangle$. ■

In Example 4.20.2 we saw that if K has class number 1, then $\mathcal{O}_S^\times$ has rank equal $\text{rank}(\mathcal{O}_K^\times) + \#S$. By Dirichlet's unit Theorem it follows that $\text{rank}(\mathcal{O}_K^\times) = r + s - 1$ where r is the number of real embeddings $K \hookrightarrow \mathbb{R}$ and s is the amount of conjugate pairs of embeddings $K \hookrightarrow \mathbb{C}$ that are not contained in $\mathbb{R}$. The tuple (r, s) is called the *signature* of K.

Proposition 4.21. (Dirichlet) Let K be a number field of signature (r, s) and let S be a finite set of primes in K. Then $\mathcal{O}_S^\times$ has rank $r + s + \#S - 1$. ■

Proof. For every $\mathfrak{p} \in S$ do the following. There is an element $a_\mathfrak{p}$ in $\mathcal{O}_K$ with positive $\mathfrak{p}$-adic valuation and such that $v_\mathfrak{q}(a_\mathfrak{p}) = 0$ for all primes $\mathfrak{q} \neq \mathfrak{p}$. Indeed, if h denotes the class number of K, then $\mathfrak{p}^h$ is a principal ideal and we can take a generator of $\mathfrak{p}^h$ to be $a_\mathfrak{p}$. Since such an $a_\mathfrak{p}$ exists, there exists an element $\pi_\mathfrak{p} \in \mathcal{O}_K$ which satisfies $v_\mathfrak{q}(\pi_\mathfrak{p}) = 0$ for all $\mathfrak{q} \neq \mathfrak{p}$ and minimizes $v_\mathfrak{p}$. It then follows that

$$\mathcal{O}_S^\times = \mathcal{O}_K^\times \times \prod_{\mathfrak{p} \in S} \langle \pi_\mathfrak{p} \rangle.$$

Then the result follows from Dirichlet's unit theorem. □

By [5, Proposition 5.6] we have that the localization of an integrally closed ring is integrally closed. The S-units generalize the idea of localization and is not far off from a localization, thus we expect $\mathcal{O}_S$ to be integrally closed.

Proposition 4.22. Let K be a number field and S a finite set of primes in K, then $\mathcal{O}_S$ is integrally closed. ■

Proof. The field of fractions of $\mathcal{O}_S$ is K. Let $x \in K$ and suppose there exists, $a_{n-1}, \ldots, a_0 \in \mathcal{O}_S$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0 = 0.$$

There is an element $s \in \mathcal{O}_K$ such that $v_\mathfrak{p}(s) = 0$ for all $\mathfrak{p} \notin S$ and such that $sa_i \in \mathcal{O}_K$ for all i. To see this, take s to be a product of sufficiently large powers of the $\pi_\mathfrak{p}$ in the proof of Proposition 4.21. We have

$$(sx)^n + sa_{n-1}(sx)^{n-1} + \ldots + s^{n-1}a_1(sx) + s^n a_0.$$

Since $\mathcal{O}_K$ is integrally closed, it follows that $sx \in \mathcal{O}_K$. For every prime $\mathfrak{p} \notin S$ we have

$$v_\mathfrak{p}(x) = v_\mathfrak{p}(s) + v_\mathfrak{p}(x) = v_\mathfrak{p}(sx) \geqslant 0$$

which shows that $x \in \mathcal{O}_S$. □

The S-units are often studied, mainly due to the following equation. In this thesis we study a similar equation but the results relating to the S-unit equation are still relevant.

Definition 4.23. Let K be a number field, S a finite set of primes of K and $a, b \in K^\times$. The *S-unit equation* is the equation

$$ax + by = 1 \quad \text{for} \quad x, y \in \mathcal{O}_S^\times.$$ ■

Theorem 4.24. (Siegel) Let K be a number field, S be a finite set of primes of K and $a, b \in K^\times$, then the S-unit equation $ax + by = 1$ has finitely many solutions in $\mathcal{O}_S^\times$. ■

The original proof is by Siegel who studied curves of genus $\geqslant 1$, his proof can be found in [49]. An alternate geometric proof can be found in [31, Theorem 8.3.1]. These two geometric proofs do not explicitly give these finite solutions. However, De Weger developed an effective algorithm in his famous thesis [14] for $K = \mathbb{Q}$. These algorithms were generalized to general number fields in, for example, [53]. A robust algorithm, which has been implemented in Sage [60], has been developed by Alejandra Alvarado, Angelos Koutsianas, Beth Malmskog, Christopher Rasmussen, David Roe, Christelle Vincent, Mckenzie West in [3].

We end this section by extending the notion of the class group to S-integers.

Definition 4.25. Let K be number field and let S be a finite set of primes of K. For a prime $\mathfrak{p}$ in K let $[\mathfrak{p}]$ denote the class of $\mathfrak{p}$ in $\text{Cl}(K)$. The *S-class group* $Cl_S(K)$ is defined to be

$$\text{Cl}_S(K) = \text{Cl}(K)/\langle [\mathfrak{p}] \rangle_{\mathfrak{p} \in S}.$$ ■

Since the extension of prime ideals $\mathfrak{p} \in S$ become unit ideals under the inclusion $\mathcal{O}_K \to \mathcal{O}_S$ it makes sense to define $\mathrm{Cl}_S(K)$ this way as it sets these ideals equal to 0 in the class group. Following this intuition, we see that if a fractional ideal I in $\mathcal{O}_K$ is such that I^k is principal for some $k \nmid \#\mathrm{Cl}_S(K)$ and I does not extend to the unit ideal under the inclusion $\mathcal{O}_K \to \mathcal{O}_S$, then I is principal. We call a fractional ideal I which extends to the unit ideal under $\mathcal{O}_K \to \mathcal{O}_S$ an *S-ideal*. Equivalently, an S-ideal is an ideal only divisible by ideals in S.

4.4.2 Asymptotic result from S-units

Let K be a number field with ring of integers $\mathcal{O}_K$ and let $A, B, C \in \mathcal{O}_K$. Let W_K be the set of non-trivial primitive solutions $(a, b, c) \in \mathcal{O}_K^3$ to

$$Aa^p + Bb^p = Cc^3 \tag{4.8}$$

such that every prime $\mathfrak{q}$ above 3 divides ab. So this is the exact situation as in Sections 4.1 and 4.2. As in these sections, define

$$T_K = \{\mathfrak{P} : \mathfrak{P} \text{ is a prime in } K \text{ and } \mathfrak{P} \mid 3ABC\}.$$

The main result of this section is as follows.

Theorem 4.26. (Nomden) Let K be a number field with $\mathrm{Cl}_{T_K}(K)[3] = 1$ and satisfying Conjectures 1 and 2. Further suppose that for every solution $(\alpha, \beta, \gamma) \in \mathcal{O}_{T_K}^\times \times \mathcal{O}_{T_K}^\times \times \mathcal{O}_{T_K}$ to $\alpha + \beta = \gamma^3$, there exists a prime $\mathfrak{q}$ in K above 3 such that

$$|v_\mathfrak{q}(\alpha\beta^{-1})| \leqslant 3v_\mathfrak{q}(3).$$

Then there is a constant $V = V(K, A, B, C) > 0$ depending only on K, A, B and C such that for $p > V$, the equation (4.8) has no solutions in W_K. ■

Theorem 4.26 generalizes Theorem 2.5 of [29] in the sense that [29] restricts to totally real number fields. What allows this generality in our case is the slightly modified level lowering technique from Section 4.2 which is also used in [23, Section 3]. A slight downside of this method is that we need to assume two conjectures instead of one. In the totally real case only one is assumed due to the level lowering result [20, Theorem 7] of Freitas and Siksek for elliptic curves. The restriction of K regarding T_K-units in the assumptions of Theorem 4.26 are due to Mocanu [37], we will be employing the methods used by her in this section. These methods are also used in [29].

Mocanu's method makes use of a few lemmas, we will make use of these too. The following result is a summary of Lemma 15.ii, 16.ii and 17.ii of [37] and is stated here for convenience.

Lemma 4.27. [37, Section 2.1] Let E/K be an elliptic curve with a K-rational point of order 3. Then E has a model of the form

$$E\colon y^2 + cxy + dy = x^3.$$

Further, if S is a finite set of primes in K including the primes above 3 and E has good reduction outside of S. Then $\lambda := \frac{c^3}{d}$ is such that $\lambda\mathcal{O}_K = I^3J$ where I and J are fractional ideals and J is an S-ideal. ■

We are now ready to prove Theorem 4.26. The following reasoning is essentially the same as in [37, Section 4.4] and [29, Section 2.5].

Proof of Theorem 4.26. Let $(a, b, c) \in W_K$ be a solution to (4.8). Then by Theorem 4.10 there is an elliptic curve E'/K such that E' has a K-rational point of order 3. Then, by Lemma 4.27, E' has a model of the form

$$E'\colon y^2 + exy + dy = x^3$$

for some $d, e \in K$. Then the j-invariant $j_{E'}$ of E is equal to

$$j_{E'} = \frac{e^3(e^3 - 24d)^3}{d^3(e^3 - 27d)}.$$

By Theorem 4.10, E' has good reduction away from T_K. From this and Proposition 2.15 it follows that $v_\mathfrak{P}(j_{E'}) \geqslant 0$ for all $\mathfrak{P} \notin T_K$. In other words, $j_{E'} \in \mathcal{O}_{T_K}$. Set $\lambda := \frac{e^3}{d}$ and $\mu := \lambda - 27$. Then

$$j_{E'} = \frac{\lambda(\lambda - 24)^3}{\lambda - 27} = \frac{(\mu + 27)(\mu + 3)^3}{\mu} = \mu^3(1 + 27\mu^{-1})(1 + 3\mu^{-1})^3. \tag{4.9}$$

Rearranging the equations above and using the fact that $j_{E'} \in \mathcal{O}_{T_K}$, we see that λ and μ satisfy monic polynomials with coefficients in $\mathcal{O}_{T_K}$. Since $\mathcal{O}_{T_K}$ is integrally closed by Proposition 4.22, it follows that λ and μ are elements in $\mathcal{O}_{T_K}$. Using the right hand side of (4.9) we then see that μ^{-1} also satisfies a monic polynomial with coefficients in $\mathcal{O}_{T_K}$. It then follows that $\mu^{-1} \in \mathcal{O}_{T_K}$ and hence $\mu \in \mathcal{O}_{T_K}^\times$. By Lemma 4.27, the prinicipal ideal (λ) is equal to I^3J for some fractional ideal I and T_K-ideal J. Since J is a T_K-ideal, we have $[I]^3 = 1$ in $\mathrm{Cl}_{T_K}(K)$. By assumption, $\mathrm{Cl}_{T_K}(K)$ has no 3-torsion so we find that $I = \gamma\tilde{I}$ for some T_K-ideal $\tilde{I}$ and $\gamma \in \mathcal{O}_K$. So

$$(\lambda) = \gamma^3 \tilde{I}J \quad \Leftrightarrow \quad \left(\frac{\lambda}{\gamma^3}\right) = \tilde{I}J.$$

The right hand side of the latter is a T_K-ideal so it follows that $u \coloneqq \lambda/\gamma^3 \in \mathcal{O}_{T_K}^\times$. Recall that we have $\mu + 27 = \lambda$. Dividing this equation by u gives

$$\alpha + \beta = \gamma^3$$

where $\alpha = \mu/u$ and $\beta = 27/\mu$ which are both elements of $\mathcal{O}_{T_K}^\times$. By assumption, there is some $\mathfrak{q} \in S_K$ such that

$$|v_\mathfrak{q}(\tfrac{\mu}{27})| = |v_\mathfrak{q}(\alpha\beta^{-1})| \leqslant 3v_\mathfrak{q}(3).$$

This is equivalent to saying that $0 \leqslant v_\mathfrak{q}(\mu) \leqslant 6v_\mathfrak{q}(3)$. We show that these bounds on $v_\mathfrak{q}(\mu)$ imply that $v_\mathfrak{q}(j_{E'}) \geqslant 0$. From the expression in (4.9) in μ we find that

$$v_\mathfrak{q}(j_{E'}) = v_\mathfrak{q}(\mu + 27) + 3v_\mathfrak{q}(\mu + 3) - v_\mathfrak{q}(\mu) \tag{4.10}$$

We distinguish three cases. First suppose that $0 \leqslant v_\mathfrak{q}(\mu) \leqslant v_\mathfrak{q}(3)$. Then $v_\mathfrak{q}(\mu + 27) = v_\mathfrak{q}(\mu)$ and $v_\mathfrak{q}(\mu + 3) \geqslant v_\mathfrak{q}(\mu)$. Then (4.10) implies that $v_\mathfrak{q}(j_{E'}) \geqslant 0$.
If $v_\mathfrak{q}(3) < v_\mathfrak{q}(\mu) \leqslant 3v_\mathfrak{q}(3)$ then $v_\mathfrak{q}(\mu + 27) \geqslant v_\mathfrak{q}(\mu) > v_\mathfrak{q}(3)$ and $v_\mathfrak{q}(\mu + 3) = v_\mathfrak{q}(3)$. Then (4.10) implies that $v_\mathfrak{q}(j_{E'}) > 0$.
Finally, if $3v_\mathfrak{q}(3) < v_\mathfrak{q}(\mu) \leqslant 6v_\mathfrak{q}(3)$, then $v_\mathfrak{q}(\mu + 27) = 3v_\mathfrak{q}(3)$ and $v_\mathfrak{q}(\mu + 3) = v_\mathfrak{q}(3)$. Then $v_\mathfrak{q}(j_{E'}) = 6v_\mathfrak{q}(3) - v_\mathfrak{q}(\mu) \geqslant 0$. In all cases, this contradicts with the fact that $v_\mathfrak{q}(j_{E'}) < 0$ by Theorem 4.10.iv and Proposition 2.15. □

As in [37], under some stricter conditions on K, A, B and C, we may replace the S-unit equation in the statement of Theorem 4.26 by a simpler one. The proof of this Theorem is again similar to that of [37, Theorem 11] and [29, Proposition 2.7].

Theorem 4.28. Let K be a number field such that there is only one prime $\mathfrak{q}$ above 3. Suppose that $\mathfrak{q}$ is principal and that $3 \nmid h_K h_{K(\zeta_3)}$. Let A, B and C be elements in $\mathcal{O}_K$ supported only on $\mathfrak{q}$. Let $S_K = \{\mathfrak{q}\}$ and suppose that for every solution $(\alpha, \gamma) \in \mathcal{O}_{S_K}^\times \times \mathcal{O}_{S_K}$ to

$$\alpha + 1 = \gamma^3 \tag{4.11}$$

with $v_\mathfrak{q}(\alpha) \geqslant 0$ satisfies $v_\mathfrak{q}(\alpha) \leqslant 3v_\mathfrak{q}(3)$. Then there is a constant $V = V(K, A, B, C)$ such that the equation $Aa^p + Bb^p = Cc^3$ with exponent $p > V$ has no asymptotic solutions in W_K. ■

Proof. With notation as in Theorem 4.26, we have $T_K = \{\mathfrak{q}\}$ Note that since $3 \nmid h_K$, by Theorem 4.26, it suffices to show that for every solution $(\alpha, \beta, \gamma) \in \mathcal{O}_{S_K}^\times \times \mathcal{O}_{S_K}^\times \times \mathcal{O}_{S_K}$ to $\alpha + \beta = \gamma^3$ satisfies $|v_\mathfrak{q}(\alpha\beta^{-1})| \leqslant 3v_\mathfrak{q}(3)$. Let (α, β, γ) be such a solution. Scale this solution by cubic powers (this is where the assumption that $\mathfrak{q}$ is principal comes in) and swap α and β if necessary so that $v_\mathfrak{q}(\beta) = 0, 1$ or 2 and $0 \leqslant v_\mathfrak{q}(\beta) \leqslant v_\mathfrak{q}(\alpha)$. We consider several cases.
Case 1: Suppose that $v_\mathfrak{q}(\beta) = 1$ or 2. If $v_\mathfrak{q}(\alpha) \neq v_\mathfrak{q}(\beta)$, then $v_\mathfrak{q}(\alpha) > v_\mathfrak{q}(\beta)$ and

$$v_\mathfrak{q}(\gamma^3) = v_\mathfrak{q}(\alpha + \beta) = v_\mathfrak{q}(\beta)$$

which contradicts since $v_\mathfrak{q}(\beta)$ is not a multiple of 3. Therefore, $v_\mathfrak{q}(\alpha) = v_\mathfrak{q}(\beta)$. It follows that $|v_\mathfrak{q}(\alpha\beta^{-1})| = 0 \leqslant 3v_\mathfrak{q}(3)$.
Case 2: Suppose that $v_\mathfrak{q}(\beta) = 0$ and that β is not a cube. Suppose for a contradiction that $v_\mathfrak{q}(\alpha) > 3v_\mathfrak{q}(3)$ so that $3^3 = \mathfrak{q}^{3v_\mathfrak{q}(3)} \mid \alpha$. The field $L = K(\zeta_3, \sqrt[3]{\beta})$ is an abelian extension of degree 3 of $K(\zeta_3)$. We

show that $L/K(\zeta_3)$ is unramified above $\mathfrak{q}$. The element $\theta = \frac{\gamma^2+\gamma\zeta_3\sqrt[3]{\beta}+\zeta_3^2\sqrt[3]{\beta}}{3} \in L$ has minimal polynomial over K

$$\begin{aligned} f_K^\theta(X) &= X^3 + \frac{\gamma(\gamma^3-\beta)}{3}X^2 - \gamma^2 X - \frac{(\gamma^3-\beta)^2}{27} \\ &= X^3 + \frac{\gamma\alpha}{3}X^2 - \gamma^2 X - \frac{\alpha^2}{27}. \end{aligned}$$

Since $3^3 \mid \alpha$ and $v_\mathfrak{q}(\gamma) = \frac{1}{3}v_\mathfrak{q}(\alpha+\beta) = 0$, the polynomial f_K^θ belongs to $\mathcal{O}_K[X]$ and has discriminant

$$\Delta(f_K^\theta) = -\frac{2\gamma^3\alpha^3}{3^5} - \frac{4\gamma^3\alpha^5}{3^9} + \frac{\gamma^6\alpha^2}{3^2} - 4\gamma^6 - \frac{\alpha^4}{3^3}.$$

Since $3^3 \mid \alpha$ and $v_\mathfrak{q}(\gamma) = 0$, it follows that $\Delta \equiv -4\gamma^6 \bmod \mathfrak{q}$. We have $\Delta \not\equiv 0 \bmod \mathfrak{q}$ since $v_\mathfrak{q}(\gamma) = 0$ and hence $L/K(\zeta_3)$ is unramified at $\mathfrak{q}$. The other primes where $L/K(\zeta_3)$ may ramify are the primes dividing β. However, since $\beta \in \mathcal{O}_{S_K}^\times$, it follows that β is supported on $\mathfrak{q}$. It follows that $L/K(\zeta_3)$ is unramified above all places (also the infinite ones since $K(\zeta_3)$ and L have the same signature) and hence $3 \mid h_K$ by Proposition 1.20 which contradicts with our assumption. Therefore, $v_\mathfrak{q}(\alpha) \leqslant 3v_\mathfrak{q}(3)$ and $|v(\alpha\beta^{-1})| = v_\mathfrak{q}(\alpha) \leqslant 3v_\mathfrak{q}(3)$.
Case 3: Suppose that $v_\mathfrak{q}(\beta) = 0$ and β is a cube. By dividing the equation $\alpha+\beta=\gamma^3$ by β, we may assume that $\beta = 1$. We get an equation of the form (4.11) and by assumption we get that $v_\mathfrak{q}(\alpha) \leqslant 3v_\mathfrak{q}(3)$ and hence $|v_\mathfrak{q}(\alpha\beta^{-1})| = v_\mathfrak{q}(\alpha) \leqslant 3v_\mathfrak{q}(3)$. In all possible cases we find that $|v_\mathfrak{q}(\alpha\beta^{-1})| \leqslant 3v_\mathfrak{q}(3)$. The result then follows from Theorem 4.26. □

The proofs of Theorems 4.26 and 4.28 requires a lot of machinery and still, if we want to find out whether a number field K has no asymptotic solutions in W_K to (4.8), we would need to find solutions to the T_K unit equation $\alpha+\beta=\gamma^3$ or, at least, have a sufficient amount of information on the solutions of this equation. A priori this means that we simply translated our problem of finding a triple in $\mathcal{O}_K$ which satisfies a relation to finding a triple in $\mathcal{O}_{T_K}^\times \times \mathcal{O}_{T_K}^\times \times \mathcal{O}_{T_K}$ satisfying a relation. Luckily, the result below shows that there is a major difference between the two problems.

Let K be a number field and S a finite set of primes in K. We say that two solutions $(\alpha_1,\beta_1,\gamma_1)$ and $(\alpha_2,\beta_2,\gamma_2)$ in $\mathcal{O}_S^\times \times \mathcal{O}_S^\times \times \mathcal{O}_S$ to $\alpha+\beta=\gamma^3$ are *equivalent* if there is some $\varepsilon \in \mathcal{O}_S^\times$ such that

$$\alpha_1 = \varepsilon^3\alpha_2, \quad \beta_1 = \varepsilon^3\beta_2 \quad \text{and} \quad \gamma_1 = \varepsilon\gamma_2.$$

Write $(\alpha_1,\beta_1,\gamma_1) \sim (\alpha_2,\beta_2,\gamma_2)$ when these two solutions are equivalent. The result is then as follows

Proposition 4.29. [37, Theorem 39] Let K be a number field and let S be a finite set of primes in K. The equation

$$\alpha+\beta=\gamma^3 \qquad \text{with } \alpha,\beta \in \mathcal{O}_S^\times \text{ and } \gamma \in \mathcal{O}_S$$

has a finite number of solutions up to the equivalence '$\sim$'. Moreover, these are effectively computable. ■

This result is due to Mocanu, we copy her proof here as it highlights an algorithm as to how to compute non-equivalent solutions to $\alpha+\beta=\gamma^3$.

Proof of Proposition 4.29. Suppose that

$$\alpha+\beta=\gamma^3 \tag{4.12}$$

with $\alpha,\beta \in \mathcal{O}_S^\times$ and $\gamma \in \mathcal{O}_S$. By Proposition 4.21, the quotient $\mathcal{O}_S^\times/\mathcal{O}_S^{\times 3}$ is finite. Let $\{\beta_1,\dots,\beta_\ell\}$ be a full set of representatives for $\mathcal{O}_S^\times/\mathcal{O}_S^{\times 3}$. We can scale (α,β,γ) and obtain an equivalent solution to (4.12) so that $\beta \in \{\beta_1,\dots,\beta_\ell\}$. This shows that (up to equivalence) β is contained in a finite set. Now fix β, we show that there is a finite amount of possible solutions for α. Rewrite (4.12) as

$$(\gamma - \sqrt[3]{\beta})(\gamma - \zeta_3\sqrt[3]{\beta})(\gamma - \zeta_3^2\sqrt[3]{\beta}) = \alpha \tag{4.13}$$

over $L = K(\zeta_3, \sqrt[3]{\beta})$. Define

$$S' = \{\mathfrak{P} : \mathfrak{P} \text{ is a prime in } L \text{ such that } \mathfrak{P} \mid \mathfrak{p} \text{ for some } \mathfrak{p} \in S\}.$$

If $\beta \neq -1$, define $x := \gamma - \sqrt[3]{\beta}$ and $y := \gamma - \zeta_3\sqrt[3]{\beta}$. Then, by examining (4.13), it follows that x and y are S'-units in L. Further, x and y satisfy

$$\frac{1}{(\zeta_3 - 1)\sqrt[3]{\beta}}x - \frac{1}{(\zeta_3 - 1)\sqrt[3]{\beta}}y = 1.$$

Thus, by Siegel's Theorem (Theorem 4.24), there is a finite amount of pairs (x, y) such that this equation is satisfied. Further, by the discussion below Theorem 4.24, these solutions are effectively computable. Finally, noting that,

$$\alpha = xy(y - \zeta_3(\zeta_3 - 1)\sqrt[3]{\beta})$$

shows that there is a finite possible solutions α and these are effectively computable. If $\beta = -1$ take instead $L = K(\zeta_3)$, $x = \gamma + 1$ and $y = \gamma + \zeta_3$ and repeat the argument above. □

The proof of Proposition 4.29 gives a method for finding all equivalence classes of solutions $(\alpha, \beta, \gamma) \in \mathcal{O}_S^\times \times \mathcal{O}_S^\times \times \mathcal{O}_S$ $\alpha + \beta = \gamma^3$. This is done in the following steps

1. Determine a full set of representatives $\{\beta_1, \ldots, \beta_\ell\}$ for $\mathcal{O}_S^\times/\mathcal{O}_S^{\times 3}$.
2. For every $\beta \in \{\beta_1, \ldots, \beta_\ell\}$, let $L = K(\zeta_3, \sqrt[3]{\beta})$ and define

$$S' = \{\mathfrak{P} : \mathfrak{P} \text{ is a prime in } L \text{ such that } \mathfrak{P} \mid \mathfrak{p} \text{ for some } \mathfrak{p} \in S\}.$$

Then solve the S'-unit equation

$$\frac{1}{(\zeta_3 - 1)\sqrt[3]{\beta}}x - \frac{1}{(\zeta_3 - 1)\sqrt[3]{\beta}}y = 1 \tag{4.14}$$

in L.
3. For every solution (x, y) computed in 2 check whether $x + \sqrt[3]{\beta}$ and $y + \zeta_3\sqrt[3]{\beta}$ are equal and elements of K. In the case they are equal, define γ to be the common value.
4. For every x and y which satisfy the condition in 3, compute $\alpha = xy(y - \zeta_3(\zeta_3 - 1)\sqrt[3]{\beta})$.

Note that, in step 2, since $\beta \in \mathcal{O}_S$, we find that $\sqrt[3]{\beta} \in \mathcal{O}_{S'}$. If we are in the special case where $\zeta_3 - 1 \in \mathcal{O}_{S'}^\times$ then the map $(x, y) \mapsto (\tilde{x}, \tilde{y}) = (x/(\zeta_3 - 1), -y/(\zeta_3 - 1))$ is a bijection between solutions of the S'-unit equation (4.14) and solutions to the S'-unit equation

$$\tilde{x} + \tilde{y} = 1. \tag{4.15}$$

The equation (4.15) can be solved using Sage [60] thanks to the work done in [3]. If we try to solve (4.11) to check the condition in Theorem 4.28 then we may simply set $\beta = 1$ in every step. In [38] this recipe is implemented for number fields of the form $\mathbb{Q}(\sqrt{-d})$ where $d \geqslant 2$ is a square-free integer such that $d \equiv 1 \bmod 3$. Running this implementation for several values of d, one may suspect that the solutions are independent of d. This is explored more in the next section.

4.4.3 Imaginary quadratic number fields

Let $K = \mathbb{Q}(\sqrt{-d})$ where $d \geqslant 2$ is a square-free integer such that $d \equiv 1 \bmod 3$ and let $\mathcal{O}_K$ be the ring of integers of K. The condition that $d \equiv 1 \bmod 3$ means that the prime 3 is inert in K (see, for example, [55, Corollary 3.11]). Let A, B and C be elements of $\mathcal{O}_K$ which are only supported on 3. In this section we show using Theorem 4.28 that the equation

$$Aa^p + Bb^p = Cc^3 \tag{4.16}$$

has no asymptotic solutions (a, b, c) in W_K, with W_K as in Section 4.4.2. Let $S = \{(3)\}$. As seen in Section 4.4.2 solving the equation (4.16) over W_K comes down to solving the S-unit equation $\alpha + \beta = \gamma^3$ with $\alpha, \beta \in \mathcal{O}_S^\times$ and $\gamma \in \mathcal{O}_S$. The following result solves this S-unit equation. Some parts of the proof are inspired by [37, Section 4.6].

Proposition 4.30. (Nomden) Let $d \geqslant 2$ be a positive square-free integer such that $d \equiv 1 \bmod 3$. Let $K = \mathbb{Q}(\sqrt{-d})$ and let S be the set of primes in K above 3. The only solutions to the S-unit equation $\alpha + 1 = \gamma^3$ with $(\alpha, \gamma) \in \mathcal{O}_S^\times \times \mathcal{O}_S$ are $(-1, 0)$ and $(-9, -2)$. ■

Proof. Let $(\alpha,\gamma)\in\mathcal{O}_S^\times\times\mathcal{O}_S$ be a solution to $\alpha+1=\gamma^3$. The condition that $d\equiv 1 \bmod 3$ is precisely the condition that 3 is inert in K. Therefore $S=\{(3)\}$ and $\mathcal{O}_S=\mathcal{O}_K[\frac{1}{3}]$ and $\mathcal{O}_S^\times=\{\pm1\}\times\langle 3\rangle$. It follows that $\alpha=\pm 3^n$ for some $n\in\mathbb{Z}$. First suppose that $n\leqslant 0$. Then $\pm 3^n=\pm\frac{1}{3^k}$ where $k=|n|$. It follows that

$$\gamma^3=\frac{\pm 1+3^k}{3^k}. \tag{4.17}$$

Therefore, $3v_3(\gamma)=-k$ which shows that k is divisible by 3 and that $\gamma=\frac{c}{3^{k/3}}$ for some $c\in\mathcal{O}_K$. Then (4.17) shows that $c^3=\pm 1+3^k$. We have

$$\pm 1=c^3-3^k=\big(c-3^{\frac{k}{3}}\big)\big(c^2+3^{\frac{k}{3}}+3^{\frac{2k}{3}}\big).$$

This is an equality in $\mathcal{O}_K$ and hence it follows that $c-3^{\frac{k}{3}}\in\mathcal{O}_K^\times=\{\pm 1\}$. It follows that $c=\pm 1+3^{\frac{k}{3}}$ and

$$c^3=\pm 1+3^{\frac{k}{3}+1}\pm 3^{\frac{2k}{3}+1}+3^k \quad\Longleftrightarrow\quad c^3-3^k=\pm 1+3^{\frac{k}{3}+1}\pm 3^{\frac{2k}{3}+1}.$$

The left hand side of the last equation is equal to 1 or -1 which forces $k=0$ and hence $n=0$. We conclude that $n\geqslant 0$. Next, suppose for a contradiction that $n>2$. Since $\gamma^3=\pm 3^n+1$ it follows that $v_3(\gamma)=0$ and hence $\gamma\in\mathcal{O}_K$. Write

$$\pm 3^n=(\gamma-1)(\gamma-\zeta_3)(\gamma-\zeta_3^2)$$

in $L\coloneqq K(\zeta_3)$. Define

$$x=\gamma-1,\quad y=\gamma-\zeta_3\quad\text{and}\quad z=\gamma-\zeta_3^2.$$

Then $x-y=\zeta_3-1$ and $y-z=\zeta_3(\zeta_3-1)$. Let $\sigma\in\mathrm{Gal}(L/K)$ be the generator of $\mathrm{Gal}(L/K)$ i.e. σ is the element of $\mathrm{Gal}(L/K)$ such that $\sigma(\zeta_3)=\zeta_3^2$. Let $\mathfrak{p}=(\zeta_3-1)$ be the prime above 3 in L. Then $\sigma(\mathfrak{p})=\mathfrak{p}$ and since $\sigma(z)=y$ we have that $v_\mathfrak{p}(z)=v_\mathfrak{p}(y)=:r$. We have

$$1=v_\mathfrak{p}(\zeta_3(\zeta_3-1))=v_\mathfrak{p}(y-z)\geqslant r.$$

We claim that r is equal to 1. Suppose for a contradiction that $r\leqslant 0$. We have

$$v_\mathfrak{p}(x)\geqslant v_\mathfrak{p}(xyz)=v_\mathfrak{p}(3^n)>4$$

Using this, it follows that

$$1=v_\mathfrak{p}(\zeta_3-1)=v_\mathfrak{p}(x-y)=\min\{v_\mathfrak{p}(x),v_\mathfrak{p}(y)\}=r\leqslant 0,$$

a contradiction. We conclude that $r=1$. It follows that $2n=v_\mathfrak{p}(xyz)=v_\mathfrak{p}(x)+2$ and hence $v_\mathfrak{p}(x)>2$. Using this fact, define

$$u=\frac{x}{\zeta_3-1}\in\mathcal{O}_L\quad\text{and}\quad v=\frac{-y}{\zeta_3-1}\in\mathcal{O}_L^\times.$$

We have that $\mathfrak{p}^2=(3)\mid u$ and since $u+v=1$ it follows that $v\equiv 1 \bmod 3$. Let τ be the generator of $\mathrm{Gal}(L/\mathbb{Q}(\zeta_3))$. Then, since $\tau(\mathfrak{p})=\mathfrak{p}$, it follows that $(3)\mid\tau(u)$ and hence also $\tau(v)\equiv 1 \bmod 3$. It follows that $N_{L/\mathbb{Q}(\zeta_3)}(v)=\tau(v)v\equiv 1 \bmod 3$. Since $v\in\mathcal{O}_L^\times$ we also have that $N_{L/\mathbb{Q}(\zeta_3)}(v)\in\mathcal{O}_{\mathbb{Q}(\zeta_3)}^\times=\langle-\zeta_3\rangle$. Combining these two facts it follows that $N_{L/\mathbb{Q}(\zeta_3)}(v)=1$. Let $F\coloneqq\mathbb{Q}(\sqrt{3d})$ denote the unique totally real subfield of L. Suppose that $v\in\mathcal{O}_L^\times\setminus\mathcal{O}_F^\times=\zeta_3\mathcal{O}_F^\times$. Then $N_{L/\mathbb{Q}(\zeta_3)}(v)$ is a multiple of ζ_3 which contradicts $N_{L/\mathbb{Q}(\zeta_3)}(v)=1$. It follows that $v\in\mathcal{O}_F^\times$ and hence $u=v-1\in\mathcal{O}_F$. Since $x\in\mathcal{O}_K$ and u is a quotient of x and ζ_3-1, one readily verifies that this is a contradiction. We conclude that $n\in\{0,1,2\}$. It follows that

$$\pm 3^n+1\in\{0,2,4,-2,10,-8\}.$$

The only cubes in this set are 0 and -8. This concludes the proof. □

Corollary 4.31. (Nomden) Let $d\geqslant 2$ be a square-free integer such that $d\equiv 1 \bmod 3$ and let $K=\mathbb{Q}(\sqrt{-d})$. Let A, B and C be elements of $\mathcal{O}_K$ supported only on the primes above 3 in K. Suppose that $3\nmid h_K h_{K(\zeta_3)}$ and that K satisfies conjectures 1 and 2. Then there is a constant $V=V(d,A,B,C)$ such that the equation $Aa^p+Bb^p=Cc^3$ has no solutions in W_K when $p>V$. ■

Proof. Let $S = \{(3)\}$ consist of the only prime above 3 in K, from Proposition 4.30 it follows that the solutions to $\alpha + 1 = \gamma^3$ in $\mathcal{O}_S^\times \times \mathcal{O}_S$ are $(-1, 0)$ and $(-9, -2)$. The result then follows from Theorem 4.28. □

Due to a recent result by Caraiani and Newton, by adding an additional assumption on K in Corollary 4.31 we may dispose of one of the assumed conjectures. To state this condition, recall that the modular curve $X_0(15)$ is an elliptic curve over $\mathbb{Q}$ with rank 0 over $\mathbb{Q}$. The theorem is then as follows.

Theorem 4.32. [9, Theorem 1.1] Let F be an imaginary quadratic field such that the Mordell–Weil group $X_0(15)(F)$ is finite. Then Conjecture 2 holds for F. ■

Theorem 4.32 then gives the following, altered, form of Corollary 4.31.

Corollary 4.33. Let $d \geqslant 2$ be a square-free integer such that $d \equiv 1 \bmod 3$ and let $K = \mathbb{Q}(\sqrt{-d})$. Let A, B and C be elements of $\mathcal{O}_K$ supported only on the primes above 3 in K. Suppose that $3 \nmid h_K h_{K(\zeta_3)}$, that K satisfies Conjecture 1 and that $X_0(15)(K)$ is finite. Then there is a constant $V = V(d, A, B, C)$ such that the equation $Aa^p + Bb^p = Cc^3$ has no solutions in W_K when $p > V$. ■

References

[1] Abyankar, S.S. Resolution of singularities of arithmetical surfaces. *Arithmetical Algebraic Geometry* (1963), 111–152.

[2] Abyankar, S.S. Resolution of singularities of algebraic surfaces. *Algebraic Geometry* (1969), 1–11.

[3] Alvarado, A. Koutsianas, A. Malmskog, B. Rasmussen, C. Roe, D. Vincent, C. West, M. *A Robust Implementation for Solving the S-Unit Equation and Several Applications*. Springer, 2021. In: Balakrishnan, J.S. Elkies, N. Hassett, B. Poonen, B. Sutherland, A.V. Voight, B. Arithmetic Geometry, Number Theory, and Computation.

[4] Ash, A. Stevens, G. Cohomology of arithmetic groups and congruences between systems of hecke eigenvalues. *Journal für die reine und angewandte Mathematik, Volume 365* (1986), 192–220.

[5] Atiyah, M.F. Macdonald, I.G. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.

[6] Bennett, M.A. Vatsal, V. Yazdani, S. Ternary Diophantine equations of signature $(p, p, 3)$. *Compositio Mathematica, Volume 140 No. 6* (2004), 1399 – 1416.

[7] Breuil, C., Conrad, B., Diamond, F., and Taylor, R. On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises. *Journal of the American Mathematical Society, Volume 14* (2001), 843–939.

[8] Brumer, A. Krammer, K. The conductor of an abelian variety. *Compositio Mathematica, Volume 92* (1994), 227–248.

[9] Caraiani, A. Newton, J. On the modularity of elliptic curves over imaginary quadratic fields. *Preprint* `arXiv:2301.10509` (2023).

[10] Conrad, B. *The Flat Deformation Functor*. Springer, 1997. In: Cornell, G., Silverman, J.H., Stevens, G. (eds) Modular Forms and Fermat's Last Theorem.

[11] Conrad, B. Conrad, C. Helfgott, H. Root numbers and ranks in positive characteristic. *Advances in Mathematics, Volume 198* (2005), 684 – 631.

[12] Cornell, G. Silverman, J.H. *Arithmetic Geometry*. Springer, 1986.

[13] Darmon, M. Merel, L. Winding quotients and some variants of fermat's last theorem. *Journal für die reine und angewandte Mathematik, Volume 490* (1997), 81–100.

[14] De Weger, B.M.M. Algorithms for diophantine equations. *PhD Thesis* (1988).

[15] Deconinck, H. On the generalized fermat equation over totally real fields. *Acta Arithmetica, Volume 173, No. 3* (2016), 225–237.

[16] Edixhoven, B. The weight in serre's conjectures on modular forms. *Inventiones Mathematicae, Volume 109* (1992), 563–594.

[17] Etropolski, A. Local-global principles for certain images of galois representations. *Preprint* `arXiv:1502.01288` (2015).

[18] Freitas, N. Recipes to fermat-type equations of the form $x^r + y^r = cz^p$. *Mathematische Zeitschrift, Volume 279* (2015), 605 – 639.

[19] Freitas, N. Kraus, A. Siksek, S. Class field theory, diophantine analysis and the asymptotic fermat's last theorem. *Advances in Mathematics, Volume 363* (2019).

[20] Freitas, N. Siksek, S. The asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields. *Compositio Mathematica, Volume 151, No. 8* (2015), 1395–1415.

[21] Frey, G. Links between stable elliptic curves and certain diophantine equations. *Annales Universitatis Saraviensis, Volume 1* (1986), 1–40.

[22] Hartshorne, R. *Algebraic Geometry*. Springer, 1977.

[23] Isik, E. Kara, Y. Ozman, E. On ternary diophantine equations of signature $(p, p, 3)$ over number fields. *Canadian Journal of Mathematics, Volume 75, Issue 4* (2022), 1293 – 1313.

[24] Işik, E. Kara, Y. Ozman, E. On Ternary Diophantine Equations of Signature $(p, p, 2)$ over number fields. *Turkish Journal of Mathematics, Volume 44* (2020), 1197–1211.

[25] Kara, Y. Ozman, E. Asymptotic Generalized Fermat's Last Theorem over Number Fields. *International Journal of Number Theory, Volume 16, No. 05* (2020), 907–924.

[26] Katz, N.M. Galois properties of torsion points on abelian varieties. *Inventiones mathematicae, Volume 62* (1980), 481 – 502.

[27] Kodaira, K. On the structure of compact complex analytic surfaces I,II. *American Journal of Mathematics, Volume 86 and Volume 88* (1964,1966), 751–798, 682–721.

[28] Kraus, A. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Math, Volume 69 No. 4* (1990), 353 – 385.

[29] Kumar, N. Sahoo, S. Asymptotic solutions of generalized fermat-type equations of signature $(p, p, 3)$ over totally real number fields. *Preprint* (2024).

[30] Kumar, N. Sahoo, S. On the solutions of $x^p + y^p = 2^r z^p, x^p + y^p = z^2$ over totally real number fields. *Acta Arithmetica, Volume 212, No. 1* (2024), 31 – 47.

[31] Lang, S. *Fundamentals of Diophantine Geometry.* Springer, 1962.

[32] Lichtenbaum, S. Curves over discrete valuation rings. *American Journal of Mathematics, Volume 90* (1968), 380–403.

[33] Lipman, J. Desingularization of two-dimensional schemes. *Annals of Mathematics, Volume 107.* (1970), 151–207.

[34] Lipman, J. Rational singularities with applications to algebraic surfaces and unique factorization. *Publications mathématiques de l'IHÉS, Volume 38.* (1970), 195–279.

[35] Liu, Q. *Algebraic Geometry and Arithmetic Curves.* Oxford University Press, 2002.

[36] Lockhart, P. Rosen, M. and Silverman, J. An upper bound for the conductor of an abelian variety. *Journal of Algebraic Geometry, Volume 2* (1993), 569–601.

[37] Mocanu, D. Asymptotic fermat for signatures $(p, p, 2)$ and $(p, p, 3)$ over totally real fields. *Mathematika, Volume 68, No. 4* (2022), 1233 – 1257.

[38] Nomden, S. *S-Unit-Equation-Solver.* GitHub, 2025. https://github.com/stefnomden/S-Unit-Equation-Solver.

[39] Néron, A. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Publications Mathématiques de l'IHÉS, Volume 21* (1964), 5–128.

[40] Ogg, A.P. Elliptic curves and wild ramification. *American Journal of Mathematics, Volume 89* (1967), 1–21.

[41] Raynaud, M. Schémas en groupes de type $(p, ..., p)$. *Bulletin de la Société Mathématique de France, Tome 102* (1974), 241 – 280.

[42] Ribet, K.A. From the Taniyama-Shimura conjecture to Fermat's last theorem. *Annales de la faculté des sciences de Toulouse, Tome 11* (1990), 116–139.

[43] Ribet, K.A. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Inventiones Mathematicae, Volume 100* (1990), 431 – 476.

[44] Serre, J-P. *Abelian ℓ-Adic Representations and Elliptic Curves.* W.A. Benjamin, Inc., 1968.

[45] Serre, J-P. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inveventiones math, Volume 15* (1972), 259 – 331.

[46] Serre, J-P. Sur les Représentations Modularies de Degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). *Duke Mathematical Journal, Volume 54* (1987), 179 – 230.

[47] Serre, J-P. Tate, J. Good reduction of abelian varieties. *The Annals of Mathematics, Volume 88* (1968), 492–517.

[48] Shafarevich, I.R. Lectures on minimal models, 1966.

[49] Siegel, C. L. *Über einige Anwendungen diophantischer Approximationen.* Verlag der Akademie der Wissenschaften, 1930.

[50] Siksek, S. The modular approach to diophantine equations. accessed on the 20th June 2025 at https://www.birs.ca/workshops/2012/12ss131/files/samirnotes.pdf.

[51] Silverman, J. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer, 1994.

[52] Silverman J.H. *The Arithmetic of Elliptic Curves.* Springer, 1986.

[53] Smart, N.P. The algorithmic resolution of diophantine equations. *London Mathematical Society Student Texts, Volume 41* (1998).

[54] Stacks Project Authors, T. *Stacks Project.* https://stacks.math.columbia.edu, 2018.

[55] Stevenhagen, P. Number rings. Version of November 14, 2020, accessed at https://websites.math.leidenuniv.nl/algebra/ant.pdf.

[56] Suzuki, M. *Group Theory I.* Springer, 1980.

[57] Tate, J. *Algorithm for determining the type of a singular fiber in an elliptic pencil.* Springer, 1975. In: Birch, B.J., Kuyk, W. (eds) Modular Functions of One Variable IV.

[58] Tate, J. *Finite Flat Group Schemes.* Springer, 1997. In: Cornell, G., Silverman, J.H., Stevens, G. (eds) Modular Forms and Fermat's Last Theorem.

[59] Tate, J. *A review of non-Archimedean elliptic functions.* International Press of Cambridge, 1995. In: Elliptic curves, modular forms, & Fermat's last theorem.

[60] The Sage Developers. *SageMath, the Sage Mathematics Software System*, 2025. https://www.sagemath.org.

[61] Wiese, G. Galois representations. Version of 13th February 2012 accessed at math.uni.lu/wiese/notes.

[62] Wiles, A. J. Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics, Volume 141* (1995), 443–551.

[63] Özman, E. Siksek, S. S-unit Equations and the Asymptotic Fermat Conjecture over Number Fields.

[64] Şengün, M. H. Siksek, S. On the Asymptotic Fermat's Last Theorem over Number Fields. *Commentarii Mathematici Helvetici, Volume 93, No. 2* (2018), 359–375.

[65] Ţurcaş, G.C. On fermat's equation over some quadratic imaginary number fields. *Research in Number Theory, Volume 4, No. 2* (2018).

[66] Ţurcaş, G.C. On serre's modularity conjecture and fermat's equation over quadratic imaginary field of class number one. *Journal of Number Theory, Volume 209* (2020), 516–530.