VRIJE UNIVERSITEIT

Automating the modular method for $\mathbb{Q}$-curves to solve Diophantine equations

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad Doctor of Philosophy aan
de Vrije Universiteit Amsterdam,
op gezag van de rector magnificus
prof.dr. C.M. van Praag,
in het openbaar te verdedigen
ten overstaan van de promotiecommissie
van de Faculteit der Bètawetenschappen
op donderdag 27 januari 2022 om 13.45 uur
in een bijeenkomst van de universiteit,
De Boelelaan 1105

door

Joey Matthias van Langen

geboren te Haarlemmermeer

promotor:	prof.dr. R.M.H. de Jeu
copromotor:	dr. S.R. Dahmen
promotiecommissie:	prof.dr. R.C.A.M. van der Vorst prof.dr. G.L.M. Cornelissen prof.dr. M.A. Bennett dr. P.J. Bruin dr. V. Patel

Deze publicatie maakt deel uit van het project "New Diophantine directions" (met projectnummer 639.032.613) van het onderzoeksprogramma Vidi dat (mede) is gefinancierd door de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO).

Table of contents

Introduction

Diophantine equations – polynomial equations for which we seek integer solutions – have interested mathematicians for millennia. Certain solutions – like the formulas found for Pythagorean triples in Euclid's "Elements" – have been known for a similar amount of time, but the scribbling of Fermat in a copy of Diophantus' "Arithmetica" posed a problem that would take centuries to solve. Fermat claimed that the equation $x^n + y^n = z^n$ had no integer solutions x, y, z, n with $xyz \neq 0$ and $n > 2$, but that the margin had too little room for his proof. The search for the proof of – what was later known as – Fermat's Last Theorem incited many new techniques to solve Diophantine equations. The final technique that finished the proof has since grown into the modular method, a technique that can be applied to various (exponential) Diophantine equations to prove the non-existence of solutions, possibly outside some particular solutions that do exist.

A basic form of the modular method boils down to the following. To a putative solution of a Diophantine equation one associates an elliptic curve $E/\mathbb{Q}$ known as a Frey curve. Using the modularity theorem one then shows that there is a newform associated with this Frey curve, in the sense that their Galois representations are isomorphic. By constructing the Frey curve such that some additional constraints are satisfied with respect to a prime exponent l appearing in the Diophantine equation, level lowering results can be used to ensure the mod l Galois representation of E is also isomorphic to a mod $\lambda \mid l$ Galois representation of a newform f, whose level N no longer depends on the putative solution but only on the Diophantine equation. By computing the newforms of level N one then verifies that none can have such an isomorphic mod $\lambda \mid l$ Galois representation, thereby proving the non-existence of the putative solution.

This simple form of the modular method can and has been extended in various ways. Most commonly we replace the Frey curve $E/\mathbb{Q}$ with an elliptic curve E/K with K a number field for which modularity is (conjecturally or partially) known. In this dissertation we will look at Frey curves which are also $\mathbb{Q}$-curves, i.e. elliptic curves that are isogenous to all their Galois conjugates. Modularity for non-CM $\mathbb{Q}$-curves was proven by Ribet in [Rib04] based on the Serre conjectures now proven by Khare and Wintenberger [KW09a, KW09b]. Using Frey $\mathbb{Q}$-curves in the modular method has already proven useful to solve various Diophantine equations, see e.g. [DU09], [Ell04], [Che10], [BC12], and [BCDY14].

The modular method involves quite some computational work. Besides the spaces of newforms that should be computed, the level of these newforms depends on the conductor of the Frey curve. For Frey $\mathbb{Q}$-curves there is also some $\mathbb{Q}$-curve data that should be computed to determine the levels of the associated newforms. Furthermore the latter can only be done for a certain twist of a Frey $\mathbb{Q}$-curve which should be computed as well. Finally there is also the comparison of Galois representations with which the final contradiction should be reached, which in this dissertation relies on the computation of traces of Frobenius. In the first three chapters of this dissertation we discuss how these steps can be automated to easily apply the modular method to a new Diophantine problem.

Chapter 1 discusses how the conductor of a Frey curve can be computed automatically. This relies on a special implementation of Tate's algorithm which works for elliptic curves in which the coefficients depend on a putative solution. Besides explaining how this implementation works, we also compare it to other semi-automated methods in Section 1.7.

Chapter 2 introduces the basic theory for $\mathbb{Q}$-curves that is needed for the modular method. Most of this theory is standard and can be found in [Que00, Rib04]. In this dissertation we however focus on automation, describing how the level and character of a corresponding newform can be computed, as well as how to compute a corresponding Galois representation. We also introduce some new results: Proposition 2.5.5, which helps compute the twist of the $\mathbb{Q}$-curve for which newform levels can be computed, Theorem 2.10.1 and Theorem 2.10.7, which allow the computation of traces of Frobenius for the corresponding Galois representations, and Theorem 2.11.1, which expands Proposition 3.2 in [Ell04].

Chapter 3 presents an outline of the modular method for Frey $\mathbb{Q}$-curves and shows how Chapter 1 and Chapter 2 can be used to automate the first part thereof. It then fills in the last part of the automation by presenting an automated way of eliminating newforms.

Throughout the first three chapters we also discuss the framework [vL21a], which is an implementation in SageMath [Sag20] of all the automation described in these chapters. Besides explanation of the functionality in the framework [vL21a] throughout the text, there are also explicit code examples contained in the examples in these chapters.

The framework [vL21a] also comes with a variety of examples which contain written text interjected with code fragments. The files containing these examples are referenced in this dissertation by a boxed text and can be found in the `examples` folder. Amongst them are worked out examples from the literature, which are all listed in Table 3.1. Furthermore there are files that verify all the computations in the examples in this dissertation, which are mentioned at the start of the corresponding examples.

In Chapter 4 and Chapter 5 we apply the framework [vL21a] to two distinct Diophantine problems. Chapter 4 is based on the article [vL21b] and solves the exponential Diophantine equation $(x - y)^4 + x^4 + (x + y)^4 = z^n$ in coprime integers x, y with $z, n \in \mathbb{Z}$ and $n > 1$. Chapter 5 is joint work with Sander Dahmen of which a modified version will be submitted as an article. In that chapter we prove that certain elliptic divisibility sequences do not contain l-th powers for l a sufficiently large prime number.

After this introduction there is a section containing notation and conventions that are used throughout the dissertation. The dissertation ends with a brief discussion in Chapter 6. Here we reflect on the strengths and weaknesses of the framework [vL21a], and discuss possible future improvements.

Notation & Conventions

Throughout the thesis we will use the following notation and conventions.

- For a field K we will denote by $\overline{K}$ an algebraic closure, which we will assume to be fixed unless otherwise stated. Furthermore we assume for finite field extensions L/K that $\overline{L} = \overline{K}$ by making appropriate identifications if necessary.

- We will denote the Galois group of a Galois field extension L/K by G_K^L. If K is a perfect field we use G_K to denote the absolute Galois group $G_K^{\overline{K}}$ of K.

- We denote the action of a Galois element $\sigma \in G_K^L$ by a prescript on the top left. For example we write ${}^{\sigma}x$ for σ acting on an element $x \in L$ and ${}^{\sigma}E$ for σ acting on an elliptic curve E defined over L.

- Within an algebraically closed field K we will denote a fixed primitive n-th root of unity by ζ_n. Here we assume n is not divisible by the characteristic of K, and choices are made such that $\zeta_n = \zeta_m^k$ if $n = mk$ with $k, m, n \in \mathbb{Z}$ strictly positive.

- For a number field or p-adic field K we will denote the ring of integers by $\mathcal{O}_K$. As usual p-adic field means a non-archimedean local field of characteristic 0, i.e. a finite extension of $\mathbb{Q}_p$ for some prime number p.

- For a number field or p-adic field K we will use the term *prime* to indicate a maximal ideal of $\mathcal{O}_K$. Therefore primes in this dissertation are always finite unless explicitly stated otherwise. We denote primes by $\mathfrak{m}, \mathfrak{p}, \mathfrak{q}, \ldots$.

- For a prime $\mathfrak{p}$ of a number field or p-adic field K we denote the corresponding normalised valuation by $\operatorname{ord}_{\mathfrak{p}}$. The corresponding completion (when K is a number field) is denoted by $K_{\mathfrak{p}}$.

- We denote the residue field of a prime $\mathfrak{p}$ by $\mathbb{F}_{\mathfrak{p}}$. Similarly we denote by $\mathbb{F}_p$ the field of order p when p is a prime number.

- We assume elliptic curves E are always given by a Weierstrass equation
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$
We use the same notation as in [Sil09, III.1] for invariants associated to such a Weierstrass equation, and talk about such invariants as invariants of E.

- For a finite field extension L/K and an abelian variety A/L we denote by $\operatorname{Res}_K^L A$ the restriction of scalars of A over K. The restriction of scalars $\operatorname{Res}_K^L A$ – also known as the Weil restriction – is defined as a variety B/K together with an L-morphism $\pi : B_L \to A$ such that for any variety T/K together with an L-morphism $T_L \to A$ we can complete the commutative diagram
$$\begin{tikzcd}
T \arrow[r, dashed, "\exists!"] & B \\
T_L \arrow[u] \arrow[r, dashed, "\exists!"] \arrow[rr, bend right] & B_L \arrow[u] \arrow[r, "\pi"] & A.
\end{tikzcd}$$
Here T_L and B_L are the base changes of T and B over L, the top horizontal map is a K-morphism, and the bottom horizontal maps are L-morphisms. We will also use that if L/K is Galois then $B_L = \prod_{\sigma \in G_K^L} {}^\sigma A$. Note that the universal property makes B with π unique up to unique isomorphism. For existence see e.g. Section 1.3 in [Wei82].

- We often implicitly change the field over which an elliptic curve E is defined. For a field extension L/K we might talk about an elliptic curve E defined over K as if it were defined over L without explicitly stating we base change E over L. Similarly if E were originally defined over L we may talk about E as if defined over K if there is an elliptic curve E'/K that base changed to L is the same as E. We do the same for (abelian) varieties and morphisms.

- For classical modular forms we shall denote by $\mathcal{S}_k(\Gamma)$ the space of cusp forms of weight k with respect to the modular group Γ. The subspace of $\mathcal{S}_k(\Gamma_1(N))$ that is spanned by the eigenforms with character χ is denoted by $\mathcal{S}_k(N, \chi)$.

- For a newform $f \in \mathcal{S}_2(\Gamma_1(N))$ we denote by A_f the abelian variety associated to f as defined in Definition 6.6.3 of [DS05]. This is a quotient of the jacobian $J_1(N)$ of the modular curve $X_1(N)$. We denote by K_f the number field generated by the Fourier coefficients of f ([DS05, Definition 6.5.3]). Furthermore we will use $\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\lambda})$ and $\overline{\rho_{f,\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ to denote the λ-adic and mod λ Galois representations associated to f for any prime λ of K_f, as defined in Section 9.5 and Section 9.6 of [DS05]. Section 2.8 talks a bit more about the definition of these representations.

- In code examples throughout this dissertation we will use \ to denote a line break that was not part of the original output.

Chapter 1

Computing Conductors of Frey Curves

One important part of the modular method is the computation of the conductor of a given Frey elliptic curve as it determines the level of associated newforms. For an explicit elliptic curve this is a straightforward computation on the coefficients that is often implemented using Tate's algorithm. For Frey curves this may not be as straightforward a calculation as the coefficients depend on a putative solution of a Diophantine equation.

Manually one can still try to perform Tate's algorithm on a Frey curve. In each step of the algorithm one can make case distinctions depending on the corresponding solution if necessary. This is a tedious process that is very error prone when done by hand. Therefore the author has worked on an automated approach to Tate's algorithm, that works for elliptic curves of which the coefficients may be polynomials in some parameters.

In this chapter we will discuss how this automated Tate's algorithm works. First Tate's algorithm is outlined in Section 1.1. Section 1.2 then dissects the algorithm into smaller parts that should be automated to perform Tate's algorithm. An efficient method for one of the most prominent parts – computing roots of a polynomial modulo a prime power – is provided in Section 1.3. Section 1.4 then discusses an alternative way of storing the data for the case distinctions made in Tate's algorithm. It is followed by Section 1.5 which proves that finitely many steps in the subalgorithm in Step 7 of Tate's algorithm suffice, if one is only interested in the conductor exponent, Kodaira symbol, or number of geometrically irreducible components.

Section 1.6 talks about the implementation by the author [vL21a] of the theory in the previous sections. Most subsections here give an outline of the various classes and methods in this implementation. Section 1.6.4 introduces classes in the framework [vL21a] that can be used to enforce restrictions that might arise from a Diophantine equation. Everything culminates in Section 1.6.6

where the class representing a Frey curve is introduced. This final subsection also includes an explicit example with SageMath syntax.

Finally Section 1.7 compares the automated approach discussed here to other semi-automated approaches. These other approaches include 'looking up' the conductor using the table by Papadopoulos and the more algorithmic approach introduced by Chen.

Section 1.1

A quick overview of Tate's algorithm

Let K be a p-adic field with prime $\mathfrak{p}$. We will write $v = \operatorname{ord}_{\mathfrak{p}} : K^* \to \mathbb{Z}$ and let π be a uniformizer, i.e. an element such that $\mathfrak{p} = \pi\mathcal{O}_K$. Let

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{1.1}$$

be an elliptic curve over K with integral coefficients, i.e. $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_K$.

For $u \in K^*$ and $r, s, t \in K$ we note that substituting both $X = u^2X' + r$ and $Y = u^3Y' + u^2sX' + t$ in Equation (1.1) gives a Weierstrass equation

$$E' : Y'^2 + a_1'X'Y' + a_3'Y' = X'^3 + a_2'X'^2 + a_4'X' + a_6',$$

of an isomorphic elliptic curve. We call such a change in Weierstrass model a (u, r, s, t)-transformation or simply a u-scaling if $r = s = t = 0$. The way the corresponding invariants change by such a transformation is written out fully in [Sil09, III.1, Table 3.1].

Using this notation we can now describe Tate's algorithm for the curve E. Whenever the algorithm terminates it will produce the value of the following quantities it has then computed.

- E_{min}: A minimal model of E, i.e. a (u, r, s, t)-transformation of E with the highest possible $v(u)$, such that the coefficients of E_{min} are still in $\mathcal{O}_K$.
- *Type*: The Kodaira symbol that describes the reduction type of the special fiber of E_{min} over $\overline{\mathbb{F}_{\mathfrak{p}}}$.
- m: The number of components of the special fiber of E_{min} over $\overline{\mathbb{F}_{\mathfrak{p}}}$, counted with multiplicity.
- f: The exponent of the conductor of E.

- c: The number of components of the special fiber of $E_{\min}$ over $\overline{\mathbb{F}_{\mathfrak{p}}}$ that have multiplicity 1 and are defined over $\mathbb{F}_{\mathfrak{p}}$.

Below is the description of Tate's algorithm in pseudocode. Note that it is a function with input E, but also requires $\mathcal{O}_K$, v and a choice of π. Mathematically these can be inferred from E, but for an actual implementation they have to be specified explicitly. For the framework [vL21a] this happens through a single object specified in Section 1.6.1. On the left of the algorithm are several labels that can be used as jumping points. Most of these correspond to steps of the algorithm as given in [Sil94, IV.9]. These steps are the same, except that we reformulated the stopping conditions in some cases such that they are easier to work with later on.

```
          Function TatesAlgorithm($E$; $\mathcal{O}_K$, $v$, $\pi$)

Step 1:   If $v(\Delta) < 1$
            Return $E_{\min} = E$, Type $\mathrm{I}_0$, $m = 1$, $f = 0$, $c = 0$
                       (good reduction)

Step 2:   With a solution $x_0, y_0 \in \mathcal{O}_K$ to

            $\begin{cases} y_0^2 + a_1 x_0 y_0 + a_3 y_0 \equiv x_0^3 + a_2 x_0^2 + a_4 x_0 + a_6 \\ a_1 y_0 \equiv 3\,x_0^2 + 2\,a_2 x_0 + a_4 \\ 2\,y_0 + a_1 x_0 + a_3 \equiv 0 \end{cases} \pmod{\mathfrak{p}}$

            Perform a $(1, x_0, 0, y_0)$-transformation on $E$
          If $v(b_2) < 1$
            If $T^2 + a_1 T - a_2 \in \mathcal{O}_K[T]$ has roots in $\mathbb{F}_{\mathfrak{p}}$
              Return $E_{\min} = E$, Type $\mathrm{I}_{v(\Delta)}$, $m = v(\Delta)$, $f = 1$, $c = v(\Delta)$
                       (split multiplicative reduction)
            Else
              If $v(\Delta)$ is odd
                Return $E_{\min} = E$, Type $\mathrm{I}_{v(\Delta)}$, $m = v(\Delta)$, $f = 1$, $c = 1$
                       (non-split multiplicative reduction)
              Else
                Return $E_{\min} = E$, Type $\mathrm{I}_{v(\Delta)}$, $m = v(\Delta)$, $f = 1$, $c = 2$
                       (non-split multiplicative reduction)

Step 3:   If $v(a_6) < 2$
            Return $E_{\min} = E$, Type II, $m = 1$, $f = v(\Delta)$, $c = 1$
```

```
Step 4:            If $v(b_8) < 3$
                     Return $E_{\min} = E$, Type III, $m = 2$, $f = v(\Delta) - 1$, $c = 2$
Step 5:            If $v(b_6) < 3$
                     If $T^2 + \frac{a_3}{\pi} T - \frac{a_6}{\pi^2}$ has roots in $\mathbb{F}_\mathfrak{p}$
                       Return $E_{\min} = E$, Type IV, $m = 3$, $f = v(\Delta) - 2$, $c = 3$
                     Else
                       Return $E_{\min} = E$, Type IV, $m = 3$, $f = v(\Delta) - 2$, $c = 1$
Step 6:            With a solution $\alpha, \beta \in \mathcal{O}_K$ of
                       $$\begin{cases} 2\alpha & \equiv -a_1 \\ \alpha^2 & \equiv -a_2 \\ 2\beta & \equiv -\frac{a_3}{\pi} \\ \beta^2 & \equiv -\frac{a_6}{\pi^2} \end{cases} \pmod{\mathfrak{p}}$$
                     Perform a $(1, 0, \alpha, \beta\pi)$-transformation on $E$
                   If $v(-4\, a_2^3 a_6 + a_2^2 a_4^2 - 4\, a_4^3 - 27\, a_6^2 + 18\, a_2 a_4 a_6) < 7$
                     Return $E_{\min} = E$, Type $\mathrm{I}_0^*$, $m = 5$, $f = v(\Delta) - 4$,
                         $c = 1 + \#\left\{T \in \mathbb{F}_\mathfrak{p} : T^3 + \frac{a_2}{\pi} T^2 + \frac{a_4}{\pi^2} T + \frac{a_6}{\pi^3} = 0\right\}$
Step 7:            If $v(3\, a_4 - a_2^2) < 3$
Subalgorithm:        With a solution $x_1 \in \mathcal{O}_K$ of
                       $$\begin{cases} x_1^3 + \frac{a_2}{\pi} x_1^2 + \frac{a_4}{\pi^2} x_1 + \frac{a_6}{\pi^3} & \equiv 0 \\ 3\, x_1^2 + 2\, \frac{a_2}{\pi} x_1 + \frac{a_4}{\pi^2} & \equiv 0 \end{cases} \pmod{\mathfrak{p}}$$
                     Perform a $(1, x_1\pi, 0, 0)$-transformation on $E$
                     Set $n := 1$
                     Set $k := 2$
Substep $n$ (odd):   If $v(b_6) < n + 4$
                       If $T^2 + \frac{a_3}{\pi^k} T - \frac{a_6}{\pi^{2k}}$ has roots in $\mathbb{F}_\mathfrak{p}$
                         Return $E_{\min} = E$, Type $\mathrm{I}_n^*$, $m = n + 5$, $f = v(\Delta) - n - 4$, $c = 4$
                       Else
                         Return $E_{\min} = E$, Type $\mathrm{I}_n^*$, $m = n + 5$, $f = v(\Delta) - n - 4$, $c = 2$
                     With a solution $y_k \in \mathcal{O}_K$ of
                       $$y_k^2 + \frac{a_3}{\pi^k} y_k - \frac{a_6}{\pi^{2k}} \equiv 0 \pmod{\mathfrak{p}}$$
                       Perform a $(1, 0, 0, y_k\pi^k)$-transformation on $E$
                     Set $n := n + 1$
```

```
Substep $n$ (even):   If $v(a_4^2 - 4\,a_2a_6) < n+5$
                        If $\frac{a_2}{\pi}T^2 + \frac{a_4}{\pi^{k+1}}T + \frac{a_6}{\pi^{2k+1}}$ has roots in $\mathbb{F}_\mathfrak{p}$
                          Return $E_{\text{min}} = E$, Type $\mathrm{I}_n^*$, $m = n+5$, $f = v(\Delta) - n - 4$, $c = 4$
                        Else
                          Return $E_{\text{min}} = E$, Type $\mathrm{I}_n^*$, $m = n+5$, $f = v(\Delta) - n - 4$, $c = 2$
                      With a solution $x_k \in \mathcal{O}_K$ of

                        $$\frac{a_2}{\pi}x_k^2 + \frac{a_4}{\pi^{k+1}}x_k + \frac{a_6}{\pi^{2k+1}} \equiv 0 \pmod{\mathfrak{p}}$$

                        Perform a $(1, x_k\pi^k, 0, 0)$-transformation on $E$
                      Set $n := n+1$
                      Set $k := k+1$
                      Jump to Substep $n$ (odd)

Step 8:             With a solution $x_1 \in \mathcal{O}_K$ of

                      $$x_1^3 + \frac{a_2}{\pi}x_1^2 + \frac{a_4}{\pi^2}x_1 + \frac{a_6}{\pi^3} \equiv 0 \pmod{\mathfrak{p}}$$

                      Perform a $(1, x_1\pi, 0, 0)$-transformation on $E$
                    If $v(b_6) < 5$
                      If $T^2 + \frac{a_3}{\pi^2}T - \frac{a_6}{\pi^4}$ has roots in $\mathbb{F}_\mathfrak{p}$
                        Return $E_{\text{min}} = E$, Type $\mathrm{IV}^*$, $m = 7$, $f = v(\Delta) - 6$, $c = 3$
                      Else
                        Return $E_{\text{min}} = E$, Type $\mathrm{IV}^*$, $m = 7$, $f = v(\Delta) - 6$, $c = 1$

Step 9:             With a solution $y_1 \in \mathcal{O}_K$ of

                      $$y_1^2 + \frac{a_3}{\pi^2}y_1 - \frac{a_6}{\pi^4} \equiv 0 \pmod{\mathfrak{p}}$$

                      Perform a $(1, 0, 0, y_1\pi^2)$-transformation on $E$
                    If $v(a_4) < 4$
                      Return $E_{\text{min}} = E$, Type $\mathrm{III}^*$, $m = 8$, $f = v(\Delta) - 7$, $c = 2$

Step 10:            If $v(a_6) < 6$
                      Return $E_{\text{min}} = E$, Type $\mathrm{II}^*$, $m = 9$, $f = v(\Delta) - 8$, $c = 1$

Step 11:            Perform a $(\pi, 0, 0, 0)$-transformation on $E$
                    Jump to Step 1
```

Section 1.2

Tate's algorithm for curves with parameters

Looking closely at the algorithm as presented above, it is clear that this algorithm can be successfully used if one is able to perform four types of checks.

1. Determine whether a polynomial in the coefficients of E has valuation smaller than a given bound.
2. Find solutions in $\mathbb{F}_\mathfrak{p}$ of polynomial equations of which the coefficients are polynomials in the coefficients of E.
3. Determine the number of roots of a polynomial over $\mathbb{F}_\mathfrak{p}$ where the coefficients of the polynomial are polynomials in the coefficients of E.
4. Determine the exact valuation of a polynomial in the coefficients of E.

If the coefficients of E are polynomials in some parameters, one can still try to determine the values of the parameters for which the different outcomes of these checks arise. In fact for each of the first three checks the outcome only depends on the value of the parameters modulo some sufficiently high power of the prime ideal $\mathfrak{p}$. The same is not true for a check of type 4, but note that such a check is only needed for the valuation of the discriminant and some of the return values. In most use cases – where one is not necessarily interested in all of the return values – this valuation is bounded, meaning we can find a sufficiently high power of $\mathfrak{p}$ for this check as well. In case $\mathbb{F}_\mathfrak{p}$ is finite, this makes every check a finite computation.

Example 1.2.1. `Conductor.rst` We will illustrate these checks by performing the first four steps of Tate's algorithm on the curve

$$E : Y^2 = X(X - A)(X + B)$$

with undetermined parameters $A, B \in \mathbb{Z}$ such that $AB(A + B) \neq 0$. We interpret this as an elliptic curve over $\mathbb{Q}_2$.

Step 1: Since $\Delta = 2^4\, A^2B^2\,(A + B)^2$ it is clear that $v(\Delta) \geq 1$.

Step 2: The equations in $x_0, y_0 \in \mathbb{Z}_2$ become

$$\begin{cases} y_0^2 & \equiv x_0^3 + (B - A)x_0^2 - ABx_0 \\ 0 & \equiv x_0^2 - AB \\ 0 & \equiv 0 \end{cases} \pmod 2$$

and by substituting every value for A and B modulo 2 we find the solution

$$(x_0, y_0) = \begin{cases} (0,0) & \text{if } AB \equiv 0 \pmod 2 \\ (1,0) & \text{if } AB \equiv 1 \pmod 2. \end{cases}$$

This check of type 2 tells us that from now on we have two cases to consider with respective models

$$E : \begin{cases} Y^2 = X^3 + (B-A)X^2 - ABX & \text{if } AB \equiv 0 \pmod 2 \\ Y^2 = X^3 + (B-A+3)X^2 & \\ \qquad + (2\,B - 2\,A + 3 - AB)X & \\ \qquad\quad + 1 + B - A - AB & \text{if } AB \equiv 1 \pmod 2. \end{cases}$$

Now we find that

$$b_2 = \begin{cases} 4\,(B-A) & \text{if } AB \equiv 0 \pmod 2 \\ 4\,(B-A+3) & \text{if } AB \equiv 1 \pmod 2, \end{cases}$$

so clearly $v(b_2) \geq 1$ in both cases.

Step 3: We have that

$$a_6 = \begin{cases} 0 & \text{if } AB \equiv 0 \pmod 2 \\ (1-A)(1+B) & \text{if } AB \equiv 1 \pmod 2. \end{cases}$$

We can see that in both cases we have $v(a_6) \geq 2$.

Step 4: We have that

$$b_8 = \begin{cases} -A^2B^2 & \text{if } AB \equiv 0 \pmod 2 \\ 3 - 4\,A + 4\,B - 6\,AB - A^2B^2 & \text{if } AB \equiv 1 \pmod 2. \end{cases}$$

By substituting the possible values of A and B modulo 8 we can determine for which cases we have $v(b_8) < 3$. By doing this check of type 1 we determine that this is the case if and only if $v(AB(A+B)) = 1$. To determine the conductor exponent in that case we also need to perform a check of type 4 to find the valuation of $\Delta = 2^4A^2B^2(A+B)^2$. Using what we determined before, this is easily computed to be 6 giving us the local data for Type III: $m = 2$, $f = 5$, $c = 2$, and

$$E_{min} : \begin{cases} Y^2 = X^3 + (B-A)X^2 - ABX & \text{if } AB \equiv 0 \pmod 2 \\ Y^2 = X^3 + (B-A+3)X^2 & \\ \qquad + (2\,B - 2\,A + 3 - AB)X & \\ \qquad\quad + 1 + B - A - AB & \text{if } AB \equiv 1 \pmod 2. \end{cases}$$

Note that there are a few different ways in which Tate's algorithm might not terminate for a curve depending on parameters. For example the algorithm does not terminate when a_1, a_2, a_3, a_4, a_6 are taken as parameters, as for any values for which Tate's algorithm ends in the n-th iteration one has a set of values that ends in the $n+1$-th iteration by scaling these coefficients. For most Frey curves coprimality conditions on the solution ensure that the valuations of a_1, a_2, a_3, a_4, a_6 can not all be unbounded, implying that the algorithm can not infinitely loop through Step 11. An infinite loop in the Step 7 Subalgorithm is still possible, but can be prevented if one is only interested in the conductor as will be discussed in Section 1.5. Finally we might have a case in which we terminate but the valuation of the discriminant remains unbounded. As mentioned before, this seems not to happen in practice, as either coprimality conditions on the parameters force $v(\Delta)$ to be bounded, or one is simply not interested in a return value that requires $v(\Delta)$ to be computed.

From now on suppose $a_1, a_2, a_3, a_4, a_6 \in L[x_1, \ldots, x_n]$ with L be a number field. We will assume that $x_1, \ldots, x_n$ take on explicit, yet unspecified values in $\mathcal{O}_K$ for some subfield $K \subseteq L$, such that the Weierstrass equation with coefficients $a_1, \ldots, a_n$ defines an elliptic curve E over L. Therefore for a finite prime $\mathfrak{q}$ of L we can also consider E as an elliptic curve over $L_{\mathfrak{q}}$. Since we leave $x_1, \ldots, x_n$ unspecified we can use the strategy above to compute the possible local data of E at $\mathfrak{q}$ using Tate's algorithm. This will involve making case distinctions based on the value of $x_1, \ldots, x_n$ modulo some power of $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$. Note that all the computations in this case can just be done in L as none of the steps in the algorithm actually require additional elements from $L_{\mathfrak{q}}$.

We will not discuss the algorithm in detail as it is just performing Tate's algorithm as described before, distinguishing cases for each of the checks performed. We will however discuss how to perform a check of type 1 in an efficient way using Hensel lifting in the next section.

Section 1.3

Roots modulo a prime power

In this section we will describe how to perform a check of type 1 on the elliptic curve E in an efficient way. In such a check we have a bound r and a polynomial $f \in L[x_1, \ldots, x_n]$ in the parameters. Our goal is to determine for which values $x_1, \ldots, x_n \in \mathcal{O}_K$ we have $\operatorname{ord}_{\mathfrak{q}} f(x_1, \ldots, x_n) \geq r$. By rescaling f such that the coefficients are $\mathfrak{q}$-integral and adjusting r accordingly, this is equivalent to finding all roots of $f(x_1, \ldots, x_n)$ modulo $\mathfrak{q}^r$. We may assume here that $r \geq 0$

as after rescaling the solutions for $r < 0$ are the same as for $r = 0$.

One could easily try to solve this problem by substituting every possible value of $x_1, \ldots, x_n$ modulo $\mathfrak{q}^r \cap \mathcal{O}_K$. When $\mathfrak{q}^r \cap \mathcal{O}_K \subsetneq \mathfrak{p}$ we can compute which $x_1, \ldots, x_n$ are roots faster by using a process called Hensel Lifting. Since this is quite subtle for our case where we might have $K \neq L$ we discuss this in detail here.

Fix the localizations $R = \{a \in K : \operatorname{ord}_{\mathfrak{p}} a \geq 0\}$ and $S = \{b \in L : \operatorname{ord}_{\mathfrak{q}} b \geq 0\}$ of $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively. Since $\mathcal{O}_K$ and $\mathcal{O}_L$ are Dedekind domains and not fields, we know that R and S are discrete valuation rings. This implies that $\mathfrak{p}R = \pi R$ and $\mathfrak{q}S = \rho S$ for some $\pi \in \mathfrak{p}$ and $\rho \in \mathfrak{q}$. A choice of these elements will be our fixed uniformizers from now on, which they also are in $K_{\mathfrak{p}}$ and $L_{\mathfrak{q}}$ respectively.

We can now reformulate the problem that needs to be solved to

Problem 1.3.1. For a polynomial $f \in S[x_1, \ldots, x_n]$ and fixed $r \in \mathbb{Z}_{\geq 0}$ find all $a_1, \ldots, a_n \in R$ such that

$$f(a_1, \ldots, a_n) \equiv 0 \pmod{\rho^r}. \tag{1.2}$$

Note that we have here slightly deviated from the setup we described before. Originally we would consider $a_1, \ldots, a_n$ to be elements of $\mathcal{O}_K$. We shall later see that the distinctions are made modulo powers of $\mathfrak{p}$, hence we may as well work in the bigger ring R.

Choose a set $A \subset R$ such that the canonical map $R \to R/\pi R \cong \mathbb{F}_{\mathfrak{p}}$ restricted to A is surjective. Since R embeds into $\mathcal{O}_{K_{\mathfrak{p}}}$ the elements $a_1, \ldots, a_n$ are $\mathfrak{p}$-adic integers. Therefore all $a_i \in R$ can be written as power series $a_i = \sum_{j=0}^{\infty} \alpha_{i,j} \pi^j$ with $\alpha_{i,j} \in A$. If we write $a_{i,k} = \sum_{j=0}^{k-1} \alpha_{i,j} \pi^j$ for any fixed $k \in \mathbb{Z}_{>0}$ we find that

$$\begin{aligned} f(a_1, \ldots, a_n) = {} & f(a_{1,k}, \ldots, a_{n,k}) \\ & + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a_{1,k}, \ldots, a_{n,k}) \cdot \alpha_{i,k}\, \pi^k + O(\pi^{k+1}), \end{aligned} \tag{1.3}$$

for any $k \in \mathbb{Z}_{>0}$. This allows us to make two important observations:

1. The value of $f(a_1, \ldots, a_n)$ modulo π^k for some $k \in \mathbb{Z}_{>0}$ is completely determined by the values of $a_{1,k}, \ldots, a_{n,k}$.
2. The value of $f(a_1, \ldots, a_n)$ modulo π^{k+1} for $k \in \mathbb{Z}_{>0}$ can be computed using only the values of the function f and its first order derivatives in $a_{1,k}, \ldots, a_{n,k}$, together with the values of $\alpha_{1,k}, \ldots, \alpha_{n,k}$.

These two observations allow us to solve Problem 1.3.1 by Hensel lifting.

Subsection 1.3.1

Hensel lifting

Note that there is some $s \in \mathbb{Z}_{>0}$ such that $\rho^s S = \pi S$. Now assume that we have $f(a_{1,k}, \dots, a_{n,k}) \equiv 0 \pmod{\pi^k}$ for some $k \geq 1$. For any integer r such that $sk < r \leq s(k+1)$ Equation (1.3) shows us that $f(a_1, \dots, a_n) \equiv 0 \pmod{\rho^r}$ if and only if

$$0 \equiv \frac{f(a_{1,k}, \dots, a_{n,k})}{\pi^k} + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a_{1,k}, \dots, a_{n,k}) \cdot \alpha_{i,k} \pmod{\rho^{r_0}}, \tag{1.4}$$

where $r_0 = r - sk$. Note that $S/\rho^{r_0}S$ is a vector space over $\mathbb{F}_\mathfrak{p} = R/\pi R$, as the canonical map $R \to S \to S/\rho^{r_0}S$ has kernel πR. Equation (1.4) is thus a set of linear equations over $\mathbb{F}_\mathfrak{p}$ in the variables $\alpha_{1,k}, \dots, \alpha_{n,k}$, which could be explicity solved. Computing a root modulo a higher power in this way is what is known as Hensel Lifting.

For $s > 1$ or $r_0 > 1$ determining the vector space structure of $S/\rho^{r_0}S$ is not trivial. To see what this vector space structure is, we note that for $1 < r_0 \leq s$ we have a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & S/\rho^{r_0-1}S \arrow[r, "\cdot\rho"] & S/\rho^{r_0}S \arrow[r] & S/\rho S \arrow[r] & 0, \end{tikzcd}$$

of $\mathbb{F}_\mathfrak{p}$-vector spaces. In this short exact sequence the first non-zero map is induced by multiplication by ρ on S.

Since a short exact sequence of vector spaces is split we can immediately conclude that $S/\rho^{r_0}S \cong S/\rho S \oplus S/\rho^{r_0-1}S$. Furthermore, this isomorphism can be made explicit if we fix a section $\sigma : S/\rho S \to S/\rho^{r_0}S$. In this case an element $a \in S/\rho^{r_0}S$ maps to an element $(b, c) \in S/\rho S \oplus S/\rho^{r_0-1}S$, where b is the reduction of a modulo ρ and c is the unique element that maps to $a - \sigma(b)$ under multiplication by ρ. By induction we get an isomorphism $S/\rho^{r_0}S \cong (S/\rho S)^{r_0}$, for any $r_0 \in \{1, \dots, s\}$, which can be made explicit using the explicit lifts described before.

It remains to represent $S/\rho S$ as an $\mathbb{F}_\mathfrak{p}$-vector space. Note that $S/\rho S \cong \mathbb{F}_\mathfrak{q}$ is the residue field of $\mathfrak{q}$ and hence a field extension of $\mathbb{F}_\mathfrak{p}$. Furthermore, as $\mathbb{F}_\mathfrak{q}$ is a finite field, the group of units is generated by a single element γ. Therefore we have that $\mathbb{F}_\mathfrak{q} = \mathbb{F}_\mathfrak{p}[\gamma]$, hence the isomorphism $\mathbb{F}_\mathfrak{p}^m \to \mathbb{F}_\mathfrak{q}$ is explicitly given by $(c_i)_{i=0}^{m-1} \mapsto \sum_{i=0}^{m-1} c_i \gamma^i$.

Remark 1.3.2. Note that cases where $s > 1$ can make the process of Hensel lifting considerably faster. Computing roots of a polynomial modulo ρ^r will only require $\lceil \frac{r}{s} \rceil - 1$ steps, as each increase in the power of π increases the power of ρ by s. Therefore Tate's algorithm for Frey curves defined over a number field K might actually be faster than Tate's algorithm for Frey curves over $\mathbb{Q}$, if the parameters are all in $\mathbb{Z}$. This often happens in practice when the parameters are the solutions of Diophantine equations over $\mathbb{Z}$.

We have tried to find an example that illustrates the Hensel lifting in the case where $s > 1$ and $r_0 > 1$ using Tate's algorithm on a Frey curve. Unfortunately for the Frey curves we tried, the distinctions between cases are made modulo ρ^r with $r \leq s$ or $r \equiv 1 \pmod{s}$, or made in one of the transformations. Therefore these Frey curves do not seem to provide examples that illustrate the true potential of this type of Hensel lifting.

Subsection 1.3.2

The algorithm

Using Hensel lifting as described in the previous section, we now have an efficient algorithm to solve Problem 1.3.1. We here give a pseudocode outline of this algorithm. It includes two helper functions Vector1 and Vector2 that convert an element $x \in S/\rho^r S$ into an appropriate vector in $\mathbb{F}_{\mathfrak{q}}^r$ and $\mathbb{F}_{\mathfrak{p}}^{rm}$.

```
Function Vector1($x$, $r$; $\rho$, $\mathbb{F}_\mathfrak{q}$, LiftS)
  Set $x_\mathfrak{q} := x \in \mathbb{F}_\mathfrak{q}$
  If $r = 1$
    Return $[x_\mathfrak{q}]$
  Else
    Return $[x_\mathfrak{q}$, Vector1($x -$ LiftS($x_\mathfrak{q}$))$/\rho$, $r - 1$)$]$
Function Vector2($x$, $r$; $\rho$, $\mathbb{F}_\mathfrak{q}$, LiftS, $\psi$)
  Set $v := [\,]$
  For $w$ in Vector1($x$, $r$)
    Set $v := [v, \psi(w)]$
  Return $v$
Function ComputeRootsModulo($f$, $r$; $\pi$, $\rho$, $\mathbb{F}_\mathfrak{p}$, $\mathbb{F}_\mathfrak{q}$, LiftR, LiftS, $\psi$)
  Set $B := \{\}$
  If $r \leq s$
    For $[v_1, \ldots, v_n]$ in $\mathbb{F}_\mathfrak{p}^n$
      Set $a_1 :=$ LiftR($v_1$), $a_2 :=$ LiftR($v_2$), $\ldots$, $a_n :=$ LiftR($v_n$)
      If $\rho^r \mid f(a_1, ..., a_n)$
```

```
            Set $B := B \cup \{(a_1, \dots, a_n)\}$
      Else
         Set $k := \lceil \frac{r}{s} \rceil - 1$
         Set $r_0 := r - ks$
         For $(a_1, ..., a_n)$ in ComputeRootsModulo($f$, $ks$)
            Set $M := \begin{bmatrix} \texttt{Vector2(}\frac{\partial f}{\partial x_1}(a_1, ..., a_n), r_0\texttt{)} \\ \texttt{Vector2(}\frac{\partial f}{\partial x_2}(a_1, ..., a_n), r_0\texttt{)} \\ \vdots \\ \texttt{Vector2(}\frac{\partial f}{\partial x_n}(a_1, ..., a_n), r_0\texttt{)} \end{bmatrix}$
            Set $w :=$ Vector2($f(a_1, ..., a_n)/\pi^k, r_0$)
            For $[v_1, \dots, v_n]$ in $\{v \in \mathbb{F}_{\mathtt{p}}^n : Mv = w\}$
               Set $b_1 :=$ LiftR($v_1$), $b_2 :=$ LiftR($v_2$), ..., $b_n :=$ LiftR($v_n$)
               Set $B := B \cup \{(a_1 + b_1\pi^k, \dots, a_n + b_n\pi^k)\}$
      Return $B$
```

The arguments π, ρ, $\mathbb{F}_{\mathtt{p}}$, $\mathbb{F}_{\mathtt{q}}$, LiftR, LiftS, and ψ are part of the context. Mathematically they could either be inferred from the other arguments or their choice does not matter. They are given to indicate that an actual implementation might need them as an input. The statement $x_{\mathtt{q}} := x \in \mathbb{F}_{\mathtt{q}}$ means we are taking the image of x under the canonical map to $\mathbb{F}_{\mathtt{q}}$. The maps LiftR and LiftS are right inverses of the canonical maps $R \to \mathbb{F}_{\mathtt{p}}$ and $S \to \mathbb{F}_{\mathtt{q}}$ respectively, that map 0 to 0. The map ψ is the inverse of the map $\mathbb{F}_{\mathtt{p}}^m \to \mathbb{F}_{\mathtt{q}}$ given by $(c_i)_{i=1}^m \mapsto \sum_{i=1}^m c_i\gamma^i$.

To solve Problem 1.3.1 for a specific polynomial f and $r \in \mathbb{Z}_{\geq 0}$ one simply calls the function computeRootsModulo with these arguments. Note that the result of this function is not all possible roots, but rather representatives of the roots modulo π^k, where $k = \lceil \frac{r}{s} \rceil$. According to Equation (1.3) these are actually sufficient to determine all solutions, as the solutions only depend on their value modulo π^k.

We can see that this algorithm would perform better than naively trying all possible roots when $r > s$. First of all the algorithm does not have to try all solutions, but only those that were solutions for $r' = \left(\lceil \frac{r}{s} \rceil - 1\right) s$. Secondly the most expensive computation – evaluating a polynomial – only has to be done $n + 1$ times for each of these solutions for r', rather than once for every derived solution, i.e. $\#\mathbb{F}_{\mathtt{p}}^n$ times. Instead we do some linear algebra to find the derived solutions directly.

Section 1.4

$\mathfrak{p}$-adic trees

Looking at the algorithm in the previous section, we see that multiple solutions come from the same solutions modulo a lower power. It would therefore make sense to store each solution modulo a lower power once, and store only the additional coefficients in the $\mathfrak{p}$-adic expansion for each solution modulo a higher power. This naturally gives rise to a tree structure, that we will call a $\mathfrak{p}$-adic tree.

Definition 1.4.1. Let A be a finite set. A *labeled tree* is a directed and possibly infinite graph T such that:

1. There exists a unique node in T with no incoming arrow. We call this node the *root* of the tree.

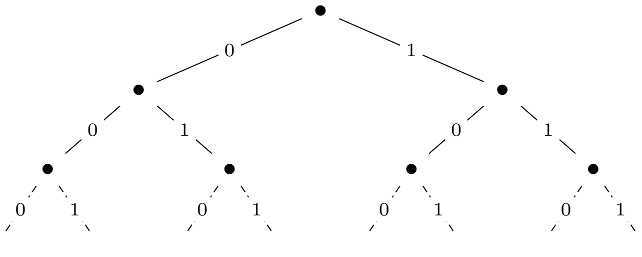
2. For each node of T there is a unique finite path from the root to that node.

3. Each arrow is labeled by an element of A such that all outgoing arrows at a node have a distinct label.

We call A the *set of labels* of T. We say that a labeled tree is *full* if each node has an outgoing arrow for each label.

A $\mathfrak{p}$-*adic tree* is a labeled tree with as set of labels the residue field $\mathbb{F}_{\mathfrak{p}}$ of $\mathfrak{p}$, or more generally $\mathbb{F}_{\mathfrak{p}}^n$ for some $n > 0$. If $\mathfrak{p} = (p)$ we will also write p-adic tree instead of $\mathfrak{p}$-adic tree. We call n the *width* of the tree.

As an example of a $\mathfrak{p}$-adic tree look at the case $K = \mathbb{Q}$ and $\mathfrak{p} = (2)$. We can label our arrows using the numbers 0 and 1 as $\mathbb{F}_2 = \{0, 1\}$. A possible 2-adic tree might now be represented as follows.



Here we put the root on top and assume that all arrows point downward. Furthermore the tree continues with infinitely many nodes.

Note that the bijection $A \to \mathbb{F}_{\mathfrak{p}}$ allows one to interpret a path in a $\mathfrak{p}$-adic tree as a sequence of coefficients of a power series in π, i.e. as $\mathfrak{p}$-adic numbers. In fact each element of the ring of integers $\mathcal{O}_{\mathfrak{p}}$ of the corresponding local field corresponds to a unique infinite path of a full $\mathfrak{p}$-adic tree in this way. If we limit ourselves to finite paths of length n starting at the root we get instead a one-to-one correspondence with $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^n$.

The idea now is to use a $\mathfrak{p}$-adic tree to represent the set of solutions to Problem 1.3.1. A priori it might seem that this would require an infinite amount of information to be stored, but note that a full tree is completely fixed. Therefore, if a node contains all possible nodes beneath it, we only have to store that this node is the root of a full subtree.

Explicitly, we would start with a full $\mathfrak{p}$-adic tree in the algorithm in Section 1.3.2. We would modify this tree in each call of `ComputeRootsModulo` as follows.

- If $r \leq s$ we remove all the labelled arrows of the root that do not correspond to roots of the equation $f(x_1, \ldots, x_n) \equiv 0 \pmod{\mathfrak{q}^r}$ and return the remaining tree.
- If $r > s$ we look at the nodes at level $k = \left\lceil \frac{r}{s} \right\rceil$ of the tree produced by the recursive call to `computeRootsModulo`. For each of these nodes, we take $a_1, \ldots, a_n$ as the elements of R corresponding to the finite power series in π represented by the path to that node. These are representatives of the corresponding element in $\left(\mathcal{O}_{\mathcal{K}}/\mathfrak{p}^k\right)^n$. Next we keep all the arrows connected to this node with any of the labels $b_1, \ldots, b_n$ that follow from the calculation thereafter, and remove all other arrows. After doing this for each node at level k we return the resulting tree.

Here the level of a node is simply the length of the unique path from the root to that point. Note that the resulting tree will contain all infinite paths of elements of $R \subset \mathcal{O}_p$ that correspond to solutions of Problem 1.3.1, and not contain the infinite paths corresponding to non-solutions.

A useful property of using $\mathfrak{p}$-adic trees in the algorithm is that we do not have to start with a full tree. We may for example start with a tree containing only those paths corresponding to previous calculations and limit it to those that also solve a specific instance of Problem 1.3.1. This is what will happen most often in performing Tate's algorithm. Furthermore it is also easy to keep track of the elements that do not solve Problem 1.3.1 by just keeping track of the nodes that would be removed. Therefore the $\mathfrak{p}$-adic trees seem a good way to keep track of the different cases we might encounter when performing Tate's algorithm on an elliptic curve depending on parameters.

Section 1.5

A finite step 7 subalgorithm.

We will now look again at the subalgorithm of Step 7 of Tate's algorithm as discussed in Section 1.1. Looking at it closely we will find that we only have to do a finite number of steps if we are only interested in the conductor, Kodaira type, minimal model, or the total number of geometrically irreducible components. We are not aware of this being explicitly stated somewhere else in the literature, but in retrospect we found that the final result – as stated in Corollary 1.5.4 – can also be obtained from the tables in [Pap93] with some careful analysis.

Let

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

be a model of an elliptic curve at the start of some substep in the subalgorithm of Step 7. We here again use the conventions of Section 1.1, so E is a curve over a p-adic field K with valuation v. In Substep n of this subalgorithm we may assume that this model satisfies

$$\begin{aligned} v(a_1) &\geq 1 \\ v(a_2) &= 1 \\ v(a_3) &\geq \left\lceil \frac{n+3}{2} \right\rceil \\ v(a_4) &\geq \left\lceil \frac{n+4}{2} \right\rceil \\ v(a_6) &\geq n+3, \end{aligned}$$

which we will prove later by induction. We stop the algorithm at Substep n if the polynomial

$$\begin{cases} T^2 + \frac{a_3}{\pi^{\frac{n+3}{2}}}T + \frac{a_6}{\pi^{n+3}} & \text{if } n \text{ is odd} \\ \frac{a_2}{\pi}T^2 + \frac{a_4}{\pi^{\frac{n+4}{2}}}T + \frac{a_6}{\pi^{n+3}} & \text{if } n \text{ is even} \end{cases}$$

has distinct roots in $\overline{\mathbb{F}_\mathfrak{p}}$. In that case the reduction information is given by

$$\text{Type } I_n^*, \quad m = n+5, \quad f = v(\Delta) - n - 4, \quad c = \begin{cases} 4 & \text{if all roots are in } \mathbb{F}_\mathfrak{p} \\ 2 & \text{otherwise.} \end{cases}$$

Otherwise we will continue towards step $n+1$. Since in that case there is a double root for the polynomial which necessarily lives in $\mathbb{F}_{\mathfrak{p}}$, we can do a transformation on E to change the double root to 0, thereby guaranteeing the assumptions for step $n+1$ are satisfied. Note that the assumptions for Substep 1 can be satisfied by performing the necessary transformations before starting the subalgorithm, as described on page 367 of [Sil94].

We now prove some results about the invariants if we end in Substep n.

Lemma 1.5.1. *If the subalgorithm ends at Substep n the corresponding model for E satisfies*

$$\begin{aligned} v(b_2) &= \begin{cases} 2v(a_1) & \text{if } v(a_1) \leq v(2) \\ 2v(2)+1 & \text{if } v(a_1) > v(2) \end{cases} \\ v(b_8) &= n+4. \end{aligned}$$

Proof. For the first part note that $b_2 = a_1^2 + 4\,a_2$. We have that $v(a_1^2) = 2\,v(a_1)$ is even and $v(4\,a_2) = 2\,v(2)+1$ is odd, hence $v(b_2)$ is the smallest of the two. This immediately implies the mentioned result.

Now for the result about $v(b_8)$ we first mention that

$$b_8 = a_1^2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 + 4 a_2 a_6 - a_4^2.$$

Note that for the first two terms on the right hand side we have

$$v(a_1^2 a_6) = 2v(a_1) + v(a_6) \geq n+5$$

and

$$v(a_1 a_3 a_4) = v(a_1) + v(a_3) + v(a_4) \geq 1 + \left\lceil \frac{n+3}{2} \right\rceil + \left\lceil \frac{n+4}{2} \right\rceil = n+5.$$

Now in case n is odd the term $a_2 a_3^2 + 4 a_2 a_6$ is precisely $a_2 \pi^{n+3}$ times the determinant of the polynomial considered in this step. Since we ended at this step, this polynomial has distinct roots and we find that

$$v(a_2 a_3^2 + 4 a_2 a_6) = v(a_2 \pi^{n+3}) = n+4.$$

Furthermore we have that

$$v(a_4^2) = 2\,v(a_4) \geq 2 \left\lceil \frac{n+4}{2} \right\rceil = n+5,$$

hence we must have $v(b_8) = n + 4$ in this case.

In the case that n is even we similarly find that $4a_2a_6 - a_4^2$ is $-\pi^{n+4}$ times the determinant of the polynomial considered in this step. Since this polynomial has distinct roots as we ended in this step, we find that

$$v(4a_2a_6 - a_4^2) = v(\pi^{n+4}) = n + 4.$$

In this case we also have

$$v(a_2a_3^2) = v(a_2) + 2\,v(a_3) \geq 1 + 2\left\lceil \frac{n+3}{2} \right\rceil = n + 5,$$

hence $v(b_8) = n + 4$ also when n is even. □

Proposition 1.5.2. *If the subalgorithm ends at Substep $n > 4\,v(2)$ we have that*

$$\begin{aligned} v(c_4) &= 2\,v(b_2) \\ v(c_6) &= 3\,v(b_2) \\ v(\Delta) &= 2\,v(b_2) + v(b_8). \end{aligned}$$

Proof. We will use the model of E used in Substep $n \geq 4v(2) + 1$ of the subalgorithm. First of all we note that

$$\begin{aligned} 2\,v(b_4) - n &= 2\,v(2\,a_4 + a_1a_3) - n \\ &\geq \min\{2\,v(2) + 2\,v(a_4) - n, 2\,v(a_1) + 2\,v(a_3) - n\} \\ &\geq \min\{2\,v(2) + 4, 2\,v(a_1) + 3\} = v(b_2) + 3 \end{aligned}$$

and

$$\begin{aligned} v(b_6) - n &= v(a_3^2 + 4\,a_6) - n \\ &\geq \min\{2\,v(a_3) - n, 2\,v(2) + v(a_6) - n\} \\ &\geq \min\{3, 2\,v(2) + 3\} = 3. \end{aligned}$$

Now we compute that

$$\begin{aligned} 2\,v(24\,b_4) &= 6\,v(2) + 2\,v(3) + n + (2\,v(b_4) - n) \\ &\geq 10\,v(2) + 2\,v(3) + v(b_2) + 4 \\ &> 4\,v(b_2) = 2\,v(b_2^2), \end{aligned}$$

hence $v(24\,b_4) > v(b_2^2)$. Therefore $c_4 = b_2^2 - 24\,b_4$ has valuation $v(b_2^2) = 2\,v(b_2)$ as claimed.

Next we note that

$$\begin{aligned} 2\,v(36\,b_2b_4) &= 4\,v(2)+4\,v(3)+2\,v(b_2)+n+(2\,v(b_4)-n) \\ &\geq 8\,v(2)+4\,v(3)+3\,v(b_2)+4 \\ &> 6\,v(b_2) = 2\,v(b_2^3), \end{aligned}$$

hence $v(36\,b_2b_4) > v(b_2^3)$ and

$$\begin{aligned} v(216\,b_6) &= 3\,v(2)+3\,v(3)+n+(v(b_6)-n) \\ &\geq 7\,v(2)+3\,v(3)+4 \\ &> 3v(b_2) = v(b_2^3). \end{aligned}$$

Therefore we find that

$$c_6 = -b_2^3 + 36\,b_2b_4 - 216\,b_6$$

has valuation $v(b_2^3) = 3v(b_2)$ as claimed.

For the last part we note that

$$\begin{aligned} 2\,v(8\,b_4^3) &= 6\,v(2)+3\,n+3(2\,v(b_4)-n) \\ &\geq 10\,v(2)+3\,v(b_2)+2\,n+10 \\ &> 4\,v(b_2)+2\,v(b_8) = 2\,v(b_2^2b_8), \end{aligned}$$

hence $v(8\,b_4^3) > v(b_2^2b_8)$,

$$\begin{aligned} v(27b_6^2) &= 3\,v(3)+2\,n+2(v(b_6)-n) \\ &\geq 4\,v(2)+3\,v(3)+n+7 \\ &> 2\,v(b_2)+v(b_8) = v(b_2^2+b_8), \end{aligned}$$

and

$$\begin{aligned} 2\,v(9\,b_2b_4b_6) &= 4\,v(3)+2\,v(b_2)+3\,n+(2\,v(b_4)-n)+2(v(b_6)-n) \\ &\geq 4\,v(2)+4\,v(3)+3\,v(b_2)+2\,n+10 \\ &> 4\,v(b_2)+2v(b_8) = 2\,v(b_2^2b_8), \end{aligned}$$

hence $v(9\,b_2b_4b_6) > v(b_2^2b_8)$. All these imply that

$$\Delta = -b_2^2b_8 - 8\,b_4^3 - 27\,b_6^2 + 9\,b_2b_4b_6$$

has valuation $v(b_2^2b_8) = 2\,v(b_2)+v(b_8)$ as claimed. □

Remark 1.5.3. Note that the expression for $v(c_4)$ is true for all n and the expression for $v(c_6)$ is already true for all $n > 3v(2)$. Furthermore $v(c_4)$, $v(c_6)$ and $v(\Delta)$ are independent of the transformations done in the subalgorithm.

Corollary 1.5.4. *If the subalgorithm ends at Substep $n > 4v(2)$, then*

$$n = v(b_8) - 4 = v(\Delta) - 2v(b_2) - 4 = v(\Delta) - v(c_4) - 4,$$

hence part of the local data is

$$E_{min} = E, \quad \textit{Type } I^*_{v(\Delta)-v(c_4)-4}, \quad m = v(\Delta) - v(c_4) + 1, \quad f = v(c_4)$$

It is clear from Corollary 1.5.4 that the conductor exponent, Kodaira symbol, minimal model, and number of irreducible components can already be computed with at most $4\,v(2)$ steps of the step 7 subalgorithm. In particular the subalgorithm is unnecessary if one only wants to compute this data for primes of odd characteristic, as is already mentioned in [Sil94].

Example 1.5.5. $\boxed{\texttt{Conductor.rst}}$ We look again at the curve from Example 1.2.1. If AB is divisible by 8 and $A - B \equiv 1 \pmod 4$, then Tate's algorithm would end up in the subalgorithm of step 7. We will show that the number of steps required in this subalgorithm will depend on the power of 2 dividing AB.

To start of we will assume that $8 \mid AB$ and $A - B \equiv 1$ modulo 4, as this will guarantee we end up in step 7 of Tate's algorithm. We also replace the curve by its $(0, 1, 0)$-transform

$$E : y^2 + 2\,xy = x^3 + (-A + B - 1)\,x^2 + (-AB)\,x,$$

such that all the transformations in Tate's algorithm will be trivial.

It is easy to see that with these assumptions we have

$$\begin{aligned} \operatorname{ord}_2 a_1, \operatorname{ord}_2 a_2 &= 1, \\ \operatorname{ord}_2 a_3, \operatorname{ord}_2 a_4 &\geq 3, \text{ and} \\ \operatorname{ord}_2 a_6 &\geq 4. \end{aligned}$$

Using this information when performing Tate's algorithm as in Section 1.1, we see that we get to the `If` statement in step 6 of Tate's algorithm by only performing trivial transformations. Now look at the polynomial

$$P(T) = T^3 + \frac{a_2}{2}T^2 + \frac{a_4}{4}T + \frac{a_6}{8} \text{ modulo 2.}$$

The `If` statement in step 6 is equivalent to this polynomial not having a double root, and the `If` statement in step 7 is equivalent to this polynomial not having a triple root. In this case we have $P(T) = T^3 + T^2$, so 0 is a double root. Therefore we would end up in the subalgorithm of Step 7, and the initial transformation of the subalgorithm is trivial.

Since our model has $a_3 = a_6 = 0$ we have $b_6 = 0$. Therefore the algorithm will not terminate in an odd substep of the subalgorithm, and every transformation in such a substep is trivial. Since $a_4^2 - 4a_2a_6 = A^2B^2$ we stop in the subalgorithm in substep $n = 2k$ if and only if $\operatorname{ord}_2(AB) < k + 3$. Again we get a trivial transformation if we continue in substep n, justifying that we used the same model everywhere.

We see that the subalgorithm ends in substep $n = 2\operatorname{ord}_2(AB) - 4$. Furthermore we have $\operatorname{ord}_2 \Delta = \operatorname{ord}_2 \left((16) \cdot B^2 \cdot A^2 \cdot (A+B)^2\right) = 2\operatorname{ord}_2(AB) + 4$, so the corresponding local data would be

$$\text{Type } I^*_{2\operatorname{ord}_2(AB)-4},\ m = 2\operatorname{ord}_2(AB) + 1, \text{ and } f = 4.$$

In case $n > 4$, i.e. when $32 \mid AB$, we could also compute this data using Corollary 1.5.4 by noting that $\operatorname{ord}_2(c_4) = \operatorname{ord}_2\left((16) \cdot (A^2 + AB + B^2)\right) = 4$.

In this example we see that by using Corollary 1.5.4 we can determine part of the local data by performing at most 4 steps of the subalgorithm. Note that the Kodaira symbol and number of geometrically irreducible components m still depends on $\operatorname{ord}_2(\Delta)$, which is unbounded when we only assume $8 \mid AB$. Computing this data for all A and B would therefore be impossible in finite time. We can however compute the conductor exponent for all A and B in this way.

Section 1.6

SageMath implementation

The author has implemented the theory and algorithms above as part of the `modular_method` package [vL21a] for SageMath [Sag20]. In this section we will give an overview of the different objects and functions that the `modular_method` package provides with regards to the theory discussed in this chapter. This includes some custom classes to work with $\mathfrak{p}$-adic numbers in Section 1.6.1, an implementation of $\mathfrak{p}$-adic trees in Section 1.6.2, an implementation of the algorithm from Section 1.3.2 in Section 1.6.3, and an implementation of Tate's algorithm as described in Section 1.2 in Section 1.6.5. Section 1.6.4 introduces a user-friendly way to provide restrictions on parameters – which might arise from a Diophantine equation – to the algorithm in Section 1.6.5. In Section 1.6.6 we present objects that represent Frey curves. These provide an interface to all the other code, which we illustrate with some examples.

Subsection 1.6.1

$\mathfrak{p}$-adics

As discussed in Section 1.3 we will work exclusively inside number fields, as all $\mathfrak{p}$-adic computation we need can be performed already in those fields. This allows us to avoid choosing a precision.

To determine which $\mathfrak{p}$-adic field we are interested in, i.e. the $\mathfrak{p}$-adics we use, the file `modular_method.padics.pAdic_base` provides the class `pAdicBase`. An instance of this class describes the $\mathfrak{p}$-adics by a prime $\mathfrak{p}$ of a number field K. It provides useful shorthands to access particular information about the $\mathfrak{p}$-adics, such as a uniformizer, the valuation, and primes below $\mathfrak{p}$ in subfields of K.

Note that throughout the code, if a function requests an argument called `pAdics`, it means an instance of `pAdicBase`. You can easily create a new instance thereof by providing a number field and a prime as a maximal ideal of the ring of integers. If the number field is the rationals one might also provide a prime number instead.

Note that `pAdicBase` is not loaded into the `modular_method` namespace by default, as it is often only used indirectly.

Subsection 1.6.2

$\mathfrak{p}$-adic trees

The $\mathfrak{p}$-adic trees as discussed in Section 1.4 are implemented in the module `modular_method.padics.pAdic_tree`. They are constructed from the classes `pAdicNode` and `pAdicNodeCollection`. These respectively represent a node in the tree and a collection of children of a node.

An instance of `pAdicNode` contains

- the $\mathfrak{p}$-adics of the entire tree,
- the width $n > 0$ of the tree,
- a list of n elements of $\mathbb{F}_\mathfrak{p}$ representing the label of the incoming arrow,
- an instance of `pAdicNodeCollection` representing the children of this node, and

- the direct parent of this node if it has one.

Any node that does not have a parent is considered to be a root of a $\mathfrak{p}$-adic tree. In that case the element of $\mathbb{F}_{\mathfrak{p}}^n$ has no meaning. Using the reference to its parent a node can recursively compute its level k in the tree. It can also recursively compute the representative of $\left(\mathcal{O}_K/\mathfrak{p}^k\right)^n$ that represents the path from the root to that node.

A standard instance of `pAdicNodeCollection` contains a reference to the parent node, and a dictionary containing labels of arrows as keys and the corresponding children as values. The subclass `pAdicNodeCollection_inverted` does not necessarily keep track of all nodes that belong to it explicitly. Rather it keeps track of a list of labels for which there is no corresponding node and only creates a node of a specific label when it is requested. All nodes not yet created by an instance `pAdicNodeCollection_inverted` are assumed to be roots of a full subtree.

When using this implementation one should note that all references to parent nodes are weak references. This means that Python's garbage collection will remove a `pAdicNode` instance if nothing besides its children and corresponding `pAdicNodeCollection` refer to it. This is necessary as otherwise a tree will persist indefinitely after creation. When working explicitly with nodes in a $\mathfrak{p}$-adic tree, one should always keep a reference to the root to prevent the tree from breaking.

Note that the trees represented by a `pAdicNode` root are mutable, which allows the algorithm in Section 1.3.2 to work with them with the least amount of copying possible. An immutable version is available for the user's convenience in the form of the class `pAdicTree`. An instance of the class `pAdicTree` represents possible $\mathfrak{p}$-adic values of n variables, where the values are those in an internal $\mathfrak{p}$-adic tree. Most top level functions will return an instance of `pAdicTree` rather than a root of a $\mathfrak{p}$-adic tree.

When creating an instance of `pAdicTree` one has to provide names for the variables to be used and the $\mathfrak{p}$-adics to be used. The latter can also be provided as a number field and a finite prime thereof. By default the corresponding $\mathfrak{p}$-adic tree is always full. Alternatively one could provide a root of a tree with the appropriate width, which will then serve as the collection of possible values for the variables.

The class `pAdicTree` has methods that allow you to work with it as if it was a set. Furthermore it has methods to change the variables by adding, removing or reordering them. Note that none of the non-hidden methods modify the actual tree stored, but rather modify a copy and return it as another `pAdicTree` object.

This makes the object less error-prone but slower for computation.

Subsection 1.6.3

$\mathfrak{p}$-adic solver

The module `modular_method.padics.pAdic_solver` provides a function called `find_pAdic_roots`. This is an implementation of the algorithm in Section 1.3.2 using the $\mathfrak{p}$-adic trees from Section 1.6.2. It solves Problem 1.3.1 when provided with the polynomial f, the $\mathfrak{q}$-adics given by L and $\mathfrak{q}$, and the precision r. The $\mathfrak{q}$-adics may be given as a `pAdicBase` object or as L and q separately. The result will be the root of a $\mathfrak{p}$-adic tree containing the solutions of Problem 1.3.1, and the root of a $\mathfrak{p}$-adic tree with the non-solutions.

The function `find_pAdic_roots` also has some additional options. First of all one can provide a $\mathfrak{p}$-adic tree containing the values to which the computation should be limited. This is the only way to ensure that the $\mathfrak{p}$-adics of the used tree are different from those defined by L and $\mathfrak{q}$. Note that the given $\mathfrak{p}$-adic tree will be modified if it is given by the root `pAdicNode`. One can also provide a `precision_cap` which is the maximal level of the $\mathfrak{p}$-adic tree on which computations may be performed. Note that setting this `precision_cap` too low might make it so `find_pAdic_roots` can not compute the roots modulo $\mathfrak{q}^r$ accurately. In that case a warning is printed and r is lowered to the value for which the solutions can still be computed. By default the `precision_cap` is set at 20.

Another feature of `find_pAdic_roots` is the option `give_list`. When enabled, the function will return a list of trees and an integer s. The values in the first tree will be solutions of f modulo $\mathfrak{q}^s$ that are no longer solutions modulo $\mathfrak{q}^{s+1}$, whereas the second tree will be solutions of f modulo $\mathfrak{q}^{s+1}$ that are no longer solutions modulo $\mathfrak{q}^{s+2}$, and so on. Note that the last tree will be those that are solutions modulo $\mathfrak{q}^r$, but these might still be solutions modulo higher powers. This is used to solve a check of type 4, as described in Section 1.2.

Subsection 1.6.4

Conditions

The parameters of Frey curves usually satisfy additional constraints, so it is useful to have objects that represent such restrictions. Such restrictions are called conditions in the framework [vL21a]. Various conditions are defined in the module `modular_method.diophantine_equations.conditions` as classes. Here are the most common ones and what an instance of them represents.

- PolynomialCondition represents the fact that parameters satisfy some polynomial equation. It can be created by giving a polynomial in the parameters that should equal 0.
- CongruenceCondition represents the fact that a certain polynomial in the parameters is congruent to zero modulo some integer or ideal. It can be created by giving the polynomial and this modulus.
- ExistsCondition represents the fact that there exist additional parameters such that the parameters and the additional parameters satisfy some polynomial equation. This can be thought of as a condition of the form

  $$\exists x_1, \ldots, x_m : f(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0.$$

  It can be created with the polynomial f and a specification of which parameters are additional.
- PowerCondition represents the fact that a certain polynomial in the variables is known to be at least a certain power, i.e. a condition of the form

  $$\exists y \, \exists n \geq n_0 : f(x_1, \ldots, x_m) = y^n.$$

  It can be created with the polynomial f and the value of n_0.
- CoprimeCondition represents the fact that the parameters are coprime in some way. It can be created from a list of parameters and a positive integer n. It represents that any combination of n parameters from that list have no common prime factors.
- OrderCondition represents that a certain polynomial in the variables has a maximal valuation for each prime, i.e. it represents a condition of the form

  $$\forall \mathfrak{p} : \operatorname{ord}_{\mathfrak{p}} f(x_1, \ldots, x_m) \leq n.$$

  It can be created from the polynomial f and the integer n.
- TreeCondition represents that the values of the parameters should be part of some $\mathfrak{p}$-adic tree. It can be constructed from a pAdicTree object.

Conditions can also be combined to form new conditions. For example using two conditions C1 and C2 one can make the condition that both of them hold C1 & C2, and the condition that either of them holds C1 | C2. One can also negate a condition C by writing ~C. One can recursively combine these conditions to make more complicated ones, but note that their printed representation might get a bit convoluted. One can always check what the left and right part of the top level combination were using the attributes `_left` and `_right`.

Each condition also has a method `pAdic_tree` that computes a $\mathfrak{p}$-adic tree for given $\mathfrak{p}$-adics. This $\mathfrak{p}$-adic tree contains all the values of the parameters for which the condition holds. The $\mathfrak{p}$-adics should be provided as a `pAdicBase` object. Alternatively one could provide a `pAdicTree` object as the argument `pAdic_tree`, in which case the result will be a new `pAdicTree` of those values in the given one that satisfy the condition.

Using the argument `complement` one can request the method `pAdic_tree` to also return the tree of values that do not satisfy the condition. Note that the trees returned always err on the side of caution, meaning they contain all possible values for which the condition could hold (or not hold). This means that the two trees returned might overlap. For example when asking the $\mathfrak{p}$-adic tree and complement of a `CongruenceCondition` for which $\mathfrak{p}$ does not divide the modulus both trees will be full.

Some conditions might accept additional arguments for `pAdic_tree`, such as `precision_cap` for the maximal level at which to do computations in $\mathfrak{p}$-adic trees, and `precision` for the precision of computations in $\mathfrak{p}$-adic fields. These additional arguments are used by conditions that use `find_pAdic_roots` to compute the corresponding $\mathfrak{p}$-adic tree. Note the remark about setting `precision_cap` too low in Section 1.6.3. If no warning is given, but `precision` was provided, it is only guaranteed the returned $\mathfrak{p}$-adic tree is correct up to the given `precision`. If a condition is built from several conditions it will pass these arguments on to those conditions as well. If a condition does not accept these arguments they are ignored.

Each condition also has the methods `always` and `never`, which return true when it can be asserted that a condition either always holds or never holds at all respectively.

The module `modular_method.diophantine_equations.conditions` also contains the class `ConditionalValue`, which represents data of which the specific value might depend on certain conditions on parameters. It can be constructed by a list of pairs where each pair consists of a value and the condition that asserts this value is attained. Similarly a `ConditonalValue` can also be indexed or iterated as if it is such a list, but it comes with its own visual representation. Many functions in the `modular_method` package produce `ConditionalValue` objects as output or accept them as input.

When arithmetic is performed on `ConditionalValue` objects an instance of `ConditionalExpression` is created. These objects store the expressions without evaluating them. These come with a visual representation that display all `ConditionalValue` objects in the expression simultaneously. When necesary one can attempt to evaluate a `ConditionalExpression` to a single `ConditionalValue` with the method `value`. This method simply determines each possible value for the `ConditionalValue` objects in the expression and performs the appropriate arithmetic on those. Note that this might not work as the `ConditionalExpression` could contain parts that do not allow arithmetic normally such as strings.

To apply a function to each case in a `ConditionalValue` one can use the function `apply_to_conditional_value`. Another utility function provided is the function `conditional_product` which can be used to combine multiple `ConditionalValue` objects into one. You would use the latter for example if you have two `ConditionalValue` objects with integer values and want to combine them into one with possible tuples of these integers.

Subsection 1.6.5

Tate's algorithm

The module `modular_method.elliptic_curves.tates_algorithm` provides an implementation of Tate's algorithm based on the material covered in this chapter. The main function in this module – called `tates_algorithm` – will compute the data from Tate's algorithm for a given elliptic curve with coefficients in some polynomial ring over a number field and a given localization of that number field. The localization should be given by a corresponding `pAdicBase` object or a given finite prime of the number field.

The function performs Tate's algorithm as described in Section 1.1 by keeping track of cases in a queue. Each case contains a $\mathfrak{p}$-adic tree of values for the parameters, and tracks up to what point Tate's algorithm has been performed for that case. Until the queue is empty the function takes a case from the queue, performs a single step of Tate's algorithm on it, and then puts any resulting cases back into the queue. Here a step is any part of Tate's algorithm that contains exactly one check as described in Section 1.2, which in particular separates the transformations. Each of these checks might result in multiple cases as the outcome might depend on a further distinction between values. A case is removed from the queue when all the data that Tate's algorithm computes has been computed for that case.

Note that each step in Tate's algorithm makes use of the `find_pAdic_roots` function discussed before. It also makes use of the `give_list` functionality of that function to determine the valuation of various invariants when needed, such as to determine the precise type for Step 2. Note that a general `precision_cap` can be provided for these functions when calling `tates_algorithm`.

When the queue is empty the function collects all finished cases and constructs a `FreyCurveLocalData` object combining the local data computed. If the data is the same for all cases then one `FreyCurveLocalData` object is returned. Otherwise the return value is a `ConditionalValue` containing the different `FreyCurveLocalData` obtained and the conditions on the parameters for which they are attained.

To limit the values of the parameters from the start one can provide a $\mathfrak{p}$-adic tree as the argument `initial_values`. Here $\mathfrak{p}$ may be a prime in a subfield of the field over which the elliptic curve is defined. This is the only way to make `tates_algorithm` work with parameters in a smaller field. Note that when the $\mathfrak{p}$-adic tree is provided as a root `pAdicNode`, then this tree will be modified during the computation.

Besides computing all local data, one may also limit what local data is computed by providing the argument `only_calculate`. This should be a list containing keywords of the data one actually wants to compute. Rather than constructing a `FreyCurveLocalData` object at the end the function will in that case construct a list containing the requested local data for each case. Furthermore the implementation will skip steps that are not required for the data requested. For example it uses the results from Section 1.5 to limit the Step 7 subalgorithm to finitely many steps when only the minimal model or the conductor is requested.

Note that one cannot determine a priori if `tates_algorithm` will terminate on a provided input in general, as was remarked in Section 1.2. It is therefore strongly advised to rerun the algorithm with the optional `verbose` argument, when the algorithm does not seem to terminate. This will print which step is being computed, so one can better analyse what might be the issue.

As a sanity check, the function `tates_algorithm` has been tested various times against a random sample of 10 000 curves from the Cremona database, by considering them as curves with zero parameters.

Subsection 1.6.6

Frey curves

A user interface to the functionality discussed in previous sections is provided by the class `FreyCurve` in `modular_forms.elliptic_curves.frey_curves`. An object of this class can be used to represent a Frey curve of which one can find a more precise description in Section 3.1. For the code a `FreyCurve` is an elliptic curve of which the coefficients are polynomials over a number field L in a finite number of parameters. The parameters are assumed to have undetermined values in the ring of integers of a subfield $K \subseteq L$ that are subject to a given condition. The class provides functionality to compute with a `FreyCurve` as if it were an elliptic curve defined over L.

To construct a `FreyCurve` one has to either provide an elliptic curve of which the coefficients are polynomials over L, or the data that would make such a curve when passed to SageMath's `EllipticCurve`. Furthermore one can provide a ring of which the field of fractions will be the field K as `parameter_ring`, and a condition which the parameters should satisfy as `condition`.

Besides the standard functionality inherited from normal SageMath elliptic curves, the `FreyCurve` class provides methods to compute local data at primes of L. For example there are methods to compute the `conductor_exponent`, the `minimal_model` and the `reduction_type` at such a prime, as well as all `local_data`. Note that all these operations are backed by the implementation of Tate's algorithm described before, but are cached for easy reuse. Furthermore one can call these methods with a different condition than the one stored in the `FreyCurve` for more specific results.

Another local computation that can be performed for a `FreyCurve` E is computing the traces of Frobenius elements under the l-adic and mod l Galois representations associated with the curve. For a prime $\mathfrak{q}$ of L the method `trace_of_frobenius` computes an integer $a_{\mathfrak{q}}$. Let $\sigma \in G_L$ be a Frobenius element of $\mathfrak{q}$ and $\rho_{E,l}$ be the l-adic or mod l Galois representation of E for l a prime number not divisible by $\mathfrak{q}$. If $\rho_{E,l}$ is unramified, then $\operatorname{Tr} \rho_{E,l}(\sigma) = a_{\mathfrak{q}}$ inside $\mathbb{Q}_l$ or $\mathbb{F}_l$. Furthermore one can also compute the integer that would correspond to $\rho_l(\sigma^n)$ for any $n \in \mathbb{Z}_{>0}$ with `trace_of_frobenius` by setting the argument `power` to n. Note that this method does not require l and makes no assertions about the existence of l that satisfy the mentioned properties. It does require the curve to not have additive reduction at the given prime $\mathfrak{q}$.

Besides local computations one can also attempt to compute the entire conductor of a `FreyCurve` using the method `conductor`. This method requires that there are only finitely many primes for which the curve may have additive reduction. By default it determines these primes using the method `primes_of_possible_additive_reduction` which simply computes all the primes that could divide both c_4 and the discriminant. In case there is only one parameter these are determined by the resultant. In case of two parameters in which c_4 and the discriminant are homogeneous, the resultant is also used, but a warning is printed that the parameters should be coprime. In any other case only the primes dividing all the coefficients of c_4 and the discriminant are considered, and a warning is printed that it is assumed c_4 and the discriminant are coprime outside these primes.

For each additive prime – either provided by the argument `additive_primes` or computed – the method `conductor` will compute the conductor exponent explicitly. These are then combined into a `ConditionalExpression` of which the left side is just the product of the additive primes to their respective conductor exponent. The right side of this expressions is a string, which states that the remainder is the radical of some polynomial outside the additive primes. This polynomial is the discriminant of the elliptic curve, potentially scaled by a constant factor. When c_4 and the discriminant are coprime outside the additive primes, this is indeed what the remainder of the conductor should be.

Another method provided by a `FreyCurve` is `newform_candidates`. This method can be used to compute newforms associated to the Frey curve for the modular method. We discuss the details of this method in Chapter 3.

Example 1.6.1. `Conductor.rst` We will show some explicit code examples for the curve from Example 1.2.1, but in this example we will also assume A and B are coprime. First of all we construct the corresponding `FreyCurve` object.

```
sage: from modular_method import *
sage: R.<A, B> = QQ[]
sage: con = CoprimeCondition([A, B])
sage: E = FreyCurve([0, B - A, 0, -A*B, 0], condition=con); E
Frey curve defined by y^2 = x^3 + (-A+B)*x^2 + (-A*B)*x over \
Rational Field with parameters (A, B)
```

Now we can compute the conductor over $\mathbb{Q}$ with one method.

```
sage: N = E.conductor(); N
Warning: Assuming that A and B are coprime.
2^n0*Rad_P( (16) * B^2 * A^2 * (A + B)^2 )
 where
n0 = 5 if ('A', 'B') is 1 of 6 possibilities mod 4
     4 if ('A', 'B') is 1 of 3 possibilities mod 4
     3 if ('A', 'B') is 1 of 36 possibilities mod 16
     0 if ('A', 'B') is 1 of 24 possibilities mod 32
     1 if ('A', 'B') is 1 of 24 possibilities mod 32
```

The warning comes from the necessary assumption that c_4 and Δ are coprime outside some finite set of primes. In this case the finite set was chosen as $\{2\}$ by the default method.

```
sage: E.primes_of_possible_additive_reduction()
[2]
```

Note that the Rad_P part is not explicitly computed. It just displays the factorisation of the discriminant Δ. It indicates that the remaining part of the conductor is just the product of all primes dividing Δ that are not in $\{2\}$.

We can also change the set $\{2\}$ to compute more conductor exponents explicitly.

```
sage: E.conductor(additive_primes=[2, 3, 5, 7])
2^n0*3^n1*5^n2*7^n3*Rad_P( (16) * B^2 * A^2 * (A + B)^2 )
 where
n0 =  5 if ('A', 'B') is 1 of 6 possibilities mod 4
      4 if ('A', 'B') is 1 of 3 possibilities mod 4
      3 if ('A', 'B') is 1 of 36 possibilities mod 16
      0 if ('A', 'B') is 1 of 24 possibilities mod 32
      1 if ('A', 'B') is 1 of 24 possibilities mod 32
n1 =  0 if ('A', 'B') == (1, 1), (2, 2) mod 3
      1 if ('A', 'B') is 1 of 6 possibilities mod 3
n2 =  0 if ('A', 'B') is 1 of 12 possibilities mod 5
      1 if ('A', 'B') is 1 of 12 possibilities mod 5
n3 =  0 if ('A', 'B') is 1 of 30 possibilities mod 7
      1 if ('A', 'B') is 1 of 18 possibilities mod 7
```

We can also impose additional conditions. For example we could compute the conductor exponent at 2 as in Example 1.5.5.

```
sage: con2 = (CongruenceCondition(A*B, 8) &
....:         CongruenceCondition(A - B - 1, 4))
sage: E.conductor_exponent(2, condition=con2)
4
```

Note that E is also the Frey curve associated with Fermat's Last Theorem in case we take A, B and $A + B$ to be l-th powers with $l \geq 3$. We also compute the conductor imposing these additional conditions.

```
sage: conFLT = (con &
....:           PowerCondition(A, 3) &
....:           PowerCondition(B, 3) &
....:           PowerCondition(A + B, 3))
sage: E.conductor(condition=conFLT)
```

```
2^n0*Rad_P( (16) * B^2 * A^2 * (A + B)^2 )
 where
n0 = 3 if ('A', 'B') is 1 of 12 possibilities mod 16
     4 if ('A', 'B') is 1 of 6 possibilities mod 8
     0 if ('A', 'B') is 1 of 24 possibilities mod 32
     1 if ('A', 'B') is 1 of 24 possibilities mod 32
```

The results of these functions can be conditional values or conditional expressions. We illustrate how one can inspect such values with the conductor computed earlier

```
sage: N.left()
2^n0
 where
n0 = 5 if ('A', 'B') is 1 of 6 possibilities mod 4
     4 if ('A', 'B') is 1 of 3 possibilities mod 4
     3 if ('A', 'B') is 1 of 36 possibilities mod 16
     0 if ('A', 'B') is 1 of 24 possibilities mod 32
     1 if ('A', 'B') is 1 of 24 possibilities mod 32
sage: N.left().right()
5 if ('A', 'B') is 1 of 6 possibilities mod 4
4 if ('A', 'B') is 1 of 3 possibilities mod 4
3 if ('A', 'B') is 1 of 36 possibilities mod 16
0 if ('A', 'B') is 1 of 24 possibilities mod 32
1 if ('A', 'B') is 1 of 24 possibilities mod 32
sage: N.left().right()[1]
(4, The condition that ('A', 'B') == (0, 3), (1, 0), (3, 1) \
mod 4)
```

For more examples see the examples listed in Table 3.1

Section 1.7

Comparison to other methods

Among papers where Frey curves are used there are different approaches to computing the conductor of these Frey curves. Some papers such as [Dar93] and [DM97] simply claim they applied Tate's algorithm, indicating they probably did the computation by hand. A small mistake in [DM97] – as pointed out in the framework [vL21a] example `Darmon-Merel-1997.rst` – shows this can be error prone. Other papers use more automated approaches to compute the conductor. We shall compare these other approaches to the framework [vL21a] based on the theory in this Chapter.

Subsection 1.7.1

Papadopoulos' tables

In [Pap93] Papadopoulus presented tables that can be used to determine the result of Tate's algorithm for an elliptic curve E based on the valuation of c_4, c_6 and Δ. One could use these tables to 'read off' the conductor of a Frey curve, presenting an alternative approach to the algorithm presented in this chapter. There are some caveats to this approach as we will discuss here.

First of all it should be noted that the tables in [Pap93] are not conclusive based on the valuation of c_4, c_6 and Δ alone. For some cases additional criteria are introduced to distinguish between results. These are often not as easy to determine as the valuation of c_4, c_6 and Δ. For example for a prime of characteristic 2 one has to distinguish between a case that ends in Step 6 and one that ends in Step 7 of Tate's algorithm. To do this [Pap93] presents the following check.

1. Check if there is an r such that $v(b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4) \geq 5$. If there is none we end in Step 6.

2. Find a t such that $v(a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1) \geq 3$.

3. Determine $v(a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1)$ precisely. If it is 3 we end in Step 6, otherwise in Step 7.

Such conditions can be difficult to check by hand for a Frey curve. They arise from the transformations needed in Tate's algorithm. Since the framework [vL21a] takes care of these transformations during Tate's algorithm, it does not have to check such existence statements. Furthermore the supplementary conditions necessary for the subcases of Step 7 are indicated in the table, but not actually provided in the mentioned section. They could though be inferred from the later sections, such as Proposition 1 in Section III.

Another disadvantage of Papadopoulos' tables is that it can only compute the conductor for a minimal model of an elliptic curve. If the elliptic curve is not minimal it does conclude so, but can not present a minimal model. In contrast Tate's algorithm will transform the curve into a minimal model to compute the conductor. This is especially relevant for Frey curves, as the minimal model might depend on the value of the parameters. The framework [vL21a] automatically creates the minimal model for each prime and can also give the minimal models if needed.

It should also be noted that the tables in [Pap93] contain at least one error, as pointed out in [Dah08, Appendix A].

Overall 'reading off' Papadopoulos's tables can be quite tedious, especially in the case $v(2) > 1$ where the table has many different cases. One could try to automate this 'lookup' process, but this would require a program that computes $v(c_4)$, $v(c_6)$, $v(\Delta)$ and all the necessary additional conditions. Besides the fact that these calculations might not be finite, as $v(c_4)$, $v(c_6)$ and $v(\Delta)$ are not necessarily all bounded, this seems like more computational work than doing Tate's algorithm itself. Therefore the implementation presented in this chapter seems to be a more efficient automated approach.

It should be noted that there are cases in which the tables in [Pap93] are indeed a good approach. For example in [Kra98] it is used to determine the conductor of a Frey curve as the valuation of c_4, c_6 and the discriminant could be determined from the related Diophantine equation. In general this 'lookup' method can be used as a check on a conductor computed by other means.

Subsection 1.7.2

Chen's approach

In [Che10], [Che12], [BC12], and [BCDY14] another method of automating Tate's algorithm is presented. As this method was first introduced by Imin Chen in [Che10] and he worked on all these papers, we will call this Chen's approach. Chen's approach works roughly as follows.

- Determine a high enough power n of a prime $\mathfrak{p}$ such that the conductor exponent at $\mathfrak{p}$ only depends on the Weierstrass coefficients modulo $\mathfrak{p}^n$.
- Compute the conductor of the elliptic curves in a set of representatives for the parameters modulo $\mathfrak{p}^n$.

In most papers using Chen's approach the first step is a lemma stating two curves have the same reduction type if their coefficients are congruent modulo a sufficiently high power. Examples of such lemmas include Lemma 5 in [BC12], Lemma 30 and 31 in [Che10], and Lemma 9 in [Che12]. In these lemmas it is assumed that the reduction type of one of the two curves is already known. The proof is going through Tate's algorithm for both curves simultaneously, and noting that the decisions in each step are the same for the second curve with congruent coefficients.

In [BCDY14] the most general version of this kind of lemma is claimed in Lemma 2.1. It is stated there that for two elliptic curves

$$\begin{aligned} E &: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \\ E' &: Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6' \end{aligned}$$

if there is a $k > 0$ such that $v(a_i - a_i') \geq ik$ for all i and the discriminants of E and E' satisfy

$$\max\left\{v\left(\Delta_E\right), v\left(\Delta_{E'}\right)\right\} \leq 12k,$$

then their reduction type is the same or both have a reduction type I_m^* for some $m > 2$. However the result as stated is false as the two curves

$$\begin{aligned} E &: Y^2 &&= X^3 + X^2 + 1 \\ E' &: Y^2 + 2XY &&= X^3 + X^2 + 1 \end{aligned}$$

do not have the same reduction type at 2 but satisfy the other criteria. In fact performing Tate's algorithm on two curves simultaneously will yield a result where $v(a_i - a_i') \geq ik$ is replaced by $v(a_i - a_i') \geq nk$ for some n independent of i. Here n will most likely be 6.

This first step is the main disadvantage of Chen's approach compared to the framework [vL21a]. The second step requires Tate's algorithm to be performed roughly $(\#\mathfrak{p})^{mn}$ times, where m is the number of parameters, so the lemma for the first step has to be chosen such that this computation is still feasible. To do this, one effectively has to know what the outcome of Tate's algorithm will be for your Frey curve beforehand, with the final computation serving only as a proof of correctness. Although results like Lemma 2.1 in [BCDY14] would give bounds if one knows an upper bound on the discriminant, these bounds might not be feasible in practice. Therefore Chen's approach is not truly an automated approach like the framework [vL21a] is. When the first step can be provided, as in [Che10], [Che12], [BC12], and [BCDY14], Chen's approach is quite a good solution as it requires no new implementation of Tate's algorithm.

To see how Chen's approach compares to the framework [vL21a] in terms of efficiency, we timed some computations on the Frey curves in [Che10], [Che12], [BC12], and [BCDY14]. The results are collected in Table 1.1. We see that in most cases Tate's algorithm as implemented in the framework [vL21a] is considerably faster than Chen's approach. Note that both algorithms need to perform each step of Tate's algorithm with representatives of the parameters modulo some sufficiently high power of the chosen prime. However the framework [vL21a] adapts what power is sufficiently high for each step whereas Chen's approach chooses an upper bound on this power beforehand. Therefore the framework [vL21a] actually does less computational work for most steps as compared to Chen's approach.

The notable exception to this is the case for the curve E_β from [BC12] at a prime $\mathfrak{p}_2$ above 2. Here there is a case in which the curve is not minimal and we have to do step 6 a second time. In this step one has to compute whether a certain polynomial $P(T)$ in the coefficients of the curve has a double root modulo $\mathfrak{p}_2$. The framework [vL21a] does this by checking the valuation of the discriminant of P which requires computing with the parameters modulo $\mathfrak{p}_2^{19}$. However looking at the polynomial $P(T)$ modulo $\mathfrak{p}_2$ one can see that it is already uniquely determined by the value of the parameters modulo a much smaller power of $\mathfrak{p}_2$. This is precisely what happens in the bound chosen by Chen's approach, hence that method is faster in this particular case.

Note that in fact in most of the steps of Tate's algorithm we are computing the valuation of the discriminant of some polynomial. Therefore it might be possible to compute with the parameters modulo a smaller power of the chosen prime by looking whether the corresponding polynomial has a double root instead. Note however that this is a check of type 2 rather than one of type 1, as described in Section 1.2, meaning we do not have an efficient algorithm besides trying all the options. For most use cases the check of type 1 still seems to be the fastest option.

It should be remarked that in most use cases time only plays a role in the sense that the computation is still feasible. One often only computes the conductor of a Frey curve once, so it is just important that this computation does not take weeks. However when experimenting with curves a faster time could be very desirable, e.g. when comparing conductors of many different Frey curves associated with a Diophantine equation.

Computation times

Table 1.1 contains the computation times of conductor exponents using both Chen's approach and the framework [vL21a]. All Frey curves for which these are done are taken from the articles [Che10], [Che12], [BC12], and [BCDY14] and denoted like they are in the corresponding article. The primes are taken in the appropriate field and by $\mathfrak{p}_p$ we denote a prime above p.

The time of the original Magma [BCP97] code can be found in the column named “Magma”. For the curves in [BCDY14] no code was explicitly linked to in the article. The time in the column “Magma” for these curves corresponds to Magma code found in `ChenMethod.m`, which resembles the Magma code for the other curves. The time of a simple implementation of Chen’s approach in SageMath [Sag20] can be found in the column “SageMath”. The time of the framework [vL21a] is listed in the column “framework”.

All computations have been performed on an AMD Ryzen 7 3700x processor (3.6 GHz) using Magma [BCP97] version 2.25-7 and SageMath [Sag20] version 9.1. The SageMath code to time the SageMath and framework examples can be found in `ChenMethod.sage`. The original code can be found on Imin Chen’s website.

			Chen's approach		
article	curve	prime	Magma	SageMath	framework
[Che10]	E^s_β	$\mathfrak{p}_2$	70 ms	642 ms	450 ms
		$\mathfrak{p}_3$	1.84 s	57.3 s	716 ms
		$\mathfrak{p}_5$	240 ms	216 ms	113 ms
[Che10]	E^t_β	$\mathfrak{p}_2$	80 ms	623 ms	448 ms
		$\mathfrak{p}_3$	1.2 s	57 s	727 ms
		$\mathfrak{p}_5$	110 ms	213 ms	107 ms
[Che12]	E_β	$\mathfrak{p}_2$	410 ms	431 ms	1.41 s
		$\mathfrak{p}_3$	950 ms	7.2 s	147 ms
[BC12]	E_β	$\mathfrak{p}_2$	230 ms	4.09 s	6 min 6s
		$\mathfrak{p}_3$	750 ms	7.45 s	148ms
[BC12]	E'	2	30 ms	108 ms	15.3 ms
		3	630 ms	2.19 s	33.4 ms
[BCDY14]	E_1 case c odd	2	380 ms	862 ms	22.5 ms
		3	2 min 4s	2 min 33s	11.3 ms
[BCDY14]	E_2 case c odd	$\mathfrak{p}_2$	30 ms	238 ms	28 ms
[BCDY14]	E_1 case c even	2	330 ms	832 ms	13.3 ms
			390 ms	839 ms	20.5 ms
		3	1 min 49 s	2min 32s	10.8 ms
			2 min 24 s	2min 32s	40.9 ms
[BCDY14]	E_2 case c even	$\mathfrak{p}_2$	30 ms	434 ms	40.9 ms
			30 ms	386 ms	38 ms
[BCDY14]	E_3 case c even	$\mathfrak{p}_2$	30 ms	397 ms	38.4 ms
			40 ms	396 ms	37.7 ms

Table 1.1: Computation times of the conductor exponent using Chen's approach and the framework [vL21a].

Chapter 2

$\mathbb{Q}$-curve computations

A particular type of elliptic curves that can be used for the modular method is formed by $\mathbb{Q}$-curves. In [Rib04] Ribet proved that $\mathbb{Q}$-curves without complex multiplication are modular, based on the now proven Serre conjectures. In particular there are classical modular forms associated with non-CM $\mathbb{Q}$-curves, which can be computed through various computer algebra packages. The $\mathbb{Q}$-curves with complex multiplication were already known to be modular before, see e.g. [Shi71].

In this chapter we will discuss the basic theory of $\mathbb{Q}$-curves without complex multiplication. Most of this theory is obtained directly from the article [Que00] by Quer and the original article [Rib04] by Ribet. We will however focus on the computational aspect, where we describe the process which in the end computes the newforms associated with a (Frey) $\mathbb{Q}$-curve. All this computational work has been implemented in the framework [vL21a]. Throughout this chapter we mention the relevant methods, functions, and classes in the framework [vL21a] when new theory is introduced. Most of the examples in this chapter also contain explicit code examples that show how to perform the relevant computations in practice.

Besides new algorithmic results, this chapter also introduces some new theoretical results. This includes Proposition 2.5.3, Proposition 2.5.5, and the results from Section 2.10. Proposition 2.11.1 can also be considered new, although it is mostly an extension of Proposition 3.2 in [Ell04].

After a general introduction to $\mathbb{Q}$-curves in Section 2.1 the first few sections focus on associating an abelian variety of GL_2-type to a $\mathbb{Q}$-curve. Section 2.2 introduces the relevant algebra of the restriction of scalars of a $\mathbb{Q}$-curve and relates an associated abelian variety of GL_2-type to a splitting map. Section 2.3 then discusses how a splitting map could be computed from a splitting character. Section 2.4 shows what local constraints define a splitting character of a $\mathbb{Q}$-curve. Section 2.5 discusses the final adjustments necessary to turn the corresponding map into a splitting map. Section 2.6 then discusses the different splitting maps associated to a $\mathbb{Q}$-curve and which splitting maps may relate to the same abelian variety of GL_2-type. Finally Section 2.7 presents some results about the different fields that play a role in this theory.

The last sections of this chapter are about the Galois representations and newforms associated with $\mathbb{Q}$-curves. Section 2.8 introduces the Galois representations associated with the abelian varieties of GL_2-type associated with a $\mathbb{Q}$-curve. Section 2.9 uses these Galois representations to find the level of newforms associated with a $\mathbb{Q}$-curve. Section 2.10 shows how to compute the traces of these Galois representations at Frobenius elements. Finally Section 2.11 gives a result that can be used to show these Galois representations are irreducible for some families of $\mathbb{Q}$-curves.

Section 2.1

Generic properties of $\mathbb{Q}$-curves

We will start with the definition of a $\mathbb{Q}$-curve.

Definition 2.1.1. A $\mathbb{Q}$-*curve* is an elliptic curve E defined over $\overline{\mathbb{Q}}$ such that each Galois conjugate of E is isogenous to E.

Remark 2.1.2. Throughout this chapter, whenever we talk about a $\mathbb{Q}$-curve E we assume it comes with a choice of isogenies $\phi_\sigma : {}^\sigma E \to E$ for $\sigma \in G_\mathbb{Q}$. Unless explicitly stated the choice of isogenies does not matter.

To work with a $\mathbb{Q}$-curve on a computer we need to store both a defining Weierstrass equation and a choice of corresponding isogenies ϕ_σ. Since the Weierstrass coefficients of a $\mathbb{Q}$-curve are algebraic, we can always find a Galois number field K over which the curve is defined. In this case we can choose our isogenies ϕ_σ so they only depend on $\sigma \in G_\mathbb{Q}^K$, so only a finite amount of them have to be stored. Note that they may still be defined over a larger field than K. What follows is a result summarising the necessary data of an isogeny.

Proposition 2.1.3. *Let E_1, E_2 be elliptic curves over a field K with respective Weierstrass equations $f_1(x, y) = 0$ and $f_2(x, y) = 0$. Let $\phi : E_1 \to E_2$ be an isogeny over $\overline{K}$.*

- *We have $\phi(x, y) = (F(x), G(x)y + H(x))$ outside points in the kernel of ϕ for some $F(x), G(x), H(x) \in \overline{K}(x)$.*
- *The degree of ϕ is equal to the degree of the numerator of F.*

- *There exists a* $\lambda \in \overline{K}$ *such that* $\phi^*\omega_2 = \lambda\omega_1$*, where* $\omega_i = \frac{dx}{\frac{\partial f_i}{\partial y}(x,y)}$ *is the invariant differential of* E_i*.*
- *The associated* $\lambda \in \overline{K}$ *satisfies*

$$\lambda \frac{\partial f_2}{\partial y}(F(x), G(x)y + H(x)) = F'(x)\frac{\partial f_1}{\partial y}(x,y). \tag{2.1}$$

Proof. Note that for both elliptic curves we have a morphism $x : E_i \to \mathbb{P}^1$ given by the x-coordinate. This is in fact the quotient map when we associate a point P with its additive inverse $-P$. We know that $\phi(-P) = -\phi(P)$ as ϕ is an isogeny, so ϕ factors as

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "x"] & E_2 \arrow[d, "x"] \\ \mathbb{P}^1 \arrow[r, "F"] & \mathbb{P}^1 \end{tikzcd}$$

over $\overline{K}$. Note that the only point mapping to the point at infinity in $\mathbb{P}^1$ under x is the point at infinity of E_2, so outside x-coordinates of points mapping to $O \in E_2$ under ϕ, the morphism F is a rational map. Since the map x has degree 2, we see that the function field of E_2 is of the form $K(x)[y]/(f_2(x,y))$ where $f_2(x,y)$ is a quadratic polynomial in y. Therefore rational functions on E_2 are always of the form $G(x)y + H(x)$ for some $G(x), H(x) \in \overline{K}(x)$. These facts combined prove that ϕ is indeed of the given form outside points mapping to $O \in E_2$.

Note that by the multiplicativity of degrees we find that

$$2\deg(\phi) = \deg(x)\deg(\phi) = \deg(F)\deg(x) = 2\deg(F).$$

The degree of F is easily determined by determining the number of points that map to $0 \in \mathbb{P}^1$ counting multiplicity. This is equal to the degree of the numerator of $F(x)$ as ∞ is mapped to ∞.

We know that $\phi^*\omega_2 = \lambda\omega_1$ for some $\lambda \in \overline{K}(E_1)$ as Ω_{E_1} is 1-dimensional over $\overline{K}(E_1)$. Now note that

$$\operatorname{div}\lambda = \operatorname{div}(\phi^*\omega_2) - \operatorname{div}\omega_1 = \phi^*\operatorname{div}(\omega_2) - 0 = 0,$$

hence $\lambda \in \overline{K}$.

Now let x_i, y_i be coordinates for E_i, then the invariant differential of E_i is

$$\omega_i = \frac{dx_i}{\frac{\partial f_i}{\partial y_i}(x_i, y_i)}.$$

It follows that

$$\begin{aligned}\lambda\frac{\partial f_2}{\partial y_2}(F(x_1), G(x_1)y_1 + H(x_1))\omega_1 &= \phi^*\left(\frac{\partial f_2}{\partial y_2}(x_2, y_2)\,\omega_2\right) = \phi^*(dx_2)\\ &= dF(x_1) = F'(x_1)dx_1\\ &= F'(x_1)\frac{\partial f_1}{\partial y_1}(x_1, y_1)\omega_1,\end{aligned}$$

proving the last formula. □

Note that Equation (2.1) implies that in characteristic $\neq 2$ the rational map $F(x)$ and the invariant λ are sufficient to fix the entire isogeny. Therefore there are three different ways in the framework [vL21a] to define an isogeny ϕ_σ for a $\mathbb{Q}$-curve.

1. As a SageMath isogeny object.
2. As a triple of rational maps $(F(x), G(x), H(x))$ as presented in the first point of Proposition 2.1.3.
3. As a tuple $(F(x), \lambda)$ where $F(x)$ is the same rational map as in the previous way and λ is the constant mentioned in the third point of Proposition 2.1.3.

In the framework [vL21a] $\mathbb{Q}$-curves are represented by the class `Qcurve` provided in `modular_method.elliptic_curves.Qcurves`. To make an instance of `Qcurve` one has to provide either an elliptic curve or the same data that would make an elliptic curve with the constructor `EllipticCurve`. This curve should be defined over a number field K which will be replaced by a Galois closure if it is not Galois over $\mathbb{Q}$. A choice of isogenies should be provided as the argument `isogenies`. This should be a dictionary with $\sigma \in G_{\mathbb{Q}}^K$ as keys and isogenies $E \to {}^\sigma E$ as values. The isogenies should be given as described by one of the choices of data above. Note that an entry for each generator of $G_{\mathbb{Q}}^K$ suffices as the framework [vL21a] can infer an isogeny for $\sigma\tau$ from the one for σ and the one for τ. Furthermore it will always take the isogeny for the $1 \in G_{\mathbb{Q}}^K$ to be the identity. Internally all the isogenies are stored as the maps $F(x)$ and $G(x)y + H(x)$ as presented in Proposition 2.1.3.

Rather than providing isogenies explicitly, one can also provide possible degrees of isogenies through the argument `guessed_degrees`. If the framework [vL21a] has insufficient isogeny data from `isogenies` to construct all isogenies it will look among this list. For each positive integer d in `guessed_degrees` it will then construct all isogenies of degree d with domain E. If the image of such an isogeny is isomorphic to a Galois conjugate of E, it is combined with the corresponding isomorphism and added to the list of isogenies. This is the easiest way to provide isogenies, but offers the least control over the actual isogenies used.

Note that in the framework [vL21a] the isogenies $E \to {}^{\sigma}E$ are stored whereas in the theory in this chapter we will always consider isogenies $\phi_\sigma : {}^{\sigma}E \to E$. We shall see in Section 2.10 why it is useful to store this information instead. Whenever we want to compute data from the isogenies ϕ_σ we shall make a remark of how to do so from the isogenies $E \to {}^{\sigma}E$ instead.

The module `modular_method.elliptic_curves.frey_curves` offers the class `FreyQcurve` representing a $\mathbb{Q}$-curve that is also a Frey curve. This class works similar to the class `FreyCurve` explained in Section 1.6.6, except that it also keeps track of the $\mathbb{Q}$-curve structure. One should therefore also supply isogeny data to its constructor similar as with the constructor of `Qcurve`. One other difference is the newforms produced by the method `newform_candidates` as they will reflect the $\mathbb{Q}$-curve modularity instead. This will be further explained in Section 3.1.

Example 2.1.4. `Qcurve1.rst` `Qcurve1Frey.rst` Look at the elliptic curve

$$E : Y^2 = X^3 + 12\,X^2 + 18\left(1 + \sqrt{3}\right)X.$$

Using the 2-isogeny described in Example 4.5 of [Sil09, III.4] we see that E is 2-isogenous to

$$E' : Y^2 = X^3 - 24\,X^2 + 72\left(1 - \sqrt{3}\right)X.$$

Note that E' is isomorphic to the Galois conjugate of E over $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$, hence E is a $\mathbb{Q}$-curve. We can put this $\mathbb{Q}$-curve in the framework [vL21a] by only specifying the degree of the isogeny.

```
sage: _.<sqrt3> = QuadraticField(3)
sage: E = Qcurve([0, 12, 0, 18*(1 + sqrt3), 0],
....:             guessed_degrees=[2]); E
Q-curve defined by y^2 = x^3 + 12*x^2 + (18*sqrt3+18)*x over \
Number Field in sqrt3 with defining polynomial x^2 - 3 with \
sqrt3 = 1.732050807568878?
```

The curve E is part of the larger family of $\mathbb{Q}$-curves

$$E : Y^2 = X^3 + 12\,aX^2 + 18\left(a^2 + b\sqrt{3}\right)X,$$

parameterised by coprime $a, b \in \mathbb{Z}$. Since the discriminant of this curve is equal to $2^9 \cdot 3^6(a^2 - b\sqrt{3})(a^2 + b\sqrt{3})^2$, this is actually a Frey curve for the Diophantine equation

$$(a^2 - b\sqrt{3})(a^2 + b\sqrt{3}) = a^4 - 3b^2 = c^l \quad \text{with } c, l \in \mathbb{Z} \text{ and } l > 0 \text{ prime.}$$

As with the case $a = b = 1$ there is a 2-isogeny, so we can enter this Frey $\mathbb{Q}$-curve in the framework [vL21a] as follows.

```
sage: R.<a, b> = QQ[]
sage: _.<sqrt3> = QuadraticField(3)
sage: con = CoprimeCondition([a, b])
sage: E = FreyQcurve([0, 12*a, 0, 18*(a^2 + b*sqrt3), 0],
....:                 condition=con, guessed_degrees=[2]); E
Frey Q-curve defined by y^2 = x^3 + 12*a*x^2 + \
(18*a^2+(18*sqrt3)*b)*x over Number Field in sqrt3 with \
defining polynomial x^2 - 3 with sqrt3 = 1.732050807568878? \
with parameters (a, b)
```

Throughout this chapter there are multiple examples where these curves return. Unless explicitly stated it does not matter whether the curve E refers to the explicit curve at the start or the Frey curve introduced later, as the theory is all the same. Similarly in the framework [vL21a] all code examples work on both the `Qcurve E` and the `FreyQcurve E` with the same output, unless otherwise stated.

Note that since the isogeny class of a $\mathbb{Q}$-curve E is defined over $\mathbb{Q}$, so is its reduction behaviour.

Proposition 2.1.5. *Let $\phi : E \to E'$ be an isogeny defined over K with E and E' elliptic curves. If E has good (respectively split multiplicative, non-split multiplicative, or additive) reduction at a finite prime $\mathfrak{p}$ of K, then E' also has good (respectively split multiplicative, non-split multiplicative, or additive) reduction at $\mathfrak{p}$.*

Proof. This can be derived from the fact that an isogeny (on a Néron model) must map a singular point to a singular point and tangent lines to tangent lines. It can also be obtained from Table 1 in [DD15]. □

Corollary 2.1.6. *Let E be a $\mathbb{Q}$-curve defined over a Galois number field K for which the isogenies ϕ_σ are also defined over K. If E has good (respectively* *split multiplicative, non-split multiplicative, or additive) reduction at a prime $\mathfrak{p}$ of K above a prime number p, then E has good (respectively split multiplicative, non-split multiplicative, or additive) reduction at all primes above p.*

Definition 2.1.7. For a $\mathbb{Q}$-curve E defined over K for which all isogenies ϕ_σ are also defined over K, we will say that E is *completely defined* over K.

For a $\mathbb{Q}$-curve E completely defined over a Galois number field K we will say it has good (respectively split multiplicative, non-split multiplicative, or additive) reduction at a prime number p (with respect to K) if it has this type of reduction at any (hence all) primes of K above p.

Most important to us is that $\mathbb{Q}$-curves are modular. The way this modularity works depends on whether the curve has complex multiplication. We focus here on $\mathbb{Q}$-curves without complex multiplication for which modularity follows in two steps. For modularity of $\mathbb{Q}$-curves with complex multiplication we refer the reader to [Shi71].

Definition 2.1.8. An abelian variety A over $\mathbb{Q}$ is called of GL_2-type if the algebra $\mathrm{End}^0_{\mathbb{Q}} A := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{\mathbb{Q}} A$ contains a number field of degree $\dim A$.

Theorem 2.1.9 (Theorem 6.1 in [Rib04])**.** *Every $\mathbb{Q}$-curve without complex multiplication is the quotient over $\overline{\mathbb{Q}}$ of a $\mathbb{Q}$-simple abelian variety of GL_2-type.*

Theorem 2.1.10 (Theorem 4.4 in [Rib04] using the proven Serre conjectures)**.** *Every $\mathbb{Q}$-simple abelian variety A of GL_2-type is isogenous to the abelian variety associated to a classical newform $f \in \mathcal{S}_2(\Gamma_1(N))$ for some level N, i.e. A is isogenous to a quotient of $J_1(N)$.*

In this chapter we will work out these theorems in more detail such that we can compute the corresponding data algorithmically. In particular we discuss how to compute particular properties of the abelian variety mentioned in Theorem 2.1.9, and we explicitly determine the level and character of the associated newform in Theorem 2.1.10.

Throughout this chapter E will always denote a $\mathbb{Q}$-curve without complex multiplication unless explicitly stated otherwise.

Section 2.2

The algebra associated to a $\mathbb{Q}$-curve

We will start by determining how we could construct the abelian variety of GL_2-type mentioned in Theorem 2.1.9.

Suppose that E is the quotient over some number field K of a $\mathbb{Q}$-simple abelian variety A. In that case we know that A must be isogenous to a subvariety of the restriction of scalars $B = \operatorname{Res}_{\mathbb{Q}}^{K} E$. It is well known that in that case there must be some abelian subvariety A' of B such that B is isogenous to $A \times A'$. If there are no non-trivial isogenies between A and A' – which happens exactly when A is not isogenous to a $\mathbb{Q}$-simple factor of A' – we see that $\operatorname{End}_{\mathbb{Q}}^0 B \cong \operatorname{End}_{\mathbb{Q}}^0 A \times \operatorname{End}_{\mathbb{Q}}^0 A'$ and we have a surjective $\mathbb{Q}$-algebra homomorphism $\beta : \operatorname{End}_{\mathbb{Q}}^0 B \to \operatorname{End}_{\mathbb{Q}}^0 A$.

Conversely given any $\mathbb{Q}$-algebra R and a surjective $\mathbb{Q}$-algebra homomorphism $\beta : \operatorname{End}_{\mathbb{Q}}^0 B \to R$, we know that $\operatorname{End}_{\mathbb{Q}}^0 B \cong \ker \beta \times R$ as $\operatorname{End}_{\mathbb{Q}}^0 B$ is semisimple. Therefore there is a $\pi \in \operatorname{End}_{\mathbb{Q}}^0 B$ corresponding to $(0, 1) \in \ker \beta \times R$, so in particular $\pi^2 = \pi$ and $\pi \operatorname{End}_{\mathbb{Q}}^0 B \cong R$. Note that the projection π defines an abelian subvariety A of B with $\operatorname{End}_{\mathbb{Q}}^0 A \cong R$ up to isogeny, by taking $A = (n\pi)(B)$ for $n \in \mathbb{Q}^*$ such that $n\pi \in \operatorname{End}_{\mathbb{Q}} B$. Furthermore as A is a subvariety of B over $\mathbb{Q}$ it will have E as a quotient over K.

Note that we have the following result

Theorem 2.2.1 (part of Theorem 2.1 in [Rib04])**.** *Let A be an abelian variety of GL_2-type over $\mathbb{Q}$, then the following are equivalent.*

1. *$A/\mathbb{Q}$ is simple.*

2. *$\operatorname{End}_{\mathbb{Q}}^0 A$ is a number field of degree $\dim A$.*

Therefore to construct the abelian variety from Theorem 2.1.9 it suffices to find a $\mathbb{Q}$-algebra homomorphism $\beta : \operatorname{End}_{\mathbb{Q}}^0 B \to L$ with L a number field. For our purposes we want to compute this map explicitly, so we will study the structure of $\operatorname{End}_{\mathbb{Q}}^0 B$ in detail.

Take $B = \operatorname{Res}_{\mathbb{Q}}^{K} E$ for some Galois number field K over which E is completely defined. By the properties of the restriction of scalars we have that

$$\begin{aligned}\operatorname{End}_{\mathbb{Q}} B = \hom_K(B_K, E) &= \hom_K\left(\prod_{\sigma \in G_{\mathbb{Q}}^{K}} {}^{\sigma}E, E\right) \\ &= \bigoplus_{\sigma \in G_{\mathbb{Q}}^{K}} \hom_K({}^{\sigma}E, E)\end{aligned}$$

Note that $\mathbb{Q} \otimes_{\mathbb{Z}} \hom_K({}^{\sigma}E, E)$ can be seen as a module over $\operatorname{End}_K^0 E = \mathbb{Q}$ with basis $\{\phi_\sigma\}$. This shows that $\operatorname{End}_{\mathbb{Q}}^0 B$ is a $\mathbb{Q}$-algebra generated by the ϕ_σ. For any $\sigma, \tau \in G_{\mathbb{Q}}^{K}$ the product of ϕ_σ and ϕ_τ is given by $\phi_\sigma {}^{\sigma}\phi_\tau$ as an element of $\hom_K({}^{\sigma\tau}E, E)$. Furthermore we have

$$\phi_\sigma {}^{\sigma}\phi_\tau = c_E(\sigma, \tau)\phi_{\sigma\tau},$$

for some $c_E(\sigma, \tau) \in (\operatorname{End}_K^0 E)^* = \mathbb{Q}^*$.

This discussion shows that all the information about $\operatorname{End}_{\mathbb{Q}}^0 B$ is encoded in the map $c_E : \left(G_{\mathbb{Q}}^{K}\right)^2 \to \mathbb{Q}^*$, which is defined by

$$c_E(\sigma, \tau) = \phi_\sigma {}^{\sigma}\phi_\tau \phi_{\sigma\tau}^{-1} \in \operatorname{End}_K^0 E = \mathbb{Q}, \tag{2.2}$$

where $\phi_{\sigma\tau}^{-1} = \frac{1}{\deg \phi_{\sigma\tau}} \widehat{\phi_{\sigma\tau}}$. A simple calculation shows that the map c_E is a 2-cocycle and its cohomology class $\xi_E = [c_E] \in H^2\left(G_{\mathbb{Q}}^{K}, \mathbb{Q}^*\right)$ in fact does not depend on the choice of isogenies ϕ_σ. Note that we can define c_E over $G_{\mathbb{Q}}^2$ and that its cohomology class ξ_E is in this case also invariant under replacing the curve E by an isogenous curve over $\overline{\mathbb{Q}}$. Another simple computation shows that any two $\mathbb{Q}$-algebras generated by $G_{\mathbb{Q}}^{K}$ with multiplication given by distinct choices of cocycles in ξ_E are isomorphic, hence $\operatorname{End}_{\mathbb{Q}}^0 B$ is also independent of these changes.

To compute c_E explicitly we may choose any Galois field K over which E is completely defined and compute c_E on $(G_{\mathbb{Q}}^{K})^2$ using an explicit choice of isogenies. An easier way to do this computation is to use for every isogeny ϕ_σ the constant $\lambda_\sigma \in \overline{\mathbb{Q}}^*$ presented in Proposition 2.1.3 such that

$$\phi_\sigma^*(\omega) = \lambda_\sigma {}^{\sigma}\omega,$$

where ω is the invariant differential of E. Note that the constant associated to a composition of isogenies is just the product of the individual constants and that the constant of the multiplication by n map is just n. Therefore we find that

$$c_E(\sigma, \tau) = \lambda_\sigma {}^{\sigma}\lambda_\tau \lambda_{\sigma\tau}^{-1} \quad \text{for all } \sigma, \tau \in G_{\mathbb{Q}}.$$

The last part of Proposition 2.1.3 shows it is easy to compute the λ_σ from the other isogeny data.

Remark 2.2.2. The isogenies $E \to {}^{\sigma}E$ stored by the framework [vL21a] can be seen as the dual of the isogenies ϕ_σ. A quick computation then shows that the λ_σ associated to these dual isogenies also satisfy the same equation with c_E. Therefore we can compute c_E from the stored isogenies by computing these scalars for each isogeny first.

In the framework [vL21a] one can easily compute c_E using the method `c` of a `Qcurve` object. This method accepts two arguments which should both be Galois homomorphisms σ, τ from the Galois group of a complete definition field or its Galois closure if it is not Galois over $\mathbb{Q}$. It then returns the rational number that is $c_E(\sigma, \tau)$. As mentioned these are computed from the scalars λ_σ associated with the isogenies. The method `isogeny_scalar` provides these scalars for a given Galois homomorphism. As remarked these are the scalars of the isogenies stored, which are the dual of the isogenies ϕ_σ we talk about here.

Using the description of the algebra $\operatorname{End}^0_{\mathbb{Q}} B$ in terms of c_E we can describe a $\mathbb{Q}$-algebra homomorphism $\operatorname{End}^0_{\mathbb{Q}} B \to L$ for some number field L simply by defining a map $\beta : G^K_{\mathbb{Q}} \to L^*$ that satisfies

$$\beta(\sigma)\beta(\tau) = c_E(\sigma, \tau)\beta(\sigma\tau) \text{ for all } \sigma, \tau \in G^K_{\mathbb{Q}} \tag{2.3}$$

and extending linearly. Such a map is called a *splitting map for c_E*. We define a splitting map for a general 2-cocycle $c : (G^K_{\mathbb{Q}})^2 \to \mathbb{Q}^*$ similarly. We will also talk about splitting maps for cohomology classes, in which case we mean a splitting map for any representative 2-cocycle of that cohomology class. Note that as with c_E we might as well forget about K and let β be a continuous map $G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ instead. In that case the field $L_\beta := \mathbb{Q}(\beta(\sigma) : \sigma \in G_{\mathbb{Q}})$ is called the *splitting image field* of such a splitting map, and we say β is *defined over a Galois number field K* if it factors over $G^K_{\mathbb{Q}}$. As mentioned before such maps β induce abelian varieties of GL_2-type A with endomorphism algebra $\operatorname{End} A \otimes \mathbb{Q} \cong L_\beta$ and dimension $[L_\beta : \mathbb{Q}]$. These are precisely the varieties as mentioned in Theorem 2.1.9, hence we would like to compute candidates for these splitting maps explicitly.

Example 2.2.3. `Qcurve1.rst` `Qcurve1Frey.rst` We continue with Example 2.1.4. The curve E is completely defined over the field $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$. To denote elements of the Galois group of $K/\mathbb{Q}$ we will write σ_2 and σ_3 for the generators of $G^K_{\mathbb{Q}(\sqrt{-2})}$ and $G^K_{\mathbb{Q}(\sqrt{3})}$ respectively. Using the framework [vL21a] we now compute the scalars corresponding to the isogenies.

```
sage: K = E.complete_definition_field()
sage: sqrtm2, sqrt3 = sqrt(K(-2)), sqrt(K(3))
sage: G = K.galois_group()
sage: s2 = next(s for s in G if s != G(1) and
....:             s(sqrtm2) == sqrtm2)
sage: s3 = next(s for s in G if s != G(1) and s(sqrt3) == sqrt3)
```

```
sage: (E.isogeny_scalar(G(1)) == 1 and
....:  E.isogeny_scalar(s2) == sqrtm2 and
....:  E.isogeny_scalar(s3) == 1 and
....:  E.isogeny_scalar(s2*s3) == sqrtm2)
True
```

Note that these are the scalars of the dual isogenies to ϕ_σ. To obtain the scalars discussed here we divide the degree of these isogenies by the scalar and get

$$\lambda_\sigma = \begin{cases} 1 & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{3})} \\ -\sqrt{-2} & \text{if } \sigma \notin G_{\mathbb{Q}(\sqrt{3})}. \end{cases}$$

From this we can compute the map c_E on $G_{\mathbb{Q}}^K$. We show the input for the framework [vL21a] here, but present the output as a formatted table instead.

```
sage: matrix([[E.c(s, t)
....:           for t in [G(1), s2, s3, s2*s3]]
....:          for s in [G(1), s2, s3, s2*s3]])
```

$c(\sigma, \tau)$	1	σ_2	σ_3	$\sigma_2\sigma_3$
1	1	1	1	1
σ_2	1	-2	1	-2
σ_3	1	-1	1	-1
$\sigma_2\sigma_3$	1	2	1	2

This table shows that the endomorphism algebra $\operatorname{End}_{\mathbb{Q}}^0 B$ of $B = \operatorname{Res}_{\mathbb{Q}}^K E$ is the $\mathbb{Q}$-algebra generated by ϕ_{σ_2} and ϕ_{σ_3} with relations

$$\begin{cases} \phi_{\sigma_2}^2 = -2 \\ \phi_{\sigma_3}^2 = 1 \\ \phi_{\sigma_2}\phi_{\sigma_3} = -\phi_{\sigma_3}\phi_{\sigma_2} \end{cases}$$

This is a quaternion algebra and in fact even isomorphic to the matrix algebra $M_2(\mathbb{Q})$ under the correspondence

$$\phi_{\sigma_2} \leftrightarrow \begin{bmatrix} 0 & -2 \\ 1 & 0 \end{bmatrix} \qquad \phi_{\sigma_3} \leftrightarrow \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Note that any $\mathbb{Q}$-algebra homomorphism from $M_2(\mathbb{Q})$ to a commutative algebra must be trivial, meaning that no splitting map for c defined over K can exist. One can also see this by noting that the table for c is not symmetric. We will see later how we can still find a splitting map for c by extending the field K.

Section 2.3

Computing a splitting map

We first note a special property about the map c_E. Taking degrees in equation (2.2) we find that

$$\deg \phi_\sigma \deg \phi_\tau / \deg \phi_{\sigma\tau} = \deg c_E(\sigma, \tau) = (c_E(\sigma,\tau))^2 \tag{2.4}$$

Therefore c_E^2 is the coboundary of the map $d : G_\mathbb{Q} \to \mathbb{Q}^*$ given by $d(\sigma) = \deg \phi_\sigma$. This map is called the *degree map* of E. In the framework [vL21a] one can request the values of the degree map with the method `degree_map` of the class `Qcurve`.

Note that Equation (2.4) tells us that the degree map when considered as a map $d : G_\mathbb{Q} \to \mathbb{Q}^* / (\mathbb{Q}^*)^2$ is a homomorphism. It is easily verified that this homomorphism does not change if we change the ϕ_σ or replace E with an isogenous curve. Furthermore if we look at the long exact sequence induced by the short exact sequence

$$1 \longrightarrow (\mathbb{Q}^*)^2 \hookrightarrow \mathbb{Q}^* \longrightarrow \mathbb{Q}^* / (\mathbb{Q}^*)^2 \longrightarrow 1,$$

Equation (2.4) tells us that the class $[d] \in H^1\left(G_\mathbb{Q}, \mathbb{Q}^*/(\mathbb{Q}^*)^2\right)$ maps to the class $[c_E^2] \in H^2\left(G_\mathbb{Q}, (\mathbb{Q}^*)^2\right)$. Noting that the short exact sequence

$$1 \longrightarrow \{\pm 1\} \hookrightarrow \mathbb{Q}^* \xrightarrow{\cdot^2} (\mathbb{Q}^*)^2 \longrightarrow 1,$$

induces a long exact sequence containing

$$H^2(G_\mathbb{Q}, \{\pm 1\}) \longrightarrow H^2(G_\mathbb{Q}, \mathbb{Q}^*) \xrightarrow{\cdot^2} H^2\left(G_\mathbb{Q}, (\mathbb{Q}^*)^2\right),$$

we see that the degree map determines ξ_E up to elements of $H^2(G_\mathbb{Q}, \{\pm 1\})$. In fact by writing $c_E = c_{E,\pm}|c_E|$ we see that the part not completely fixed by the image of the degree map in $H^2\left(G_\mathbb{Q}, (\mathbb{Q}^*)^2\right)$ is $\xi_{E,\pm} = [c_{E,\pm}] \in H^2(G_\mathbb{Q}, \{\pm 1\})$.

We can use the degree map also for computing a splitting map for c_E. Since any splitting map $\beta : G_\mathbb{Q} \to \overline{\mathbb{Q}}^*$ for c_E should satisfy Equation (2.3), we find that

$$\beta(\sigma)^2 \beta(\tau)^2 \beta(\sigma\tau)^{-2} = c_E(\sigma,\tau)^2 = d(\sigma) d(\tau) d(\sigma\tau)^{-1}.$$

Therefore the map

$$\varepsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*, \quad \sigma \mapsto \frac{\beta(\sigma)^2}{d(\sigma)},$$

is a homomorphism, i.e. a character. This is called the *splitting character* corresponding to β. We will compute splitting maps by first computing characters that could be splitting characters.

Example 2.3.1. $\boxed{\texttt{Qcurve2.rst}}$ Look at the elliptic curve

$$E : Y^2 = X^3 + 12\sqrt{2}X^2 + 36(1+\sqrt{2})X.$$

Using the isogeny from Example 4.5 in [Sil09, III.4] we see it is 2-isogenous to

$$E' : Y^2 = X^3 - 24\sqrt{2}X^2 + 144(1-\sqrt{2})X,$$

which is isomorphic to the Galois conjugate of E over $K = \mathbb{Q}(\sqrt{2})$. We thus see that E is a $\mathbb{Q}$-curve completely defined over K with degree map

$$d(\sigma) = \begin{cases} 1 & \text{if } \sigma \in G_K \\ 2 & \text{otherwise.} \end{cases}$$

Using Equation (2.4) this shows us that

$c(\sigma,\tau)^2$	1	σ_2
1	1	1
σ_2	1	4

where σ_2 is a generator of $G_{\mathbb{Q}}^K$. Using the framework [vL21a] we obtain the same degree map and can compute the actual c_E, which we present as a formatted table like in Example 2.2.3.

```
sage: K.<sqrt2> = QuadraticField(2)
sage: E = Qcurve([0, 12*sqrt2, 0, 36*(1 + sqrt2), 0],
....:            guessed_degrees=[2])
sage: G = K.galois_group()
sage: [E.degree_map(s) for s in G]
[1, 2]
sage: matrix([[E.c(s, t) for t in G] for s in G])
```

$c(\sigma,\tau)$	1	σ_2
1	1	1
σ_2	1	-2

From this table we can easily see that

$$\beta(\sigma) = \begin{cases} 1 & \text{if } \sigma \in G_K \\ \sqrt{-2} & \text{otherwise.} \end{cases}$$

is a splitting map for c defined over K. The corresponding splitting character is the quadratic character of K.

Section 2.4

Local conditions of splitting characters

Note that a splitting character can be considered as an element of $H^1(G_\mathbb{Q}, \overline{\mathbb{Q}}^*)$ with the trivial action of $G_\mathbb{Q}$ on $\overline{\mathbb{Q}}$. The short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \{\pm 1\} \arrow[r] & \overline{\mathbb{Q}}^* \arrow[r, ".^2"] & \overline{\mathbb{Q}}^* \arrow[r] & 1 \end{tikzcd}$$

induces a map $H^1(G_\mathbb{Q}, \overline{\mathbb{Q}}^*) \to H^2\left(G_\mathbb{Q}, \{\pm 1\}\right)$ which maps ε to a cohomology class $[\theta_\varepsilon] \in H^2(G_\mathbb{Q}, \{\pm 1\})$. Here θ_ϵ is the coboundary of a map $\varepsilon' : G_\mathbb{Q} \to \overline{\mathbb{Q}}^*$ with $(\varepsilon')^2 = \varepsilon$.

Since $c_E^2 = \partial d$ we can write $|c_E| = \partial\sqrt{d}$ where $\sqrt{d}$ is given by $\sigma \mapsto \sqrt{d(\sigma)}$ ($d(\sigma)$ is positive by definition) for the positive square root. If β is a splitting map for c_E, then by choosing $\varepsilon' = \frac{\beta}{\sqrt{d}}$ we see that the corresponding splitting character ε has $[\theta_\varepsilon] = [c_{E,\pm}] \in H^2(G_\mathbb{Q}, \{\pm 1\})$. Conversely any character ε satisfying $[\theta_\varepsilon] = [c_{E,\pm}] \in H^2(G_\mathbb{Q}, \{\pm 1\}$ gives rise to a map $\beta : G_\mathbb{Q} \to \overline{\mathbb{Q}}^*$ of which the coboundary has class ξ_E, where $\beta = \varepsilon'\sqrt{d}$ for some ε' with $(\varepsilon')^2 = \varepsilon$ and coboundary $c_{E,\pm}$.

Our goal is to find all characters ε satisfying $[\theta_\varepsilon] = [c_{E,\pm}] \in H^2(G_\mathbb{Q}, \{\pm 1\})$. Note that we know that ε satisfies this equation if and only if it satisfies this equation locally. This follows from the correspondence of $H^2(G_\mathbb{Q}, \{\pm 1\})$ with the two-torsion $\mathrm{Br}_2(\mathbb{Q})$ of the Brauer group and the local-global principle for Brauer groups. Furthermore we have

$$H^2\left(G_{\mathbb{Q}_p}, \{\pm 1\}\right) \cong \mathrm{Br}_2\left(\mathbb{Q}_p\right) \cong \{\pm 1\},$$

where again Br_2 denotes the two-torsion of the Brauer group. Therefore we can identify the restriction $[\theta_\varepsilon]_p$ of $[\theta_\varepsilon]$ to $G_{\mathbb{Q}_p}$ with $+1$ or -1.

We can interpret the character ε as a Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \bar{\mathbb{Q}}$. This allows us to write this character as

$$\varepsilon = \prod_{p|N} \varepsilon_p,$$

where ε_p is a Dirichlet character of conductor a power of the prime number p. Setting each ε_p to be trivial if $p \nmid N$ we can write this as a product over all primes.

There is a useful relation between the local $[\theta_\varepsilon]_p$ and ε_p.

Proposition 2.4.1. *Let $\varepsilon : G_{\mathbb{Q}} \to \bar{\mathbb{Q}}$ be a Galois character. For any prime number p we have that*

$$[\theta_\varepsilon]_p = \varepsilon_p(-1).$$

Proof. This result is stated near the top of page 302 in [Que00]. We here present a short outline of a proof.

By noting that $[\theta_\varepsilon] = \prod_p [\theta_{\varepsilon_p}]$ it suffices to prove

$$[\theta_{\varepsilon_p}]_q = \begin{cases} \varepsilon_p(-1) & \text{if } p = q \\ 1 & \text{otherwise} \end{cases}$$

for any two prime numbers p and q.

The short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \{\pm 1\} \arrow[r] & \overline{\mathbb{Q}}^* \arrow[r, ".^2"] & \overline{\mathbb{Q}}^* \arrow[r] & 1 \end{tikzcd}$$

gives a diagram of long exact sequences in cohomology by considering the Galois groups $G_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p^\infty)}$, $G_{\mathbb{Q}_q}^{\mathbb{Q}_q(\zeta_p^\infty)}$, $G_{\mathbb{Q}_q}$ and $G_{\mathbb{Q}}$ acting on them. Here ζ_p^∞ denotes adding all p^n-th roots of unity for $n \in \mathbb{Z}_{>0}$. Chasing the element $\varepsilon_p \in H^1\left(G_{\mathbb{Q}}^{\mathbb{Q}(\zeta_p^\infty)}, \overline{\mathbb{Q}}^*\right)$ around this diagram to $[\theta_{\varepsilon_p}]_q \in H^2(G_{\mathbb{Q}_q}, \{\pm 1\})$ through the right cohomology groups gives the desired result.

In case $p \neq q$ the chase goes through the cohomology groups of $G_{\mathbb{Q}_q}^{\text{unram}}$, the Galois group of the maximal unramified extension of $\mathbb{Q}_q$. Since $H^1(G_{\mathbb{Q}_q}, \overline{\mathbb{Q}}^*)$ is isomorphic to the group of all roots of unity in $\overline{\mathbb{Q}}$, squaring here forms an isomorphism. Therefore ε_p becomes trivial when chasing through this long exact sequence.

In case $p = q$ part of the long exact sequence of $G_{\mathbb{Q}_q}^{\mathbb{Q}_q(\zeta_q^\infty)}$ is isomorphic to

$$1 \longrightarrow \hom_c(\mathbb{Z}_p^*, \overline{\mathbb{Q}}^*) \xrightarrow{\cdot^2} \hom_c(\mathbb{Z}_p^*, \overline{\mathbb{Q}}^*) \xrightarrow{\varepsilon \mapsto \varepsilon(-1)} \{\pm 1\} \longrightarrow 1,$$

so chasing through this gives the desired result. Here $\hom_c$ denotes continuous homomorphisms. Showing that the maps in this exact sequence are correct can be shown by comparing cardinalities of $\hom\left((\mathbb{Z}/p^n\mathbb{Z})^*, \overline{\mathbb{Q}}^*\right)$. □

Proposition 2.4.1 shows us that any character with local components ε_p satisfying $\xi_{E,\pm,p} = \varepsilon_p(-1)$ could be a splitting character. What remains is to compute $\xi_{E,\pm,p}$ as an element of $H^2(G_{\mathbb{Q}_p}, \{\pm 1\}) \cong \{\pm 1\}$ from $c_{E,\pm}$ which is not so easy. Luckily Quer provides an easier way of computing $\xi_{E,\pm,p}$ in [Que00].

Let K_d be the fixed field of the kernel of the degree map $d : G_{\mathbb{Q}} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$. The field K_d is called the *degree field* of E. Note that as $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ consists only of 2-torsion, the degree field must be Galois with a Galois group that consists only of 2-torsion. Therefore $K_d = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_m})$ for some integers $a_1, \dots, a_m$. Now pick elements $\sigma_i \in G_{\mathbb{Q}}$ such that ${}^{\sigma_i}\sqrt{a_j} = (-1)^{\delta_{ij}}\sqrt{a_j}$ for all $i, j \in \{1, \dots, m\}$ and set $d_i = d(\sigma_i)$. If m is minimal the sets $\{a_1, \dots, a_m\}$ and $\{d_1, \dots, d_m\}$ are called a *dual basis* for d.

Theorem 2.4.2 (Theorem 3.1 in [Que00]). *Let $\{a_1, \dots, a_m\}$ and $\{d_1, \dots, d_m\}$ be a dual basis for d, then*

$$\xi_{E,\pm} = \prod_{i=1}^{m} (a_i, d_i),$$

as an element of $H^2(G_{\mathbb{Q}}, \{\pm 1\}) = \mathrm{Br}_2(\mathbb{Q})$, where (a_i, d_i) is the quaternion algebra over $\mathbb{Q}$ generated by $1, x_i, y_i, z_i$ with relations

$$x_i^2 = a_i, \qquad y_i^2 = d_i, \qquad x_i y_i = z_i = -y_i x_i.$$

Corollary 2.4.3. *Let $\{a_1, \dots, a_m\}$ and $\{d_1, \dots, d_m\}$ be a dual basis for d, then*

$$\xi_{E,\pm,p} = \prod_{i=1}^{m} (a_i, d_i)_p,$$

as an element of $H^2(G_{\mathbb{Q}_p}, \{\pm 1\}) = \mathrm{Br}_2(\mathbb{Q}_p) = \{\pm 1\}$, where $(a_i, d_i)_p$ denotes the Hilbert symbol.

Using Corollary 2.4.3 one can now compute a splitting character ε as

$$\varepsilon = \prod_{\substack{p \text{ prime} \\ \xi_{E,\pm,p}=-1}} \varepsilon_p,$$

where ε_p is a generator of $\hom((\mathbb{Z}/p\mathbb{Z})^*, \overline{\mathbb{Q}}^*)$ if $p \neq 2$ or $\hom((\mathbb{Z}/4\mathbb{Z})^*, \overline{\mathbb{Q}}^*)$ if $p = 2$. Note that this product is finite and we only have to compute $\xi_{E,\pm,p}$ for finitely many primes p, as a Hilbert symbol $(a, b)_p$ is 1 for any prime $p \nmid 2ab$. From this splitting character we find a splitting map

$$\beta : \sigma \mapsto \sqrt{\varepsilon(\sigma)}\sqrt{d(\sigma)},$$

for ξ_E by making a choice of square roots.

All of these computations are implemented in the code [vL21a] as part of the `Qcurve` class. The method `dual_basis` gives a dual basis for the curve as two lists of integers. The method `xi_pm` gives the representation of $\xi_{E,\pm}$ as a list of tuples. Each tuple (a, d) corresponds to the similarly marked quaternion algebra over $\mathbb{Q}$ and $\xi_{E,\pm}$ is the product of these. Using the method `xi_pm_local` one can compute $\xi_{E,\pm,p} \in \{\pm 1\}$ for a prime number p. This is all used by the methods `splitting_character` and `splitting_map` to compute a possible splitting character and the corresponding splitting map. Note that the first is by default a Dirichlet character, but can also be given as a Galois character if the argument `galois` is set to `True`.

Example 2.4.4. `Qcurve1.rst` `Qcurve1Frey.rst` We return to the curve E of Example 2.1.4. Note that its degree map is given by

$$d(\sigma) = \begin{cases} 1 & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{3})} \\ 2 & \text{otherwise,} \end{cases}$$

hence $\{3\}, \{2\}$ is a dual basis for the degree map. By Theorem 2.4.2 we then find that $\xi_{E,\pm} = (3, 2)$, so locally we have

$$\xi_{E,\pm,p} = (3, 2)_p = \begin{cases} -1 & \text{if } p = 2, 3 \\ 1 & \text{otherwise.} \end{cases}$$

By Proposition 2.4.1 we see that the pro p-part of the splitting character should satisfy

$$\varepsilon_p(-1) = \begin{cases} -1 & \text{if } p = 2, 3 \\ 1 & \text{otherwise,} \end{cases}$$

hence we can choose our splitting character as the unique character of conductor 4 times the unique character of conductor 3. This gives the unique character of conductor 12 that is the quadratic character of $\mathbb{Q}(\sqrt{3})$. A corresponding splitting map for ξ_E is therefore given by

$$\beta(\sigma) = \begin{cases} \pm 1 & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{3})} \\ \pm\sqrt{-2} & \text{otherwise.} \end{cases}$$

The signs here can be chosen freely for each $\sigma \in G_{\mathbb{Q}}$ as long as β remains continuous. These results are confirmed by the framework [vL21a].

```
sage: [E.degree_map(s) for s in [G(1), s2, s3, s2*s3]]
[1, 2, 1, 2]
sage: E.dual_basis()
([3], [2])
sage: E.xi_pm()
[(3, 2)]
sage: E.xi_pm_local(2), E.xi_pm_local(3), E.xi_pm_local(5)
(-1, -1, 1)
sage: eps = E.splitting_character()
sage: eps == next(eps for eps in DirichletGroup(12)
....:             if eps.conductor() == 12)
True
sage: beta = E.splitting_map()
sage: [beta(s)^2 for s in [G(1), s2, s3, s2*s3]]
[1, -2, 1, -2]
```

Note that as mentioned in Example 2.2.3 the map β can not be a splitting map for c_E over $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$. The only thing we know thus far is that the coboundary of β – when considered as a map on $G_{\mathbb{Q}}$ with trivial action – represents the class $\xi_E \in H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$. We shall see in the next section that there is an extension of K and a choice of signs for β for which β in fact is a splitting map for c_E.

Section 2.5

Correcting the splitting map

The theory in Quer [Que00] and described above gives us a way to construct a splitting map for a given $\xi \in H^2\left(G_{\mathbb{Q}}, \mathbb{Q}^*\right)$, but this might not necessarily be a splitting map for the 2-cocycle c_E coming from the $\mathbb{Q}$-curve E. Let us denote by c_β the cocycle for which β is a splitting map. In the framework [vL21a] c_β can be obtained with the method `c_splitting_map` of the class `Qcurve` that works similar to the method `c`.

Note that both c_β^2 and c_E^2 are the coboundary of the degree map d. Therefore $c_\beta c_E^{-1}$ must be a 2-cocycle with values in $\{\pm 1\}$. If $c_\beta c_E^{-1}$ is the coboundary of some continuous function $\alpha : G_\mathbb{Q} \to \{\pm 1\}$ then we know that $c_{\alpha^{-1}\beta} = c_E$ so $\alpha^{-1}\beta$ is a splitting map for c_E. We already know that the class of $c_\beta c_E^{-1}$ is trivial in $H^2(G_\mathbb{Q}, \mathbb{Q}^*)$. Since the short exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{Q}^* \xrightarrow{\cdot^2} \left(\mathbb{Q}^*\right)^2 \longrightarrow 1$$

is split, we have that $H^2\left(G_\mathbb{Q}, \mathbb{Q}^*\right) = H^2\left(G_\mathbb{Q}, \{\pm 1\}\right) \oplus H^2\left(G_\mathbb{Q}, \left(\mathbb{Q}^*\right)^2\right)$. Therefore the class of $c_\beta c_E^{-1}$ is also trivial in $H^2(G_\mathbb{Q}, \{\pm 1\})$ and we could find such a map α.

Note that a continuous $\alpha : G_\mathbb{Q} \to \{\pm 1\}$ with coboundary $c_\beta c_E^{-1}$ must factor over $G_\mathbb{Q}^K$ for some Galois number field K. Extending K such that E is completely defined over K and β is defined over K we see that $[c_\beta c_E^{-1}] = 0 \in H^2(G_\mathbb{Q}^K, \{\pm 1\})$. Assuming such a field K is known it thus suffices to find a map $\alpha : G_\mathbb{Q}^K \to \{\pm 1\}$ with coboundary $c_\beta c_E^{-1}$ to correct the splitting map β. This can be easily done with linear algebra over $\mathbb{F}_2$ using the values of $\alpha(\sigma)$ for $\sigma \in G_\mathbb{Q}^K$ as variables and the values of $c_\beta c_E^{-1}(\sigma, \tau)$ for $\sigma, \tau \in G_\mathbb{Q}^K$ as relations.

What remains is to find a Galois number field K such that $[c_\beta c_E^{-1}] = 0$ inside $H^2(G_\mathbb{Q}^K, \{\pm 1\})$ without a priori knowing the map α. A corollary of a well-known result tells us what the smallest such field K would be.

Proposition 2.5.1. *Let G be a finite group and A be an abelian group with an action of G. Let $S(G, A)$ be the collection of exact sequences*

$$1 \to A \xrightarrow{\iota} \tilde{G} \xrightarrow{\pi} G \to 1$$

with $x \cdot \iota(a) = \iota({}^{\pi(x)}a) \cdot x$ for all $x \in \tilde{G}$ and $a \in A$. When we have a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "\mathrm{Id}"] & \tilde{G} \arrow[r] \arrow[d, "\sim"] & G \arrow[r] \arrow[d, "\mathrm{Id}"] & 1 \\
1 \arrow[r] & A \arrow[r] & \tilde{G}' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

with the rows elements of $S(G, A)$ and $\tilde{G} \to \tilde{G}'$ an isomorphism, we say these exact sequences are equivalent and denote the corresponding equivalence relation by $\sim$. There is a bijection between $H^2(G, A)$ and $S(G, A)/\sim$.

Furthermore let $m : \hat{G} \to G$ be a homorphism of finite groups that induces a map $m^* : H^2(G, A) \to H^2(\hat{G}, A)$ and let $\xi \in H^2(G, A)$, then $m^*\xi = 0$ if and only if we have a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] & \tilde{G} \arrow[r] & G \arrow[r] & 1 \\
& & \hat{G} \arrow[u] \arrow[ur, "m"] & &
\end{tikzcd}$$

where the top row is an exact sequence corresponding to ξ.

Proof. The first part is a classical result. A detailed explanation can for example be found in [AM04, Chapter I]. We will use that in the exact sequence we may take $\tilde{G}$ to be the group with elements $G \times A$ and group law given by

$$(x, a) * (y, b) = (xy, a + {}^{x}b + c(x, y)),$$

where c is a 2-cocycle representing the corresponding element in $H^2(G, A)$. We will denote this group by $G \rtimes_c A$. Note that this is unrelated to the direct product.

For the second part we may now assume the commutative diagram looks like

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\iota"] & G \rtimes_c A \arrow[r, "\pi"] & G \arrow[r] & 1 \\
& & \hat{G}, \arrow[u, "F"] \arrow[ur, "m"] & &
\end{tikzcd}$$

with $\xi = [c] \in H^2(G, A)$, $\iota(a) = (1, a - c(1, 1))$ for all $a \in A$, and $\pi(x, a) = x$ for all $(x, a) \in G \rtimes_c A$.

First suppose that $m^*\xi = 0$, then there must be an $\alpha : \hat{G} \to A$ such that for any $x, y \in \hat{G}$

$$c(x, y) = \alpha(x) + {}^{m(x)}\alpha(y) - \alpha(xy)$$

It is easy to check that $F : \hat{G} \to G \rtimes_c A$ given by $F(x) = (m(x), -\alpha(x))$ is a homomorphism that makes the diagram commute. Conversely given a diagram with a homomorphism F, let $\alpha : G \rtimes_c A \to A$ be given by $\alpha((x, a)) = -a$. For any $(x,a),(y,b) \in G \rtimes_c A$ we have

$$\begin{aligned}
&\alpha\left((x,a)\right) + {}^x\alpha\left((y,b)\right) - \alpha\left((x,a) * (y,b)\right)\\
&\qquad = -a - {}^xb - \alpha\left((xy, a + {}^xb + c(x,y)\right)\\
&\qquad = -a - {}^xb + a + {}^xb + c(x,y)\\
&\qquad = c(x,y)
\end{aligned}$$

so $\alpha \circ F : \hat{G} \to A$ is a map with coboundary m^*c. This completes the proof. □

Corollary 2.5.2. *Let K be a Galois number field and let $\xi \in H^2\left(G_{\mathbb{Q}}^K, \{\pm 1\}\right)$. If there exists a Galois number field L/K such that $\xi = 1 \in H^2\left(G_{\mathbb{Q}}^L, \{\pm 1\}\right)$, then a smallest such field L is of the form $K(\sqrt{\gamma})$ for some $\gamma \in K$.*

If $K(\sqrt{\gamma}) \neq K$, then the equivalence class of the exact sequence

$$1 \longrightarrow G_K^{K(\sqrt{\gamma})} = \{\pm 1\} \longrightarrow G_{\mathbb{Q}}^{K(\sqrt{\gamma})} \longrightarrow G_{\mathbb{Q}}^K \longrightarrow 1 \tag{2.5}$$

corresponds to $\xi \in H^2\left(G_{\mathbb{Q}}^K, \{\pm 1\}\right)$ as in Proposition 2.5.1. Conversely if $\gamma \in K^*$ is a non-square with $K(\sqrt{\gamma})/\mathbb{Q}$ Galois such that the equivalence class of the exact sequence in (2.5) corresponds to the class $\xi \in H^2(G_{\mathbb{Q}}^K, \{\pm 1\})$, then we have $\xi = 1 \in H^2(G_{\mathbb{Q}}^{K(\sqrt{\gamma})}, \{\pm 1\})$.

Proof. To start let M/K be any Galois number field for which we have $\xi = 1$ inside $H^2\left(G_{\mathbb{Q}}^M, \{\pm 1\}\right)$. By Proposition 2.5.1 we know that we have a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \{\pm 1\} \arrow[r, "\iota"] & \tilde{G} \arrow[r, "\pi"] & G_{\mathbb{Q}}^K \arrow[r] & 1\\
 & & G_{\mathbb{Q}}^M \arrow[u, "F"] \arrow[ur, "m"'] & &
\end{tikzcd}$$

where in this case we also know that m is surjective. Let N be the kernel of the map F and let L be the fixed field of N. Since the kernel of F is contained in the kernel of m, the field L is a Galois number field that extends K.

We may now replace M with L in the commutative diagram in which case F becomes injective and m is still surjective. Inspecting cardinalities we note that we have only two cases: F is an isomorphism or m is an isomorphism. Both cases clearly indicate that $L = K(\sqrt{\gamma})$ for some $\gamma \in K$. The case $K(\sqrt{\gamma}) \neq K$ corresponds to the case where F is an isomorphism, so that the exact sequence corresponds to ξ follows immediately.

The converse result directly follows from the second part of Proposition 2.5.1 by taking $G = G_{\mathbb{Q}}^{K}$, $A = \{\pm 1\}$ and $\tilde{G} = \hat{G} = G_{\mathbb{Q}}^{K(\sqrt{\gamma})}$. □

Note that for our case we can take K in Corollary 2.5.2 to be a field over which E is completely defined and β is also defined. The class of $c_\beta c_E^{-1}$ will then become trivial in a quadratic extension of that K. What is still missing is a way to compute this quadratic extension for which the following result will provide an answer.

Proposition 2.5.3. *Let K be a Galois number field and $c : \left(G_{\mathbb{Q}}^{K}\right)^2 \to \{\pm 1\}$ be a 2-cocycle. The following are equivalent.*

- *There exists a non-square $\gamma \in K^*$ with $K(\sqrt{\gamma})/\mathbb{Q}$ Galois such that the equivalence class of the exact sequence*

$$1 \to G_{K}^{K(\sqrt{\gamma})} = \{\pm 1\} \to G_{\mathbb{Q}}^{K(\sqrt{\gamma})} \to G_{\mathbb{Q}}^{K} \to 1$$

  corresponds to $[c] \in H^2\left(G_{\mathbb{Q}}^{K}, \{\pm 1\}\right)$ as in Proposition 2.5.1.

- *There exists an $\alpha : G_{\mathbb{Q}}^{K} \to K^*$ with*

$$c(\sigma, \tau) = \alpha(\sigma)\ {}^{\sigma}\alpha(\tau)\ \left(\alpha(\sigma\tau)\right)^{-1},$$

  for all $\sigma, \tau \in G_{\mathbb{Q}}^{K}$.

Furthermore corresponding α and γ are related by

$$^{\sigma}\gamma = \gamma\, \alpha(\sigma)^2 \quad \textit{for all } \sigma \in G_{\mathbb{Q}}^{K}.$$

Proof. First of all suppose we have a non-square $\gamma \in K^*$ with $K(\sqrt{\gamma})/\mathbb{Q}$ Galois and the equivalence class of

$$1 \longrightarrow \{\pm 1\} \xrightarrow{\iota} G_{\mathbb{Q}}^{K(\sqrt{\gamma})} \xrightarrow{\pi} G_{\mathbb{Q}}^{K} \longrightarrow 1$$

corresponding to $[c] \in H^2(G_{\mathbb{Q}}^{K}, \{\pm 1\})$. Since $K(\sqrt{\gamma})$ is Galois over $\mathbb{Q}$ we know that $K(\sqrt{^{\sigma}\gamma}) = K(\sqrt{\gamma})$ for all $\sigma \in G_{\mathbb{Q}}^{K}$. This implies a map $\alpha : G_{\mathbb{Q}}^{K} \to K^*$ exists such that

$$^{\sigma}\gamma = \gamma\, \alpha(\sigma)^2 \quad \text{for all } \sigma \in G_{\mathbb{Q}}^{K}.$$

Now let $s : G_{\mathbb{Q}}^K \to G_{\mathbb{Q}}^{K(\sqrt{\gamma})}$ be given by ${}^{s(\sigma)}\sqrt{\gamma} = \alpha(\sigma)\sqrt{\gamma}$ and ${}^{s(\sigma)}x = {}^{\sigma}x$ for all $x \in K$. Since $\pi \circ s = \mathrm{Id}_{G_{\mathbb{Q}}^K}$ there exists a 2-cocycle $c_s : \left(G_{\mathbb{Q}}^K\right)^2 \to \{\pm 1\}$ defined by $\iota \circ c_s(\sigma,\tau) = s(\sigma)s(\tau)s(\sigma\tau)^{-1}$. Furthermore we have for all $\sigma, \tau \in G_{\mathbb{Q}}^K$

$$\begin{aligned}
\alpha(\sigma)\ {}^{\sigma}\alpha(\tau)\ \left(\alpha(\sigma\tau)\right)^{-1} &= \frac{{}^{s(\sigma)}\sqrt{\gamma}}{\sqrt{\gamma}}\ \frac{{}^{s(\sigma)s(\tau)}\sqrt{\gamma}}{{}^{s(\sigma)}\sqrt{\gamma}}\ \frac{\sqrt{\gamma}}{{}^{s(\sigma\tau)}\sqrt{\gamma}} \\
&= \frac{{}^{s(\sigma)s(\tau)}\sqrt{\gamma}}{{}^{s(\sigma\tau)}\sqrt{\gamma}} \\
&= c_s(\sigma,\tau).
\end{aligned}$$

Let $G_{\mathbb{Q}}^K \rtimes_{c_s} \{\pm 1\}$ be the group introduced in the proof of Proposition 2.5.1. A simple computation shows that the map

$$G_{\mathbb{Q}}^K \rtimes_{c_s} G_K^{K(\sqrt{\gamma})} \to G_{\mathbb{Q}}^{K(\sqrt{\gamma})}, \quad (\sigma,\tau) \mapsto \tau s(\sigma)$$

is an isomorphism giving a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \{\pm 1\} \arrow[r] \arrow[d, "\mathrm{Id}"] & G_{\mathbb{Q}}^K \rtimes_{c_s} \{\pm 1\} \arrow[r] \arrow[d, "\sim"] & G_{\mathbb{Q}}^K \arrow[r] \arrow[d, "\mathrm{Id}"] & 1 \\
1 \arrow[r] & \{\pm 1\} \arrow[r] & G_{\mathbb{Q}}^{K(\sqrt{\gamma})} \arrow[r] & G_{\mathbb{Q}}^K \arrow[r] & 1.
\end{tikzcd}$$

Therefore the cocycles c and c_s are associated by a coboundary, so changing α by a map $G_{\mathbb{Q}}^K \to \{\pm 1\}$ with coboundary cc_s^{-1} gives us the sought map α.

For the converse start with a map $\alpha : G_{\mathbb{Q}}^K \to K^*$ satisfying

$$c(\sigma,\tau) = \alpha(\sigma)\ {}^{\sigma}\alpha(\tau)\ \left(\alpha(\sigma\tau)\right)^{-1} \quad \text{for all } \sigma,\tau \in G_{\mathbb{Q}}^K.$$

Since c takes values in $\{\pm 1\}$ we find that $[\alpha^2] \in H^1\left(G_{\mathbb{Q}}^K, K^*\right)$ by squaring the above equation. By Hilbert 90 we thus know that there is some $\gamma \in K^*$ such that

$${}^{\sigma}\gamma = \gamma\,\alpha(\sigma)^2 \quad \text{for all } \sigma \in G_{\mathbb{Q}}^K.$$

In particular this implies that $K(\sqrt{{}^{\sigma}\gamma}) = K(\sqrt{\gamma})$ for all $\sigma \in G_{\mathbb{Q}}^K$, hence $K(\sqrt{\gamma})$ is a Galois number field that extends K. We may assume γ is non-square as we can replace it with $a\gamma$ for $a \in \mathbb{Q}^* \setminus (K^*)^2$ otherwise. Therefore we have a short exact sequence

$$1 \longrightarrow G_K^{K(\sqrt{\gamma})} \equiv \{\pm 1\} \longrightarrow G_{\mathbb{Q}}^{K(\sqrt{\gamma})} \longrightarrow G_{\mathbb{Q}}^K \longrightarrow 1.$$

The cocycle associated with such an exact sequence in the proof of Proposition 2.5.1 can be obtained by choosing a section $s : G_{\mathbb{Q}}^K \to G_{\mathbb{Q}}^{K(\sqrt{\gamma})}$ and computing its coboundary. Choosing $s(\sigma)$, $\sigma \in G_{\mathbb{Q}}^K$ such that ${}^{s(\sigma)}\sqrt{\gamma} = \alpha(\sigma)\sqrt{\gamma}$ and ${}^{s(\sigma)}x = {}^{\sigma}x$ for all $x \in K$, the same computations from before show that this coboundary is the coboundary of α which is c. □

Another way to view the previously mentioned data is to look at the diagram

$$\begin{tikzcd}
 & H^1\left(G_{\mathbb{Q}}^K, K^*\right) = 1 \arrow[d] & \\
H^0\left(G_{\mathbb{Q}}^K, K^*/\left(K^*\right)^2\right) \arrow[r] & H^1\left(G_{\mathbb{Q}}^K, \left(K^*\right)^2\right) \arrow[r] \arrow[d] & H^1\left(G_{\mathbb{Q}}^K, K^*\right) = 1 \\
 & H^2\left(G_{\mathbb{Q}}^K, \{\pm 1\}\right) &
\end{tikzcd}$$

in which the row is from the long exact sequence associated to the short exact sequence

$$1 \to \left(K^*\right)^2 \to K^* \to K^*/\left(K^*\right)^2 \to 1$$

and in which the column comes from the long exact sequence associated to the short exact sequence

$$1 \to \{\pm 1\} \to K^* \to \left(K^*\right)^2 \to 1.$$

The fact that $H^1\left(G_{\mathbb{Q}}^K, K^*\right) = 1$ is Hilbert 90.

The cohomology classes $[\gamma] \in H^0\left(G_{\mathbb{Q}}^K, K^*/\left(K^*\right)^2\right)$, $[\alpha^2] \in H^1\left(G_{\mathbb{Q}}^K, \left(K^*\right)^2\right)$ and $[c] \in H^2\left(G_{\mathbb{Q}}^K, \{\pm 1\}\right)$ of any γ, α and c associated as in Proposition 2.5.3, map to one another in the diagram above. This even shows that for the case that $[c]$ is trivial we have an associated α, namely any α with trivial cohomology class $[\alpha^2] \in H^1(G_{\mathbb{Q}}^K, (K^*)^2)$ will suffice after changing it with a sufficient coboundary with values in $\{\pm 1\}$. Seeing there is also a γ related to this is Hilbert 90 again, since $[\alpha^2] \in H^1\left(G_{\mathbb{Q}}^K, K^*\right)$.

Proposition 2.5.3 and Corollary 2.5.2 prove together that the bottom vertical map in the diagram surjects onto the kernel of $H^2(G_{\mathbb{Q}}^K, \{\pm 1\}) \to H^2(G_{\mathbb{Q}}, \{\pm 1\})$. We thus have an exact sequence

$$1 \to \mathbb{Q}^* \cap (K^*)^2 \to \mathbb{Q}^* \to \left(K^*/\left(K^*\right)^2\right)^{G_{\mathbb{Q}}^K} \to H^2\left(G_{\mathbb{Q}}^K, \{\pm 1\}\right) \to H^2\left(G_{\mathbb{Q}}, \{\pm 1\}\right)$$

which arises from the row in the diagram before. Note that $\left(K^*/\left(K^*\right)^2\right)^{G_{\mathbb{Q}}^K}$ is represented by all those $\gamma \in K^*$ such that ${}^{\sigma}\gamma\gamma^{-1} \in \left(K^*\right)^2$ for all $\sigma \in G_{\mathbb{Q}}^K$. This implies that the kernel of $H^2(G_{\mathbb{Q}}^K, \{\pm 1\}) \to H^2(G_{\mathbb{Q}}, \{\pm 1\})$ corresponds 1 to 1 to all such γ considered modulo $\mathbb{Q}^* \left(K^*\right)^2$. Note that such a γ also defines a function $\alpha : G_{\mathbb{Q}}^K \to K^*$ by $\sigma \mapsto \sqrt{{}^{\sigma}\gamma\gamma^{-1}}$ of which the coboundary sits in the corresponding class of $H^2\left(G_{\mathbb{Q}}^K, \{\pm 1\}\right)$. Furthermore any specific c in this class can be obtained by a choice of signs for the square roots.

Example 2.5.4. `Qcurve1.rst` `Qcurve1Frey.rst` We once again return to the curve E from Example 2.1.4. Note that in Example 2.4.4 we found multiple maps $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ for $\xi_E \in H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$, of which we now choose one. Using the framework [vL21a] we compute the values of the cocycle $c_\beta c_E^{-1}$ over the field $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$, again replacing the output with a nicely formatted table as in Example 2.2.3.

```
sage: matrix([[E.c_splitting_map(s, t) / E.c(s, t)
....:           for t in [G(1), s2, s3, s2*s3]]
....:          for s in [G(1), s2, s3, s2*s3]])
```

$c_\beta c_E^{-1}$	1	σ_2	σ_3	$\sigma_2\sigma_3$
1	1	1	1	1
σ_2	1	1	1	1
σ_3	1	-1	1	-1
$\sigma_2\sigma_3$	1	-1	1	-1

Note that as the table is not symmetric there is no map $\alpha : G_{\mathbb{Q}}^K \to \{\pm 1\}$ which has this as a coboundary, corresponding to the fact that β can not be corrected in a way to form a splitting map for c_E over K.

We will try to find a map $\alpha : G_{\mathbb{Q}}^K \to K^*$ with coboundary $c_\beta c_E^{-1}$ as in Proposition 2.5.3. Seeing the shape of the table for $c_\beta c_E^{-1}$ a decent guess would be something of the form

$$\alpha(\sigma) = \begin{cases} 1 & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{3})} \\ a & \text{otherwise.} \end{cases}$$

This has the correct coboundary if ${}^{\sigma_2}a = a^{-1}$ and ${}^{\sigma_3}a = -a$. Note that the second condition implies a must be of the form $\sqrt{-2}(x + y\sqrt{3})$ for some $x, y \in \mathbb{Q}$ and then the first condition implies that $1 = {}^{\sigma_2}aa = 6y^2 - 2x^2$. The latter has a solution $x = y = -\frac{1}{2}$ meaning that

$$\alpha(\sigma) = \begin{cases} 1 & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{3})} \\ \frac{1+\sqrt{3}}{\sqrt{-2}} & \text{otherwise} \end{cases}$$

is a map $\alpha : G_K \to K^*$ with coboundary $c_\beta c_E^{-1}$.

Now note that the element

$$\gamma = \sum_{\sigma \in G_{\mathbb{Q}}^K} \alpha(\sigma)^{-2} = 1 + 1 + (-2 + \sqrt{3}) + (-2 + \sqrt{3}) = -2 + 2\sqrt{3} \in K$$

has coboundary α^2 according to Hilbert 90, hence by Proposition 2.5.3 we have that $[c_\beta c_E^{-1}] \in H^2(G_{\mathbb{Q}}^{K(\sqrt{\gamma})}, \{\pm 1\})$ is trivial. In fact as shown by the discussion above this example the same remains true when we change γ by a non-zero rational

We now take $\gamma = 1 - \sqrt{3}$ and show how to change our map β such that it becomes a splitting map for c_E over $K_\gamma = K(\sqrt{\gamma})$. First we compute the table for $c_\beta c_E^{-1}$ over K_γ using the framework [vL21a]. Again we format the table rather than giving the direct output.

```
sage: gamma = 1 - sqrt3
sage: R.<x> = K[]
sage: Kgamma.<sqrtgamma> = K.extension(x^2 - gamma)
sage: sqrtm6 = Kgamma(sqrtm2*sqrt3)
sage: Kgamma.<a> = Kgamma.absolute_field()
sage: sqrtgamma, sqrtm6 = Kgamma(sqrtgamma), Kgamma(sqrtm6)
sage: Ggamma = Kgamma.galois_group()
sage: sgamma = next(s for s in Ggamma
....:               if s != Ggamma(1) and
....:               s(sqrtgamma) == sqrtgamma)
sage: s6 = next(s for s in Ggamma
....:           if s(sqrt(Kgamma(-2))) != sqrt(Kgamma(-2)) and
....:           s(sqrtm6) == sqrtm6)
sage: Gls = [Ggamma(1), s6, s6^2, s6^3,
....:        sgamma, s6*sgamma, s6^2*sgamma, s6^3*sgamma]
sage: all(s in Gls for s in Ggamma)
True
sage: matrix([[E.c_splitting_map(s, t) / E.c(s, t)
....:          for t in Gls] for s in Gls])
```

$c_\beta c_E^{-1}$	1	σ_6	σ_6^2	σ_6^3	σ_γ	$\sigma_6\sigma_\gamma$	$\sigma_6^2\sigma_\gamma$	$\sigma_6^3\sigma_\gamma$
1	1	1	1	1	1	1	1	1
σ_6	1	-1	1	-1	1	-1	1	-1
σ_6^2	1	1	1	1	1	1	1	1
σ_6^3	1	-1	1	-1	1	-1	1	-1
σ_γ	1	-1	1	-1	1	-1	1	-1
$\sigma_6\sigma_\gamma$	1	1	1	1	1	1	1	1
$\sigma_6^2\sigma_\gamma$	1	-1	1	-1	1	-1	1	-1
$\sigma_6^3\sigma_\gamma$	1	1	1	1	1	1	1	1

Here σ_6 and σ_γ are the generators of $G_{\mathbb{Q}(\sqrt{-6})}^{K_\gamma}$ and $G_{\mathbb{Q}(\sqrt{\gamma})}^{K_\gamma}$ respectively.

With some trial and error it is easy to find a map $\alpha : G_{\mathbb{Q}}^{K_\gamma} \to \{\pm 1\}$ with coboundary $c_\beta c_E^{-1}$. For example one can choose

$$\alpha(\sigma) = \begin{cases} 1 & \text{if } \sigma = 1, \sigma_6, \sigma_\gamma, \sigma_6\sigma_\gamma \\ -1 & \text{otherwise} \end{cases}$$

as we can confirm with the framework [vL21a].

```
sage: alpha = {s : 1 if s in [G(1), s6, sgamma, s6*sgamma]
....:          else -1 for s in Gls}
sage: all(E.c_splitting_map(s, t) / E.c(s, t) ==
....:     alpha[s] * alpha[t] / alpha[s*t]
....:     for s in Gls for t in Gls)
True
```

Therefore we find that by changing the map β to

$$\beta(\sigma) = \begin{cases} 1 & \text{if } \sigma = 1, \sigma_\gamma \\ -1 & \text{if } \sigma = \sigma_6^2, \sigma_6^2\sigma_\gamma \\ \sqrt{-2} & \text{if } \sigma = \sigma_6, \sigma_6\sigma_\gamma \\ -\sqrt{-2} & \text{if } \sigma = \sigma_6^3, \sigma_6^3\sigma_\gamma \end{cases}$$

we obtain a splitting map for c_E over K_γ. We check this is correct with the framework [vL21a].

```
sage: beta = {s : E.splitting_map()(s) * alpha[s]
....:         for s in Gls}
sage: all(E.c(s, t) == beta[s] * beta[t] / beta[s*t]
....:     for s in Gls for t in Gls)
True
```

To ease calculation of the map $\alpha : G_{\mathbb{Q}}^{K} \to K^*$ it would be nice to assume that the image of α is in a finitely generated subgroup of K^*. In [Che10], [Che12], [BC12] and [DU09] various examples of Frey $\mathbb{Q}$-curves appear for which the subgroup $\mathcal{O}_K^*$ already suffices. For a set S of primes of K, let

$$\mathcal{O}_{K,S}^* = \{a \in K^* : \operatorname{ord}_{\mathfrak{p}} a \geq 0 \,\forall\, \mathfrak{p} \notin S\},$$

the group of *S-units.* We shall prove here that in general a subgroup $\mathcal{O}_{K,S}^* \subseteq K^*$ for S finite will suffice.

Proposition 2.5.5. *Let K be a Galois number field and let $c : \left(G_{\mathbb{Q}}^{K}\right)^2 \to \{\pm 1\}$ be a 2-cocycle. Let C be the class group of K modulo ideals of the form $\prod_{\mathfrak{p} \mid p} \mathfrak{p}$ for p a prime number. Let S_0 be a collection of representatives for the two-torsion of C, and S be the collection of prime ideals that divide an ideal in S_0 or their Galois conjugates.*

If $[c]$ is in the kernel of $H^2(G_{\mathbb{Q}}^{K}, \{\pm 1\}) \to H^2(G_{\mathbb{Q}}, \{\pm 1\})$, then there exists a function $\alpha : G_{\mathbb{Q}}^{K} \to \mathcal{O}_{K,S}^*$ satisfying

$$c(\sigma, \tau) = \alpha(\sigma)\ {}^{\sigma}\alpha(\tau)\ (\alpha(\sigma\tau))^{-1},$$

for all $\sigma, \tau \in G_{\mathbb{Q}}^{K}$.

Proof. As shown by Corollary 2.5.2, Proposition 2.5.3, and the discussion that followed, we know that there is some $\gamma \in K^*$ such that ${}^{\sigma}\gamma\gamma^{-1} \in (K^*)^2$ for all $\sigma \in G_{\mathbb{Q}}^{K}$ corresponding to $[c] \in H^2\left(G_{\mathbb{Q}}^{K}, \{\pm 1\}\right)$. Furthermore we know that this γ is unique up to elements from $\mathbb{Q}^*(K^*)^2$, and that we can construct a function $\alpha : G_{\mathbb{Q}}^{K} \to K^*$, $\sigma \to \pm\sqrt{{}^{\sigma}\gamma\gamma^{-1}}$, which has coboundary c for an appropiate choice of signs. It thus suffices to prove that there is a choice of γ such that ${}^{\sigma}\gamma\gamma^{-1} \in \mathcal{O}_{K,S}^*$, as $\left(\mathcal{O}_{K,S}^*\right)^2 = \mathcal{O}_{K,S}^* \cap (K^*)^2$.

Start with any choice of γ. For any finite prime $\mathfrak{p}$ of K and $\sigma \in G_{\mathbb{Q}}^{K}$ we know that ${}^{\sigma^{-1}}\gamma\gamma^{-1} \in (K^*)^2$, hence

$$\operatorname{ord}_{{}^{\sigma}\mathfrak{p}} \gamma = \operatorname{ord}_{\mathfrak{p}} {}^{\sigma^{-1}}\gamma \equiv \operatorname{ord}_{\mathfrak{p}} \gamma \pmod 2.$$

This implies for a prime number p that all $\operatorname{ord}_{\mathfrak{p}} \gamma$ for $\mathfrak{p} \mid p$ are congruent modulo 2.

Now for each prime number p choose an $a_p \in \mathbb{Z}$ that is congruent to $\operatorname{ord}_{\mathfrak{p}} \gamma$ modulo 2 for each $\mathfrak{p} \mid p$. Choose the a_p such that only finitely many are non-zero and construct the fractional ideal

$$I = \prod_{p} \prod_{\mathfrak{p} \mid p} \mathfrak{p}^{\frac{\operatorname{ord}_{\mathfrak{p}} \gamma - a_p}{2}}.$$

Here p will always denote a prime number and a product over p will always denote the product over all prime numbers.

It is clear that $I^2 = (\gamma) \prod_p \left(\prod_{\mathfrak{p}|p} \mathfrak{p} \right)^{-a_p}$, hence the class of I belongs to the 2-torsion of C. Note that changing I by a principal ideal (β) is the same as changing γ with $\gamma\beta^2$. Furthermore changing I by an element of the form $\prod_{\mathfrak{p}|p} \mathfrak{p}$ for a prime number p is the same as changing the corresponding a_p. Therefore without loss of generality we may assume that $I \in S_0$.

It is now clear that for any finite prime $\mathfrak{p} \mid p$ of K and $\sigma \in G_{\mathbb{Q}}^K$

$$\begin{aligned}
\operatorname{ord}_{\mathfrak{p}} \left(\frac{{}^{\sigma}\gamma}{\gamma} \right) &= \operatorname{ord}_{\mathfrak{p}} {}^{\sigma}\gamma - \operatorname{ord}_{\mathfrak{p}} \gamma \\
&= \operatorname{ord}_{\sigma^{-1}\mathfrak{p}} \gamma - \operatorname{ord}_{\mathfrak{p}} \gamma \\
&= \left(\operatorname{ord}_{\sigma^{-1}\mathfrak{p}} \gamma - a_p \right) - \left(\operatorname{ord}_{\mathfrak{p}} \gamma - a_p \right) \\
&= \operatorname{ord}_{\sigma^{-1}\mathfrak{p}} I^2 - \operatorname{ord}_{\mathfrak{p}} I^2 \\
&= 2 \left(\operatorname{ord}_{\mathfrak{p}} {}^{\sigma}I - \operatorname{ord}_{\mathfrak{p}} I \right).
\end{aligned}$$

It is now clear this can only be non-zero if $\mathfrak{p} \in S$, hence cleary ${}^{\sigma}\gamma\gamma^{-1} \in \mathcal{O}_{K,S}^*$ for all $\sigma \in G_{\mathbb{Q}}^K$. □

Remark 2.5.6. Note that $\mathcal{O}_{K,S}^*$ is an abelian group and that each $\sigma \in G_{\mathbb{Q}}^K$ is a group homomorphism on $\mathcal{O}_{K,S}^*$, hence given the values of c and regarding the values of α as unknown, the coboundary relation of c and α give us n^2 equations in n unknowns where $n = [K : \mathbb{Q}]$. Choosing a minimal generating set of $\mathcal{O}_{K,S}^*$ as a $\mathbb{Z}$-module with k generators this translates to kn^2 equations in kn unknowns of which some are defined over $\mathbb{Z}$ whilst others are defined over $\mathbb{Z}/N\mathbb{Z}$ for some $N \in \mathbb{Z}_{>0}$.

Now using the splitting map β for ξ_E constructed before, we can explicitly compute an $\alpha : G_{\mathbb{Q}}^K \to K^*$ with coboundary $c_\beta c_E^{-1}$ using Proposition 2.5.5 and linear algebra. Applying Hilbert 90 we can then compute a $\gamma \in K^*$ with coboundary α^2. According to Proposition 2.5.3 this γ defines the field $K(\sqrt{\gamma})$ over which we have $[c_E] = [c_\beta] \in H^2(G_{\mathbb{Q}}^{K(\sqrt{\gamma})}, \{\pm 1\})$. We can then compute the map $G_{\mathbb{Q}}^{K(\sqrt{\gamma})} \to \{\pm 1\}$ with which we have to change β in order to have $c_E = c_\beta$, hence making β a splitting map for c_E.

The framework [vL21a] can compute the set S in Proposition 2.5.5 with the method `_decomposable_twist_set` of the class `Qcurve`. The associated field will be the one returned by `decomposition_field` which is a field over which the curve, its given isogenies, and a computed splitting map for ξ_E are defined. Furthermore the method `_decomposable_twist` can be used to compute the associated γ in the manner described above. The reason these functions are named like this will become apparent in Section 2.7.

For a given field K there might be many sets S for which there is a map $\alpha : G_{\mathbb{Q}}^K \to \mathcal{O}_{K,S}^*$ as in Proposition 2.5.5. Preferably we would find the smallest S such that the proposition is still true. It is however not always possible to make S smaller than the one given in Proposition 2.5.5 as shown by the example below.

Example 2.5.7. `Qcurve3.rst` Let E be the $\mathbb{Q}$-curve given by

$$E : y^2 = x^3 + 12x^2 + 18\left(1 + \sqrt{17}\right)x.$$

The framework [vL21a] will check for us that it is indeed a $\mathbb{Q}$-curve with an isogeny of degree 2.

```
sage: _.<sqrt17> = QuadraticField(17)
sage: E = Qcurve([0, 12, 0, 18*(1 + sqrt17), 0],
....:            guessed_degrees=[2])
```

The framework [vL21a] implicitly computes a splitting map β for ξ_E when we compute $c_E c_\beta^{-1}$ over the complete definition field $K = \mathbb{Q}(\sqrt{-2}, \sqrt{17})$. As in Example 2.2.3 we present a formatted table here, rather than the direct output of the framework [vL21a].

```
sage: K = E.complete_definition_field()
sage: sqrtm2, sqrt17 = sqrt(K(-2)), sqrt(K(17))
sage: K.is_isomorphic(QQ[sqrtm2, sqrt17])
True
sage: G = K.galois_group()
sage: s2 = next(s for s in G if s != G(1) and
....:           s(sqrtm2) == sqrtm2)
sage: s17 = next(s for s in G if s != G(1) and
....:            s(sqrt17) == sqrt17)
sage: matrix([[E.c(s, t) / E.c_splitting_map(s, t)
....:          for t in [G(1), s2, s17, s2*s17]]
....:         for s in [G(1), s2, s17, s2*s17]])
```

$c_E c_\beta^{-1}$	1	σ_2	σ_{17}	$\sigma_2\sigma_{17}$
1	1	1	1	1
σ_2	1	-1	1	-1
σ_{17}	1	-1	1	-1
$\sigma_2\sigma_{17}$	1	1	1	1

Here σ_2 and σ_{17} are the generators of $G_{\mathbb{Q}(\sqrt{-2})}^K$ and $G_{\mathbb{Q}(\sqrt{17})}^K$ respectively.

Suppose we have an $\alpha : G_{\mathbb{Q}}^K \to \mathcal{O}_K^*$ which has this cocycle as coboundary. We compute generators of $\mathcal{O}_K^*$ using SageMath [Sag20].

```
sage: u0, u1 = K.unit_group().gens_values()
sage: u0 == -1 and u1^(-1) == 4 + sqrt17
True
```

Since $\mathcal{O}_K^*$ is generated by -1 and $4 + \sqrt{17}$ there are functions $x, y : G_{\mathbb{Q}}^K \to \mathbb{Z}$ such that

$$\alpha(\sigma) = (-1)^{x(\sigma)} \left(4 + \sqrt{17}\right)^{y(\sigma)} .$$

Since $\partial\alpha = c_E c_\beta^{-1}$ we now find that

$$\begin{aligned} x(1) + y(\sigma_2) &\equiv 1 \pmod{2} \\ x(1) + y(\sigma_2\sigma_{17}) &\equiv 0 \pmod{2} \\ y(1) &= 0 \\ 2\,y(\sigma_{17}) &= y(1) \\ y(\sigma_2) + y(\sigma_{17}) &= y(\sigma_2\sigma_{17}) \end{aligned}$$

from computing $\partial\alpha(\sigma_2, \sigma_2)$, $\partial\alpha(\sigma_2\sigma_{17}, \sigma_2\sigma_{17})$, $\partial\alpha(\sigma_{17}, \sigma_{17})$, and $\partial\alpha(\sigma_{17}, \sigma_2)$. This is clearly an inconsistent system, hence no such α can exist.

We compute the set S for K as in Proposition 2.5.5 by using the framework [vL21a], and note it consists of the primes above 2.

```
sage: S = E._decomposable_twist_set()
sage: S.reverse()
sage: S == K.primes_above(2)
True
```

We compute the element $\gamma \in K^*$ corresponding to $c_E c_\beta^{-1}$ and show that we have a corresponding map

$$\alpha : G_{\mathbb{Q}}^K \to \mathcal{O}_{K,S}^*, \quad \sigma \mapsto \begin{cases} 1 & \text{if } {}^{\sigma}\sqrt{17} = \sqrt{17} \\ \frac{7\sqrt{17}-29}{2\sqrt{-2}} & \text{if } {}^{\sigma}\sqrt{17} = -\sqrt{17}. \end{cases}$$

as in Proposition 2.5.3.

```
sage: gamma = E._decomposable_twist()
sage: alpha = {s : sqrt(s(gamma) / gamma) for s in G}
sage: (alpha[G(1)] == 1 and
....:  alpha[s2] == (7*sqrt17 - 29) / (2*sqrtm2) and
....:  alpha[s17] == 1 and
....:  alpha[s2*s17] == (7 * sqrt17 - 29) / (2*sqrtm2))
True
sage: all(P in S for P, _ in K.ideal(alpha[s2]).factor())
True
sage: all(E.c(s, t) / E.c_splitting_map(s, t) ==
....:     alpha[s] * s(alpha[t]) / alpha[s*t]
....:     for s in G for t in G)
True
```

We thus see that S is minimal in this case.

Section 2.6

Different splitting maps

The previous section allows us to explicitly compute a splitting map for c_E. We would like to compute all possible splitting maps for c_E and determine which ones would give the same abelian variety of GL_2-type.

First of all suppose that $\beta, \beta' : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ are both splitting maps for c_E. Since both have coboundary c_E with respect to the trivial action we must have that $\chi = \beta'/\beta$ is a homomorphism. Therefore if we have a single splitting map β for c_E we know each splitting map for c_E. In particular given a Galois number field K over which E is completely defined and over which β is defined, all splitting characters $G_{\mathbb{Q}}^K \to \overline{\mathbb{Q}}^*$ can be found by multiplying with a character of K. For a given field K we will call these χ *twist characters*. Note that the corresponding splitting characters differ by the square of the corresponding twist character.

In the framework [vL21a] the class `Qcurve` allows one to compute twist characters for the field K returned by `decomposition_field`, a field over which the curve, its isogenies, and a computed splitting map for ξ_E are defined. The number of twist characters is given by the method `number_of_splitting_maps` and each of them can be obtained by calling `twist_character` with the corresponding index. Note that as with splitting characters these characters are by default given as Dirichlet characters, but can be given as Galois characters if the argument `galois` is set to `True`. One can obtain the splitting map or splitting character obtained by twisting with a twist character by calling the method `splitting_map` or `splitting_character` with the same index as the twist character. It is also possible to obtain a list of these characters or maps by passing a list of indices as the index or by passing the string `"all"`.

Next suppose that two splitting maps $\beta, \beta' = \chi\beta : G_{\mathbb{Q}}^K \to \overline{\mathbb{Q}}^*$ over a field K over which E is completely defined define the same subvariety of $B = \mathrm{Res}_{\mathbb{Q}}^K$. This happens precisely when the induced linear maps on the endomorphism ring $\mathrm{End}_{\mathbb{Q}}^0 B$ have the same kernel. Note that $\mathrm{End}_{\mathbb{Q}}^0 B$ can be seen as the $\mathbb{Q}$-vector space with basis $G_{\mathbb{Q}}^K$ which implies these kernels are the same if and only if

$$\sum_{\sigma \in G_{\mathbb{Q}}^K} a_\sigma \beta(\sigma) = 0 \iff \sum_{\sigma \in G_{\mathbb{Q}}^K} a_\sigma \beta'(\sigma) = 0,$$

for all $a_\sigma \in \mathbb{Q}$. This implies that β' must be a Galois conjugate of β, i.e. that $\chi = {}^\sigma\beta\beta^{-1}$ for some $\sigma \in G_{\mathbb{Q}}$. The latter is easy to check given a splitting map β for c_E and the possible twist characters over K.

In the framework [vL21a] the methods `twist_character`, `splitting_map`, and `splitting_character` can be limited to only returning a list of one map or character per Galois conjugacy class of splitting maps, by passing `"conjugacy"` as an index. To obtain the number of conjugacy classes one can call the method `number_of_splitting_maps` and set the argument `count_conjugates` to `False`.

Example 2.6.1. `Qcurve1.rst` `Qcurve1Frey.rst` We again return to the curve E from Example 2.1.4. From Example 2.5.4 we have a splitting map β for c_E over the field K_γ. Note that K_γ has four different characters which are the trivial character and the characters of the subfields $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{-6})$. This implies there are also four different splitting maps for c_E over K_γ which can also be obtained from the four different choices for the map $\alpha : G_{\mathbb{Q}}^{K_\gamma} \to \{\pm 1\}$. The framework [vL21a] confirms this.

```
sage: iota = E.definition_field().embeddings(Kgamma)[0]
sage: Egamma = E.change_ring(iota)
sage: Egamma.number_of_splitting_maps()
4
sage: chis = Egamma.twist_character('all', galois=True)
sage: kernels = [Ggamma.subgroup(s for s in Ggamma
....:                            if chi(s) == 1)
....:            for chi in chis]
sage: fields = [kernel.fixed_field()[0] for kernel in kernels]
sage: [(field.degree(),
....:   field.discriminant().squarefree_part())
....:  for field in fields]
[(1, 1), (2, -2), (2, 3), (2, -6)]
```

Note that each of the splitting maps for c_E over K_γ only has a single Galois conjugate, namely by flipping the sign of $\sqrt{-2}$. This tells us that the four splitting maps for c_E come as two pairs of conjugate splitting maps. This is confirmed by the framework [vL21a], where we format the splitting maps in a table.

```
sage: Egamma.number_of_splitting_maps(count_conjugates=False)
2
sage: beta1, beta2 = Egamma.splitting_map('conjugacy')
```

σ	1	σ_6	σ_6^2	σ_6^3	σ_γ	$\sigma_6\sigma_\gamma$	$\sigma_6^2\sigma_\gamma$	$\sigma_6^3\sigma_\gamma$
$\beta_1(\sigma)$	1	$-\sqrt{-2}$	-1	$\sqrt{-2}$	1	$-\sqrt{-2}$	-1	$\sqrt{-2}$
$\beta_2(\sigma)$	1	$\sqrt{-2}$	-1	$-\sqrt{-2}$	-1	$-\sqrt{-2}$	1	$\sqrt{-2}$

We can thus find two distinct abelian varieties of GL_2-type by looking at the restriction of scalars $\mathrm{Res}_{\mathbb{Q}}^{K_\gamma} E$.

Section 2.7

Fields of $\mathbb{Q}$-curves

Throughout the previous sections we have seen that many different fields play a role for $\mathbb{Q}$-curves. This section contains some additional results about these fields. In particular we will see what the minimal possibilities for certain definition fields are. Taking these fields as small as possible will make the computations much easier.

First of all we will look at Galois number fields K over which E can be defined. Note that by definition of the degree map such a field K must contain the fixed field K_d of the kernel of the degree map as a map $d : G_{\mathbb{Q}} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$. As the degree map in this form is independent of the isogeny class of E over $\overline{\mathbb{Q}}$, the field K_d is a lower bound for Galois number fields over which curves isogenous to E are defined. In fact it is also a minimum.

Theorem 2.7.1 (Theorem 8.2 in [Rib04])**.** *Let E be a $\mathbb{Q}$-curve, then E is isogenous to some $\mathbb{Q}$-curve defined over a number field K if and only if ξ_E is in the kernel of the restriction map*

$$\mathrm{Res} : H^2(G_{\mathbb{Q}}, \mathbb{Q}^*) \to H^2(G_K, \mathbb{Q}^*)$$

Corollary 2.7.2. *Any $\mathbb{Q}$-curve E is isogenous over $\overline{\mathbb{Q}}$ to some $\mathbb{Q}$-curve defined over the degree field K_d.*

Proof. We follow the arguments given on page 290 of [Que00]. Let E be a $\mathbb{Q}$-curve with two cocycle c_E and degree map $d : G_{\mathbb{Q}} \to \mathbb{Q}^*$. Associate constants $\lambda_\sigma \in \overline{\mathbb{Q}}^*$ with each isogeny ϕ_σ such that

$$c_E(\sigma, \tau) = \lambda_\sigma \ {}^\sigma\lambda_\tau \lambda_{\sigma\tau}^{-1} \quad \text{for all } \sigma, \tau \in G_{\mathbb{Q}}.$$

This implies that

$$\lambda_\sigma^2 \ {}^\sigma\lambda_\tau^2 \lambda_{\sigma\tau}^{-2} = c_E(\sigma, \tau)^2 = d(\sigma)d(\tau)d(\sigma\tau)^{-1} \quad \text{for all } \sigma, \tau \in G_{\mathbb{Q}},$$

hence the map $\sigma \mapsto \lambda_\sigma^2 d(\sigma)^{-1}$ is a 1-cocycle. By Hilbert 90 we then find some $\gamma \in \overline{\mathbb{Q}}^*$ such that

$$\lambda_\sigma^2 = d(\sigma) \ {}^\sigma\gamma\gamma^{-1} \quad \text{for all } \sigma \in G_{\mathbb{Q}}.$$

Taking square roots we find that $\sqrt{d} : \sigma \mapsto \sqrt{d(\sigma)}$ and $\lambda : \sigma \mapsto \lambda_\sigma$ have the same cohomology class in $H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*)$.

Now note that the short exact sequence

$$1 \to \mathbb{Q}^* \to \overline{\mathbb{Q}}^* \to \overline{\mathbb{Q}}^*/\mathbb{Q}^* \to 1,$$

induces a long exact sequence containing a map $H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*) \to H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$ that maps $[\lambda] = [\sqrt{d}]$ to $[c_E] = \xi_E$. Since $d : G_{\mathbb{Q}} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ factors over $G_{\mathbb{Q}}^{K_d}$ so does $\sqrt{d} : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*/\mathbb{Q}^*$. Thus we know that $\sqrt{d(\sigma)} \in \mathbb{Q}^*$ for all $\sigma \in G_{K_d}$. Since ξ_E is the class of the coboundary of $\sqrt{d}$, this implies the restriction of ξ_E to $H^2(G_{K_d}, \mathbb{Q}^*)$ is trivial. Now applying Theorem 2.7.1 gives the desired result. □

In the framework [vL21a] the field K over which a `Qcurve` object is defined can be obtained by the method `definition_field`. This field is not necessarily the minimal field over which the coefficients are defined, but rather the Galois closure of the number field over which the coefficients were given upon creation.

The fixed field K_d can be obtained by the method `degree_field` and will be given as a subfield of the field K. Note that no method to find an isogenous curve that is defined over K_d has currently been implemented, but the proof of Theorem 8.2 in [Rib04] is constructive.

Next we look at Galois number fields K over which curves isogenous to a $\mathbb{Q}$-curve can be completely defined. Note that if a $\mathbb{Q}$-curve is completely defined over a Galois number field, then we can define its 2-cocycle c_E as the inflation of one defined on $G_{\mathbb{Q}}^K$. The converse is also true for the isogeny class.

Proposition 2.7.3 (Proposition 2.3 in [Que00])**.** *Let E be a $\mathbb{Q}$-curve defined over a Galois number field K. If there exists an element $\xi_K \in H^2(G_{\mathbb{Q}}^K, \mathbb{Q}^*)$ such that ξ_E is just the inflation of ξ_K, then there exists a curve E' isomorphic to E such that E is completely defined over K.*

Corollary 2.7.4. *Let E be a $\mathbb{Q}$-curve and let $\{d_1, \ldots, d_n\} \subset \mathbb{Q}^*$ be a basis of the image of the degree map in $\mathbb{Q}^*/(\pm(\mathbb{Q}^*)^2)$, then there is a $\mathbb{Q}$-curve E' isogenous to E completely defined over $K_d(\sqrt{d_1}, \ldots, \sqrt{d_n})$.*

Proof. Since $\{d_1, \ldots, d_n\}$ generate the image of the degree map in $\mathbb{Q}^*/(\pm(\mathbb{Q}^*)^2)$ we can write

$$d(\sigma) = (-1)^{x_0(\sigma)} \left(\prod_{i=1}^{n} d_i^{x_i(\sigma)} \right) y(\sigma)^2 \text{ for all } \sigma \in G_{\mathbb{Q}},$$

with $x_i : G_{\mathbb{Q}} \to \mathbb{Z}$ and $y : G_{\mathbb{Q}} \to \mathbb{Q}^*$. Note that as $d : G_{\mathbb{Q}} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is a homomorphism all the x_i are homomorphisms as maps $G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$. In particular this makes $\sigma \mapsto (-1)^{x_0(\sigma)}$ a homomorphism, so d has the same coboundary as $d' : G_{\mathbb{Q}} \to \mathbb{Q}^*$ given by

$$d'(\sigma) = \left(\prod_{i=1}^{n} d_i^{x_i(\sigma)} \right) y(\sigma)^2 \text{ for all } \sigma \in G_{\mathbb{Q}},$$

Now we apply the same arguments as in the proof of Corollary 2.7.2 to d'. So we note that $[\lambda] = [\sqrt{d'}] \in H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*)$ and that the coboundary of $\sqrt{d'}$ is a representative of ξ_E. Note that

$$(\partial d')(\sigma, \tau) = \sqrt{d'(\sigma)}^{\sigma} \sqrt{d'(\tau)} \sqrt{d'(\sigma\tau)}^{-1} \text{ for all } \sigma, \tau \in G_{\mathbb{Q}}$$

Since the x_i are homomorphisms $G_{\mathbb{Q}}^{K_d} \to \mathbb{Z}/2\mathbb{Z}$ the value of $d'(\sigma)$ only depends on the restriction of σ to K_d. Furthermore the action of σ on $\sqrt{d'(\tau)}$ only depends on the restriction of σ to $\mathbb{Q}(\sqrt{d'(\tau)})$. Therefore ξ_E can be defined from a 2-cocycle defined over $K_d(\sqrt{d'(\tau)} : \tau \in G_{\mathbb{Q}}) = K_d(\sqrt{d_1}, \ldots, \sqrt{d_n})$. Applying Proposition 2.7.3 now gives the desired result. □

Note that the field given in Corollary 2.7.4 is not necessarily minimal. In fact there is a refinement of Proposition 2.7.4.

Theorem 2.7.5 (Theorem 3.2 from [Que00])**.** *Given a $\mathbb{Q}$-curve E there exists an isogenous curve completely defined over a Galois number field K if and only if*

1. *K_d is a subfield of K; and*
2. *$\xi_{E,\pm}$ arises from an element in $H^2(G_{\mathbb{Q}}^K, \{\pm 1\})$.*

In the framework [vL21a] one can obtain a field over which a `Qcurve` is completely defined by the method `complete_definition_field`. Note that this field is simply the composite field of the `definition_field` and the fields over which each stored isogeny is defined. Furthermore the code takes a Galois closure thereof as this field is used as a basis for the function `c`. Note that for correct conversions the class `Qcurve` also keeps track of an inclusion from the `definition_field` to the `complete_definition_field`.

Next we look at Galois number fields over which our splitting maps for c_E can be defined. We start with the associated splitting character $\varepsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$. Since they are continuous homomorphisms we can take the fixed field K_ε of their kernel and know that this is the smallest number field for which ε factors over $G_{\mathbb{Q}}^{K_\varepsilon}$. In fact we can realize this field as a subfield of the cyclotomic field $\mathbb{Q}(\zeta_N)$ where N is the conductor of ε.

Let β be a splitting map for c_E with splitting character ε. Note that we have

$$\beta(\sigma) \in \mathbb{Q}^* \iff \beta(\sigma)^2 = \varepsilon(\sigma)d(\sigma) \in (\mathbb{Q}^*)^2 \iff \varepsilon(\sigma) = 1 \text{ and } d(\sigma) \in (\mathbb{Q}^*)^2,$$

for all $\sigma \in G_{\mathbb{Q}}$, hence the fixed field of the homomorphism $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^* / \mathbb{Q}^*$ must be $K_\beta = K_d K_\varepsilon$. In particular by changing β if necessary we may assume that $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ is defined over K_β.

The class `Qcurve` provides the methods `splitting_character_field` and `splitting_field` to compute the fields K_ε and K_β respectively with the framework [vL21a]. Note that these methods can be indexed similar to the methods `splitting_character`, `splitting_map` and `twist_character`. Note that the fields returned by `splitting_character_field` are the fields over which the

Galois characters returned by `splitting_character` are defined. In particular all of these fields are Galois. Note that a `splitting_field` is the composite field of the corresponding `splitting_character_field` and the `degree_field`, and that the class `Qcurve` keeps track of the corresponding inclusions.

The class `Qcurve` also has a method `decomposition_field`. This field is the composite field of the `complete_definition_field` and the `splitting_field` of the default splitting character (index 0). This is a field K over which the curve is completely defined and the default splitting map for ξ_E is defined. We will see in Section 2.9 that $\mathrm{Res}_{\mathbb{Q}}^{K} E$ decomposes as a product of abelian varieties of GL_2-type if K is abelian, hence the name. As with the other fields the class `Qcurve` keeps track of the inclusions from the `complete_definition_field` and the `splitting_field`.

One more note to make about the implementation is that in the tower of fields `degree_field`, `definition_field`, `complete_definition_field`, and `decomposition_field` two fields are actually the same if the extension has degree 1. This makes objects of `Qcurve` easier to use, for example by redefining the curve over `decomposition_field` so that all of these fields actually become the same field.

One last remark about these fields of definition is that an isogenous curve completely defined over that field can often be realized as a twist.

Proposition 2.7.6. *Let E be a $\mathbb{Q}$-curve defined over a field K and let $\gamma \in K^*$. The curve E_γ of E twisted by γ has isogenies ${}^\sigma E_\gamma \to E_\gamma$ with corresponding constants λ'_σ satisfying*

$$(\lambda'_\sigma)^2 = \lambda_\sigma^2 \, {}^\sigma\gamma\gamma^{-1}.$$

Corollary 2.7.7. *Let E be a $\mathbb{Q}$-curve defined over K and let $d_1, \ldots, d_n$ be a basis of the image of the degree map in $\mathbb{Q}^*/(\pm(\mathbb{Q}^*)^2)$, then there is a $\gamma \in K^*$ such that E_γ is completely defined over $K(\sqrt{d_1}, \ldots, \sqrt{d_n})$.*

Proof. Following the proof of Corollary 2.7.4 we find a $\gamma \in \overline{\mathbb{Q}}^*$ such that

$$\lambda_\sigma^2 = d'(\sigma)\, {}^\sigma\gamma\gamma^{-1} \text{ for all } \sigma \in G_{\mathbb{Q}}.$$

Now without loss of generality we may assume that all isogenies $\phi_\sigma : {}^\sigma E \to E$ for $\sigma \in G_K$ are trivial, hence ${}^\sigma\gamma = \gamma$ for all such σ. This implies that $\gamma \in K^*$, and hence by Proposition 2.7.6 the curve $E_{\gamma^{-1}}$ has isogenies with corresponding constants $\sqrt{d'(\sigma)}$. These are defined over $K(\sqrt{d_1}, \ldots, \sqrt{d_n})$, hence $E_{\gamma^{-1}}$ is completely defined over that field. □

Corollary 2.7.8. *Let E be a $\mathbb{Q}$-curve completely defined over a field K over which a splitting map β for ξ_E is defined, then there exists a $\gamma \in K^*$ such that $c_{E_\gamma} = c_\beta$.*

Proof. Let $\gamma \in K^*$ be the element corresponding to $c_\beta c_E^{-1}$ of which existence was shown in Corollary 2.5.2 and which can be computed using Proposition 2.5.5. The latter also tells us there is a map $\alpha : G_{\mathbb{Q}}^K \to K^*$ such that $c_\beta c_E^{-1} = \partial\alpha$ and $\alpha^2 = \partial\gamma$. Using Proposition 2.7.6 we now find that

$$c_{E_\gamma} = c_E \partial\alpha = c_E c_\beta c_E^{-1} = c_\beta. \qquad \square$$

The framework [vL21a] can immediately compute the twists in the previous corollaries from a given `Qcurve`. The twisted curve from Corollary 2.7.7 can be obtained with the method `complete_definition_twist` where the field K is taken to be the `definition_field`. The twisted curve from Corollary 2.7.8 can be obtained with the method `decomposable_twist` where the field K is taken to be the `decomposition_field`. One can also obtain the respective twist parameters γ using the hidden methods `_complete_definition_twist` and `_decomposable_twist` respectively.

One can also manually perform twists using a twisting parameter γ by using the method `twist`. Note that the method `twist` will always return a `Qcurve` as do the methods above. Furthermore the returned `Qcurve` will have its definition field and complete definition field minimal for a particular Weierstrass model, so not up to isogeny or isomorphism.

Example 2.7.9. `Qcurve1.rst` `Qcurve1Frey.rst` We return to the curve E from Example 2.1.4. Using the degree map as determined in Example 2.4.4 the framework [vL21a] shows us that $K_d = \mathbb{Q}(\sqrt{3})$.

```
sage: E.degree_field()
Number Field in sqrt3 with defining polynomial x^2 - 3 with \
sqrt3 = 1.732050807568878?
```

We see that E is defined over this field, hence trivially proving Corollary 2.7.2 for E.

Note that we determined in Example 2.2.3 that E is completely defined over $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3}) = K_d(\sqrt{-2})$. This confirms Corollary 2.7.4 for E as $\{-2\}$ spans the image of the degree map modulo $\pm (\mathbb{Q}^*)^2$ (see also Example 2.4.4). Note that the splitting character β found in Example 2.4.4 has coboundary c_β that has the same cohomology class as ξ_E. Therefore $\xi_{E,\pm}$ arises from a cohomology class in $H^2(G_{\mathbb{Q}}^{K_d}, \{\pm 1\})$, namely the class of the sign of c_β. Therefore by

Theorem 2.7.5 we find that E must be isogenous to a curve completely defined over K_d.

In fact we can find this isogenous curve completely defined over K_d as a twist of E. From Example 2.5.4 we have a $\gamma \in K_d$ which satisfies Proposition 2.5.3 for $c = c_\beta c_E^{-1}$. Therefore Proposition 2.7.6 tells us that the twisted curve E_γ must have isogenies such that $c_{E_\gamma} = c_\beta$. In particular this means that these isogenies are defined over K_d as c_β is, so E_γ is completely defined over K_d. It is also immediately clear that β is a splitting map for c_{E_γ} that is also defined over K_d, giving us an example of Corollary 2.7.8. Similarly the framework [vL21a] will give such a curve as the `decomposable_twist`.

```
sage: E.decomposable_twist() # E is a Qcurve
Q-curve defined by y^2 = x^3 + (-6*lu0-12)*x^2 + (-18*lu0-36)*x \
over Number Field in lu0 with defining polynomial x^2 - 12 \
with lu0 = -1/5*lu^3 + 7/5*lu
```

Note that the method is the same for a Frey $\mathbb{Q}$-curve but the output is a little different.

```
sage: E.decomposable_twist() # E is a FreyQcurve
Frey Q-curve defined by y^2 = x^3 + ((-6*lu0-12)*a)*x^2 + \
((18*lu0+72)*a^2+(36*lu0+108)*b)*x over Number Field in lu0 \
with defining polynomial x^2 - 12 with \
lu0 = -1/5*lu^3 + 7/5*lu with parameters (a, b)
```

The last field we should talk about is the image field L_β of a splitting map β. Since β factors over $G_{\mathbb{Q}}^{K_\beta}$ we know that $L_\beta = \mathbb{Q}(\beta(\sigma) : \sigma \in G_{\mathbb{Q}}^{K_\beta})$, but Quer [Que00] also gives a more direct formula.

Proposition 2.7.10 (Proposition 4.1 from [Que00])**.** *Let E be a $\mathbb{Q}$-curve with splitting map β for c_E. If $\{a_1, \ldots, a_m\}$ and $\{d_1, \ldots, d_m\}$ is a dual basis of the degree map d of E and the corresponding character ε has order n then*

$$L_\beta = \begin{cases} \mathbb{Q}(\zeta_{2n}, \sqrt{d_1}, \ldots, \sqrt{d_n}) & \textit{if } K_\varepsilon \cap K_d = \mathbb{Q} \\ \mathbb{Q}(\zeta_{2n}\sqrt{d_1}, \ldots, \sqrt{d_n}) & \textit{if } K_\varepsilon \cap K_d = \mathbb{Q}(\sqrt{a_1}). \end{cases}$$

Note that by choosing the dual basis correctly one is always in one of the two cases mentioned.

The class `Qcurve` in the framework [vL21a] provides the field L_β for a splitting map for ξ_E with `splitting_image_field`. This method is indexed in the same way as `splitting_map`. Note that the associated `splitting_map` is a function with codomain the corresponding `splitting_image_field`.

Example 2.7.11. `Qcurve4.rst` Look at the curve

$$\begin{aligned} E : Y^2 = X^3 &- 60\left(15 + 10\sqrt{2} + 5\sqrt{5} + 2\sqrt{10}\right) X \\ &+ 80\left(210 + 135\sqrt{2} + 70\sqrt{5} + 49\sqrt{10}\right) \end{aligned}$$

defined over $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Using the framework [vL21a] we find that this is a $\mathbb{Q}$-curve as E is isogenous to its Galois conjugates by isogenies of degree 2, 3 and 6. We can also compute that the degree map is

$$d(\sigma) = \begin{cases} 1 & \text{if } \sigma \in G_K \\ 2 & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{2})} \text{ and } \sigma \notin G_K \\ 3 & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{5})} \text{ and } \sigma \notin G_K \\ 6 & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{10})} \text{ and } \sigma \notin G_K. \end{cases}$$

We ask the framework [vL21a] to compute a splitting character ε for E which gives us a character of conductor 15 and order 4. The corresponding field is

$$K_\varepsilon = \mathbb{Q}\left(\zeta_{15} + \zeta_{15}^{-1}\right) = \mathbb{Q}\left(\sqrt{\frac{15 - 3\sqrt{5}}{2}}\right).$$

This implies that the minimal field over which the corresponding splitting map β for ξ_E is defined is

$$K_\beta = K\left(\sqrt{\frac{15 - 3\sqrt{5}}{2}}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{15 - 3\sqrt{5}}\right).$$

Note that $K_d \cap K_\beta = \mathbb{Q}(\sqrt{5})$ so by choosing the dual basis $\{5, 2\}$ and $\{2, 3\}$ for the degree map we can apply Proposition 2.7.10 to find that the image field of such a splitting map β for ξ_E must be

$$L_\beta = \mathbb{Q}(\zeta_8\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{-1}, \sqrt{3}).$$

Section 2.8

Associated Galois representations

Thus far we have looked into explicitly computing splitting maps for $\mathbb{Q}$-curves, which give $\mathbb{Q}$-simple abelian varieties A of GL_2-type as in Theorem 2.1.9. Now we want to make the modularity of these abelian varieties A more explicit than in Theorem 2.1.10 by computing the character and level of the newform f. For this we first want an explicit description of Galois representations associated with A.

For a regular elliptic curve E defined over a number field K one can define Galois representations by looking at the action of G_K on $E(\overline{K})$. Since this action commutes with isogenies defined over K it restricts to the torsion points $E[m]$. For a prime number l this action therefore induces 2-dimensional representations on $E[l]$ and the Tate module $T_l(E) = \varprojlim E[l^n]$. We will denote these by

$$\begin{aligned} \rho_{E,l} &: G_K \to \mathrm{Aut}(T_l(E)) \cong \mathrm{GL}_2(\mathbb{Z}_l), \text{ and} \\ \overline{\rho_{E,l}} &: G_K \to \mathrm{Aut}(E[l]) \cong \mathrm{GL}_2(\mathbb{F}_l). \end{aligned}$$

Sometimes (made clear by the context) we will also use $\rho_{E,l}$ as a representation

$$\rho_{E,l} : G_K \to \mathrm{Aut}(V_l(E)) \cong \mathrm{GL}_2(\mathbb{Q}_l),$$

where $V_l(E) = \mathbb{Q} \otimes_{\mathbb{Z}} T_l(E)$. The representations $\rho_{E,l}$ and $\overline{\rho_{E,l}}$ are called the *l-adic* and *mod l representation* of E respectively. Note that $\overline{\rho_{E,l}}$ is the reduction mod l of $\rho_{E,l} : G_K \to \mathrm{Aut}(T_l(E))$.

For a $\mathbb{Q}$-simple abelian variety A of GL_2-type we can do a similar construction, i.e. we take the representations induced by the action of $G_{\mathbb{Q}}$ on $A[l]$ and $T_l(A) = \varprojlim A[l^n]$ for a prime number l. Note that in this case we have more isogenies defined over $\mathbb{Q}$ that commute with the action of $G_{\mathbb{Q}}$, as $L = \mathrm{End}_{\mathbb{Q}}^0 A$ is a number field of degree $\dim A$ by Theorem 2.2.1. This implies we can see $V_l(A) = \mathbb{Q} \otimes_{\mathbb{Z}} T_l(A)$ as a module over $L \otimes_{\mathbb{Q}} \mathbb{Q}_l = \prod_{\lambda | l} L_\lambda$, where the product is over primes of L. This gives us 2-dimensional λ-adic Galois representations

$$\rho_{A,\lambda} : G_{\mathbb{Q}} \to \mathrm{Aut}(V_l(A)) \cong \mathrm{GL}_2(L \otimes_{\mathbb{Q}} \mathbb{Q}_l) \to \mathrm{GL}_2(L_\lambda),$$

for each prime λ of L above a prime number l. If $\mathrm{End}_{\mathbb{Q}} A = \mathcal{O}_L$ we can interpret $T_l(A)$ and $A[l]$ as $\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}_l = \prod_{\lambda | l} \mathcal{O}_{L,\lambda}$ and $\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{F}_l = \prod_{\lambda | l} \mathbb{F}_\lambda$ modules respectively to obtain representations

$$\rho_{A,\lambda} : G_{\mathbb{Q}} \to \mathrm{Aut}(T_l(A)) \cong \mathrm{GL}_2(\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}_l) \to \mathrm{GL}_2(\mathcal{O}_{L,\lambda}),$$

and 2-dimensional mod λ representations

$$\overline{\rho_{A,\lambda}} : G_{\mathbb{Q}} \to \mathrm{Aut}(A[l]) \cong \mathrm{GL}_2(\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{F}_l) \to \mathrm{GL}_2(\mathbb{F}_\lambda),$$

for each prime λ of L above a prime number l. Here $\overline{\rho_{A,\lambda}}$ is the reduction of $\rho_{A,\lambda}$ modulo λ. If $\operatorname{End}_{\mathbb{Q}} A \neq \mathcal{O}_L$ we can still see $\rho_{A,\lambda}$ as a representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{L,\lambda})$ by either replacing A with an isogenous abelian variety A' with $\operatorname{End}_{\mathbb{Q}} A' = \mathcal{O}_L$ or choosing an appropriate basis. Given such a choice we define the mod λ representation $\overline{\rho_{A,\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ as its reduction modulo λ. To make these mod λ representations unique we will always replace $\overline{\rho_{A,\lambda}}$ by its semi-simplification.

Now let E be a $\mathbb{Q}$-curve completely defined over a Galois number field K. Suppose there is a splitting map $\beta : G_{\mathbb{Q}}^K \to \overline{\mathbb{Q}}^*$ for E, which by Section 2.2 defines a $\mathbb{Q}$-simple abelian variety A of GL_2-type that has E as a quotient. We can associate Galois representations to the pair (E, β) by taking the corresponding Galois representations of A. In particular we shall write $\rho_{\beta,\lambda} = \rho_{A,\lambda}$ and $\overline{\rho_{\beta,\lambda}} = \overline{\rho_{A,\lambda}}$, which are called the *$\lambda$-adic* and *mod λ Galois representations associated with β* respectively. Note that isogenous A have isomorphic Galois representations, hence these Galois representations are well-defined up to isomorphism.

To see how these Galois representations relate to E and β, note that A is a subvariety of $B = \operatorname{Res}_{\mathbb{Q}}^K E$. For each isogeny $\phi_\sigma : {}^\sigma E \to E$ there is an isogeny $\Phi_\sigma \in \operatorname{End}_{\mathbb{Q}}(B)$ and a corresponding element $\beta(\sigma) \in L_\beta = \operatorname{End}_{\mathbb{Q}}^0 A$. In case $\beta(\sigma) \in \operatorname{End}(A)$ we obtain a commutative diagram (on $\overline{\mathbb{Q}}$-points)

$$\begin{tikzcd}
E \arrow[r, "\sigma"] & {}^\sigma E \arrow[r, "\phi_\sigma"] & E \\
B \arrow[u, "\pi"] \arrow[r, "\sigma"] & B \arrow[u, "{}^\sigma\pi"] \arrow[r, "\Phi_\sigma"] & B \arrow[u, "\pi"] \\
A \arrow[u, hook] \arrow[r, "\sigma"] & A \arrow[u, hook] \arrow[r, "\beta(\sigma)"] & A, \arrow[u, hook]
\end{tikzcd} \tag{2.6}$$

with the inclusion $A \hookrightarrow B$ and canonical map $\pi : B \to E$. Note that the maps σ are not morphisms, and that the top part of the diagram must be defined over K whereas the bottom part may also be taken over $\mathbb{Q}$. Furthermore the top row together with the maps π and $A \hookrightarrow B$ fix the entire diagram.

Note that in the diagram (2.6) we may replace the abelian varieties with their m-torsion points for any $m > 0$, hence we may also replace them with Tate modules T_l or V_l for some prime number l. This shows us the Galois representations $\rho_{\beta,l}$ and $\overline{\rho_{\beta,l}}$ are fixed by β, and the action of $\phi_\sigma \circ \sigma$ on E, as expressed by the following proposition.

Proposition 2.8.1. *Given the setting above and a finite prime $\lambda \mid l$ of L_β we have that*

$$\begin{aligned} \rho_{\beta,\lambda} : G_{\mathbb{Q}} \to\ & L_\beta^* \otimes \operatorname{Aut}(V_l(E)) \ \cong \mathrm{GL}_2(L_\beta \otimes_{\mathbb{Q}} \mathbb{Q}_l) \to \mathrm{GL}_2(L_{\beta,\lambda}) \\ \sigma\ \mapsto\ & \beta(\sigma)^{-1} \otimes (\phi_\sigma \circ \sigma). \end{aligned}$$

Proof. Note that we obtain a diagram like (2.6) if we replace ϕ_σ, Φ_σ, and $\beta(\sigma)$ by $n\phi_\sigma$, $n\Phi_\sigma$ and $n\beta(\sigma)$ for any $n \in \mathbb{Z}_{>0}$ such that $n\beta(\sigma) \in \operatorname{End}(A)$. Since multiplication by n is an isomorphism on the Tate modules $V_l(E), V_l(B), V_l(A)$ we obtain a commutative diagram as in (2.6) by replacing each variety with their Tate module. The result now follows directly from the fact such a diagram commutes. □

Using this description we can see that these Galois representations behave nicely under changing E by an isogeny.

Proposition 2.8.2. *Let $\psi : E \to E'$ be an isogeny of $\mathbb{Q}$-curves, let $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ be a splitting map for c_E, and let λ be a finite prime of L_β, then there exists a splitting map $\beta' : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ for $c_{E'}$ with image field L_β such that*

$$\rho_{\beta,\lambda} \cong \rho_{\beta',\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(L_{\beta,\lambda}).$$

Proof. Let $\phi'_\sigma : {}^\sigma E' \to E'$ denote the isogenies associated to E'. For all $\sigma \in G_{\mathbb{Q}}$ we have two isogenies $\psi \circ \phi_\sigma$, $\phi'_\sigma \circ {}^\sigma\psi \in \hom_{\overline{\mathbb{Q}}}({}^\sigma E, E')$. Since $\operatorname{End}^0_{\overline{\mathbb{Q}}}(E') = \mathbb{Q}$ these spaces are 1-dimensional $\mathbb{Q}$-vector spaces, hence there exist $a_\sigma \in \mathbb{Q}^*$ such that

$$\phi'_\sigma \circ {}^\sigma\psi = a_\sigma\, \psi \circ \phi_\sigma \in \hom_{\overline{\mathbb{Q}}}({}^\sigma E, E') \otimes_{\mathbb{Z}} \mathbb{Q}.$$

A quick computation shows that

$$\begin{aligned} c_{E'}(\sigma,\tau) &= \phi'_\sigma\, {}^\sigma\phi'_\tau\, (\phi'_{\sigma\tau})^{-1} \\ &= \phi'_\sigma\, {}^\sigma\psi\, ({}^\sigma\psi)^{-1}\, {}^\sigma\phi'_\tau\, {}^{\sigma\tau}\psi\, (\phi'_{\sigma\tau}\, {}^{\sigma\tau}\psi)^{-1} \\ &= a_\sigma a_\tau a_{\sigma\tau}^{-1} \psi \phi_\sigma\, {}^\sigma\phi_\tau\, (\phi_{\sigma\tau})^{-1}\, \psi^{-1} \\ &= a_\sigma a_\tau a_{\sigma\tau}^{-1} c_E(\sigma,\tau), \end{aligned}$$

for all $\sigma, \tau \in G_{\mathbb{Q}}$ where inverses are taken in the corresponding homomorphism ring tensored with $\mathbb{Q}$. Therefore $\beta' : \sigma \mapsto a_\sigma \beta(\sigma)$ is a splitting map for $c_{E'}$ with the same image field L_β.

Note that the induced map $\psi : V_l(E) \to V_l(E')$ is an isomorphism with inverse $\psi^{-1} = \frac{\hat{\psi}}{\deg \psi}$. Therefore we have for each $\sigma \in G_{\mathbb{Q}}$ that

$$\begin{aligned}\rho_{\beta',\lambda}(\sigma) &= \beta'(\sigma)^{-1}\, \phi'_\sigma\, \sigma\, \psi\, \psi^{-1} \\ &= \beta(\sigma)^{-1}\, a_\sigma^{-1}\, \phi'_\sigma\, {}^\sigma\psi\, \sigma\, \psi^{-1} \\ &= \beta(\sigma)^{-1}\, \psi\, \phi_\sigma\, \sigma\, \psi^{-1} \\ &= \psi\, \rho_{\beta,\lambda}\, \psi^{-1},\end{aligned}$$

which completes the proof. □

In particular the above result shows that we may assume without loss of generality that $\phi_\sigma = \mathrm{Id}$ for all $\sigma \in G_K$ in which case we have

$$\rho_{\beta,\lambda}|_{G_K} = \rho_{E,l} : G_K \to \mathrm{GL}_2(\mathbb{Q}_l) \subseteq \mathrm{GL}_2(L_{\beta,\lambda}),$$

and similarly for $\overline{\rho_{\beta,\lambda}}$. This allows us to prove an important result.

Theorem 2.8.3. *Let K be a Galois number field over which E is completely defined, for which we have a splitting map $\beta : G_{\mathbb{Q}}^K \to \overline{\mathbb{Q}}^*$ for c_E, and for which we have $\phi_\sigma = \mathrm{Id}$ for all $\sigma \in G_K$. Let p be a prime number that does not ramify in K.*

- *If E has good reduction at p (recalling Definition 2.1.7), then $\rho_{\beta,\lambda}$ and $\overline{\rho_{\beta,\lambda}}$ are finite at p for every prime λ. In particular $\rho_{\beta,\lambda}$ and $\overline{\rho_{\beta,\lambda}}$ are unramified at such p for every prime $\lambda \nmid p$.*
- *If E has multiplicative reduction at p (recalling Definition 2.1.7), then $\overline{\rho_{\beta,\lambda}}$ is finite at p for every prime $\lambda \mid l$ where l is a prime number dividing the order of a prime $\mathfrak{p} \mid p$ of K in the minimal discriminant of E. In particular $\overline{\rho_{\beta,\lambda}}$ is unramified at such p for every prime $\lambda \nmid p$ with this property.*

Proof. Note that the assumptions imply that the ramification subgroup $I_p \subseteq G_{\mathbb{Q}}$ is a subset of the ramification group $I_{\mathfrak{p}} \subset G_K$ for any prime $\mathfrak{p} \mid p$ of K, and that $\rho_{\beta,\lambda}|_{G_K} = \rho_{E,l}$ for any prime $\lambda \mid l$. To prove the statements it therefore suffices to prove that $\rho_{E,l}$ or $\overline{\rho_{E,l}}$ is finite at a prime $\mathfrak{p} \mid p$ if the mentioned conditions are satisfied. This is a standard result known about Galois representations of elliptic curves. See for example [DS05, Theorem 9.4.1] and [Dah08, page 26-27] for results with $K = \mathbb{Q}$ that can easily be extended to general number fields K. □

Note that there is one other way of defining Galois representations associated to the $\mathbb{Q}$-curve E as was done in for example [Ell04]. We can derive these representations from the representations $\rho_{\beta,\lambda}$ and $\overline{\rho_{\beta,\lambda}}$ by taking the projectivization of these representations. Note that these do no longer depend on the specific splitting map β for c_E, but rather only on the action of $\phi_\sigma \circ \sigma$ on $\mathbb{P}V_l(E)$ or $\mathbb{P}E[l]$ respectively. Here $\mathbb{P}V$ denotes the space of all lines through the origin in the 2-dimensional vector space V, which is itself a projective line.

Definition 2.8.4. For a $\mathbb{Q}$-curve E and a prime number l we define the projective representations

$$\begin{aligned} \mathbb{P}\rho_{E,l} : G_{\mathbb{Q}} &\to \mathrm{Aut}(\mathbb{P}V_l(E)) \cong \mathrm{PGL}_2(\mathbb{Q}_l) \\ \sigma &\mapsto \quad \phi_\sigma \circ \sigma \\ \text{and} & \\ \mathbb{P}\overline{\rho_{E,l}} : G_{\mathbb{Q}} &\to \ \mathrm{Aut}(\mathbb{P}E[l]) \ \cong \mathbb{P}\,\mathrm{PGL}_2(\mathbb{F}_l) \\ \sigma &\mapsto \quad \phi_\sigma \circ \sigma. \end{aligned}$$

Note that $\mathbb{P}\rho_{E,l} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\overline{\mathbb{Q}_l})$ and $\mathbb{P}\overline{\rho_{E,l}} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\overline{\mathbb{F}_l})$ are the projectivizations of $\rho_{\beta,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}_l})$ and $\overline{\rho_{\beta,\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_l})$ respectively for any splitting map β for c_E and $\lambda \mid l$, up to isomorphism and noting that we might have to take semisimplifications for the mod l representations. By Proposition 2.8.2 the isomorphism classes of $\mathbb{P}\rho_{E,l}$ and $\mathbb{P}\overline{\rho_{E,l}}$ therefore only depend on the class of E modulo isogenies of a degree not divisible by l. Furthermore we may assume without loss of generality that E is defined over a field K with $\phi_\sigma = \mathrm{Id}$ for all $\sigma \in G_K$, hence we see that $\mathbb{P}\rho_{E,l}|_{G_K}$ and $\mathbb{P}\overline{\rho_{E,l}}|_{G_K}$ are the projectivizations of the usual Galois representations $\rho_{E,l} : G_K \to \mathrm{Aut}(V_l(E))$ and $\overline{\rho_{E,l}} : G_K \to \mathrm{Aut}(E[l])$ associated with E as a regular elliptic curve over K.

By Theorem 2.1.10 we know that the abelian variety A associated to (E, β) is isogenous to a variety A_f associated to a newform $f \in \mathcal{S}_2(\Gamma_1(N))$. By definition (see e.g. [DS05, page 401]) the λ-adic Galois representation $\rho_{f,\lambda}$ associated with f is the representation $\rho_{A_f,\lambda}$. This implies that $\rho_{\beta,\lambda} \cong \rho_{f,\lambda}$ for each prime λ of L_β. Since many of the properties of $\rho_{f,\lambda}$ depend directly on f, and $\rho_{\beta,\lambda}$ depends only on β, E, and the isogenies ϕ_σ, we can now do most computations without explicitly computing A. In particular the character and the level of the newform f can be derived from the determinant and the conductor of $\rho_{\beta,\lambda}$ respectively.

Proposition 2.8.5. *Let E be a $\mathbb{Q}$-curve and β be a splitting map for c_E, then*

$$\rho_{\beta,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(L_\lambda)$$

has determinant given by

$$\det \rho_{\beta,\lambda} = \varepsilon^{-1}\chi_l,$$

where χ_l is the l-adic cyclotomic character and ε is the splitting character corresponding to β.

Proof. Note that for an arbitrary $\sigma \in G_{\mathbb{Q}}$ we have

$$\det \rho_{\beta,\lambda}(\sigma) = \beta(\sigma)^{-2} \det(\phi_\sigma \circ \sigma),$$

by Proposition 2.8.1. To compute $\det(\phi_\sigma \circ \sigma)$ we can use the Weil pairing e on $V_l(E)$. Let $\{v_1, v_2\}$ be a basis for $V_l(E)$ and let

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

be the matrix for $\phi_\sigma \circ \sigma$ with respect to this basis. By the properties of the Weil pairing we find that

$$\begin{aligned} e(v_1, v_2)^{\det(\phi_\sigma \circ \sigma)} &= e(v_1, v_2)^{ad-bc} \\ &= e(av_1 + bv_2, cv_1 + dv_2) \\ &= e\left((\phi_\sigma \circ \sigma)\, v_1, (\phi_\sigma \circ \sigma)\, v_2\right) \\ &= e\left(\hat{\phi_\sigma}\phi_\sigma {}^\sigma v_1, {}^\sigma v_2\right) \\ &= e\left({}^\sigma v_1, {}^\sigma v_2\right)^{\deg \phi_\sigma} \\ &= \left({}^\sigma e(v_1, v_2)\right)^{\deg \phi_\sigma} \\ &= e(v_1, v_2)^{\chi_l(\sigma) \deg \phi_\sigma}. \end{aligned}$$

Since e is nondegenerate this implies that

$$\det(\phi_\sigma \circ \sigma) = \chi_l(\sigma) d(\sigma).$$

Noting that $\varepsilon = \beta^2 d^{-1}$ we see that the determinant of $\rho_{E,\lambda}$ is as claimed. □

Corollary 2.8.6. *Let E be a $\mathbb{Q}$-curve, let β be a splitting map for c_E, and let f be a newform associated to (E, β) by Theorem 2.1.10, then f has character ε^{-1}, where ε is the splitting character associated to β.*

Proof. This is immediate as by Theorem 9.5.4 in [DS05] the determinant of the λ-adic Galois representation associated to f for $\lambda \mid l$ is the character of f times the l-adic cyclotomic character. □

Section 2.9

Computing the newform levels

For a $\mathbb{Q}$-curve E with a corresponding splitting map β for c_E the level of an associated newform f will somehow be related to the conductor of $\rho_{\beta,\lambda}$ for some prime $\lambda \mid l$. Outside powers of l this conductor is by definition equal to the conductor of the associated abelian variety A. For this we have the following result.

Proposition 2.9.1. *Let $f \in \mathcal{S}_2(\Gamma_1(N))$ be a newform, then the associated $\mathbb{Q}$-simple abelian variety A_f of* GL_2*-type has conductor $N^{[K_f:\mathbb{Q}]}$.*

Proof. This follows directly from the ingredients given in [Car89], although the result is not explicitly stated there. □

What thus remains to compute the level of the associated newform is to compute the conductor of the abelian variety A associated to a splitting map β for c_E. In case A is the restriction of scalars of E this is easy due to the following result.

Proposition 2.9.2 (Proposition 1 of [Mil72])**.** *Let E be an elliptic curve over the number field K. Let $\mathcal{N}$ be the ideal norm of K, let Δ_K be the discriminant of K, and let N_E be the conductor of E over K, then* $\mathrm{Res}_{\mathbb{Q}}^{K}$ *E has conductor*

$$\Delta_K^2 \, \mathcal{N}\left(N_E\right).$$

In the framework [vL21a] one can compute this conductor for a `Qcurve` using the method `conductor_restriction_of_scalars`. Note that this method always assumes K to be the field returned by `decomposition_field`. For a `FreyQcurve` the method works a little different as in that case conductor exponents can only be explicitly computed for finitely many primes. By providing a list of finite primes of the `decomposition_field` as the argument `additive_primes` one can limit for which primes the conductor exponent is explicitly computed. The result will in that case be an expression with on the left side the product of all prime numbers – those below the given primes and those dividing the discriminant of K – to the appropriate power, and on the right side a string that tells how to calculate the remaining part of the conductor. Similar to the implementation of `conductor` of a `FreyCurve` the code will assume the finite primes of K not in `additive_primes` do not divide both c_4 and the discriminant of the curve, so this string will denote the norm of the radical of the discriminant. Note that not specifying the argument `additive_primes` will make it default to the result of `primes_of_possible_additive_reduction`.

Example 2.9.3. `Qcurve1.rst` `Qcurve1Frey.rst` We return to the curve E from Example 2.1.4. Example 2.7.9 showed that if we twist E by $\gamma = 1 - \sqrt{3}$ as found in Example 2.5.4 we get a curve E_γ completely defined over $K_d = \mathbb{Q}(\sqrt{3})$. Furthermore this $\mathbb{Q}$-curve E_γ also has a splitting map β for c_{E_γ} as shown in Example 2.7.9.

From the definition of β as given in Example 2.4.4 it is not hard to see that $L_\beta = \mathbb{Q}(\sqrt{-2})$ meaning that the associated $\mathbb{Q}$-simple abelian variety A has dimension 2 which is equal to the dimension of $\operatorname{Res}_{\mathbb{Q}}^{K_d} E_\gamma$. This implies that $\operatorname{Res}_{\mathbb{Q}}^{K_d} E_\gamma$ must be isogenous to A meaning they have the same conductor. Note that A is again isogenous to the abelian variety of the newform f associated to (E_γ, β), hence by Proposition 2.9.1 and Proposition 2.9.2 we find that

$$N^2 = \Delta_{K_d}^2 \mathcal{N}(N_{E_\gamma}),$$

where N is the level of f, Δ_{K_d} is the discriminant of K_d, $\mathcal{N}$ is the ideal norm of K_d and N_{E_γ} is the conductor of E_γ over K_d.

We can use the framework [vL21a] to compute the right hand side of this equation, but note that the output is different depending on whether E is a $\mathbb{Q}$-curve or a Frey $\mathbb{Q}$-curve. First we do the $\mathbb{Q}$-curve case.

```
sage: Egamma = E.twist(gamma)
sage: RHS = Egamma.conductor_restriction_of_scalars(); RHS
sage: RHS.factor()
2^18 * 3^2
```

Next we do the Frey $\mathbb{Q}$-curve case.

```
sage: Egamma = E.twist(gamma)
sage: RHS = Egamma.conductor_restriction_of_scalars(); RHS
2^(n0+4)*3^(n1+2)*Norm(Rad_P( ((-22394880*lu0 + 77635584)) * \
(a^2 + (-1/2*lu0)*b) * (a^2 + (1/2*lu0)*b)^2 ))
 where
n0 =  12 if (’a’, ’b’) == (1, 0) mod 2
      14 if (’a’, ’b’) == (1, 1) mod 2
      8  if (’a’, ’b’) == (0, 3), (2, 3) mod 4
      0  if (’a’, ’b’) is 1 of 4 possibilities mod 8
      4  if (’a’, ’b’) is 1 of 4 possibilities mod 8
```

```
n1 =  0 if ('a', 'b') is 1 of 6 possibilities mod 3
      2 if ('a', 'b') == (0, 1), (0, 2) mod 3
```

By Corollary 2.8.6 the corresponding character is the inverse of the splitting character given in Example 2.4.4, i.e. the unique character ε of conductor 12. In the case E is the $\mathbb{Q}$-curve from Example 2.1.4 we thus find that $f \in \mathcal{S}_2(1536, \varepsilon)$.

In general the restriction of scalars may be much larger than the abelian variety A associated to β. However if we choose the field K in a special way we get a nice result as stated in [Que00].

Proposition 2.9.4. *Let E be a $\mathbb{Q}$-curve with splitting map β for c_E. If K is an abelian number field over which E is completely defined, over which β is defined, and over which we have $c_E = c_\beta$, then $\operatorname{Res}_{\mathbb{Q}}^{K} E$ is isogenous over $\mathbb{Q}$ to a product of $\mathbb{Q}$-simple abelian varieties of GL_2-type not two of which are $\mathbb{Q}$-isogenous.*

Proof. Let $B = \operatorname{Res}_{\mathbb{Q}}^{K} E$ and look at the algebra $\operatorname{End}_{\mathbb{Q}}^{0} B$. As mentioned in Section 2.2 it can be seen as a $\mathbb{Q}$-algebra generated by the ϕ_σ for $\sigma \in G_{\mathbb{Q}}^{K}$ with multiplication given by

$$\phi_\sigma \phi_\tau = c_E(\sigma, \tau)\phi_{\sigma\tau} = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}\phi_{\sigma\tau}.$$

Since $G_{\mathbb{Q}}^{K}$ is abelian the formula above shows that $\operatorname{End}_{\mathbb{Q}}^{0} B$ is commutative. Now by Proposition 5.1 in [Que00] the result follows. □

Remark 2.9.5. In fact the algebra $\operatorname{End}_{\mathbb{Q}}^{0} B$ being commutative is actually equivalent to $\operatorname{Res}_{\mathbb{Q}}^{K} E$ being $\mathbb{Q}$-isogenous to a product of $\mathbb{Q}$-simple mutually non-$\mathbb{Q}$-isogenous abelian varieties of GL_2-type, as both are equivalent to $\operatorname{End}_{\mathbb{Q}}^{0} B$ being a product of number fields. Quer shows in Proposition 5.2 in [Que00] that $\operatorname{End}_{\mathbb{Q}}^{0} B$ being commutative is again equivalent to K being abelian and c_E having trivial class in $H^2(G_{\mathbb{Q}}^{K}, \overline{\mathbb{Q}}^*)$ for the trivial action of $G_{\mathbb{Q}}^{K}$ on $\overline{\mathbb{Q}}^*$. The latter is equivalent to saying a splitting map β for c_E defined over K exists such that $c_E = c_\beta$ over K. Therefore the statement in the proposition is best possible and we will call such a field K a *decomposition field.*

Remark 2.9.6. Note that most of the minimal fields as discussed in Section 2.7 are abelian. In particular the minimal field of complete definition and the minimal splitting field are both abelian. Combining these we find an abelian field K over which our $\mathbb{Q}$-curve E is completely defined and the splitting map β for c_E is defined, or at least there is an isogenous $\mathbb{Q}$-curve for which this is the case. Note that the extension $K(\sqrt{\gamma})$ given by Corollary 2.5.2 over which we also have $c_E = c_\beta$ might not be abelian, but Corollary 2.7.8 guarantees that E_γ does have $c_{E_\gamma} = c_\beta$ and is also completely defined over the abelian field K. Therefore a decomposition field always exists, at least for an isogenous $\mathbb{Q}$-curve.

Remark 2.9.7. The field K returned by the method `decomposition_field` for a `Qcurve` object in the framework [vL21a] is not necessarily a decomposition field as defined above. The only properties that it might not satisfy are K being abelian or having $c_E = c_\beta$. The latter can be easily remedied by replacing the curve with the `decomposable_twist`, but the former may only be resolved by making sure the definition field and complete definition field are abelian. In practice the `definition_field` is nearly always equal to the `degree_field` preventing this problem. Whenever the field K is not a decomposition field the `Qcurve` class will print warnings when using methods that need it to be a decomposition field.

From now on we will assume that K is a decomposition field for the $\mathbb{Q}$-curve E with corresponding splitting map β for c_E. Note that, as discussed at the start of Section 2.2, each $\mathbb{Q}$-simple factor of $\operatorname{Res}_{\mathbb{Q}}^K E$ corresponds to a splitting map for c_E. Furthermore by the discussion in Section 2.6 each of these splitting maps is some twist character $\chi : G_{\mathbb{Q}}^K \to \overline{\mathbb{Q}}^*$ times β. In particular the corresponding λ-adic Galois representations are twists of $\rho_{\beta,\lambda}$ meaning that the corresponding newforms are twists of the newform corresponding to β. We can also compute exactly which twists by computing all characters $G_{\mathbb{Q}}^K \to \overline{\mathbb{Q}}^*$ and choosing only one per Galois conjugacy class of splitting maps for c_E.

There are now two different ways of computing the conductor of $\operatorname{Res}_{\mathbb{Q}}^K E$, i.e. by Proposition 2.9.2 or by using the decomposition of Proposition 2.9.4. Combined with the discussion above this gives the equation

$$\Delta_K^2 \mathcal{N}(N_E) = \prod_i N_{\chi_i^{-1} f}^{[L_i:\mathbb{Q}]}, \tag{2.7}$$

where the χ_i are a selection of relevant twist characters, the field L_i is the image field of the splitting map $\chi_i \beta$ such that $[L_i : \mathbb{Q}]$ is the dimension of the corresponding abelian variety, the number $N_{\chi_i^{-1} f}$ is the level of f twisted by χ_i^{-1}, the ideal N_E is the conductor of E over K, the function $\mathcal{N}$ is the ideal norm of K, and Δ_K is the discriminant of K.

We can use Equation (2.7) to compute the newform levels if we combine it with a result about how the level of a newform changes after twisting.

Theorem 2.9.8. *Let $F \in \mathcal{S}_k(N, \varepsilon)$ be a newform and let χ be a Dirichlet character with conductor q^β for some prime number q and $\beta \geq 1$. Let the q-part ε_q of ε have conductor q^α and let the conductor of $\varepsilon_q \chi$ be q^γ. Furthermore,* *let $N = q^\delta M$ with $q \nmid M$ and set $\delta' = \max\{\delta, \beta+1, \beta+\gamma\}$. For the newform ${}^\chi F$ that is F twisted by χ we have that*

1. ${}^\chi F \in \mathcal{S}_k\left(q^{\delta'} M, \varepsilon\chi^2\right)$.
2. ${}^\chi F$ *is not of level* $q^{\delta'} M q'^{-1}$ *for any prime* $q' \mid M$.
3. ${}^\chi F$ *is not of level* $q^{\delta'-1} M$ *if one of the following holds*
   (a) $\delta > \max(\beta+1, \beta+\gamma)$*; or*
   (b) $\delta < \max(\beta+1, \beta+\gamma)$ *and* $\gamma \geq 2$*; or*
   (c) $\alpha = \beta = \gamma = \delta = 1$.

Proof. See Appendix A □

Remark 2.9.9. This theorem is an analogue of Theorem 3.1 in [AL78]. Note that the proof is slightly different as the proof of the theorem in [AL78] had a flaw that was already noted in [SW93]. The proof in Appendix A is therefore based on the proof of Theorem 5.7 in [SW93] but then applied to classical modular forms rather than Hilbert modular forms. Furthermore we have chosen a different formulation of the result which reflects the stronger result that the proof actually achieves.

Note that Theorem 2.9.8 in particular shows we can study how the level of a newform changes for each prime exponent individually by looking only at the p-part of the corresponding characters. So to find the level of the newforms we study the p-part of Equation (2.7) for each prime number p dividing $\Delta_K^2 \mathcal{N}(N_E)$ separately. Note that for all the relevant twists we can compute the quantities α, β and γ in Theorem 2.9.8 explicitly using the corresponding characters. Next we could try to find all the δ for which Theorem 2.9.8 and Equation (2.7) are satisfied to give candidates for the p-part of the level of f. In practice this is sufficient to find the level as often a high power of p in $\Delta_K^2 \mathcal{N}(N_E)$ forces one of the newforms to be in the case 3.a) of Theorem 2.9.8.

The framework [vL21a] implements the theory of this section in the method `newform_levels` of the class `Qcurve`. Whenever the `decomposition_field` K of such a `Qcurve` E is actually a decomposition field this method computes the possible levels of the newforms $f_1, \ldots, f_n$ where $\mathrm{Res}_{\mathbb{Q}}^K E$ is isogenous to the product $\prod_{j=1}^n A_{f_j}$. Here f_j corresponds to the j-th splitting map returned by `splitting_map('conjugacy')`. To compute these levels the method uses the conductor given by `conductor_restriction_of_scalars` and applies Theorem 2.9.8 for each prime dividing that conductor as described above. The result is a list of n-tuples, where the j-th entry in each tuple is the level of f_j in that possible combination of levels.

For a FreyQcurve the method newform_levels computes a similar list, but it only consists of the possible p-parts of the levels of $f_1, \ldots, f_n$ for a finite set of prime numbers p. This finite set is specified indirectly by the argument bad_primes which consists of primes of the decomposition_field. These primes are the ones for which the conductor_exponent method of the underlying FreyCurve is used to determine the relevant part of the conductor, so it needs to include all primes above a prime number p for the p-part of the levels to be correct. By default bad_primes is equal to the default value of additive_primes for conductor_restriction_of_scalars. Although this makes it impossible to compute the entire level of corresponding newforms, this method can still be used to compute the level lowered newforms corresponding to a FreyQcurve, as will be discussed in Section 3.1.

For an instance of Qcurve an actual newform associated to the curve can be computed with the method newform. Its result is both a newform f and an n-tuple of Dirichlet characters $\chi_1, \ldots \chi_n$ such that f_i is the twist of f by χ_i. Note that f is always one of the f_i, so one of the χ_i is trivial. For an instance of FreyQcurve the method newform_candidates computes for each tuple of possible levels returned by newform_levels the newforms of the lowest level in that tuple.

Example 2.9.10. Qcurve5.rst Look at the curve

$$E : Y^2 = X^3 + 4\,\gamma\, X^2 + 18\,\gamma^2 \left(1 + \frac{\sqrt{2}}{\sqrt{5}}\right) X,$$

$$\text{where } \gamma = \left(1 + \sqrt{2}\right)\left(\sqrt{5} + \sqrt{\frac{5+\sqrt{5}}{2}}\right).$$

Note that the field $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{5}, \gamma\right)$ is the totally real subfield of $\mathbb{Q}(\zeta_{40})$ and hence abelian. We can use the framework [vL21a] to verify E is a $\mathbb{Q}$-curve with isogenies of degree 2 and show that K is a decomposition field.

```
sage: L.<zeta40> = CyclotomicField(40)
sage: K.<t> = L.subfield(zeta40 + zeta40^(-1))[0]
sage: sqrt2, sqrt5 = sqrt(K(2)), sqrt(K(5))
sage: c = sqrt((5 + sqrt5) / 2)
sage: gamma = (1 + sqrt2)*(sqrt5 + c)
```

```
sage: E = Qcurve([0, 4*gamma, 0, 2*gamma^2*(1 + sqrt2/sqrt5), 0],
....:            guessed_degress=[2])
sage: E.decomposition_field() == K
True
sage: E.does_decompose()
True
```

By Proposition 2.9.4 we find that $\operatorname{Res}_{\mathbb{Q}}^{K} E$ is isogenous to a product of $\mathbb{Q}$-simple abelian varieties of GL_2-type. Each such a factor corresponds to a splitting map for c_E. We compute the twist characters to obtain these splitting maps from the default splitting map β as well as their image fields.

```
sage: E.twist_character('conjugacy')
(Dirichlet character modulo 1 of conductor 1,
 Dirichlet character modulo 20 of conductor 20 mapping \
11 |--> -1, 17 |--> zeta4)
sage: E.splitting_image_field('conjugacy')
(Cyclotomic Field of order 8 and degree 4,
 Cyclotomic Field of order 8 and degree 4)
```

We thus see that $\operatorname{Res}_{\mathbb{Q}}^{K} E$ must be isogenous to $A_\beta \times A_{\chi_{20}\beta}$, where χ_{20} is a Dirichlet character of conductor 20 and order 4, and A_β, $A_{\chi_{20}\beta}$ are both $\mathbb{Q}$-simple abelian varieties of GL_2-type with endomorphism algebra $L_\beta = \mathbb{Q}(\zeta_8)$.

By Theorem 2.1.10 both A_β and $A_{\chi_{20}\beta}$ are isogenous to abelian varieties associated with newforms f and g respectively. In particular we thus have that $\rho_{f,\lambda} \cong \rho_{\beta,\lambda}$ and

$$\rho_{g,\lambda} \cong \rho_{\chi_{20}\beta,\lambda} = \chi_{20}^{-1}\rho_{\beta,\lambda} = \chi_{20}^{-1}\rho_{f,\lambda} = \rho_{\chi_{20}^{-1}f,\lambda}$$

for all primes λ of L_β, hence g is the twist of f by χ_{20}^{-1}. If we let N_f and N_g be the levels of f and g respectively then by comparing conductors of $A_f \times A_g$ and $\operatorname{Res}_{\mathbb{Q}}^{K} E$ we find that

$$N_f^4 N_g^4 = \Delta_K^2 \mathcal{N}(N_E), \tag{2.8}$$

where the constants on the right hand side are as in Proposition 2.9.2.

Using the framework [vL21a] we can compute the right hand side directly.

```
sage: RHS = E.conductor_restriction_of_scalars()
sage: RHS.factor()
2^72 * 3^8 * 5^12
```

This indicates N_f and N_g are only divisible by the primes 2, 3 and 5. Since g is a twist of f by a character of conductor 20 we see from Theorem 2.9.8 that $\operatorname{ord}_3 N_f = \operatorname{ord}_3 N_g$. Using the framework [vL21a] we can see that the splitting characters for β and $\chi_{20}\beta$ are χ_{20} and its inverse respectively.

```
sage: E.splitting_character(’conjugacy’)
(Dirichlet character modulo 20 of conductor 20 mapping \
11 |--> -1, 17 |--> zeta4,
 Dirichlet character modulo 20 of conductor 20 mapping \
11 |--> -1, 17 |--> -zeta4)
```

Therefore f has character χ_{20}^{-1} and g has character χ_{20} by Corollary 2.8.6. So for $q = 5$ the values of α, β and γ in Theorem 2.9.8 are all 1, independent of whether we choose $F = f$ or $F = g$. This implies that neither $\operatorname{ord}_5 N_f$ or $\operatorname{ord}_5 N_g$ could be 3 as then by part 3.a) of the theorem the other should be as well contradicting Equation (2.8). This implies one of $\operatorname{ord}_5 N_f$ and $\operatorname{ord}_5 N_g$ should be 1 meaning the other should be 2 as confirmed both by Equation (2.8) and part 3.c) of Theorem 2.9.8.

For $q = 2$ we have $\alpha = \beta = 2$ and $\gamma = 0$ in Theorem 2.9.8 for both $F = f$ and $F = g$. Note however that $\operatorname{ord}_2 N_f + \operatorname{ord}_2 N_g = 18$ by Equation (2.8), so we have a choice of F with $\delta \geq 9$. This implies we are in case 3.a) meaning we must have $\operatorname{ord}_2 N_f = \operatorname{ord}_2 N_g = 9$. We thus find that

$$\{N_f, N_g\} = \left\{2^9 \cdot 3 \cdot 5, 2^9 \cdot 3 \cdot 5^2\right\} = \{7680, 38400\},$$

which is confirmed by the framework [vL21a].

```
sage: E.newform_levels()
[(7680, 38400), (38400, 7680)]
```

Section 2.10

Traces of Frobenius

One important thing we want to compute for the Galois representations $\rho_{\beta,\lambda}$ and $\overline{\rho_{\beta,\lambda}}$ are the traces of these Galois representations evaluated at Frobenius elements. For explicit $\mathbb{Q}$-curves these allow the framework [vL21a] to compute the exact newform associated to a splitting map β for c_E. This is done by finding the newform f for which $\rho_{f,\lambda}$ and $\rho_{\beta,\lambda}$ have the same traces of Frobenius for all primes λ of L_β. Note that for this only finitely many traces have to be computed as for two newforms f and g of the same level and weight there are bounds on the smallest integer p such that $\rho_{f,\lambda}$ and $\rho_{g,\lambda}$ have different traces at a Frobenius element for p, for example the Sturm bound. For Frey $\mathbb{Q}$-curves we need these traces to eliminate newforms in the modular method, as will be discussed in Chapter 3.

By Theorem 2.8.3 we know about two cases in which the trace of Frobenius is independent of the chosen Frobenius element in $G_{\mathbb{Q}}$ as the corresponding Galois representations are unramified. In this section we prove two results that each include one of these cases. Note that as these results are not precisely the cases of Theorem 2.8.3 the chosen Frobenius element could matter, as we will see in Example 2.10.4. We will start with the case of good reduction.

Theorem 2.10.1. *Let E be a $\mathbb{Q}$-curve with decomposition field K and let β be a splitting map for c_E. Let p be a prime number at which E has good reduction, let $\sigma \in G_{\mathbb{Q}}$ be a Frobenius element for p, and let $\tilde{E}$ be the good reduction of E at a prime above p for which the dual isogeny $\widehat{\phi_\sigma}$ of ϕ_σ reduces to a separable isogeny ψ. For every prime $\lambda \nmid p$ the matrix $\rho_{\beta,\lambda}(\sigma)$ has characteristic equation*

$$x^2 - \beta(\sigma)^{-1} a_\sigma(E) x + \varepsilon(\sigma)^{-1} p$$

where ε is the splitting character corresponding to β and

$$a_\sigma(E) = \deg \psi + p - \#\{P \in \tilde{E}(\overline{\mathbb{F}_p}) : \psi P = \mathrm{Frob}_p P\},$$

with Frob_p the Frobenius element of $G_{\mathbb{F}_p}$.

In particular we have

$$\begin{aligned} \det \rho_{\beta,\lambda}(\sigma) &= \varepsilon(\sigma)^{-1}\, p \\ \operatorname{Tr} \rho_{\beta,\lambda}(\sigma) &= \beta(\sigma)^{-1}\, a_\sigma(E). \end{aligned}$$

Proof. The part about the determinant directly follows from Proposition 2.8.5 by evaluating the characters at σ.

For the trace part note that by Proposition 2.8.1

$$\operatorname{Tr} \rho_{\beta,\lambda}(\sigma) = \beta(\sigma)^{-1} \operatorname{Tr}(\phi_\sigma \circ \sigma),$$

hence it suffices to prove that $\operatorname{Tr}(\phi_\sigma \circ \sigma) = a_\sigma(E)$. For this note that the prime number l below λ must be distinct from p. This implies that the l^n-torsion of E maps injectively to the l^n torsion of $\tilde{E}$. To study the action of $\phi_\sigma \circ \sigma$ on $T_l(E)$ we may also study the action of $\widehat{\psi} \circ \mathrm{Frob}_p$ on $T_l(\tilde{E})$, where $\mathrm{Frob}_p \in G_{\mathbb{F}_p}$ is the

Frobenius element and $\widehat{\psi}$ is the dual of ψ. Note that Frob_p is an isogeny on $\tilde{E}$ hence we can apply Proposition 8.6 from [Sil09, III.8] to find that

$$\begin{aligned}\mathrm{Tr}(\widehat{\psi}\circ\mathrm{Frob}_p) &= 1+\deg(\widehat{\psi}\circ\mathrm{Frob}_p)-\deg(1-\widehat{\psi}\circ\mathrm{Frob}_p)\\ &= 1+(\widehat{\psi}\circ\mathrm{Frob}_p)(\widehat{\mathrm{Frob}_p}\circ\psi)-(1-\widehat{\psi}\circ\mathrm{Frob}_p)(1-(\widehat{\mathrm{Frob}_p}\circ\psi))\\ &= \widehat{\psi}\circ\mathrm{Frob}_p+\widehat{\mathrm{Frob}_p}\circ\psi\\ &= \widehat{\psi}\circ\psi+\widehat{\mathrm{Frob}_p}\circ\mathrm{Frob}_p-(\widehat{\psi}-\widehat{\mathrm{Frob}_p})(\psi-\mathrm{Frob}_p)\\ &= \deg\psi+\deg\mathrm{Frob}_p-\deg(\psi-\mathrm{Frob}_p)\\ &= \deg\psi+p-\#\{P\in\tilde{E}(\overline{\mathbb{F}_p}):\psi P=\mathrm{Frob}_p P\}.\end{aligned}$$

The last step is valid since ψ is separable and Frob_p is not, hence $\psi-\mathrm{Frob}_p$ is also separable. Its degree is thus equal to the number of points in its kernel, which is exactly the given set. □

To make the theorem above usable we need a way to calculate

$$\#\{P\in\tilde{E}(\overline{\mathbb{F}_p}):\psi P=\mathrm{Frob}_p P\},$$

for a prime number p and isogeny ψ. We also need a way to determine if the reduction of an isogeny to $\tilde{E}$ will be separable. For the latter we can use a corollary of Proposition 2.1.3.

Proposition 2.10.2. *Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves over any field, and let $F(x)$ and λ be the invariants associated to ϕ given in Proposition 2.1.3. The following are equivalent*

1. *ϕ is inseparable,*
2. *$\lambda = 0$,*
3. *$F'(x) = 0$.*

Proof. By Proposition 4.2.c in [Sil09, II.4] we know that ϕ is inseparable if and only if $\lambda = 0$. Noting that both $\frac{\partial f_1}{\partial y}(x,y)$ and $\frac{\partial f_2}{\partial y}(F(x), G(x)y + H(x))$ must be non-zero for E_1 and E_2 to be elliptic curves, we can deduce from Equation (2.1) that $\lambda = 0$ if and only if $F'(x) = 0$ as claimed. □

Now we determine a way to calculate $\#\{P\in\tilde{E}(\overline{\mathbb{F}_p}):\psi P=\mathrm{Frob}_p P\}$.

Proposition 2.10.3. *Let E be an elliptic curve over a finite field k of characteristic p. Let Frob_p be the Frobenius homomorphism of k and let ${}^{(p)}E$ be the image of E under Frob_p. Suppose $\phi : E \to {}^{(p)}E$ is a separable isogeny, then we have*

$$\begin{aligned} &\#\{P \in E(\overline{\mathbb{F}_p}) : \phi P = \mathrm{Frob}_p P\} \\ &\quad = \begin{cases} 1 + 2\deg \mathrm{Rad}(f_1, f_2) - \deg \mathrm{Rad}(f_1, R) & \text{if } p \neq 2 \\ 1 + \deg \mathrm{Rad}(f_1, f_3) + \deg \mathrm{Rad}(f_1, f_3, f_4) & \\ \quad - \deg \mathrm{Rad}(f_1, f_3, f_4, g) & \text{if } p = 2 \end{cases} \end{aligned}$$

where $Rad(g_1, \ldots, g_n)$ denotes the product of all distinct irreducible factors that divide each of the polynomials g_1 through g_n and

- *f_1 is the numerator of $F(x) - x^p$,*
- *$R = 4x^3 + b_2x^2 + 2b_4x + b_6$,*
- *f_2 is the numerator of $\lambda R^{\frac{p+1}{2}} - F'(x)R$,*
- *$g = a_1x + a_3$,*
- *$h = x^3 + a_2x^2 + a_4x + a_6$,*
- *f_3 is the numerator of $gGh + gGH + G^2h + g^2H + h^2 + H^2$, and*
- *f_4 is the numerator of $g - G$.*

Here $a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6$ are the invariants associated to the Weierstrass equation of E and $F(x)$, $G(x)$, $H(x)$, λ are the invariants associated to ϕ by Proposition 2.1.3.

Proof. Denote

$$S = \{P \in E(\overline{\mathbb{F}_p}) : \phi P = \mathrm{Frob}_p P\}.$$

Obviously we have that the point at infinity $O \in E(\overline{\mathbb{F}_p})$ is in S as

$$\phi O = O = \mathrm{Frob}_p O.$$

For arbitrary $x, y \in \overline{\mathbb{F}_p}$ we have that $(x, y) \in S$ if and only if x and y satisfy

$$\begin{cases} f(x,y) &= 0 \\ F(x) &= x^p \\ G(x)y + H(x) &= y^p. \end{cases} \tag{2.9}$$

Note that $\lambda \neq 0$ by Proposition 2.10.2, so by Proposition 2.1.3 it follows that for $p \neq 2$ the term $G(x)y + H(x)$ is completely determined by

$$\lambda\left(2\left(G(x)y + H(x)\right) + a_1^p F(x) + a_3^p\right) = F'(x)(2y + a_1 x + a_3).$$

Therefore (x, y) satisfy the conditions in (2.9) if and only if they satisfy

$$\left\{\begin{array}{rl} f(x,y) & = 0 \\ F(x) & = x^p \\ F'(x)(2y + a_1 x + a_3) & = \lambda\left(2y^p + a_1^p x^p + a_3^p\right) \\ & = \lambda\left(2y + a_1 x + a_3\right)^p . \end{array}\right. \tag{2.10}$$

Note that $2y + a_1 x + a_3 = 0$ forms a solution to the last equation, so we get equivalent conditions if we multiply the last equation by $2y + a_1 x + a_3$. Since p is odd and

$$(2y + a_1 x + a_3)^2 = 4f(x,y) + R(x) \tag{2.11}$$

the conditions in (2.10) are equivalent to

$$\left\{\begin{array}{rl} f(x,y) & = 0 \\ F(x) & = x^p \\ F'(x)R(x) & = \lambda R(x)^{\frac{p+1}{2}} . \end{array}\right. \tag{2.12}$$

Note that Equation (2.11) tells us that for each $x \in \overline{F_p}$ the equation $f(x,y) = 0$ has one solution $y \in \overline{F_p}$ if $R(x) = 0$ and two otherwise. Therefore the number of points (x, y) satisfying the conditions in (2.12) is equal to twice the number of x satisfying $F(x) = x^p$ and $F'(x)R(x) = \lambda R(x)^{\frac{p+1}{2}}$ minus the number of $x \in \overline{\mathbb{F}_p}$ that also satisfy $R(x) = 0$. This verifies the formula in the case $p \neq 2$.

If $p = 2$ we return to the conditions in (2.9). The first and third condition both consist of quadratic polynomials in y. The resultant of these two polynomials is

$$gGH + gGH + G^2 h + g^2 H + h^2 + H^2,$$

hence the only $x \in \overline{\mathbb{F}_p}$ for which there is at least one $y \in \overline{\mathbb{F}_p}$ such that $(x, y) \in S$ should satisfy

$$\left\{\begin{array}{rl} F(x) & = x^p \\ gGH + gGH + G^2 h + g^2 H + h^2 + H^2 & = 0. \end{array}\right. \tag{2.13}$$

Note that

$$f(x,y) - (y^2 - G(x)y - H(x)) = (g(x) + G(x))y - (h(x) - H(x)),$$

hence if $g(x) + G(x) = 0$ the number of solutions y for a given x is determined by the number of solutions to $f(x, y) = 0$. The latter always has two solutions unless $g(x) = 0$. In total the number of $(x, y) \in S$ is thus equal to the number of x that satisfy (2.13), plus the number of x that also satisfy $g(x) + G(x) = 0$ minus the number of x that also satisfy $g(x) = 0$. this justifies the formula in the case $p = 2$. □

Example 2.10.4. `Qcurve1.rst` We return again to the curve E of Example 2.1.4, but replace E by its twist E_γ obtained by using the γ found in Example 2.5.4. As stated in Example 2.7.9 we then know that E is completely defined over $K_d = \mathbb{Q}(\sqrt{3})$ and has splitting map β for c_E given in Example 2.4.4. We will here consider only the case where E is a $\mathbb{Q}$-curve as the Frey $\mathbb{Q}$-curve case is quite subtle. The Frey $\mathbb{Q}$-curve case has been fully worked out in `Qcurve1Frey.rst`.

Using SageMath [Sag20] we can compute that the conductor of E is only divisible by primes above 2. In fact SageMath can also tell us that E has a global minimal model

$$E : y^2 = x^3 - 2\left(1 + \sqrt{3}\right)x^2 - \left(1 + \sqrt{3}\right)x = xf(x),$$

which has its invariants c_4 and Δ coprime outside the prime above 2. We shall take this as our model for E.

Note that the framework [vL21a] stores the dual isogenies $\hat{\phi}_\sigma : E \to {}^\sigma E$ for each $\sigma \in G_\mathbb{Q}^{K_d} = \langle \sigma_3 \rangle$. Retrieving these from the framework [vL21a] we get

$$(\lambda, F(x)) = \begin{cases} (1, x) & \text{if } \sigma = 1 \\ \left(-1 - \sqrt{3}, \frac{2-\sqrt{3}}{2}\frac{f(x)}{x}\right) & \text{if } \sigma = \sigma_3, \end{cases}$$

using notation as in Proposition 2.1.3. By Proposition 2.10.2 we know these isogenies are separable and as $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$ this remains true when taking the reduction modulo a prime above an odd prime number p. Therefore we can apply Theorem 2.10.1 to compute traces of $\rho_{\beta,\lambda}$ at Frobenius elements of p for any odd prime number p and any prime $\lambda \nmid p$.

Now let $\sigma \in G_\mathbb{Q}$ be a Frobenius element of an odd prime number p. If $\sigma \in G_{K_d}$ then p must split or ramify in K_d, so any prime $\mathfrak{p} \mid p$ in K_d has $\mathbb{F}_\mathfrak{p} = \mathbb{F}_p$. Furthermore ϕ_σ is the identity hence we find that

$$a_\sigma(E) = 1+p-\#\{P \in \tilde{E}(\overline{\mathbb{F}_p}) : P = \mathrm{Frob}_p P\} = 1+p-\#\tilde{E}(\mathbb{F}_p) = 1+p-\#\tilde{E}(\mathbb{F}_\mathfrak{p}).$$

We have by definition of β that $\beta(\sigma) = 1$, so $a_\sigma(E)$ is also the trace of $\rho_{\beta,\lambda}(\sigma)$. This is what we expect as $\rho_{\beta,\lambda}|_{G_{K_d}} = \rho_{E,l}$ and the formula for $a_\sigma(E)$ is precisely that of the trace of $\rho_{E,l}$ at a Frobenius element of a prime $\mathfrak{p} \mid p$.

p	behaviour in $\mathbb{Q}(\sqrt{3})$	$\operatorname{Tr}\rho_{\beta,\lambda}(\sigma)$	
3	ramified	-2	if $\sigma \in G_{\mathbb{Q}(\sqrt{3})}$
		$2\sqrt{-2}$	if $\sigma \notin G_{\mathbb{Q}(\sqrt{3})}$
5	inert	$\sqrt{-2}$	
7	inert	$-3\sqrt{-2}$	
11	split	-4	
13	split	-2	
17	inert	$2\sqrt{-2}$	
19	inert	0	
23	split	8	
29	inert	$5\sqrt{-2}$	

Table 2.1: Traces of Frobenius for Example 2.10.4. Note that at $p = 3$ there are multiple possible traces depending on the choice of Frobenius element σ.

Now suppose $\sigma \notin G_{K_d}$ which implies p must ramify or be inert in K_d. In this case we must have

$$a_\sigma(E) = 2 + p - \#\{P \in \tilde{E}(\overline{\mathbb{F}_p}) : \psi(P) = \operatorname{Frob}_p P\},$$

where ψ is the reduction of $\widehat{\phi_{\sigma_3}}$ modulo the unique prime $\mathfrak{p} \mid p$ of K_d. We can compute this number by applying Proposition 2.10.3 for which we need the polynomials

$$\begin{aligned}
f_1 &= \frac{2-\sqrt{3}}{2} f(x) - x^{p+1} \\
f_2 &= -2f(x)\left(2^p\left(1+\sqrt{3}\right)x^{\frac{p+3}{2}} f(x)^{\frac{p-1}{2}} + \left(2-\sqrt{3}\right)\left(x^2+1+\sqrt{3}\right)\right) \\
R &= 4\,xf(x).
\end{aligned}$$

Note that x and $f(x)$ have no common factors in $\overline{\mathbb{F}_p}$ as the reduction $\tilde{E}$ of E at $\mathfrak{p}$ is good, hence f_1 and R must be coprime. The formula from Proposition 2.10.3 therefore tells us that

$$a_\sigma(E) = 1 + p - 2\deg\operatorname{Rad}(f_1', f_2'),$$

with

$$\begin{aligned}
f_1' &= 2x^{p+1} - (2-\sqrt{3})f(x), \text{ and} \\
f_2' &= 2^p(1+\sqrt{3})x^{\frac{p+3}{2}} f(x)^{\frac{p-1}{2}} + (2-\sqrt{3})(x^2+1+\sqrt{3}).
\end{aligned}$$

Since $\beta(\sigma) = \sqrt{-2}$ this implies that we have

$$\operatorname{Tr} \rho_{\beta,\lambda}(\sigma) = \sqrt{-2} \left(\deg \operatorname{Rad}(f_1', f_2') - \frac{p+1}{2} \right),$$

for any $\lambda \nmid p$.

We computed some of these traces explicitly in Table 2.1. Note that 3 appears twice as it ramifies and therefore has two distinct choices for a Frobenius element σ. For the other primes the trace of a Frobenius element is independent of the chosen Frobenius element as $\rho_{\beta,\lambda}$ is unramified by Theorem 2.8.3. Furthermore the results here are only true for $\lambda \nmid p$.

For the case of multiplicative reduction we will need some results about isogenies between Tate curves first.

Proposition 2.10.5. *Let K be a finite extension of $\mathbb{Q}_p$ for some prime number p and let $q, q' \in K^*$ be elements of positive valuation. For any non-zero isogeny $\phi : E_q \to E_{q'}$ between Tate curves there exist integers m and n such that $mn = \deg \phi$, $q^{|m|} = (q')^{|n|}$, and $\lambda_\phi = m$ where λ_ϕ is the constant associated to ϕ in Propostion 2.1.3. Furthermore for any finite extension L/K the diagram*

$$\begin{tikzcd}
L^* \arrow[r, "{[m]}"] \arrow[d, two heads] & L^* \arrow[d, two heads] \\
L^*/q^{\mathbb{Z}} \arrow[r] \arrow[d, "\sim"] & L^*/(q')^{\mathbb{Z}} \arrow[d, "\sim"] \\
E_q(L) \arrow[r, "\phi"] & E_{q'}(L)
\end{tikzcd}$$

commutes.

Proof. Note that if this proposition is true for any two isogenies $\phi : E_q \to E_{q'}$ and $\psi : E_{q'} \to E_{q''}$, then it is also true for $\psi \circ \phi$, hence it suffices to prove this proposition for cyclic isogenies ϕ.

Suppose ϕ is cyclic of degree $n > 0$, then its kernel is generated by an n-torsion point $P \in E_q(\overline{K})$. The corresponding element in $\overline{K}^*/q^{\mathbb{Z}}$ is the class of an $\alpha \in \overline{K}^*$ that is either an n-th root of unity or an n-th root of q. In the first case note that the map $x \mapsto x^n$ on K^* induces an isogeny $\overline{K}^*/q^{\mathbb{Z}} \to \overline{K}^*/q^{n\mathbb{Z}}$ with the same kernel as ϕ. In the second case, let $\hat{q}$ be the corresponding n-th root of q, then the identity map on $\overline{K}^*$ induces an isogeny $\overline{K}^*/q^{\mathbb{Z}} \to \overline{K}^*/\hat{q}^{\mathbb{Z}}$ with the same kernel as ϕ. It follows that ϕ must be one of these isogenies combined with a degree 1 isogeny. (Corollary 4.11 in [Sil09, III.4])

Note that by Lemma 5.1 in [Sil94, V.5] each isomorphism class over $\overline{\mathbb{Q}_p}$ contains at most one Tate curve $E_{\tilde{q}}$ with $\tilde{q} \in \overline{\mathbb{Q}_p}^*$ of positive valuation. Therefore the aforementioned degree 1 isogeny is in fact an automorphism. Note however, that since q has positive valuation the j-invariant of E_q has negative valuation and hence by Theorem 10.1 in [Sil09, III.10] the automorphism group is only $[\pm 1]$. This shows that the isogeny ϕ must be of the form mentioned.

As ϕ is of the form mentioned we can compute λ_ϕ using the invariant differentials on $K^*/q^{\mathbb{Z}}$ and $K^*/(q')^{\mathbb{Z}}$ corresponding to those used in Proposition 2.1.3. These are both $\frac{du}{u}$ for u a parameter on K^*. Using the map on K^* that induces ϕ on $K^*/q^{\mathbb{Z}}$ we see that

$$\phi^*\left(\frac{du}{u}\right) = \frac{du^m}{u^m} = \frac{mu^{m-1}du}{u^m} = m\frac{du}{u},$$

so $\lambda_\phi = m$. □

Corollary 2.10.6. *Let $\phi : E_q \to E_{q'}$ be an isogeny as in Proposition 2.10.5 with corresponding $m, n \in \mathbb{Z}$. Suppose $q' = {}^\sigma q$ for some $\sigma \in G_{\mathbb{Q}_p}$, then $m = n$. In particular we have $q' = \zeta q$ for ζ some n-th root of unity (not necessarily primitive) and $\deg \phi$ is a square. Furthermore there is an isogeny $\chi : E_q \to E_{q^n}$ of degree $|n|$ such that $[n]\chi = {}^\sigma\chi\phi$.*

Proof. Since the valuations of ${}^\sigma q$ and q are the same, the relation $q^{|m|} = (q')^{|n|}$ implies that $|m| = |n|$. Since $mn = \deg \phi > 0$ the signs of m and n must agree, hence $m = n$. Now note that for any finite Galois extension L/K we have the commutative diagram

$$\begin{tikzcd}
L^* \arrow[r, "{[n]}"] \arrow[d, two heads] & L^* \arrow[r, "{[1]}"] \arrow[d, two heads] & L^* \arrow[r, "{[n]}"] \arrow[d, two heads] & L^* \arrow[d, two heads] \\
L^*/q^{\mathbb{Z}} \arrow[r] \arrow[d, "\sim"] & L^*/q^{n\mathbb{Z}} \arrow[r] \arrow[d, "\sim"] & L^*/(q')^{\mathbb{Z}} \arrow[r] \arrow[d, "\sim"] & L^*/(q)^{n\mathbb{Z}} \arrow[d, "\sim"] \\
E_q(L) \arrow[r, "\chi"] \arrow[rr, bend right, "\phi"'] & E_{q^{|n|}}(L) \arrow[r] \arrow[rr, bend right, "{[n]}"'] & E_{q'}(L) \arrow[r, "{}^\sigma\chi"] & E_{q^{|n|}}(L)
\end{tikzcd}$$

indicating that we indeed have an isogeny χ such that $[n]\chi = {}^\sigma\chi\phi$. □

We can now prove a result similar to that of Theorem 2.10.1 for the multiplicative reduction case.

Theorem 2.10.7. *Let E be a $\mathbb{Q}$-curve with decomposition field K and let β be a splitting map for c_E. Let $\sigma \in G_{\mathbb{Q}}$ be a Frobenius element of a prime number p. If E has multiplicative reduction at p, then for any prime $\lambda \nmid p$ the matrix $\rho_{\beta,\lambda}(\sigma)$ has characteristic equation*

$$x^2 - \beta(\sigma)^{-1} a_\sigma(E)(1+p)x + \varepsilon(\sigma)^{-1} p,$$

where ε is the splitting character corresponding to β and

$$a_\sigma(E) = \lambda_\sigma {}^{\sigma}\sqrt{-\frac{c_4}{c_6}} \left(\sqrt{-\frac{c_4}{c_6}}\right)^{-1}.$$

Here c_4 and c_6 are the corresponding invariants of E and $\lambda_\sigma \in \overline{K}^*$ is the constant associated to ϕ_σ as in Proposition 2.1.3. In particular we have that

$$\begin{aligned} \operatorname{Tr} \rho_{\beta,\lambda}(\sigma) &= \beta(\sigma)^{-1} a_\sigma(E)(1+p) \\ \det \rho_{\beta,\lambda}(\sigma) &= \varepsilon(\sigma)^{-1} p. \end{aligned}$$

Proof. Note that as in Theorem 2.10.1 the determinant part of this proposition directly follows from Proposition 2.8.5. It thus remains to prove the result about $\operatorname{Tr} \rho_{\beta,\lambda}(\sigma)$.

Note that we have

$$\operatorname{Tr} \rho_{\beta,\lambda}(\sigma) = \beta(\sigma)^{-1} \operatorname{Tr}(\phi_\sigma \circ \sigma),$$

where the last trace is considered on $T_l(E)$. To compute this trace we use the commutative diagram

$$\begin{tikzcd}
E \arrow[r, "\sigma"] \arrow[d, "\psi"] & {}^{\sigma}E \arrow[r, "\phi_\sigma"] \arrow[d, "{}^{\sigma}\psi"] & E \arrow[d, "\psi"] \\
E_q \arrow[r, "\sigma"] \arrow[d, "\chi"] & E_{{}^{\sigma}q} \arrow[r] \arrow[d, "{}^{\sigma}\chi"] & E_q \arrow[d, "\chi"] \\
E_{q^{|n|}} \arrow[r, "\sigma"] & E_{q^{|n|}} \arrow[r, "{[n]}"] & E_{q^{|n|}},
\end{tikzcd}$$

where E_q is the Tate curve isomorphic to E over $\overline{\mathbb{Q}_p}$, ψ is the corresponding ismorphism and n and χ are the corresponding elements from Corollary 2.10.6.

We can easily determine the eigenvalues of σ on $T_l(E_{q^{|n|}})$ as the isomorphisms $E_{q^{|n|}}(L) \to L^*/q^{n\mathbb{Z}}$ for finite Galois extensions $L/\mathbb{Q}_p(q)$ respect the Galois action. Since ${}^{\sigma}(q^n) = ({}^{\sigma}q)^n = q^n$ we find that on the basis $\{q^{|n|/m}, \zeta_m\}$ of m-torsion in $\overline{K}^*/q^{n\mathbb{Z}}$ the element σ acts as

$$\begin{bmatrix} 1 & * \\ 0 & p \end{bmatrix},$$

when $p \nmid m$, hence the trace of σ on $T_l(E_{q^{|n|}})$ is $1+p$. Note that $[n] \circ \sigma$ therefore has trace $n(1+p)$. Since $\deg(\chi\psi) = |n| > 0$ the map $\chi\psi$ is an isomorphism $V_l(E) \to V_l(E_{q^{|n|}})$, meaning that the trace of $\phi_\sigma \circ \sigma$ on $T_l(E)$ must also be $n(1+p)$.

It thus remains to prove that $a_\sigma(E) = n$. We use the constants associated to isogenies in Proposition 2.1.3 and the fact that $[n]\,{}^{\sigma}\chi\,{}^{\sigma}\psi = \chi\psi\phi_\sigma$ to see that

$$n\,{}^{\sigma}\lambda_\chi\,{}^{\sigma}\lambda_\psi = \lambda_\chi\lambda_\psi\lambda_\sigma.$$

By Proposition 2.10.5 we find that $\lambda_\chi \in \mathbb{Q}^*$, so in fact we get

$$n = \lambda_\sigma \frac{\lambda_\psi}{{}^{\sigma}\lambda_\psi}.$$

The isomorphism ψ must be of the form $(x,y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ for some $u, r, s, t \in \overline{\mathbb{Q}_p}$. From calculations as found in [Sil09, section III.1] we know that

$$\begin{aligned} u^4 c_4(E) &= c_4(E_q) \\ u^6 c_6(E) &= c_6(E_q), \end{aligned}$$

hence

$$u^2 = \frac{c_4(E)c_6(E_q)}{c_4(E_q)c_6(E)},$$

as the c_4 and c_6-invariants are non-zero for curves with multiplicative reduction. The proof of Theorem 5.3 in [Sil94, V.5] tells us that $-\frac{c_4(E_q)}{c_6(E_q)} = t^2$ for some $t \in \mathbb{Q}_p^*$, hence

$$(ut)^2 = -\frac{c_4(E)}{c_6(E)}.$$

From this we conclude that

$$\begin{aligned} n &= \lambda_\sigma u^{-1} \, {}^\sigma u \\ &= \lambda_\sigma \frac{{}^\sigma(ut)}{ut} \\ &= \lambda_\sigma \frac{{}^\sigma\sqrt{-\frac{c_4(E)}{c_6(E)}}}{\sqrt{-\frac{c_4(E)}{c_6(E)}}} \\ &= a_\sigma(E). \end{aligned}$$

□

Example 2.10.8. `Qcurve5.rst` We return to the elliptic curve E from Example 2.9.10 that had the totally real subfield K of $\mathbb{Q}(\zeta_{40})$ as a decomposition field. Using SageMath [Sag20] we can easily determine that E has multiplicative reduction at 3 so we can apply Theorem 2.10.7 to a Frobenius element $\sigma \in G_\mathbb{Q}$ of 3.

First of all we compute $\gamma = -\frac{c_4}{c_6}$ using SageMath [Sag20], which happens to not be a square in K. Therefore we need to do the computation of $a_\sigma(E)$ in the Galois closure L of $K(\sqrt{\gamma})$. Using SageMath [Sag20] we compute that 3 does not ramify in L meaning we can use the Artin map to determine the restriction $\sigma_3 \in G_\mathbb{Q}^L$ of σ to L. By checking that σ_3 is the same for all primes of L above 3 we see that the choice of σ in fact does not matter. Therefore $\operatorname{Tr} \rho_{\beta,\lambda}(\sigma)$ only depends on $\sigma_3 \in G_\mathbb{Q}^L$ when $\lambda \nmid 3$. When we do the actual computation described in Theorem 2.10.7 we find that $a_\sigma(E) = 2$ and $\operatorname{Tr} \rho_{\beta,\lambda}(\sigma) = \zeta_8^3$ where we computed the splitting map β for c_E using the framework [vL21a] as in Example 2.9.10.

Remark 2.10.9. Theorem 2.10.1 and Theorem 2.10.7 consider the λ-adic Galois representations $\rho_{\beta,\lambda}$ of a splitting map β for c_E. Since the mod λ Galois representations $\overline{\rho_{\beta,\lambda}}$ are the reduction of these representation modulo λ, possibly with an additional semisimplification, the trace and determinant of $\overline{\rho_{\beta,\lambda}}$ are just the reduction of the trace and determinant of $\rho_{\beta,\lambda}$ modulo λ. This implies that Theorem 2.10.1 and Theorem 2.10.7 can be used in all the cases where Theorem 2.8.3 shows these representations are unramified to compute traces of Frobenius, which in such a case only depend on the prime p not divisible by λ.

All of this theory has been implemented in the framework [vL21a] as the method `trace_of_frobenius` of the class `Qcurve`. For a given prime number p that does not ramify in the `decomposition_field` it computes the trace of

Frobenius as given in Theorem 2.10.1 if the `Qcurve` has good reduction at the prime p or as given in Theorem 2.10.7 if the `Qcurve` has multiplicative reduction at the prime p. Note that in both cases the result will be an element of L_β which when mapped to the appropriate local or finite field is the trace of a Frobenius element at p. One can specify for which splitting map β the trace of Frobenius is computed by passing an index to the argument `splitting_map`. Theses indices are the same as those used in the method `splitting_map`.

As with the similarly named method of the class `FreyCurve` this method does not check the conditions to apply Theorems 2.10.1 and 2.10.7, but rather assumes they are true. In particular this means one does not have to specify a prime λ and the result is an algebraic integer that is the correct trace when mapped to any appropriate local or finite field.

For a `FreyQcurve` E the method `trace_of_frobenius` does not actually compute the value of $a_\sigma(E)$ in Theorem 2.10.7 as computing $-\frac{c_4}{c_6}$ explicitly would depend on the specific values of the parameters. Instead it will create two cases marked by conditions for both $a_\sigma(E) = \sqrt{\deg \phi_\sigma}$ and $a_\sigma(E) = -\sqrt{\deg \phi_\sigma}$. Note that these cases have no capabilities of actually computing for which values of the parameters they hold and will always give full $\mathfrak{p}$-adic trees.

Example 2.10.10. `Qcurve1Frey.rst` We return to the Frey $\mathbb{Q}$-curve E from Example 2.1.4, and use the twist E_γ introduced in Example 2.7.9 to compute some traces of Frobenius. Using the framework [vL21a] it is straightforward to compute the traces of Frobenius at 7 for different splitting maps.

```
sage: Egamma.trace_of_frobenius(7)
0           if (’a’, ’b’) is 1 of 12 possibilities mod 7
-3*zeta4a0 if (’a’, ’b’) is 1 of 6 possibilities mod 7
zeta4a0    if (’a’, ’b’) is 1 of 6 possibilities mod 7
-2*zeta4a0 if (’a’, ’b’) is 1 of 6 possibilities mod 7
2*zeta4a0  if (’a’, ’b’) is 1 of 6 possibilities mod 7
-zeta4a0   if (’a’, ’b’) is 1 of 6 possibilities mod 7
3*zeta4a0  if (’a’, ’b’) is 1 of 6 possibilities mod 7
sage: Egamma.trace_of_frobenius(7, splitting_map=1)
0           if (’a’, ’b’) is 1 of 12 possibilities mod 7
3*zeta4a0  if (’a’, ’b’) is 1 of 6 possibilities mod 7
-zeta4a0   if (’a’, ’b’) is 1 of 6 possibilities mod 7
2*zeta4a0  if (’a’, ’b’) is 1 of 6 possibilities mod 7
-2*zeta4a0 if (’a’, ’b’) is 1 of 6 possibilities mod 7
zeta4a0    if (’a’, ’b’) is 1 of 6 possibilities mod 7
-3*zeta4a0 if (’a’, ’b’) is 1 of 6 possibilities mod 7
```

When we compute the traces at 11, where E_γ can have multiplicative reduction, we get two cases that are indistinguishable.

```
sage: Egamma.trace_of_frobenius(11)
6   if ('a', 'b') is 1 of 5 possibilities mod 11
-6  if ('a', 'b') is 1 of 5 possibilities mod 11
0   if ('a', 'b') is 1 of 30 possibilities mod 11
-4  if ('a', 'b') is 1 of 20 possibilities mod 11
-2  if ('a', 'b') is 1 of 10 possibilities mod 11
2   if ('a', 'b') is 1 of 10 possibilities mod 11
4   if ('a', 'b') is 1 of 20 possibilities mod 11
12  if ('a', 'b') is 1 of 10 possibilities mod 11 and \
a11E == +1 or ('a', 'b') is 1 of 10 possibilities mod 11 \
and a11E == +1
-12 if ('a', 'b') is 1 of 10 possibilities mod 11 and \
a11E == -1 or ('a', 'b') is 1 of 10 possibilities mod 11 \
and a11E == -1
```

Section 2.11

Some irreducibility results

We will finish this chapter by listing some results that show irreducibility of the representations $\overline{\rho_{\beta,\lambda}}$ when the $\mathbb{Q}$-curve E has degree field $\mathbb{Q}(\sqrt{a})$ for some square-free $a \in \mathbb{Z} \setminus \{0, 1\}$. Explicitly we will devote this section to proving the following result.

Theorem 2.11.1. *Let E be a $\mathbb{Q}$-curve with dual basis $\{a\}$ and $\{2\}$ for the degree map with a square-free, and let $l > 2$ be a prime number. For any splitting map β for c_E and prime $\lambda \mid l$ of L_β if any of the following hold*

1. *$\overline{\rho_{\beta,\lambda}}$ is reducible,*
2. *$\overline{\rho_{\beta,\lambda}}$ is absolutely reducible,*
3. *$\mathbb{P}\overline{\rho_{E,l}}$ is reducible, or*
4. *$\mathbb{P}\overline{\rho_{E,l}}$ is absolutely reducible,*

then we have that either

- *$l = 3$ and*

$$\begin{aligned} j(E) = 2^6 y^{-2}\,(4\,x - 7\,y)^{-6} \\ \cdot\Big(\big(512\,x^8 - 6\,016\,x^7 y + 78\,176\,x^6 y^2 + 987\,032\,x^5 y^3 \\ + 30\,371\,282\,x^4 y^4 + 97\,063\,160\,x^3 y^5 \\ + 226\,082\,780\,x^2 y^6 + 227\,965\,064\,x y^7 \\ + 291\,927\,773\,y^8\big) \\ + 2\sqrt{a}\,(x - 22\,y)\,(x + 5\,y)^2 \\ \cdot\big(256\,x^4 - 64\,x^3 y + 65\,616\,x^2 y^2 \\ + 80\,372\,x y^3 + 187\,783\,y^4\big)\Big), \end{aligned}$$

for some $x, y \in \mathbb{Q}$ with $x^2 + 2\,y^2 = a$;

- *$l = 5$ and*

$$\begin{aligned} j(E) = 2^6 y^{-2}\,(4\,x - 3\,y)^{-10} \\ \cdot\Big(\big(131\,072\,x^{12} - 1\,015\,808\,x^{11} y + 15\,802\,368\,x^{10} y^2 \\ + 303\,943\,680\,x^9 y^3 + 8\,502\,563\,840\,x^8 y^4 \\ + 41\,661\,192\,832\,x^7 y^5 + 122\,507\,172\,512\,x^6 y^6 \\ + 219\,682\,233\,088\,x^5 y^7 + 344\,561\,617\,040\,x^4 y^8 \\ + 329\,235\,309\,720\,x^3 y^9 + 342\,028\,231\,098\,x^2 y^{10} \\ + 150\,869\,431\,408\,x y^{11} + 111\,226\,255\,277\,y^{12}\big) \\ + 2\sqrt{a}\,(2\,x + 11\,y)^2\,\big(4\,x^3 - 84\,x^2 y - 37\,x y^2 - 122\,y^3\big) \\ \cdot\big(4\,096\,x^6 + 7\,168\,x^5 y + 1\,058\,560\,x^4 y^2 + 2\,349\,440\,x^3 y^3 \\ + 4\,841\,440\,x^2 y^4 + 2\,594\,668\,x y^5 + 3\,767\,779\,y^6\big)\Big), \end{aligned}$$

for some $x, y \in \mathbb{Q}$ with $x^2 + y^2 = a$;

- *$l = 7$ and $j(E) = -3375, \frac{-10\,529 \pm 16\,471\sqrt{-7}}{8}, \frac{56\,437\,681 \pm 1\,875\,341\sqrt{-7}}{32\,768}$;*

- $l = 13$ *and* $j(E) = 3\,448\,440\,000 \pm 956\,448\,000\sqrt{13}$*; or*
- $l = 11$ *or* $l > 13$*, and* E *has potential good reduction at all primes of characteristic* > 3*.*

We start by showing that the conditions (1) through (4) are in fact equivalent. The fact that (4) is equivalent to (2) easily follows from the fact that

$$\mathbb{P}\overline{\rho_{E,l}} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\overline{\mathbb{F}_l})$$

is the projectivization of

$$\overline{\rho_{\beta,\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_l}).$$

For the remaining equivalences we note that Theorem 3.2 of [Rib04] tells us that $\overline{\rho_{\beta,\lambda}}$ and hence also $\mathbb{P}\overline{\rho_{E,l}}$ are odd. Since l is odd this implies that (1) and (2) are equivalent as well as (3) and (4). Since all the conditions are equivalent we will from now on assume all of them.

For the next part we will only assume that the dual basis for the degree map is $\{a\}$ and $\{d\}$ with a and d square-free and $l \nmid d$. First of all note that Proposition 2.8.2 and Corollary 2.7.2 allow us to assume without loss of generality that E is defined over $K := \mathbb{Q}(\sqrt{a})$ itself and that

$$\phi_\sigma = \begin{cases} \mathrm{Id} & \text{if } \sigma \in G_K \\ \phi & \text{otherwise,} \end{cases}$$

where $\phi : {}^\tau E \to E$ is an isogeny of degree d with τ a generator of $G_{\mathbb{Q}}^K$. This implies that $\overline{\rho_{\beta,\lambda}}|_{G_K}$ is isomorphic to the usual representation

$$\overline{\rho_{E,l}} : G_K \to \mathrm{Aut}(E[l]) \cong \mathrm{GL}_2(\mathbb{F}_l),$$

hence the latter must be reducible by our assumptions. It follows that E should have an l-isogeny of which the kernel is defined over K, i.e it must correspond to a K-point P on $X_0(dl)$. Since E is also d-isogenous to its Galois conjugate we have

$$ {}^\tau P = w_d P, \tag{2.14}$$

where w_d arises from the Fricke involution on $X_0(d)$. Therefore E in fact corresponds to a $\mathbb{Q}$-point on the variety $C_{d,l} := X_0(dl)/w_d$.

Our goal is now to find the $\mathbb{Q}$-points on $C_{d,l}$ that can arise from quadratic points on $X_0(dl)$. We can only do this explicitly for finitely many l and d, so we need the asymptotic result from [Ell04]. In the proof of Proposition 3.2 in [Ell04] a twisted curve $X_0(dl)^K$ – of which the $\mathbb{Q}$-points precisely correspond to K-points of $X_0(dl)$ satisfying Equation (2.14) – is used to prove the result for $l = 11$ and $l > 13$ for any d with $l \nmid d$.

We will stick to the case $d = 2$ and do some explicit computations to derive the result for the other prime numbers l. We will start with $l = 13$ in which case $X_0(2l)$ is a hyperelliptic curve of genus 2. We use Magma [BCP97] to compute the quotient $C_{2,l}$, which turns out to be an elliptic curve with only three rational points. Note that the map $X_0(2l) \to C_{2,l}$ has degree 2 and we can easily demonstrate six points over $\mathbb{Q}(\sqrt{13})$ lying above these three points. These must therefore be all points of $X_0(2l)$ lying above these three points. By computing the j-invariants of these points using Magma [BCP97] and discarding those with j-invariant infinity, we find the result as in Theorem 2.11.1 for the case $l = 13$.

Next we look at $l = 7$ in which case $X_0(2l)$ is an elliptic curve. Using Magma [BCP97] we compute the quotient $C_{2,l}$ which is also an elliptic curve with only six $\mathbb{Q}$-rational points. A quick check shows that the 12 points of $X_0(2l)$ defined over $\mathbb{Q}(\sqrt{-7})$ are precisely the points lying above these six points with regards to the degree two map $X_0(2l) \to C_{2,l}$. Computing the j-invariants of these points and disregarding infinity gives us the result as in Theorem 2.11.1 for $l = 7$.

Now look at $l = 5$ in which case $X_0(2l)$ is a rational curve, so $C_{2,l}$ is as well. By fixing the orbits of $w_2 : X_0(2l) \to X_0(2l)$ that will map to $[0 : 1]$ and $[1 : 0]$ we can describe the quotient map $\phi : X_0(2l) \to C_{2,l}$. Choosing the orbits of $[0 : 1]$ and $[1 : 0]$ as these orbits respectively, we can compute with Magma [BCP97] that

$$\phi : \mathbb{P}^1 \to \mathbb{P}^1, \quad [x : y] \to [x(x + 5\,y) : y(x + 4\,y)].$$

It now remains to find the K-points of $\mathbb{P}^1$ that map to $\mathbb{Q}$-points under ϕ. It is obvious that the points $[1 : 0], [-4, 1] \in \mathbb{P}^1(K)$ map to $[1 : 0]$ under ϕ and as $\deg \phi = 2$ they are the only points that do so. All the other points of $\mathbb{P}^1(K)$ are of the form $[x : 1]$ for some $x \in K \setminus \{-4\}$ with

$$\phi([x : 1]) = [x(x + 5) : x + 4] = [x(x + 5)(\overline{x} + 4) : N^K_{\mathbb{Q}}(x + 4)]$$

with $\overline{x}$ the Galois conjugate of x in K and $N^K_{\mathbb{Q}} : K \to \mathbb{Q}$ the norm of K.

Using the above we see that all points of $\mathbb{P}^1(K)$ mapping to $\mathbb{P}^1(\mathbb{Q})$ are of the form $[1 : 0]$ or $[x : 1]$ with $x \in K$ and $x(x + 5)(\overline{x} + 4) \in \mathbb{Q}$. Write $x = x_1 + x_2\sqrt{a}$

with $x_1, x_2 \in \mathbb{Q}$, then we find that the second condition is equivalent to

$$\begin{gathered}(x_1^2 + 8\,x_1 + 20)x_2 = ax_2^3, \text{ i.e.}\\ x_2 = 0 \text{ or } a = \left(\frac{x_1+4}{x_2}\right)^2 + \left(\frac{2}{x_2}\right)^2.\end{gathered}$$

This implies that all the points of $\mathbb{P}^1(K)$ mapping to $\mathbb{P}^1(\mathbb{Q})$ under ϕ are either $\mathbb{Q}$-points or of the form $[2(x+\sqrt{a}) - 4y : y]$ where $x, y \in \mathbb{Q}$ and $x^2 + y^2 = a$.

Note that E has degree field $K_d = \mathbb{Q}(\sqrt{a})$ and therefore can not be isomorphic to a curve over a smaller field, hence it must correspond to a point of the last form. Using Magma [BCP97] we can compute the j-invariant of such a point which matches the j-invariant stated in Theorem 2.11.1 for the case $l = 5$.

The remaining case $l = 3$ is similar to $l = 5$ as also $X_0(6)$ is a rational curve. In this case we find through computations in Magma [BCP97] that

$$\phi : \mathbb{P}^1 \to \mathbb{P}^1, \quad [x : y] \to [x(x + 9\,y) : y(x + 8\,y)].$$

So besides $[1 : 0]$ and $[-8 : 1]$ that map to $[1 : 0]$ any K-rational point $[x : 1]$ maps to

$$\phi([x : 1]) = [x(x+9) : x+8] = [x(x+9)(\overline{x}+8) : N_{\mathbb{Q}}^{K}(x+8)],$$

where again $\overline{x}$ is the Galois conjugate of x and $N_{\mathbb{Q}}^{K} : K \to \mathbb{Q}$ is the norm of K. Writing $x = x_1 + x_2\sqrt{a}$ with $x_1, x_2 \in \mathbb{Q}$ we see that $[x : 1] \in \mathbb{P}^1(K)$ maps to a $\mathbb{Q}$-rational point if and only if

$$\begin{gathered}(x_1^2 + 16\,x_1 + 72)x_2 = ax_2^3, \text{ i.e.}\\ x_2 = 0 \text{ or } a = \left(\frac{x_1+8}{x_2}\right)^2 + 2\left(\frac{2}{x_2}\right)^2.\end{gathered}$$

Therefore the K-points that map to $\mathbb{Q}$-points under ϕ are either in $\mathbb{P}^1(\mathbb{Q})$ or of the form $[2(x+\sqrt{a}) - 8y : y]$ for some $x, y \in \mathbb{Q}$ with $x^2 + 2\,y^2 = a$. The curve E must correspond to a point of the latter form, hence we can compute the j-invariant of such a point in Magma [BCP97] to find the result as stated in Theorem 2.11.1 for $l = 3$.

Chapter 3

Automating the modular method

In this chapter we will discuss how to automate a basic version of the modular method and how this has been implemented in the framework [vL21a]. This relies in part on the theory discussed in Chapter 1 and Chapter 2.

Section 3.1 provides a step-by-step description of the modular method for Frey $\mathbb{Q}$-curves, with some remarks about how this can be extended to more general Frey curves. It then discusses how the material of Chapter 1 and Chapter 2 come together to automate the first part of the modular method for Frey $\mathbb{Q}$-curves, with the latter part of the automation being discussed later in this chapter. It also outlines how this automation has been implemented in the framework [vL21a].

The final sections discuss the still remaining parts of the automation. Section 3.2 describes how the framework [vL21a] deals with modular forms that are needed for the version of the modular method discussed here. Section 3.3 discusses available functions in the framework [vL21a] to automate the newform elimination step of the modular method. This includes elimination by comparison of traces of Frobenius in Section 3.3.1 for multiple exponents l simultaneously, the Kraus method in Section 3.3.2 for a fixed exponent l, and some additional convenience functions in Section 3.3.3.

To demonstrate the power of the framework [vL21a] and as a sanity check thereof, the author has worked out various examples based on the literature. Table 3.1 gives an overview of the various examples that are distributed with the framework [vL21a]. All examples are worked out as a reStructuredText file containing explanatory text, as well as command line input and output that can be verified with SageMath's [Sag20] automated doctest system. Examples of new Diophantine problems for which the framework [vL21a] has been used can be found in the next two chapters.

Article	Equation	Full example
[DM97]	$a^l + b^l = 2c^l$ $a^l + b^l = c^2$ $a^l + b^l = c^3$	`Darmon-Merel-1997.rst`
[Kra98]	$a^3 + b^3 = c^l$	`Kraus-1998.rst`
[Ell04]	$a^4 + b^2 = c^l$	`Ellenberg-2002.rst`
[BMS08]	$c_1 a^l - 2^r c_2 b^l = 1$	`Bugeaud-Mignotte-Siksek-2008.rst`
[DU09]	$a^4 + db^2 = c^l$	`Dieulefait-Urroz-2009.rst`
[BC12]	$a^2 + b^6 = c^l$	`Bennett-Chen-2012.rst`
[BCDY14]	$a^3 + b^{3l} = c^2$	`Bennett-Chen-Dahmen-Yazdani-2014.rst`
[DF14]	$a^5 + b^5 = 2c^l$ $a^5 + b^5 = 3c^l$	`Dieulefait-Freitas-2014.rst`
[vL21b]	$(a-b)^4 + a^4 + (a+b)^4 = c^l$	`Langen-2021.rst`

Table 3.1: Worked out examples for the framework [vL21a] from the literature

Section 3.1

The modular method

In this section we will describe the modular method for Frey $\mathbb{Q}$-curves. In particular we describe how the framework [vL21a] can be used to automatically apply this method to a Diophantine equation, but we will also discuss automation in a more general context. We start with a description of this version of the modular method.

Problem Given a family of Diophantine equations parameterised by some prime exponent l, prove the non-existence of putative solutions.

Step 0 Find a Frey $\mathbb{Q}$-curve associated to the family of Diophantine equations. A Frey curve is an elliptic curve E over some number field K of which the Weierstrass coefficients depend on a putative solution of the Diophantine equation for some l. Furthermore a Frey curve E must have a finite set S of primes of K, independent of the putative solution, such that

- at every prime $\mathfrak{p} \notin S$ the given Weierstrass equation for E is minimal and E has good or multiplicative reduction at $\mathfrak{p}$, and
- the discriminant is an l-th power outside S, i.e. $l \mid \operatorname{ord}_{\mathfrak{p}} \Delta$ for every prime $\mathfrak{p}$ of K not in S.

We will also assume that E has no complex multiplication. Theory for curves with complex multiplication can be found in [Shi71], but is irrelevant to the problems considered in this dissertation.

Step 1 Show there is a newform $g \in \mathcal{S}_2(\Gamma_1(N))$ associated with the curve E for some $N \in \mathbb{Z}_{>0}$ using Theorem 2.1.9 and Theorem 2.1.10. From the theory in Chapter 2 we know that we can obtain this newform from a splitting map $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ for c_E and that we have $\rho_{\beta,\lambda} \cong \rho_{g,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(L_{\beta,\lambda})$ for all primes λ of the splitting image field L_β.

Step 2 Show that the mod λ Galois representation $\overline{\rho_{g,\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ is irreducible for a prime $\lambda \mid l$, e.g. using the result from Section 2.11. Furthermore show that $\overline{\rho_{g,\lambda}}$ is finite at all primes p not divisible by primes in S, e.g. using Theorem 2.8.3.

Step 3 Use level lowering results, e.g. Theorem 4.1 in [Dia97] and Theorem 2.1 in [Rib94], and the results from Step 2 to show that there exists a newform $f \in \mathcal{S}_2(\Gamma_1(\tilde{N}))$ with

$$\tilde{N} = \prod_{\substack{p \mid N \\ \exists \mathfrak{p} \in S : \mathfrak{p} \mid p}} p^{\operatorname{ord}_p N}$$

and

$$\overline{\rho_{\beta,\lambda}} \cong \overline{\rho_{g,\lambda}} \cong \overline{\rho_{f,\lambda'}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_l}),$$

for some primes $\lambda, \lambda' \mid l$ in the appropriate fields. Note that f and g will have the same character.

Step 4 For the newform f compute its level $\tilde{N}$, e.g. using results from Section 2.9, and its character ε, e.g. using Corollary 2.8.6. Next compute all the newforms in the space $\mathcal{S}_2(\tilde{N}, \varepsilon)$. Note that this is all a finite computation as S is finite.

Step 5 For each newform $\tilde{f} \in \mathcal{S}_2(\tilde{N}, \varepsilon)$ found in Step 4, compare its mod $\tilde{\lambda} \mid l$ Galois representation $\overline{\rho_{\tilde{f},\tilde{\lambda}}}$ to the mod λ representation $\overline{\rho_{\beta,\lambda}}$. In particular one compares the traces of these Galois representations at a Frobenius element σ. If the difference $\operatorname{Tr}\overline{\rho_{\beta,\lambda}}(\sigma) - \operatorname{Tr}\overline{\rho_{\tilde{f},\tilde{\lambda}}}(\sigma)$ is non-zero then the Galois representations can not be isomorphic. In this case we will say σ eliminates the prime l for the newform $\tilde{f}$. If we can eliminate the prime l for all newforms $\tilde{f}$, then the newform f from Step 3 can not exist for this l. This implies that no putative solution as in Step 0 can exist for such l.

Remark 3.1.1. Let $p \neq l$ be a prime number not divisible by the primes in S. By Theorem 2.10.1 and Theorem 2.10.7 we know that the trace of $\overline{\rho_{\beta,\lambda}}$ at a Frobenius element can be given as an algebraic integer independent of the prime λ. If we furthermore assume that p does not ramify in a field over which β is defined and E is completely defined, we may denote these algebraic integers by $a_p(\beta)$, as by Theorem 2.8.3 the Galois representation is unramified. By Theorem 9.5.4 in [DS05] a similar result is true for the Galois representations $\overline{\rho_{\tilde{f},\tilde{\lambda}}}$. The algebraic integer $a_p(\tilde{f})$ that reduces to the trace of Frobenius at p modulo $\tilde{\lambda}$ is the p-th coefficient of the Fourier expansion of $\tilde{f}$. Instead of doing the computation in Step 5 for each prime l separately, one could deduce which l can not be eliminated by σ by considering the primes dividing $a_p(\tilde{f}) - a_p(\beta)$.

Note that the algebraic integer $a_p(\beta)$ might still depend on the putative solution. However one can always determine a finite set $A_p(\beta)$ of the possible values of $a_p(\beta)$, as $a_p(\beta)$ only depends on the putative solution modulo a finite power of p. One can therefore find all the primes l that can definitely be eliminated by σ as those not dividing the norm of

$$p \prod_{a \in A_p(\beta)} \left(a - a_p\left(\tilde{f}\right)\right).$$

Of course this only eliminates primes l when $a_p(\tilde{f}) \notin A_p(\beta)$.

Remark 3.1.2. One can also use other properties of Galois representations to eliminate newforms in Step 5. For example one might use the image of inertia, the image of the entire Galois representation, or one of the representations being reducible to show that $\overline{\rho_{\beta,\lambda}}$ and $\overline{\rho_{\tilde{f},\tilde{\lambda}}}$ are not isomorphic. When a newform $\tilde{f}$ has complex multiplication, but E does not, such strategies might be needed to eliminate $\tilde{f}$. The theory for these elimination strategies goes beyond the scope of this chapter. Some examples based on articles that prove such results will eliminate CM newforms without further proof.

Remark 3.1.3. Actual solutions to the family of Diophantine equations could form an obstruction to the modular method. For such solutions a newform f in Step 4 does exist and Step 5 can therefore not eliminate all l. When some actual solutions are known it is sometimes possible to ensure they do not cause obstructions for the modular method. For example it might be possible to choose a Weierstrass equation for the Frey curve for which a known solution corresponds to a singular curve. In other cases a known solution might correspond to an elliptic curve with a special property, such as complex multiplication, which a general putative solution does not have. In such a case additional elimination tactics, like those discussed in Remark 3.1.2, could potentially eliminate the newform corresponding to the known solution. Furthermore the modular method could be combined with other methods, but this goes beyond the scope of this dissertation.

Remark 3.1.4. In case E is defined over $\mathbb{Q}$ one may replace modularity of $\mathbb{Q}$-curves in Step 1 with modularity of elliptic curves over $\mathbb{Q}$. In this case one would interchange $\rho_{\beta,\lambda}$ and $\overline{\rho_{\beta,\lambda}}$ with $\rho_{E,l}$ and $\overline{\rho_{E,l}}$, and f and g would be newforms in $\mathcal{S}_2(\Gamma_0(\tilde{N}))$ and $\mathcal{S}_2(\Gamma_0(N))$ respectively. Furthermore N will just be the conductor of E.

Similarly one could replace the Frey $\mathbb{Q}$-curve with a general Frey curve E over a number field K, if each of the following is true.

- Modularity of elliptic curves over K is known and we replace the newform in Step 1 with an appropriate modular form associated to such elliptic curves. For example in [FLHS15] and [DNS20] it is shown that for K a real quadratic or totally real cubic field every elliptic curve E/K is modular and the corresponding modular forms are Hilbert modular forms of parallel weight 2. For K quadratic imaginary modularity is conjecturally known, but not all elliptic curves are modular. In that case the corresponding modular forms are Bianchi modular forms.

- Irreducibility results as in Step 2 are known for the representations corresponding to these elliptic curves.

- Level lowering results as in Step 3 are known for the corresponding modular forms. This is for example the case for Hilbert modular forms as can be found in [FS15].

- Computation of the newforms in Step 4 is possible for the corresponding modular forms. Furthermore one should be able to compute with their Galois representations to perform the elimination in Step 5. For Hilbert and Bianchi modular forms there exists an implementation for this in Magma [BCP97].

Let us look at what parts of this procedure can be automated. For Step 0 there are some recipes to make Frey curves for certain families of Diophantine equations, but in general this relies on user input. Our automation therefore starts with the user input of one or several Frey curves. A user will input these curves in the framework [vL21a] as a `FreyCurve` or `FreyQcurve`. Note Remark 3.1.4 for the `FreyCurve` case. See Section 1.6.6 and Section 2.1 for more information about constructing these objects.

Steps 1 through 3 are entirely theoretical and can therefore not really be automated. Most of the necessary theory for these steps has already been discussed in Chapter 2. It should be noted that irreducibility as discussed in 2.11 does not cover all possible $\mathbb{Q}$-curves. Furthermore using Theorem 2.8.3 in Step 2 only works when primes that ramify in a field over which β is defined and E is completely defined are part of S. Level lowering has not been discussed in Chapter 2, but can be found in [Dia97]. For other Frey curves as in Remark 3.1.4 these results need to be shown separately. The framework [vL21a] assumes these steps are provided by the user and our automation starts at Step 4.

For Step 4 the level $\tilde{N}$ of the newform f can be computed using the theory of Section 2.9. The theory in that section requires E to have a decomposition field, so we might have to replace E by an isogenous curve using Corollary 2.7.2, Corollary 2.7.4, and Corollary 2.7.8. Note that in practice E is often already defined over the degree field K_d and this isogenous curve can be obtained as a twist E_γ which is easily computed with the theory in Chapter 2. In the framework [vL21a] one can obtain this twist by calling the method `decomposable_twist`. The corresponding newform levels can then be computed with the method `newform_levels`, which will require the set S as the argument `bad_primes`.

Note that the computation of the newform levels relies on the computation of the conductor of the curve E. To automate this the theory of Chapter 1 can be used. The framework [vL21a] does this implicitly in the method `newform_levels` by computing the conductor over the `decomposition_field`. For Frey curves E as in Remark 3.1.4 the level required in Step 4 is the conductor of E, so the theory in Chapter 1 can also be used to automate the level computation for those curves.

Note that the character ε in Step 4 follows from Corollary 2.8.6. It is the inverse of the splitting character for which Section 2.4 provides a way to compute it. In the framework [vL21a] the character ε can be obtained by taking the inverse of the character returned by `splitting_character`. Note that for Frey curves as in Remark 3.1.4 the character ε is always trivial and thus requires no computation.

What remains to automate in Step 4 is the computation of the newforms in $\mathcal{S}_2(\tilde{N}, \varepsilon)$. For this there already exist implementations in Magma [BCP97] and SageMath [Sag20], which the framework [vL21a] uses. As noted in Remark 3.1.4 such implementations also exist in Magma [BCP97] for Hilbert modular forms and Bianchi modular forms. The framework [vL21a] uses these to compute newform spaces associated to Frey curves over totally real fields and imaginary quadratic fields respectively. Section 3.2 discusses how the framework [vL21a] uses these various implementations.

The framework [vL21a] can do all the computations necessary for Step 4 at once using the method `newform_candidates` of the `FreyCurve` and `FreyQcurve` classes. This method returns the newforms computed at the end of Step 4 that can be used for Step 5. The set S can be provided to this method using the argument `bad_primes`. By default it is taken to be those primes in `primes_of_possible_additive_reduction`, and also the primes that ramify in the `decomposition_field` for a `FreyQcurve`.

What remains to automate is Step 5. The implementations of a newform f in Magma [BCP97] and SageMath [Sag20] provide all the necessary data to compute the algebraic integers $a_p(f)$ discussed in Remark 3.1.1. In Section 3.2 we describe wrapper classes in the framework [vL21a] that compute these with the method `trace_of_frobenius`. On the elliptic curve side the framework [vL21a] provides a `trace_of_frobenius` method for `FreyQcurve` objects based on the theory in Section 2.10. This method computes the possible algebraic integers $a_p(\beta)$ discussed in Remark 3.1.1, so they can be used to construct the set $A_p(\beta)$. This allows for elimination as described in Remark 3.1.1. The framework [vL21a] provides methods to do this elimination automatically, which are outlined in Section 3.3.

Section 3.2

Wrapped newforms

As discussed in the previous section, the modular method – as discussed here – requires the computation of newforms with which we can do further computations as well. To this end SageMath [Sag20] provides a way to compute with classical modular forms, and Magma [BCP97] provides ways to compute with classical modular forms, Hilbert modular forms, and Bianchi modular forms. The module `modular_method.modular_forms.newform_wrapper` in the framework [vL21a] provides a uniform way to work with these implementations.

The main thing this module provides is a `WrappedNewform` class for each possible kind of newform and their respective implementation. These classes provide similarly named methods to retrieve data from these newforms. For example you can use the method `level` or `character` to get the level or character of a newform respectively. There is also the method `base_field` which gives the field on which the modular forms are based, e.g. $\mathbb{Q}$ for a classical modular form, the corresponding imaginary quadratic field for a Bianchi modular form, or the corresponding totally real field for a Hilbert modular form. The `base_field` K is also the base field of Galois representations of these newforms, i.e. these Galois representations have domain G_K. Note that currently these `WrappedNewform` classes only support newforms of (parallel) weight 2 as these are the ones that show up for the Frey curves considered in this dissertation.

Most important for the modular method is that each `WrappedNewform` class has the method `trace_of_frobenius`. For a newform f and a finite prime $\mathfrak{p}$ of the `base_field` that does not divide the `level`, this method computes an algebraic integer $a_{\mathfrak{p}}(f)$ in the `coefficient_field`. For any Frobenius element σ of $\mathfrak{p}$ we have that $\operatorname{Tr} \rho_{f,\lambda}(\sigma) = a_{\mathfrak{p}}(f)$, if λ is a prime of the `coefficient_field` such that λ and $\mathfrak{p}$ have distinct characteristic and the λ-adic Galois representation $\rho_{f,\lambda}$ is unramified at $\mathfrak{p}$. The same is true if we replace $\rho_{f,\lambda}$ by the mod λ Galois representation $\overline{\rho_{f,\lambda}}$, although we then have to take $a_p(f) \pmod{\lambda}$.

For classical modular forms the corresponding wrapper can be used to obtain information about the q-expansion of a newform. For example there is the method `coefficient` to get individual coefficients and the method `q_expansion` to get the q-expansion up to a certain point. Note that each coefficient is an element of the `coefficient_field`. Furthermore wrappers around classical modular forms provide the method `determinant_of_frobenius` that can be used to compute the the determinant of a Galois representation at a Frobenius element, similar to `trace_of_frobenius`. For classical modular forms one can also use the optional argument `power` for `trace_of_frobenius` and `determinant_of_frobenius`. When `power` > 1 these methods will compute the trace or determinant of the specified power of a Frobenius element instead. Using the argument `power` for other modular forms will result in an error as it requires `determinant_of_frobenius` to be implemented.

The module also provides functions for saving and loading newforms to and from files with the methods `save_newforms` and `load_newforms`. When saving newforms one should specify which coefficients (or which traces of frobenius in case of non-classical modular forms) should be stored using the argument `coefficients`. A loaded newform will be a special `WrappedNewform` backed by the data loaded from the file. It can therefore not do any computation that requires data that was not saved in the first place.

Note that each of the methods discussed in this section will return SageMath objects even when the actual implementation is part of Magma [BCP97]. This allows work done with these newforms to be independent from the implementation used. The module provides a function `get_newforms` that can be called to obtain newforms for a given level, character and base field for every possible implementation. The actual algorithm to obtain the newforms can be specified with the argument `algorithm`. One can choose between `"sage"`, `"magma"`, or `"file"`, indicating respectively a SageMath [Sag20] implementation, a Magma [BCP97] implementation, or loading from a file with the function `load_newforms`. When `algorithm="sage"` the function only works for base field $\mathbb{Q}$ and returns classical modular forms. When `algorithm="magma"` the newforms returned are classical modular forms for a base field $K = \mathbb{Q}$, Hilbert modular forms for a totally real base field K, and Bianchi modular forms for an imaginary quadratic base field K. Any other value for K will result in an error when `algorithm="magma"`. When `algorithm="file"` the function will load newforms from the file specified by `path` and return any newforms among them of the requested base field, level, and character.

The method `newform_candidates` of a `FreyCurve` or `FreyQcurve` uses the function `get_newforms` to get the newforms of the corresponding level and character. For a `FreyQcurve` the base field is always $\mathbb{Q}$, whereas for a `FreyCurve` the base field is the same as the field over which the curve is defined. To choose the algorithm to use, the `newform_candidates` method also has an argument `algorithm` that is passed along to `get_newforms`. Note that the limitations on the algorithm are therefore the same as for `get_newforms`. In particular one can not obtain newforms for a `FreyCurve` defined over a number field K of degree $n > 2$ that is not totally real, unless they are given by a file readable with `load_newforms`.

Section 3.3

Elimination methods

In the module `modular_method.modular_forms.elimination` of the framework [vL21a] there are various functions to perform the elimination process described in Step 5 of Section 3.1. Each of these functions accepts a similar input and output, designed so a user can chain eliminations one after the other. The common input includes

1. a Frey curve or tuple of Frey curves which share the same parameters, and

2. a list of newforms or – in case of multiple Frey curves – a list of tuples of newforms. These tuples give the possible combinations of newforms where the i-th newform in each tuple corresponds to a possible newform for the i-th curve.

The common output is a list of tuples similar to input 2. Each tuple has an additional last entry that is an integer divisible only by those prime numbers l that have not been eliminated for that combination of newforms yet. Note that if the integer at the end of this tuple would be ± 1, then the tuple is removed from the list altogether. This output can be used again as input 2 of another elimination function, in which case the integer at the end of each tuple is modified rather than adding an additional entry.

The list of newforms passed as an argument may be a `ConditionalValue` (as discussed in Section 1.6.4) consisting of multiple similar such lists. In that case the elimination will be performed on each case separately taking into account the corresponding condition whenever this is relevant. Similarly the output may also be a `ConditionalValue` of the same kind. Note that the number of cases in the output may differ from the number of cases in the input.

Subsection 3.3.1

Elimination by trace

The elimination discussed in Step 5 of Section 3.1 is by comparing traces of Frobenius elements. The framework [vL21a] implements this in the function `eliminate_by_trace`. Besides the standard input this method requires a prime number p. The Frobenius element at which the traces of the Galois representations are compared will be one of p or one of a prime above p.

The computation this function does resembles the one described in Remark 3.1.1, but differs slightly to work with multiple Frey curves $E_1, \ldots, E_r$ at once. First the function calls the function `trace_of_frobenius` for each Frey curve to obtain `ConditionalValue` objects which provide the possible algebraic integers $a_{\mathfrak{p}_i}(E_i)$ that map to the trace of Frobenius in the appropriate field. Here $\mathfrak{p}_i \mid p$ is a prime in the definition field of E_i, or $\mathfrak{p}_i = p$ if E_i is a `FreyQcurve`. In the latter case we also have $a_{\mathfrak{p}_i}(E_i) = a_p(\beta_i)$ with β_i the `splitting_map` of E_i. By inspecting the corresponding conditions – which depend on the common parameters of all the curves – the function `eliminate_by_trace` finds all the tuples $(a_{\mathfrak{p}_1}(E_1), \ldots a_{\mathfrak{p}_r}(E_r))$ that might occur. We denote here by A_p the set of all these tuples. If desired a condition can be passed to `eliminate_by_trace` with the argument `condition` to put further restrictions on the traces.

Next the function computes for each tuple of newforms $(f_1, \ldots, f_r)$ in input 2 a tuple of corresponding traces $(a_{\mathfrak{q}_1}(f_1), \ldots, a_{\mathfrak{q}_r}(f_r))$ using the method `trace_of_frobenius` of each `WrappedNewform`. Here each $\mathfrak{q}_i$ is a prime in the `base_field` of f_i such that $\mathfrak{p}_i$ and $\mathfrak{q}_i$ are divisible by a common prime in an appropriate field extension. For each $i \in \{1, \ldots, r\}$ the function computes the composite field L_i of the fields in which $a_{\mathfrak{p}_i}(E_i)$ and $a_{\mathfrak{q}_i}(E_i)$ have values. The function then computes

$$B := p \operatorname{lcm}\Big(\gcd\left(N_{\mathbb{Q}}^{L_i}(a_i - a_{\mathfrak{q}_i}(f_i)) : i \in \{1, \ldots, r\}\right) : (a_1, \ldots, a_r) \in A \Big),$$

where $N_{\mathbb{Q}}^{L_i} : L_i \to \mathbb{Q}$ is the norm of $L_i/\mathbb{Q}$. This integer is then added to the end of the tuple, as it is only divisible by those l that could not be eliminated for $(f_1, \ldots, f_r)$. If the tuple already had an integer B' as a last entry, it is replaced by $\gcd(B, B')$ instead. If the last entry is different from ±1 the tuple is added to the output.

Note that the computation of L_i and following computations in L_i might not be desired, as a large degree of L_i could make this computationally expensive. Therefore `eliminate_by_trace` has an optional argument `use_minpoly` to choose for a simpler computation. When set to `True` the function will compute the minimal polynomials $m_{a_{\mathfrak{q}_i}(f_i)}(x) \in \mathbb{Q}[x]$ for each tuple of newforms $(f_1, \ldots, f_n)$ and replace $N_{\mathbb{Q}}^{L_i}(a_i - a_{\mathfrak{q}_i}(f_i))$ by $N_{\mathbb{Q}}^{L_i'}\big(m_{a_{\mathfrak{q}_i}(f_i)}(a_i)\big)$ in the formula for B. Here L_i' is the field in which the $a_{\mathfrak{p}_i}(E_i)$ are defined. Even though the latter contains $N_{\mathbb{Q}}^{L_i}(a_i - a_{\mathfrak{q}_i}(f_i))$ as a factor it loses some information as it can not make a distinction between f_i and its Galois conjugates.

If one wants to perform this elimination tactic multiple times in a row, one can use the function `eliminate_by_traces`. This function accepts a list of primes as input and performs the method `eliminate_by_trace` for each one of them.

Both `eliminate_by_trace` and `eliminate_by_traces` have an optional argument `B`. This argument is used to limit what primes can be eliminated, in the sense that no prime number $l \nmid$ `B` will be eliminated when the method is performed. This can be used for elimination where a stricter condition applies to the parameters whenever l divides `B`. This is used implicitly by the elimination method `kraus_method` discussed later on.

Remark 3.3.1. If `B` is non-zero the output might contain tuples of which the last entry is 0, even though elimination for l dividing `B` could occur. This is a limitation of the framework [vL21a] as it does not have a way to represent a finite number of l being eliminated whilst infinitely many remain. It is therefore recommended to only use elimination strategies with `B` non-zero on newform lists in which the tuples have a non-zero additional last entry. Such a list could be obtained from the output of another elimination function or by modifying the tuples manually.

Example 3.3.2. `Elimination1.rst` To illustrate the methods discussed here we use one of the examples from the article [BMS08] by Bugeaud, Mignotte, and Siksek. We will focus on their example of the Thue equation

$$5^u a^l - 2^r b^l = 1 \tag{3.1}$$

with $a, b, u, r, l \in \mathbb{Z}$, $ab \neq 0$, $0 < u < l$, $r > 0$ and $l \geq 7$ prime.

We first look at the case $r = 3$ and b odd. Here the article uses the Frey curves

$$\begin{aligned} F_\psi^1 &: Y^2 = X^3 + (2\psi + 1)X^2 + (\psi^2 + \psi)X, \\ G_\psi^2 &: Y^2 = X^3 + X^2 - \frac{\psi}{4}X, \end{aligned}$$

where $\psi = 2^r b^l$. We enter these curves in the framework [vL21a] with ψ as a parameter.

```
sage: from modular_method import *
sage: R.<psi> = QQ[]
sage: con1 = (CongruenceCondition(psi - 8, 16) &
sage:         CongruenceCondition(psi + 1, 5))
sage: F1 = FreyCurve([0, 2*psi + 1, 0, psi^2 + psi, 0],
....:                condition=con1)
sage: G2 = FreyCurve([0, 1, 0, -psi/4, 0],
....:                condition=con1)
```

The levels of the newforms after level lowering can be found from the conductor of the corresponding curve, which can easily be computed with the framework [vL21a] using the theory from Chapter 1. We use here that the set S of bad primes consists of 2 and 5.

```
sage: S = [2, 5]
sage: F1.conductor(additive_primes=S)
40*Rad_P( (16) * psi^2 * (psi + 1)^2 )
sage: G2.conductor(additive_primes=S)
160*Rad_P( (psi + 1) * psi^2 )
```

This agrees with the levels given in the article. We compute the newforms directly as pairs (f, g) of a newform f corresponding to F^1_ψ and a newform g corresponding to G^2_ψ.

```
sage: nfs = [(f, g) for f in F1.newform_candidates(bad_primes=S)
....:        for g in G2.newform_candidates(bad_primes=S)]; nfs
[(q + q^5 + O(q^6), q - 2*q^3 - q^5 + O(q^6)),
 (q + q^5 + O(q^6), q + 2*q^3 - q^5 + O(q^6)),
 (q + q^5 + O(q^6), q - a2*q^3 + q^5 + O(q^6))]
```

Next we do the elimination starting with a Frobenius element at 3.

```
sage: nfs = eliminate_by_trace((F1, G2), nfs, 3); nfs
[(q + q^5 + O(q^6), q - 2*q^3 - q^5 + O(q^6), 0),
 (q + q^5 + O(q^6), q + 2*q^3 - q^5 + O(q^6), 12),
 (q + q^5 + O(q^6), q - a2*q^3 + q^5 + O(q^6), 12)]
```

We see that a Frobenius element at 3 does not eliminate any primes for the first pair of newforms. Therefore we also do elimination at 7 as suggested in the article. Note that we use the output of the previous elimination as an input here.

```
sage: nfs = eliminate_by_trace((F1, G2), nfs, 7); nfs
[(q + q^5 + O(q^6), q - 2*q^3 - q^5 + O(q^6), 56),
 (q + q^5 + O(q^6), q + 2*q^3 - q^5 + O(q^6), 12),
 (q + q^5 + O(q^6), q - a2*q^3 + q^5 + O(q^6), 4)]
```

We see for each pair of newforms that the final integer in the tuple is not divisible by a prime $l \geq 7$. Therefore the Thue equation (3.1) has no solutions when $r = 3$ and b is odd.

As a second example we also try to solve the Thue equation (3.1) when $r = 2$ and $b \equiv 1$ modulo 4, which is also discussed in the article [BMS08]. The Frey curves here remain the same but the levels change. We will use the levels from the article directly.

```
sage: nfs = [(f, g) for f in get_newforms(40)
....:        for g in get_newforms(20)]; nfs
[(q + q^5 + O(q^6), q - 2*q^3 - q^5 + O(q^6))]
```

We do the elimination at all the primes mentioned in the article at once.

```
sage: nfs = eliminate_by_traces((F1, G2), nfs,
....:                           primes=[3, 7, 11, 13]); nfs
[(q + q^5 + O(q^6), q - 2*q^3 - q^5 + O(q^6), 0)]
```

We see that no primes can be eliminated for the only pair of newforms. The article notes that this is because of a non-trivial solution in this case.

Subsection 3.3.2

Kraus method

In his article [Kra98] Kraus introduced a refinement of comparing traces when limiting to a single prime exponent l. His method suggests to do elimination with Frobenius elements σ at a prime $\mathfrak{p}$ such that $l \mid \# \mathbb{F}_{\mathfrak{p}}^*$. This restriction makes it so the l-th powers appearing in a Diophantine equation only have $\frac{\#\mathbb{F}_{\mathfrak{p}}^*}{l} + 1$ possible values, so a Frey curve E for such a Diophantine equation will most likely have a smaller set A_p as in Section 3.3.1. A smaller set A_p might make it possible to eliminate l with Frobenius elements of p in cases where the elimination strategy described in the previous section did not do this.

In the framework [vL21a] the function `kraus_method` provides the Kraus method as an elimination strategy. Besides the standard input it requires the prime number l and one or multiple polynomials in the parameters that are known to be l-th powers. Each polynomial may be defined over a different number field K.

For a prime number p the function `kraus_method` will compute the primes $\mathfrak{p}$ of each K such that $l \mid \# \mathbb{F}_{\mathfrak{p}}^*$. The corresponding polynomial should have coefficients c_i with $\mathrm{ord}_{\mathfrak{p}}\, c_i \geq 0$ but the code does not check for this. For each $\mathfrak{p}$ found in this way it will compute the values of the parameters modulo p for which the corresponding polynomial is indeed an l-th power modulo $\mathfrak{p}$. The function then calls `eliminate_by_trace` to do the actual elimination at p, with a condition expressing all these restrictions and the argument `B` set to l. Note that Remark 3.3.1 about `B` being non-zero therefore applies here.

The primes p on which `kraus_method` does the above procedure can be provided with the argument `primes`. By default it will be all the prime numbers smaller than 200. Note that any primes p for which no candidate $\mathfrak{p}$ exists will be automatically skipped.

Example 3.3.3. `Elimination2.rst` We will use the original example of Kraus in [Kra98] to illustrate the function `kraus_method`. We start with the

Diophantine equation

$$a^3 + b^3 = c^l \quad \text{with } a, b, c \in \mathbb{Z},\ \gcd(a, b) = 1 \text{ and } l \geq 5 \text{ prime.}$$

We make some additional assumptions on a putative solution (a, b, c) of this Diophantine equation to end up in the case where the article actually performs the Kraus method.

```
sage: from modular_method import *
sage: R.<a, b> = QQ[]
sage: cl = a^3 + b^3
sage: coprime = CoprimeCondition([a, b])
sage: condition = (coprime &
....:              CongruenceCondition(a - 2, 4) &
....:              CongruenceCondition(b - 1, 4) &
....:              CongruenceCondition(cl, 3) &
....:              PowerCondition(cl, 5))
```

We introduce the Frey curve introduced in the article and immediately compute the corresponding newforms.

```
sage: Eab = FreyCurve([0, 0, 0, 3*a*b, b^3 - a^3],
....:                 condition=condition)
sage: nfs = Eab.newform_candidates(); nfs
Warning: Assuming that a and b are coprime.
Warning: The bad primes chosen by default only take into \
account primes of additive reduction.
[q + 2*q^5 + O(q^6)]
```

To perform the Kraus method we need polynomials in the parameters that are known to be l-th powers. A natural candidate to choose is $a^3 + b^3$, but we get more information by factoring first. The article factors over $\mathbb{Q}$ to get $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$. We will factor further over $K = \mathbb{Q}(\zeta_3)$ to obtain $a^3 + b^3 = (a + b)(a + \zeta_3 b)(a + \zeta_3^2 b)$. Since $\gcd(a, b) = 1$ any ideal dividing two of these factors $a + \zeta_3^i b$ and $a + \zeta_3^j b$ must divide $(\zeta_3^{j-i} - 1) \mid (1 - \zeta_3)$. Since the norm of $1 - \zeta_3$ is 3, the factors $a + \zeta_3^i b$ can only have the unique prime $\mathfrak{p}_3$ of K above 3 in common. The assumption $3 \mid c^l$ shows one must have a factor $\mathfrak{p}_3$, hence all of them do. Furthermore as $a + b$ is an integer we have $\mathfrak{p}_3^2 \mid a + b$, so $\operatorname{ord}_{\mathfrak{p}_3}(a + \zeta_3 b) = \operatorname{ord}_{\mathfrak{p}_3}(a + \zeta_3^2 b) = \operatorname{ord}_{\mathfrak{p}_3}(1 - \zeta_3) = 1$. This tells us that

$$\begin{cases} 3(a + b) = & (-1)^{i_0} c_0^l \\ a + \zeta_3 b = & \zeta_6^{i_1}(1 - \zeta_3) c_1^l \\ a + \zeta_3^2 b = & \zeta_6^{i_2}(1 - \zeta_3) c_2^l \end{cases} \qquad \text{with } c_0 \in \mathbb{Z}, \text{ and } c_1, c_2 \in \mathbb{Z}[\zeta_3],$$

where we use that K has class number 1. As $l \nmid 6$ we can without loss of generality take $i_0 = i_1 = i_2 = 0$ and obtain three l-th powers.

```
sage: K.<zeta3> = CyclotomicField(3)
sage: poly0 = 3*(a + b)
sage: poly1 = (a + zeta3*b) / (1 - zeta3)
sage: poly2 = (a + zeta3^2*b) / (1 - zeta3)
```

We apply the Kraus method to $l = 5$. Note that the article considers only $l \geq 17$, but checking all proofs shows most arguments still apply for $l = 5$. Only the original proof that the mod l Galois representation of Eab is irreducible does not work, but an alternative proof can be found in [Dah08, Section 3.3.2]. The following arguments can be done for any l, but we stick with $l = 5$ as the computations are faster.

We first show that Remark 3.3.1 applies here.

```
sage: kraus_method(Eab, nfs, 5, (poly0, poly1, poly2),
....:              primes=prime_range(7, 50), condition=coprime)
[(q + 2*q^5 + O(q^6), 0)]
```

To solve this problem we simply change nfs to have tuples of newforms with 5 as a last entry. This makes it so the framework [vL21a] treats each tuple as if 5 is the only prime which could not be eliminated yet, so it will disappear when 5 is also eliminated. With this change we perform the elimination again.

```
sage: nfs5 = [(nf, 5) for nf in nfs]
sage: kraus_method(Eab, nfs5, 5, (poly0, poly1, poly2),
....:              primes=prime_range(7, 50), condition=coprime)
[]
```

We thus see that $l = 5$ can be eliminated with the Kraus method.

Subsection 3.3.3

Convenience methods

The functions described here do not eliminate primes by comparing Galois representations, but rather provide convenient ways to modify lists of newforms. We will show examples of how these are used in the example at the end of this section.

The first of these functions is eliminate_cm_forms. All this method does is remove every tuple of newforms from the input in which there is a newform that has complex multiplication. This can be used when it is known that no newforms with complex multiplication can correspond to certain Frey curves.

The second of these functions is `eliminate_primes`. When provided with an argument `N` this method eliminates all prime numbers $l \mid N$ for every tuple of newforms in the input. This can be used when one wants to exclude these primes from the output, or if some other theory allows the exclusion of these primes. Note that Remark 3.3.1 also applies to non-zero `N` given to this function.

When working with multiple Frey curves, one might first want to do elimination on each curve separately and then do a multi-Frey approach. To this end the function `combine_newforms` exists in the framework [vL21a]. It can be used to combine the lists of newforms for distinct Frey curves into a single input for all these curves together.

Example 3.3.4. `Elimination3.rst` We perform the elimination for the article [BC12] by Bennett and Chen using the framework [vL21a]. In this article the authors consider the Diophantine equation

$$a^2 + b^6 = c^l,$$

for $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $l \geq 3$ a prime exponent. We first do the initial setup.

```
sage: from modular_method import *
sage: R.<a, b> = QQ[]
sage: cl = a^2 + b^6
sage: coprime = CoprimeCondition([a, b])
sage: condition = coprime & PowerCondition(cl, 3)
```

Next we create the Frey $\mathbb{Q}$-curve introduced in the article.

```
sage: K.<i> = QuadraticField(-1)
sage: a_invariants = [0, 0, 0, -3*(5*b^3 + 4*a*i)*b,
....:                 2*(11*b^6 + 14*i*b^3*a - 2*a^2)]
sage: E = FreyQcurve(a_invariants, condition=condition,
....:                guessed_degrees=[3])
```

The article remarks that a decomposable twist of `E` can be obtained by twisting with $\gamma = \frac{-3+\sqrt{-3}}{2}$. We use that the `decomposition_field` of `E` already has a square root of -3 and perform this twist.

```
sage: Kdec = E.decomposition_field()
```

```
sage: gamma = (-3 + sqrt(Kdec(-3))) / 2
sage: E = E.twist(gamma)
sage: E.does_decompose()
True
```

Next we compute the newform candidates using that the bad primes are those above 2 and 3, as shown in the article.

```
sage: Kdef = E.definition_field()
sage: nfs = E.newform_candidates(bad_primes=Kdef.primes_above(6))
```

Section 4 in the article is dedicated to proving CM forms can be eliminated, so we eliminate them from the list obtained.

```
sage: nfs = eliminate_cm_form(E, nfs)
```

For the remaining cases the article introduces a second Frey curve. We introduce this curve and compute the newforms associated with it.

```
sage: E2 = FreyCurve([0, 0, 0, 3*b^2, 2*a], condition=condition)
sage: nfs2 = E2.newform_candidates(bad_primes=[2, 3])
```

We do the elimination on this curve separately and then on both curves combined.

```
sage: nfs2 = eliminate_by_traces(E2, nfs2, primes=[5, 7],
....:                            condition=coprime)
sage: nfs_comb = combine_newforms(nfs, nfs2)
sage: nfs_comb = eliminate_by_traces((E, E2), nfs_comb,
....:                                primes=[5, 7],
....:                                condition=coprime)
```

What has not been eliminated are small prime exponents n, which are treated separately in the article. To show nothing else remains we now eliminate the primes $2, 3, 5, 7$ and show the final list of remaining newforms is empty.

```
sage: nfs_comb = eliminate_primes((E, E2), nfs_comb, 2*3*5*7)
sage: nfs_comb
[]
```

Chapter 4

On the sum of fourth powers in arithmetic progression

This chapter is based on the article [vL21b] with the same title as this chapter, which was written by the author of this dissertation. Most of the text here is identical to that of the article except for the section about $\mathbb{Q}$-curves. This part has been rewritten to use the results in the previous chapters. Similarly some parts of the paper have been slightly reworded to reflect results presented in previous chapters.

Section 4.1

Introduction

In this chapter we will study an equation of the form

$$(x-y)^k + x^k + (x+y)^k = z^n, \quad x, y, z \in \mathbb{Z}, \quad k, n \in \mathbb{Z}_{>1}, \tag{4.1}$$

i.e. the sum of three k-th powers in arithmetic progression being a perfect power. Such equations have been intensively studied in the case $y = 1$, i.e. consecutive k-th powers. The earliest results in that case were already formulated by Euler in the case $k = n = 3$. Zhang [Zha14] gave a complete solution for consecutive integers for $k = 2, 3, 4$ and this was extended by Bennett, Patel and Siksek [BPS16] for $k = 5, 6$. In both cases the modular method was used with Frey curves defined over the rationals.

Also the more general case of Equation (4.1) has been studied before. For the case $k = 2$ and $\gcd(x, z) = 1$ Koutsianas and Patel [KP18] used prime divisors of Lehmer sequences to determine all solutions when $1 \leq y \leq 5000$. Koutsianas

[Kou19] further studied this case when y is a prime power p^m for specific prime numbers p. The case $k = 3$ was partially solved by Argáez-García and Patel [AP19] giving all solutions in case $1 \leq y \leq 10^6$ using different techniques including the modular method for some Frey curves over the rationals. In [KP18] and [AP19] the bounds on y are merely for computational purposes, whilst the techniques would generalize to larger bounds.

Variants of Equation (4.1) with more terms on the left-hand side have also been studied. Recent results include those by Patel and Siksek [PS17] and Patel [Pat18].

In this chapter we look at Equation (4.1) for the case $k = 4$. Zhang [Zha17] proved a partial result in this case. By considering y as a parameter and using the modular method with Frey curves over $\mathbb{Q}$, he managed to prove the non-existence of solutions for certain families of values for y. Although his approach could be pushed to include more families of values for y it appears this method can not be generalized to treat all values of y simultaneously.

We will give a complete solution for the case $k = 4$ (where $\gcd(x, y) = 1$ as always). Essential in the proof is the construction of two Frey $\mathbb{Q}$-curves defined over $\mathbb{Q}(\sqrt{30})$. Using the modular method on these curves overcomes the limitations in [Zha17], allowing us to prove the following main result.

Theorem 4.1.1. *The sum of three coprime fourth powers in arithmetic progression is not a perfect power, i.e. the equation*

$$(x - y)^4 + x^4 + (x + y)^4 = z^l \tag{4.2}$$

has no solutions $x, y, z \in \mathbb{Z}$ *with* $\gcd(x, y) = 1$ *for integers* $l > 1$.

Note that any solution to Equation (4.2) gives rise to a solution for l a prime number. For our proof it thus suffices to prove Theorem 4.1.1 for l prime as we shall do throughout this paper.

As mentioned, the construction of two Frey curves over the field $\mathbb{Q}(\sqrt{30})$ will be essential in the proof. The construction of these curves can be found in Section 4.4.

Since $\mathbb{Q}(\sqrt{30})$ is a real quadratic field the most direct approach to apply the modular method is to use Hilbert modularity of curves defined over real quadratic fields. We will perform the initial steps to this approach in Section 4.5. However we will also argue that the computation of the corresponding spaces of Hilbert modular forms is out of reach for the current computational power, making this approach unfeasible.

Instead we will use that the curves in this paper are by construction also $\mathbb{Q}$-curves for which a separate modularity result is known [Rib04]. A $\mathbb{Q}$-curve approach to solving Diophantine equations has already been used in articles such as the ones by Ellenberg [Ell04], Dieulefait and Freitas [DF14], Dieulefait and Urroz [DU09], Chen [Che10, Che12], Bennett and Chen [BC12], and Bennett, Chen, Dahmen and Yazdani [BCDY14]. We will discuss this approach in Section 4.6.

As in the mentioned articles we will follow [Que00] for general results about $\mathbb{Q}$-curves. The main differences lie in that the restrictions of scalars of our curves are not abelian varieties of GL_2-type themselves, but will decompose as a product of such varieties. This also happens in [DF14] and [Che10]. In the first this issue is dealt with by studying the relation between the corresponding Galois representations. We will rather study the relation between the corresponding newforms as was done in [Che10] and will be more specific about computing the character that defines this relation.

Another difference is in the way we compute the elliptic curve of which one should take the restriction of scalars. Most mentioned articles simply refer to [Que01] to prove the existence of a twist of the original curve that will suffice and perform a small search to find this twist. In [BC12] a more direct approach is given in case one can find a map $\alpha : G_{\mathbb{Q}} \to \mathcal{O}_K^*$ with a certain coboundary. We use Corollary 2.7.8 to show the existence of such a twist and use Proposition 2.5.5 to compute it.

Furthermore the approach we took should generalize to other Frey $\mathbb{Q}$-curves and is mostly algorithmic. Therefore the author has written code [vL21a] for SageMath [Sag20] that automates the generic parts of this approach. This code includes SageMath code to work with Frey curves, $\mathbb{Q}$-curves and Frey $\mathbb{Q}$-curves as well as the associated newforms. A reasonable effort has been made to make the code work for general such curves and provide sufficient documentation. Furthermore the example `Langen-2021.rst` in [vL21a] provides a structured overview of all the computations done for this paper interjected with explanatory notes. This document describes all intermediate steps needed for the calculations in this paper such that one can easily reproduce the results. Furthermore the computations in this file can be verified automatically using SageMath's automated doctest system. Some computations in this file also make use of MAGMA [BCP97]. The code [vL21a] also provides support for working with MAGMA when computing newforms to decrease computation time.

Since the modular method approach in this setting only works for prime numbers $l > 5$, Section 4.3 is dedicated to proving the cases for small l. The case $l = 2$ follows immediately from a local obstruction, whereas the cases $l = 3$ and $l = 5$ require the computation of some points on hyperelliptic curves to prove the non-existence of solutions.

Section 4.2 introduces some preliminary results about Equation (4.2) and introduces some notation that will be used throughout this chapter.

Section 4.2

Preliminaries

In this section we will prove some general results about integer solutions to Equation (4.2) with $\gcd(x, y) = 1$. Throughout this chapter (a, b, c) will denote an arbitrary such solution. Note that we have

$$c^l = (a-b)^4 + a^4 + (a+b)^4 = 3\,a^4 + 12\,a^2b^2 + 2\,b^4, \tag{4.3}$$

which leads to the following result.

Proposition 4.2.1. *The integer c is not divisible by 2, 3 or 5, hence a is odd and b is not divisible by 3.*

Proof. This follows immediately by considering Equation (4.3) modulo 4, 9 and 5. □

Let $f(x, y)$ be the left-hand side of Equation (4.2). The most general factorization of f is obtained by factoring over the splitting field L of $f(x, 1)$. Since $f(x, 1)$ is irreducible, the polynomial $f(x, y)$ factors as a product of a constant and Galois conjugates of

$$h(x, y) = x + vy, \tag{4.4}$$

where v is a root of $f(x, 1)$. To be precise we have

$$f(x, y) = 3\,(x + vy)\,(x - vy)\,(x + \sqrt{(-v^2 - 4)}\,y)\,(x - \sqrt{(-v^2 - 4)}\,y). \tag{4.5}$$

We can say a lot about the factor $h(a, b)$ and its Galois conjugates.

Lemma 4.2.2. *The distinct Galois conjugates of $h(a, b)$ are coprime outside primes above 3. Furthermore, the valuation of $h(a, b)$ at all primes above 2 and 5 is zero and its valuation at the unique prime $\mathfrak{p}_3$ in L above 3 is -1.*

Proof. Since any field that contains $h(a, b)$ and its Galois conjugates contains L we can safely do all computations in L. Note that a and b are integers and that v is only not integral at the unique prime $\mathfrak{p}_3$ above 3, so the only prime at which $h(a,b)$ and its Galois conjugates are not integral is $\mathfrak{p}_3$. For two distinct Galois conjugates ${}^{\sigma}(h(a,b))$ and ${}^{\tau}(h(a,b))$ their difference is equal to $({}^{\sigma}v - {}^{\tau}v)\, b$. Any prime dividing both can not divide b as it then also divides a contradicting their coprimality. Therefore the only common primes are in the differences ${}^{\sigma}v - {}^{\tau}v$. Using SageMath [Sag20] we can determine that the only primes dividing these differences are those above 2, 3 and 5, hence we arrive at the first conclusion.

For the second statement, we note that a and b are integral and v only has negative valuation at $\mathfrak{p}_3$ with $\operatorname{ord}_{\mathfrak{p}_3}(v) = -1$. This implies that the valuation of $h(a,b)$ and its conjugates is at least 0 at all primes above 2 and 5 and at least -1 at $\mathfrak{p}_3$. Applying this information to Equation (4.5) and using that c has valuation 0 at all these primes by Proposition 4.2.1, the second result immediately follows. □

Lemma 4.2.2 and Equation (4.5) tell us that

$$(h(a,b)) = \mathfrak{p}_3^{-1} I^l$$

for some integral ideal I of L. We will need this general result to solve the case $l = 5$.

For the other cases, we can limit ourselves to the subfield $K = \mathbb{Q}(\sqrt{30})$ of L. In this case we have two factors

$$g_1(x,y) := x^2 + \left(2 + \frac{1}{3}\sqrt{30}\right) y^2 \tag{4.6}$$

$$g_2(x,y) := x^2 + \left(2 - \frac{1}{3}\sqrt{30}\right) y^2, \tag{4.7}$$

and the factorization is

$$z^l = f(x,y) = 3\, g_1(x,y)\, g_2(x,y). \tag{4.8}$$

Note that g_1 and g_2 are both the product of two Galois conjugates of h and since these are all distinct we can conclude that $g_1(a,b)$ and $g_2(a,b)$ are coprime outside primes above 3. Also the result about valuations carries over, so both have valuation 0 at primes above 2 and 5 and since the unique prime $\mathfrak{q}_3$ of K above 3 factors as $\mathfrak{p}_3^2$ in L they have valuation -1 at $\mathfrak{q}_3$. Furthermore we find that

$$\begin{aligned}(g_1(a,b)) &= \mathfrak{q}_3^{-1} I_1^l \\ (g_2(a,b)) &= \mathfrak{q}_3^{-1} I_2^l,\end{aligned}$$

with I_1 and I_2 coprime integral ideals of K.

Throughout this chapter K and L will be the same as in this section, as will g_1, g_2 and h.

Section 4.3

Cases for Small l

In this section we will solve Equation (4.2) for small prime exponents l as the modular method used in the next sections only works for $l > 5$. All small cases have a slightly different approach.

Subsection 4.3.1

Case $l = 2$

In case $l = 2$ Equation (4.2) has a local obstruction at 3. This can be seen by considering Equation (4.3) modulo 9, or by considering the equation modulo 3 and using that $3 \nmid c$ from Proposition 4.2.1. This proves the non-existence of solutions in this case. A similar obstruction can be found modulo 5.

Subsection 4.3.2

Case $l = 3$

Suppose that (a, b, c) is a solution to Equation (4.2) for $l = 3$ and assume that $\gcd(a, b) = 1$. From Section 4.2 we know that

$$(g_1(a, b)) = \mathfrak{q}_3^{-1} I_1^3 = \mathfrak{q}_3^{-4} \left(\mathfrak{q}_3 I_1\right)^3$$

as fractional ideals in K. Since K has class number 2 and $\mathfrak{q}_3^{-4} = \left(\frac{1}{9}\right)$ we find that $\mathfrak{q}_3 I_1$ must be a principal ideal. Hence we conclude that

$$g_1(a, b) = \frac{1}{9} u \gamma^3,$$

for $u \in \mathcal{O}_K^*$ and $\gamma \in \mathfrak{q}_3$. Note that $\mathcal{O}_K^*$ is generated by $u_0 = (-1)^3$ and an element u_1 of infinite order, hence we can take $u = u_1^j$ for $j = 0, 1, 2$. Since the set $\{3, 6 + \sqrt{30}\}$ is an integral basis of of $\mathfrak{q}_3$ we can parametrize γ with integral parameters s and t to get that

$$\begin{aligned}
\gamma &= 3s + \left(6+\sqrt{30}\right) t = 3g_1(\sqrt{s}, \sqrt{t}) \\
a^2 &= F_{3,j}(s,t) \\
b^2 &= G_{3,j}(s,t) \\
c &= 3\,s^2 + 12\,st + 2t^2
\end{aligned} \tag{4.9}$$

for $F_{3,j}(s,t)$ and $G_3(s,t)$ some homogeneous polynomials over $\mathbb{Q}$ of degree 3.

Note that $t = 0$ corresponds to solutions in which c would be divisible by 3. So by Proposition 4.2.1 we find that $t \neq 0$. By multiplying the middle two equations in (4.9) and dividing by t^6 we find hyperelliptic curves C_j in the variables $X = \frac{s}{t}$ and $Y = \frac{ab}{t^3}$. Explicitly these curves are given by

$$\begin{aligned}
C_0 : Y^2 &= 27\,X^5 + 108\,X^4 + 84\,X^3 - 288\,X^2 - 564\,X - 368 \\
C_1 : Y^2 &= -1\,242\,X^6 - 1\,269\,X^5 - 432\,X^4 + 84\,X^3 + 72\,X^2 + 12\,X \\
C_2 : Y^2 &= -599\,940\,X^6 - 627\,237\,X^5 - 273\,132\,X^4 - 63\,276\,X^3 \\
&\quad -8\,208\,X^2 - 564\,X - 16.
\end{aligned}$$

As $t \neq 0$ every solution (a, b, c) corresponds to a point on such a curve. Using MAGMA [BCP97] we see that the curve C_2 has no solution in $\mathbb{Q}_3$, hence none in $\mathbb{Q}$. Also using MAGMA we can compute that the Jacobian of C_0 has only two-torsion points as rational points. Note that such points correspond to factors of the defining polynomial, i.e. of $F_{3,0}(s,t)G_{3,0}(s,t)$. Since the only linear factor in $F_{3,0}G_{3,0}$ is t, the only rational point on C_0 corresponds to the case $t = 0$ which we already excluded from corresponding to a solution.

The curve C_1 has no local obstruction. Furthermore the rank of its Jacobian is bounded above by 1 and its L-function suggests the rank is 1. However no point of infinite order on the Jacobian can be found within a small bound. We shall therefore apply a different approach.

For the case $j = 1$ the equations in (4.9) become explicitly

$$\begin{aligned}
a^2 &= -3\,s\left(23\,s^2 + 12\,st + 2\,t^2\right) \\
b^2 &= 18\,s^3 + 9\,s^2t - 2\,t^3 \\
c &= 3\,s^2 + 12\,st + 2\,t^2.
\end{aligned}$$

Note that in the first equation $23\,s^2 + 12\,st + 2\,t^2$ is congruent to c modulo 20. By Proposition 4.2.1 this implies $23\,s^2 + 12\,st + 2\,t^2$ is not divisible by 2 or 5. Note that s and t must be coprime since a and b are coprime, so therefore s

and $23\,s^2 + 12\,st + 2\,t^2$ must be coprime outside 2. Note that 2 does not divide $23\,s^2 + 12\,st + 2\,t^2$, so the two must be coprime and we find that

$$\begin{aligned} a &= 3\,a_1\,a_2 \\ s &= (-1)^{e_1}\,3^{e_2}\,a_1^2 \\ 23\,s^2 + 12\,st + 2\,t^2 &= (-1)^{1-e_1}\,3^{1-e_2}\,a_2^2, \end{aligned}$$

with $e_1, e_2 \in \{0,1\}$. Now note that

$$23\,s^2 + 12\,st + 2\,t^2 = 2\,(\beta s + t)\left(\overline{\beta} s + t\right) = 2N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{-10})}\left(\beta s + t\right),$$

where $\beta = 3 + \sqrt{10}/2$, $\overline{\beta}$ is its Galois conjugate and $N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{-10})}$ is the norm of the field $\mathbb{Q}(\sqrt{-10})$. Since $\mathbb{Q}(\sqrt{-10})$ is an imaginary field its norm is positive, hence $e_1 = 1$. Furthermore the unique prime above 3 in $\mathbb{Q}(\sqrt{-10})$ has norm 9, so $e_2 = 1$. We thus have that

$$2\,(\beta s + t)\left(\overline{\beta} s + t\right) = a_2^2.$$

Note that the factors $\beta s + t$ and $\overline{\beta} s + t$ are coprime outside primes dividing the difference $\beta - \overline{\beta} = \sqrt{-10}$. Since a_2 is an integer not divisible by 2 and 5 which ramify in $\mathbb{Q}(\sqrt{-10})$ these factors must have valuation -1 at the unique prime $\mathfrak{p}_2$ above 2 and valuation 0 at the unique prime above 5. This implies that

$$(\beta s + t) = \mathfrak{p}_2^{-1} I^2$$

for some ideal I of $\mathcal{O}_{\mathbb{Q}(\sqrt{-10})}$. Since the class number of $\mathbb{Q}(\sqrt{-10})$ is 2 this would imply that $\mathfrak{p}_2$ is principal, which is not the case. Therefore no solution can correspond to the case $j = 1$ and thereby no solution to Equation (4.2) with $\gcd(x,y) = 1$ exists for $l = 3$.

Remark 4.3.1. Geometrically Eqs. (4.9) define a curve with a degree 4 map to $\mathbb{P}^1$. The hyperelliptic curves we constructed in these sections are quotients of these curves through which this degree 4 map factors as two degree 2 maps. The only other geometric quotients with this same property are defined by taking the equation for a^2 and setting $t = 1$ or taking the equation for b^2 and setting $t = 1$. The quotient we considered is the only quotient for which rational points correspond to rational solutions of the corresponding equations, making this the natural choice. The same will be true for the Eqs. (4.10) in the next section.

Subsection 4.3.3

Case $l = 5$

Now suppose we have a solution (a, b, c) to Equation (4.2) such that $l = 5$ and $\gcd(a, b) = 1$. Recall from Section 4.2 that

$$(h(a,b)) = \mathfrak{p}_3^{-1} I^5 = \mathfrak{p}_3^4 \left(\mathfrak{p}_3^{-1} I\right)^5$$

as fractional ideals in L. Since $\mathfrak{p}_3^4 = (3)$ and 5 does not divide the order of the class group of L we find that $\mathfrak{p}_3^{-1} I$ must be a principal ideal, hence

$$h(a,b) = 3\, u\, \gamma^5$$

for some unit $u \in \mathcal{O}_L^*$ and $\gamma \in L$. Furthermore the valuation of γ is only negative at $\mathfrak{p}_3$ where it is -1, hence $\gamma \in \frac{1}{3}\mathcal{O}_L$. Note that in these arguments we may also replace L with $\mathbb{Q}(v)$. The field $\mathbb{Q}(v)$ is a number field of degree 4 and hence $\mathcal{O}_{\mathbb{Q}(v)}$ can be parameterized by four integer coefficients. Using this description we obtain for each choice of u a parameterization of a and b together with two equations in the four indeterminates. Since $\mathcal{O}_{\mathbb{Q}(v)}^*$ is generated by $u_0 = (-1)^5$ and an element u_1 of infinite order it is sufficient to consider $u = u_1^i$ for $i \in \{0, \ldots, 4\}$. Considering the equations obtained for each of these i modulo 5, we see that only two of them can parameterize coprime a and b, leaving only the cases $i = 0, 4$.

Without loss of generality we may assume that g_1 is the product of h with ${}^{\sigma}h$, where σ is the automorphism on $\mathbb{Q}(v)$ mapping v to $-v$. This implies that we have

$$g_1(a,b) = 9\,(u\,{}^{\sigma}u)\,(\gamma\,{}^{\sigma}\gamma)^5\,.$$

Since $\mathbb{Q}(v^2) = \mathbb{Q}(\sqrt{30}) = K$ we find that $u' := u\,{}^{\sigma}u \in \mathcal{O}_K^*$ and $\gamma' := \gamma\,{}^{\sigma}\gamma \in K$. Note that again γ' is only not integral at $\mathfrak{q}_3$ and furthermore $\mathrm{ord}_{\mathfrak{q}_3}(\gamma) = -1$, so we have that $\gamma' \in \mathfrak{q}_3^{-1} = \left(\frac{1}{3}\right)\mathfrak{q}_3$. From the case $l = 3$ we know that $\mathfrak{q}_3$ has an integral basis formed by 3 times the coefficients of g_1, hence $\mathfrak{q}_3^{-1}$ has an integral basis formed by the coefficients of g_1. In particular it has an integral basis of the form $\left\{1, \frac{\sqrt{30}}{3}\right\}$ which gives us a parameterization of the form

$$\begin{aligned} \gamma' &= s + \frac{\sqrt{30}}{3} t \\ a^2 &= F_{5,u'}(s,t) \\ b^2 &= G_{5,u'}(s,t), \\ c &= 3\,s^2 - 10\,t^2 \end{aligned} \tag{4.10}$$

for each choice of unit u'. Here $F_{5,u'}$ and $G_{5,u'}$ are homogeneous polynomials over $\mathbb{Q}$ of degree 5.

The only remaining cases are $u' = 1\,{}^{\sigma}1 = 1$ and $u' = u_1^4\,{}^{\sigma}u_1^4 = u_1^8$. As in the case $l = 3$ we can see that $t \neq 0$ and hence we can construct hyperelliptic curves by multiplying the equations for a^2 and b^2 and dividing the result by t^{10}. These give us the hyperelliptic curves

$$\begin{aligned}
C_1 : Y^2 &= 405\,X^9 - 4\,050\,X^8 + 16\,200\,X^7 - 54\,000\,X^6 + 113\,400\,X^5 \\
&\qquad -198\,000\,X^4 + 180\,000\,X^3 - 120\,000\,X^2 + 50\,000\,X - 20\,000 \\
C_{u_1^8} : Y^2 &= -3\,083\,903\,014\,930\,297\,409\,520\,X^{10} \\
&\qquad -56\,304\,108\,214\,517\,165\,808\,555\,X^9 \\
&\qquad -462\,585\,452\,239\,544\,611\,432\,050\,X^8 \\
&\qquad -2\,252\,164\,328\,580\,686\,632\,342\,200\,X^7 \\
&\qquad -7\,195\,773\,701\,504\,027\,288\,934\,000\,X^6 \\
&\qquad -15\,765\,150\,300\,064\,806\,426\,395\,400\,X^5 \\
&\qquad -23\,985\,912\,338\,346\,757\,629\,798\,000\,X^4 \\
&\qquad -25\,024\,048\,095\,340\,962\,581\,580\,000\,X^3 \\
&\qquad -17\,132\,794\,527\,390\,541\,164\,120\,000\,X^2 \\
&\qquad -6\,951\,124\,470\,928\,045\,161\,550\,000\,X \\
&\qquad -1\,269\,095\,890\,917\,817\,864\,020\,000
\end{aligned}$$

in the variables $X = \frac{s}{t}$ and $Y = \frac{ab}{t^5}$. Studying the Jacobians of these curves in MAGMA [BCP97] we find that both Jacobians only contain two-torsion points. Since the polynomials $F_{5,1}G_{5,1}$ and $F_{5,u_1^8}G_{5,u_1^8}$ only contain one linear factor we conclude as in the case $l = 3$ that both curves only have one rational point. These points are a point at infinity for C_1 corresponding to $t = 0$, and the point $(-\frac{42}{23}, 0)$ on C_2. Note that these rational points correspond to values for s and t for which either $2 \mid c$ or $3 \mid c$ which is impossible by Proposition 4.2.1. This proves that no solution (a, b, c) to Equation (4.2) with $\gcd(a, b) = 1$ and $l = 5$ can exist.

Remark 4.3.2. It is necessary to first look at the factorization in $\mathbb{Q}(v)$, since some of the hyperelliptic curves that come from units we have not considered over K have Jacobians with a rank bound that is not zero. Furthermore these curves also don't have a local obstruction.

Section 4.4

The Frey Curves

In this section we construct Frey curves for our problem. As described in Step 1 of the modular method as mentioned in Section 3.1 these would be elliptic curves that depend on the solution (a, b, c). Furthermore we have a set S outside which the curve only has good or multiplicative reduction and the minimal discriminant is essentially an l-th power.

For our cases we construct such curves using the following fact. Given two non-zero elements B_1 and B_2 of a number field k of which their sum is a square, i.e. $B_1 + B_2 = A^2$, we can look at the elliptic curve

$$E : y^2 = x^3 + 2\,Ax^2 + B_1 x$$

defined over k, for which this model has discriminant $\Delta = 64\,B_1^2 B_2$. Furthermore this curve can only have additive reduction at primes above 2 and primes that divide both B_1 and B_2. This is easily verified by looking at the invariant $c_4 = 16\,(B_1 + 4\,B_2)$, which is coprime to Δ outside such primes.

Note that this recipe will give us a Frey curve if B_1 and B_2 are coprime l-th powers outside the fixed set S. In fact this is the same Frey curve considered for the generalized Fermat equation with signature $(l, l, 2)$.

Now over the field $K = \mathbb{Q}(\sqrt{30})$ we know that we have two factors $g_1(a, b)$ and $g_2(a, b)$ which are coprime l-th powers outside the set of primes above 2, 3 and 5. Furthermore we have that

$$\begin{aligned} \left(\frac{1}{2} - \frac{1}{10}\sqrt{30}\right) g_1(a,b) + \left(\frac{1}{2} + \frac{1}{10}\sqrt{30}\right) g_2(a,b) &= a^2 \\ \frac{1}{20}\sqrt{30}\, g_1(a,b) - \qquad\quad \frac{1}{20}\sqrt{30}\, g_2(a,b) &= b^2, \end{aligned}$$

hence we can apply the construction given above substituting for B_1 and B_2 the right multiples of $g_1(a, b)$ and $g_2(a, b)$. We will construct the Frey curves we will use from the four resulting Frey curves

$$\begin{aligned}
E_1' : y^2 &= x^3 + 2\,ax^2 + \left(\frac{1}{2} - \frac{1}{10}\sqrt{30}\right) g_1(a,b)x,\\
E_1'' : y^2 &= x^3 + 2\,ax^2 + \left(\frac{1}{2} + \frac{1}{10}\sqrt{30}\right) g_2(a,b)x,\\
E_2' : y^2 &= x^3 + 2\,bx^2 + \qquad \frac{1}{20}\sqrt{30}\, g_1(a,b)x, \text{ and}\\
E_2'' : y^2 &= x^3 + 2\,bx^2 - \qquad \frac{1}{20}\sqrt{30}\, g_2(a,b)x.
\end{aligned}$$

Note that E_1'' and E_2'' are Galois conjugates of E_1' and E_2' respectively, so it suffices to consider only one of each pair. We pick E_1'' and E_2' and twist these curves by 30 and 20 respectively to obtain two Frey curves with an integral model

$$\begin{aligned}
E_1 : y^2 &= x^3 + 60\,ax^2 + 30\left(\left(15 + 3\sqrt{30}\right) a^2 + \sqrt{30}\, b^2\right) x, \text{ and}\\
E_2 : y^2 &= x^3 + 40\,bx^2 + 20\left(\sqrt{30}\, a^2 + \left(10 + 2\sqrt{30}\right) b^2\right) x.
\end{aligned}$$

These models have respective discriminants

$$\begin{aligned}
\Delta_1 &= -2^9 \cdot 3^6 \cdot 5^4 \left(5 + \sqrt{30}\right) \cdot g_1(a,b) \cdot g_2(a,b)^2 \text{ and}\\
\Delta_2 &= -2^{13} \cdot 3 \cdot 5^4\, \sqrt{30} \cdot g_1(a,b)^2 \cdot g_2(a,b),
\end{aligned}$$

c_4-invariants

$$\begin{aligned}
c_{4,1} &= -2^5 \cdot 3^2 \cdot 5 \cdot \left(5 + \sqrt{30}\right) \cdot \left(\left(43 - 8\,\sqrt{30}\right) a^2 + \left(6 - \sqrt{30}\right) b^2\right) \text{ and}\\
c_{4,2} &= -2^6 \cdot 3^{-1} \cdot 5 \cdot \sqrt{30} \cdot \left(9a^2 + \left(18 - 5\sqrt{30}\right) b^2\right),
\end{aligned}$$

and j-invariants

$$\begin{aligned}
j_1(a,b) &= \left(11 + 2\,\sqrt{30}\right) \cdot 2^6 \cdot \frac{\left(\left(43 - 8\,\sqrt{30}\right) a^2 + \left(6 - \sqrt{30}\right) b^2\right)^3}{g_1(a,b) \cdot g_2(a,b)^2} \text{ and}\\
j_2(a,b) &= 2^6 \cdot 3^{-3} \cdot \frac{\left(9a^2 + \left(18 - 5\sqrt{30}\right) b^2\right)^3}{g_1(a,b)^2 \cdot g_2(a,b)}.
\end{aligned}$$

The j-invariants of these elliptic curves are not integral. We will prove this here as we will need this later on. In particular this implies that these curves do not have complex multiplication.

Lemma 4.4.1. *The j-invariants $j_1(a,b)$ and $j_2(a,b)$ are not integral. Furthermore there exists a prime of characteristic > 5 such that $j_1(a,b)$ and $j_2(a,b)$ are not integral at that prime.*

Proof. Note that since $\gcd(a,b) = 1$ the left-hand side of Equation (4.2) is the sum of at least two non-zero fourth powers, hence $c > 1$. By Proposition 4.2.1 there must be a prime number $p > 5$ dividing c. This implies that either $g_1(a,b)$ or $g_2(a,b)$ is divisible by a prime above p. It thus suffices to prove that the numerators of $j_1(a,b)$ and $j_2(a,b)$ are not divisible by the same prime.

Note that the factors

$$\left(43 - 8\sqrt{30}\right) a^2 + \left(6 - \sqrt{30}\right) b^2,$$

and

$$9\,a^2 + \left(18 - 5\sqrt{30}\right) b^2,$$

in the numerators of $j_1(a,b)$ and $j_2(a,b)$ are coprime with $g_1(a,b)$ and $g_2(a,b)$ outside primes of characteristic 2, 3 and 5. This can be easily seen by computing the resultants of those polynomials with g_1 and g_2. □

Corollary 4.4.2. *The curves E_1 and E_2 do not have complex multiplication.*

Proof. This follows directly from [Sil94, II, Theorem 6.1] as the j-invariants are not integral. □

Section 4.5

A Hilbert Modular Approach

A natural way of using the Frey curves would be to use the modularity of elliptic curves over real quadratic fields to prove that there are Hilbert modular forms which have the same mod l Galois representation as E_1 or E_2. The level of these newforms will only depend on certain congruence classes of the chosen solution and hence all possible candidates can be explicitly computed. It turns out that the dimension of the corresponding spaces is too high to perform these computations in a reasonable time. Nevertheless we here describe the start of this approach.

We first need to compute the conductor of E_1 and E_2 as the level of the Hilbert modular forms associated to them depends on it.

Proposition 4.5.1. *The conductor of* E_1 *is*

$$\mathcal{N}_1 = \begin{cases} \mathfrak{p}_2^{12}\, \mathfrak{p}_3^2\, \mathfrak{p}_5^2 \operatorname{Rad}_{30}\left(g_1(a,b)g_2(a,b)^2\right) & \textit{if } 2 \mid b \\ \mathfrak{p}_2^{10}\, \mathfrak{p}_3^2\, \mathfrak{p}_5^2 \operatorname{Rad}_{30}\left(g_1(a,b)g_2(a,b)^2\right) & \textit{if } 2 \nmid b, \end{cases}$$

and the conductor of E_2 *is*

$$\mathcal{N}_2 = \mathfrak{p}_2^{14} \mathfrak{p}_5^2 \operatorname{Rad}_{30}\left(g_1(a,b)^2 g_2(a,b)\right),$$

where $\mathfrak{p}_2$*,* $\mathfrak{p}_3$ *and* $\mathfrak{p}_5$ *are the unique primes above 2, 3 and 5 respectively and where* $\operatorname{Rad}_{30}(N)$ *is the product of all primes that divide* N *and do not divide* 30*.*

Proof. This is a computation performed by the implementation [vL21a] of the algorithm discussed in Chapter 1. □

It has been proven by Freitas, Le Hung and Siksek [FLHS15] that elliptic curves over real quadratic fields are modular. In particular the curves E_1 and E_2 are modular. According to [FLHS15] this means there are Hilbert cuspidal eigenforms f_1 and f_2 over $K = \mathbb{Q}(\sqrt{30})$ of parallel weight 2 with rational Hecke eigenvalues such that for all prime numbers p we have

$$\rho_{E_i,p} \cong \rho_{f_i,p} : G_K \to \mathrm{GL}_2(\mathbb{Q}_p), \quad i \in \{1,2\}.$$

Here $\rho_{E_i,p}$ is the p-adic Galois representation of E_i induced by the Galois action on the Tate module $T_p(E)$ and $\rho_{f_i,p}$ is the p-adic Galois representation associated to f_i by Carayol, Blasius, Rogawski, Wiles and Taylor.

Note that the conductor of $\rho_{E_i,p}$ is precisely the conductor of E_i and the conductor of $\rho_{f_i,p}$ is precisely the level of f_i. Therefore we know from Proposition 4.5.1 that f_1 and f_2 have respective levels $\mathcal{N}_1$ and $\mathcal{N}_2$.

The levels $\mathcal{N}_1$ and $\mathcal{N}_2$ are not explicit as they depend on the chosen solution (a,b,c). However if we take $p = l$ and look at the mod l Galois representations $\overline{\rho_{E_i,l}} : G_K \to \mathrm{End}(E[l]) \cong \mathrm{GL}_2(\mathbb{F}_l)$, rather than the p-adic representation, we find that these representations are irreducible. Furthermore they are finite at all primes not dividing 30. This allows us to lower the level to a level only divisible by those primes dividing 30. We prove that the representation is finite here, as irreducibility will later be proven using Theorem 2.11.1 and the fact that these curves are also $\mathbb{Q}$-curves.

Proposition 4.5.2. *The mod* l *Galois representations*

$$\overline{\rho_{E_i,l}} : G_K \to \mathrm{End}(E[l]) \cong \mathrm{GL}_2(\mathbb{F}_l)$$

are finite outside all primes dividing 30*. In particular they are unramified outside all primes dividing* $30\,l$*.*

Proof. Note that for each finite prime $\mathfrak{p}$ of K that does not divide 30 the order of $\mathfrak{p}$ in $\mathcal{N}_1$ or $\mathcal{N}_2$ is at most one. In case it is zero the curve has good reduction at $\mathfrak{p}$, hence the mod l Galois representation is finite at $\mathfrak{p}$. We are left with the case the order is one, in which case $\mathfrak{p}$ must divide $g_1(a,b)$ or $g_2(a,b)$. Since $g_1(a,b)$ and $g_2(a,b)$ are l-th powers outside primes dividing 30, this implies that the order of $\mathfrak{p}$ in the corresponding discriminant Δ_i is a multiple of l. Since the corresponding curve E_i has multiplicative reduction at $\mathfrak{p}$ the mod l Galois representation is finite at $\mathfrak{p}$. This is a standard result that can be easily proved using the Tate curve if $\mathfrak{p} \nmid l$. □

Using the level lowering result found in [FS15, Theorem 7] for $l > 5$ we now find that there must be Hilbert cuspidal eigenforms f_1' and f_2' over K of parallel weight 2 such that $\overline{\rho_{E_i,l}} \cong \overline{\rho_{f_i',\lambda}}$ for $i \in \{1,2\}$, where $\lambda \mid l$ is a prime in the coefficient field of f_i'. Here the levels of these newforms are respectively

$$\begin{aligned}\widetilde{\mathcal{N}_1} &= \begin{cases} \mathfrak{p}_2^{12}\,\mathfrak{p}_3^2\,\mathfrak{p}_5^2 & \text{if } 2 \mid b \\ \mathfrak{p}_2^{10}\,\mathfrak{p}_3^2\,\mathfrak{p}_5^2 & \text{if } 2 \nmid b \end{cases}\\ \widetilde{\mathcal{N}_2} &= \mathfrak{p}_2^{14}\mathfrak{p}_5^2.\end{aligned}$$

The strategy would now be to compute all cuspidal Hecke eigenforms over K of parallel weight 2 and levels $\widetilde{\mathcal{N}_1}$ and $\widetilde{\mathcal{N}_2}$ and prove that none of them can have a mod $\lambda \mid l$ representation isomorphic to the mod l representation of the corresponding E_i. This would prove a contradiction, hence the implicit assumption that a primitive solution (a,b,c) to Equation (4.2) exists would be false as we want.

Remark 4.5.3. Besides working with the curves E_1 and E_2 one might also want to work with curves that are isomorphic over $\overline{\mathbb{Q}}$. In case we do not want to change the field K over which the curves are defined, these isomorphic curves would be twists of our original curves. Note that twisting by an element $\gamma \in K^*$ can only change the conductor of the curve at a prime $\mathfrak{p}$ if the corresponding field extension $K(\sqrt{\gamma})$ is ramified at $\mathfrak{p}$. The values $\gamma \in K^*$ for which $K(\sqrt{\gamma})$ is unramified at a fixed prime $\mathfrak{p}$ form a subgroup $H_{\mathfrak{p}} \subseteq K^*$ of which the quotient $K^*/H_{\mathfrak{p}}$ is finite. Limiting ourselves to the primes dividing $\widetilde{\mathcal{N}_1}$ and $\widetilde{\mathcal{N}_2}$ we thus only have a finite computation to see if these levels can be made any smaller.

It turns out that by twisting we can get the lowest level

$$\widetilde{\mathcal{N}_1} = \begin{cases} \mathfrak{p}_2^{12}\,\mathfrak{p}_3^2\,\mathfrak{p}_5^2 & \text{if } 2 \mid b \\ \mathfrak{p}_2^{4}\,\mathfrak{p}_3^2\,\mathfrak{p}_5^2 & \text{if } 2 \nmid b \text{ and } a \equiv 1 \pmod 4 \\ \mathfrak{p}_3^2\,\mathfrak{p}_5^2 & \text{if } 2 \nmid b \text{ and } a \equiv 3 \pmod 4, \end{cases}$$

in case we twist E_1 with $6 + \sqrt{30}$. If we twist the curve E_1 by $-6 - \sqrt{30}$ we get the same level, but with the latter two conditions interchanged.

Using Magma we quickly find that the dimension of some of the sought spaces of newforms would be way too large to compute in. For example using the levels of the untwisted curves the dimension of the smallest space is 206 720, which is way beyond the largest computational examples done in the literature. We can only do better in case $2 \nmid b$ where the twisted curve in the remark gives us a space of dimension 542 for the newforms of level $\mathfrak{p}_3^2\,\mathfrak{p}_5^2$. A lower level for the case $2 \mid b$ is lacking though, making this insufficient to prove Theorem 4.1.1 completely.

Section 4.6

$\mathbb{Q}$-curves

In this section we use the modularity of $\mathbb{Q}$-curves to prove the non-existence of solutions. This technique has been applied to other Diophantine equations in works such as [DF14], [DU09], [BC12], [Che10], [Che12], [BCDY14], and [Ell04]. The approach here is similar to the one in the mentioned articles, leaning heavily on the work by Quer [Que00]. It differs in some crucial points, where we will give an algorithmic approach that works in a general context.

Look back at our original curve

$$E : y^2 = x^3 + 2Ax^2 + B_1 x,$$

where $A^2 = B_1 + B_2$. Note that by construction this curve has a 2-torsion point and hence an obvious 2-isogeny defined over $\mathbb{Q}$. From [Sil09, III, example 4.5] we deduce that the image of this 2-isogeny is

$$\tilde{E} : y^2 = x^3 - 4Ax^2 + \left(4A^2 - 4B_1\right) x = x^3 - 4Ax^2 + 4B_2 x,$$

which is a twist by -2 of the complementary curve

$$E' : y^2 = x^3 + 2Ax^2 + B_2 x.$$

In particular such a curve is thus 2-isogenous over a field extension containing $\sqrt{-2}$ to the curve in which the roles of B_1 and B_2 are swapped.

Note that for the Frey curves E_1 and E_2 we constructed, the chosen B_1 and B_2 were Galois conjugates of one another, whilst A was rational. This implies that the curves E_1 and E_2 are 2-isogenous to their Galois conjugates over $K(\sqrt{-2})$. This means that E_1 and E_2 are $\mathbb{Q}$-curves and we can apply the theory discussed in Section 2 to these curves.

Remark 4.6.1. Note that in Section 2 we use the standing assumption that all $\mathbb{Q}$-curves are without complex multiplication. This forms no problem as by Corollary 4.4.2 the curves E_1 and E_2 do not have complex multiplication.

Subsection 4.6.1

Basic invariants

We explicitly compute many of the quantities associated to $\mathbb{Q}$-curves for the curves E_1 and E_2 using the implementation [vL21a] of the material in Section 2.

Proposition 4.6.2. *For both E_1 and E_2 we have the same data listed below.*

- *The degree map $d : G_{\mathbb{Q}} \to \mathbb{Q}^*$ given by*

$$d(\sigma) = \begin{cases} 1 & \text{if } \sigma \in G_K \\ 2 & \text{if } \sigma \notin G_K. \end{cases}$$

- *The 2-cocycle $c : G_{\mathbb{Q}}^2 \to \mathbb{Q}^*$ given by*

$$c(\sigma,\tau) = \begin{cases} 1 & \text{if } \sigma \in G_{K(\sqrt{-2})} \text{ or } \tau \in G_K \\ -1 & \text{if } \tau \notin G_K,\ {}^{\sigma}\sqrt{-2} = -\sqrt{-2} \text{ and } {}^{\sigma}\sqrt{30} = \sqrt{30}, \\ -2 & \text{if } \tau \notin G_K,\ {}^{\sigma}\sqrt{-2} = \sqrt{-2} \text{ and } {}^{\sigma}\sqrt{30} = -\sqrt{30}, \\ 2 & \text{if } \tau \notin G_K,\ {}^{\sigma}\sqrt{-2} = -\sqrt{-2} \text{ and } {}^{\sigma}\sqrt{30} = -\sqrt{30}, \end{cases}$$

- *The degree field $K_d = K = \mathbb{Q}(\sqrt{30})$ over which the curves are defined.*

- *The field $K(\sqrt{-2}) = K_d(\sqrt{-2})$ over which the curves are completely defined.*

- *A dual basis $\{(30, 2)\}$.*

- *A splitting character $\varepsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$, that as a Dirichlet character is one of the characters of conductor 15 and order 4, with corresponding fixed field $K_\varepsilon = \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$ of degree 4.*
- *A splitting field $K_\beta = K(\zeta_{15} + \zeta_{15}^{-1}) = \mathbb{Q}(\sqrt{6}, \zeta_{15} + \zeta_{15}^{-1})$ of degree 8.*
- *A decomposition field $K_{dec} = \mathbb{Q}(\sqrt{-2}, \sqrt{-3}, \zeta_{15} + \zeta_{15}^{-1})$ of degree 16.*

Proof. All this data can be computed from the isogenies $\phi_\sigma : {}^\sigma E_i \to E_i$, which we can take to be the identity if $\sigma \in G_K$ and the 2-isogeny over $K(\sqrt{-2})$ described before otherwise. Note that the latter can be explicitly described using the formula in [Sil09, III, example 4.5] and the map scaling with $\sqrt{-2}$. In fact we can let the implementation [vL21a] guess these isogenies by giving the information that it should contain isogenies of degree 2. □

Remark 4.6.3. Note that the field $K(\sqrt{-2})$ is a minimal field over which a curve isogenous to E_1 or E_2 can be completely defined. This is easily verified through Corollary 3.3 in [Que00], as it excludes the case that an isogenous curve can be defined over the field $K_d = K$ which is the only possible smaller field. For this one checks that

$$(30, 2) \neq 1 \quad \text{and} \quad (30, 2) \neq (-1, 30),$$

inside $\mathrm{Br}_2(\mathbb{Q})$, which can be verified by checking the corresponding Hilbert symbols at 5.

Subsection 4.6.2

A decomposable twist

We now apply the theory from Section 2.5 to E_1 and E_2. In particular we use Proposition 2.5.3 to find a $\gamma \in K_{\mathrm{dec}}^*$ such that $[c_\beta] = [c_{E_i}]$ over $K_{\mathrm{dec}}(\sqrt{\gamma})$. By Corollary 2.7.8 we know that twisting E_i by this γ gives a $\mathbb{Q}$-curve $E_{i,\gamma}$ for which $c_\beta = c_{E_{i,\gamma}}$ over K_{dec}. Since K_{dec} has class number 1 Proposition 2.5.5 implies we can search for an $\alpha : G_{\mathbb{Q}}^{K_{\mathrm{dec}}} \to \mathcal{O}_{K_{\mathrm{dec}}}^*$. The code [vL21a] does this to find suitable twists of E_1 and E_2. As remarked above Example 2.5.4 we can change γ by a square or a rational number, which we do to find one for which the twist parameter has a smaller minimal polynomial. In fact we find that for $\gamma \in K_{\mathrm{dec}}$ any root of the polynomial

$$x^8 - 40x^7 - 550x^6 - 1840x^5 - 285x^4 + 3600x^3 - 1950x^2 + 200x + 25,$$

the twists $E_{1,\gamma}$ and $E_{2,\gamma}$ of E_1 and E_2 by γ decompose as intended. Note that this polynomial is not irreducible over K, but still any choice of root will suffice.

Note that by twisting the curves, the corresponding isogenies that define the $\mathbb{Q}$-curve structure should change accordingly. The way this change works is explicitly stated in Proposition 2.7.6. The code [vL21a] computes these new isogenies automatically. As these new isogenies are defined over $\mathbb{Q}(\gamma) = K_\beta$, the twisted curves $E_{1,\gamma}$ and $E_{2,\gamma}$ are completely defined over K_β. Since the splitting maps for ξ_{E_i} are splitting maps for $c_{E_{i,\gamma}}$, this means K_β is a decomposition field for $E_{1,\gamma}$ and $E_{2,\gamma}$.

Applying Proposition 2.9.4 with the facts above we get the following proposition.

Proposition 4.6.4. *For each $i \in \{1, 2\}$ the abelian variety $\operatorname{Res}_{\mathbb{Q}}^{K_\beta} E_{i,\gamma}$ is $\mathbb{Q}$-isogenous to a product of $\mathbb{Q}$-simple, mutually non $\mathbb{Q}$-isogenous abelian varieties of GL_2-type.*

Using the theory from Section 2.6 we can determine all Galois orbits of splitting maps for $c_{E_{i,\gamma}}$ over K_β for $E_{1,\gamma}$ and $E_{2,\gamma}$ allowing us to prove the following

Theorem 4.6.5. *Let $i \in \{1, 2\}$. We have that*

$$\operatorname{Res}_{\mathbb{Q}}^{K_\beta} E_{i,\gamma} \textit{ is } \mathbb{Q}\textit{-isogenous to } A_{i,1} \times A_{i,2},$$

where

- *each $A_{i,j}$ is a $\mathbb{Q}$-simple abelian variety of GL_2-type over $\mathbb{Q}$ of dimension 4 with $\operatorname{End} A_{i,j} \otimes \mathbb{Q} \cong L_\beta = \mathbb{Q}(\zeta_8)$, and*
- *the varieties $A_{i,1}$ and $A_{i,2}$ are not isogenous over $\mathbb{Q}$.*

Proof. The code [vL21a] easily allows us to compute one splitting map for $c_{E_{i,\gamma}}$ over K_β per Galois orbit, telling us there is only two. Furthermore we can use the implementation of Proposition 2.7.10 to compute that the image fields of both of these splitting maps are $L_\beta = \mathbb{Q}(\zeta_8)$. Since $A_{i,1}$ and $A_{i,2}$ are $\mathbb{Q}$-simple abelian varieties of GL_2-type this also determines their dimension as by Theorem 2.2.1. □

Subsection 4.6.3

Modularity of $\mathbb{Q}$-curves

We now apply the theory from Sections 2.8 and 2.9 to our curves E_1 and E_2 to obtain the levels and character of associated newforms.

Theorem 4.6.6. *For each $i \in \{1, 2\}$ there exists a factor $A_{i,j}$ such that $A_{i,j}$ is $\mathbb{Q}$-isogenous to the abelian variety A_f of a newform*

$$\begin{aligned} &f \in S_2\left(\Gamma_1\left(2^9 \cdot 3^2 \cdot 5 \operatorname{Rad}_{30} c\right), \varepsilon\right) && \text{if } i = 1,\ b \text{ even,} \\ &f \in S_2\left(\Gamma_1\left(2^8 \cdot 3^2 \cdot 5 \operatorname{Rad}_{30} c\right), \varepsilon\right) && \text{if } i = 1,\ b \text{ odd,} \\ &f \in S_2\left(\Gamma_1\left(2^{10} \cdot 3 \cdot 5 \operatorname{Rad}_{30} c\right), \varepsilon\right) && \text{if } i = 2. \end{aligned}$$

Here $\operatorname{Rad}_{30} c$ *is the product of all primes $p \mid c$ with $p \nmid 30$ and ε is one of the two Dirichlet characters of conductor* 15 *and order* 4 *for which the choice does not matter.*

Proof. As discussed in the text above Proposition 2.8.5 each factor $A_{i,j}$ is isogenous to some abelian variety A_f of some newform f. The character of these newforms is by Corollary 2.8.6 equal to the inverse of a corresponding splitting character. The code [vL21a] computes such a splitting character for each $A_{i,j}$, which are all one of the two characters mentioned. Since the mentioned characters are Galois conjugates of each other, and since Galois conjugates of splitting maps correspond to the same factor $A_{i,j}$ the choice indeed does not matter.

For the levels of these newforms we first compute the conductors of the curves $E_{i,\gamma}$ over K_β. As explained in the proof of Proposition 4.5.1 the framework [vL21a] can calculate these conductors to be

$$\mathcal{N}_i = \begin{cases} \left(2^6 \cdot 3 \operatorname{Rad}_{30} c\right) & \text{if } i = 1 \text{ and } 2 \mid b \\ \left(2^5 \cdot 3 \operatorname{Rad}_{30} c\right) & \text{if } i = 1 \text{ and } 2 \nmid b \\ \left(2^7 \operatorname{Rad}_{30} c\right) & \text{if } i = 2, \end{cases}$$

where $\mathcal{N}_i$ is the conductor of $E_{i,\gamma}$. From this we can compute using Proposition 2.9.2 that

$$N_i = \begin{cases} 2^{72} \cdot 3^{16} \cdot 5^{12} \left(\operatorname{Rad}_{30} c\right)^8 & \text{if } i = 1 \text{ and } 2 \mid b \\ 2^{64} \cdot 3^{16} \cdot 5^{12} \left(\operatorname{Rad}_{30} c\right)^8 & \text{if } i = 1 \text{ and } 2 \nmid b \\ 2^{80} \cdot 3^{8} \cdot 5^{12} \left(\operatorname{Rad}_{30} c\right)^8 & \text{if } i = 2, \end{cases}$$

where N_i is the conductor of $\operatorname{Res}_{\mathbb{Q}}^{K_\beta} E_{i,\gamma}$.

For each i the newforms $f_{i,1}$ and $f_{i,2}$ corresponding to $A_{i,1}$ and $A_{i,2}$ are twists of one another by the character $\chi = \varepsilon_8 \varepsilon_5$ and its inverse. Here ε_8 is the character of conductor 8 with $\varepsilon_8(-1) = -1$ and ε_5 is a character with conductor 5 and order 4. We can thus apply Theorem 2.9.8 by first twisting with ε_8 and then with ε_5 or ε_5^{-1}. We immediately see that the levels should be the same for all primes $p \neq 2, 5$.

Note that for the order of 2 in the levels $N_{i,1}$ and $N_{i,2}$ of $f_{i,1}$ and $f_{i,2}$ respectively we know that

$$4 \operatorname{ord}_2 N_{i,1} + 4 \operatorname{ord}_2 N_{i,2} \geq 64,$$

by Equation (2.7), hence the order of 2 in one of the two is at least 8. Since all splitting characters and twist characters can be defined modulo 120 the β and γ in Theorem 2.9.8 can never exceed $\operatorname{ord}_2 120 = 3$. This implies that we are in case 3(a) and the order of 2 in both levels must be the same.

Now for the order of 5 we have

$$4 \operatorname{ord}_5 N_{i,1} + 4 \operatorname{ord}_5 N_{i,2} = 12.$$

Since the characters of the corresponding newforms have a conductor divisible by 5 at least one factor 5 has to appear in both levels. This implies that one of the levels has a single factor 5 and the other has a factor 5^2. By picking the first we get the result as stated in this theorem. □

Subsection 4.6.4

Level lowering

The levels appearing in Theorem 4.6.6 still depend on the solution (a, b, c) of Equation (4.2). To get rid of the additional primes we will need to look at the mod l Galois representations and use some level lowering results.

To apply level lowering results we first need to know that the mod l Galois representations of E_1 and E_2 are absolutely irreducible and unramified at the primes that should be eliminated from the level.

Theorem 4.6.7. *The mod λ Galois representation*

$$\overline{\rho_{A_{i,j},\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$$

is absolutely irreducible for any $i, j \in \{1, 2\}$ and prime λ of L_β of characateristic $l > 5$. Furthermore we have that the mod l Galois representation

$$\overline{\rho_{E_i,l}} : G_K \to \operatorname{End} E_i[l] \cong \mathrm{GL}_2(\mathbb{F}_l)$$

is irreducible for any $i = 1, 2$ and $l > 5$.

Proof. First note that the Galois representation $\overline{\rho_{A_{i,j},\lambda}}$ is isomorphic to the representation associated with the splitting map for c_{E_i} corresponding to $A_{i,j}$. Therefore we can apply Theorem 2.11.1 to prove this result. Note that the proof of Theorem 2.11.1 in fact uses that the Galois representation $\overline{\rho_{E_i,l}}$ is reducible as an intermediate step. Therefore if we can show that neither

- $l = 7$ and $j(E_i) = -3375, \frac{-10\,529 \pm 16\,471\sqrt{-7}}{8}, \frac{56\,437\,681 \pm 1\,875\,341\sqrt{-7}}{32\,768}$;
- $l = 13$ and $j(E_i) = 3\,448\,440\,000 \pm 956\,448\,000\sqrt{13}$; or
- $l = 11$ or $l > 13$, and E_i has potential good reduction at all primes of characteristic > 3.

then we have proven that both $\overline{\rho_{A_{i,j},\lambda}}$ is absolutely irreducible and that $\overline{\rho_{E_i,l}}$ is irreducible.

Note that the cases with $l = 7$ and $l = 13$ are impossible as we have seen that the minimal field over which the isogeny class of E_i can be defined is K, so $j(E_i) \in K \setminus \mathbb{Q}$. The remaining case would imply that the j-invariant is integral at all primes of characteristic $p > 3$ ([Sil09, VII.5.5]) which contradicts Lemma 4.4.1. □

Proposition 4.6.8. *Let f be a newform as in Theorem 4.6.6 and $l > 5$ be a prime number, then for each prime $\lambda \mid l$ in the coefficient field of f the mod λ Galois representation $\overline{\rho_{f,\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ is finite outside primes dividing* 30. *In particular it is unramified outside primes dividing* $30\,l$.

Proof. Note that $\overline{\rho_{f,\lambda}}$ is isomorphic to a Galois representation from a splitting map for c_{E_i}, so by what was mentioned above Theorem 2.8.3 we know that

$$\overline{\rho_{f,\lambda}}|_{G_{K_\beta}} \sim \overline{\rho_{E_i,l}}|_{G_{K_\beta}}.$$

Since the discriminant of K_β is only divisible by the prime numbers 2, 3 and 5, we find that the ramification subgroup I_p of a prime number $p \nmid 30$ is contained in G_{K_β}. Note that $\overline{\rho_{f,\lambda}}$ being finite at $p \nmid 30$ only depends on $\overline{\rho_{f,\lambda}}|_{I_p} \sim \overline{\rho_{E_i,l}}|_{I_p}$, for which this was already proven in Proposition 4.5.2. □

We can now use level lowering results proven by Diamond in [Dia97] based on work by Ribet [Rib90] to lower the level to something independent of the chosen solution (a, b, c).

Theorem 4.6.9. *For each elliptic curve $E_{i,\gamma}$ and prime number $l > 5$ there exists a factor $A_{i,j}$ as in Proposition 4.6.6 such that for each prime ideal $\lambda \mid l$ of the field $\operatorname{End} A_{i,j} \otimes \mathbb{Q} = \mathbb{Q}(\zeta_8)$ we have $\overline{\rho_{A_{i,j},\lambda}} \sim \overline{\rho_{g,\lambda'}}$ for some prime ideal $\lambda' \mid l$ in the appropriate field and a newform g satisfying*

$$\begin{aligned} g &\in S_2\left(\Gamma_1\left(23040\right), \varepsilon\right) && \textit{if } i = 1,\ b \textit{ even,} \\ g &\in S_2\left(\Gamma_1\left(11520\right), \varepsilon\right) && \textit{if } i = 1,\ b \textit{ odd,} \\ g &\in S_2\left(\Gamma_1\left(15360\right), \varepsilon\right) && \textit{if } i = 2. \end{aligned}$$

Here ε is one of the two Dirichlet characters of conductor 15 and order 4. The choice does not matter.

Proof. We start by picking some f as in Theorem 4.6.6. Let $A_{i,j}$ be the corresponding factor. We already have that that $\overline{\rho_{A_{i,j},\lambda}} \sim \overline{\rho_{f,\lambda}}$ for an arbitrary prime $\lambda \mid l$. We will show that we can find a newform of the level as in this theorem which still has an isomorphic Galois representation.

Note that $\overline{\rho_{f,\lambda}}$ is irreducible by Theorem 4.6.7 and odd as it is the Galois representation of a newform.

We apply Theorem 4.1 in [Dia97], which tells us we can find a newform g of weight 2 with an isomorphic Galois representation $\overline{\rho_{g,\lambda}}$. The level of g is the level of f divided by all prime numbers p that appear only once in the level, do not divide l or the conductor of the character of f, and at which the Galois representation is unramified. The levels and the explicit character in Proposition 4.6.6 and the result from Proposition 4.6.8 tell us that all those prime numbers p not dividing $30l$ satisfy these conditions and can thus be removed from the level.

Lastly we use Theorem 2.1 in [Rib94] which shows that the same result holds for a newform g of weight 2 and a level in which all powers of l are also removed. The weight remains 2 as the Galois representation is finite at l by Proposition 4.6.8 and the fact that $l > 5$. The resulting level is the one given in this theorem. □

Remark 4.6.10. Note that the newforms in Theorem 4.6.9 are in fact those that have the Serre level and weight of the corresponding irreducible representation $\overline{\rho_{A_{i,j},\lambda}}$. The result of this theorem would therefore also directly follow from the Serre conjectures.

Subsection 4.6.5

Newform elimination

The strategy to complete the proof of Theorem 4.1.1 is to show that the conclusion of Theorem 4.6.9 will give a contradiction, implying that the implicit assumption of a solution (a, b, c) to Equation (4.2) existing with $\gcd(a, b) = 1$ and $l > 5$ must be false. We derive this contradiction by comparing traces of Frobenius of $\overline{\rho_{E_{i,\gamma},l}} : G_{K_\beta} \to \mathrm{GL}_2(\mathbb{F}_l)$ and $\overline{\rho_{g,\lambda'}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ for g in one of the given spaces. Note that since both representations are defined over different Galois groups, we need a small result.

Lemma 4.6.11. *We have that $\overline{\rho_{g,\lambda'}}\,(\mathrm{Frob}_{\mathfrak{p}}) \sim \overline{\rho_{g,\lambda'}}\left(\mathrm{Frob}_p^d\right)$ for any prime $\mathfrak{p}$ of K_β of characteristic $p \nmid 30\,l$ and a residue field of degree d. Here $\sim$ denotes the two are conjugates.*

Proof. Let $\mathfrak{p}$ be an arbitrary prime of K_β of characteristic $p \nmid 30l$. Note that a Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in G_{K_{\mathrm{dec},\mathfrak{p}}}$ maps to the homomorphism $x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}}$ inside $G_{\mathbb{F}_p}$, just as does Frob_p^d for a Frobenius element $\mathrm{Frob}_p \in G_{\mathbb{Q}_p}$. This means their difference lies in the ramification subgroup of $G_{\mathbb{Q}_p}$. Since $\overline{\rho_{g,\lambda'}}$ is unramified at p by Proposition 4.6.8 we find that $\overline{\rho_{g,\lambda'}}\,(\mathrm{Frob}_{\mathfrak{p}}) \sim \overline{\rho_{g,\lambda'}}\left(\mathrm{Frob}_p^d\right)$. □

Remark 4.6.12. The results from Section 2.10 were written later than the article [vL21b] this chapter is based on. Using the results from Section 2.10 one could avoid Lemma 4.6.11 by working with the Galois representation of a splitting map for $c_{E_{i,\gamma}}$ instead.

Now the rest of the proof becomes a computation.

First we compute the newforms in the spaces mentioned in Proposition 4.6.9. These computations take quite some time, especially the computation for the newforms of level 15360, which took approximately 5 days of computation time in MAGMA [BCP97] using a desktop computer (Intel core i5-6600 CPU, 3.3 GHz). For comparison computing the space of newforms of level 11520 took just under 8 minutes on the same machine and the space of newforms of level 23040 took just over an hour. For this reason all newforms were pre-computed and then stored by saving the Fourier coefficients for all primes smaller than 500, as this data is sufficient to compute the sought traces of Frobenius for those primes.

Remark 4.6.13. The computations described before were done on Magma version 2.24. Magma version 2.25 introduced a significant speedup in the computation of newforms. The mentioned spaces of newforms can now be computed in under 7 hours on a machine with similar specifications.

The table below gives some general data about each space of newforms. It lists from left to right the level of the newforms, the dimension of the corresponding newspace, the number of Galois conjugacy classes of newforms, the possible sizes of the Galois conjugacy classes, and the total number of newforms among all conjugacy classes. Note that the last is always twice the dimension mentioned before, since the Galois conjugacy class of the character consists of two characters.

Table 4.1: Data of the computed newforms

level	dim.	# conj. classes	size of conj. classes	# newforms
11520	192	30	$4, 8, 16, 24, 32, 48$	384
23040	384	20	$8, 40, 48$	768
15360	752	14	$16, 64, 80, 96, 128, 176, 192$	1504

We apply the procedure discussed in Remark 3.1.1 for all primes $\mathfrak{p}$ of K_β of characteristic p with $5 < p < 30$. Note that on the elliptic curve side we are using the Galois representation $\overline{\rho_{E_{i,\gamma},l}}$ instead. A standard result shows us that

$$a_\mathfrak{p}(E_{i,\gamma}) = \begin{cases} \#\mathbb{F}_\mathfrak{p} + 1 - \#E_{i,\gamma}(\mathbb{F}_\mathfrak{p}) \\ \#\mathbb{F}_\mathfrak{p} + 1 \\ -\#\mathbb{F}_\mathfrak{p} - 1, \end{cases}$$

where the cases correspond to $E_{i,\gamma}$ having good, split multiplicative and non-split multiplicative reduction at $\mathfrak{p}$ respectively. The possible $a_\mathfrak{p}(E_{i,\gamma})$ can be computed with the framework [vL21a] using the method `trace_of_frobenius`. Note that as we use the Galois representation $\overline{\rho_{E_{i,\gamma}}}$ rather than a Galois representation of a specific splitting map, we have to use a `FreyCurve` rather than a `FreyQcurve` for $E_{i,\gamma}$. This gives us the set $A_\mathfrak{p}(E_{i,\gamma})$.

To compute the values $a_\mathfrak{p}(g)$ for each newform g found before, we need to compute $\operatorname{Tr}\overline{\rho_{g,\lambda'}}(\mathrm{Frob}_\mathfrak{p})$, where $\lambda' \mid l$ is the prime ideal corresponding to a fixed $\lambda \mid l$ in Proposition 4.6.9. By Lemma 4.6.11 these traces are the same as $\operatorname{Tr}\overline{\rho_{g,\lambda'}}(\mathrm{Frob}_p^d)$, where p is the characteristic of $\mathfrak{p}$ and $d = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$. This trace can be computed from $\operatorname{Tr}\overline{\rho_{g,\lambda'}}(\mathrm{Frob}_p)$ and $\det\overline{\rho_{g,\lambda'}}(\mathrm{Frob}_p)$ by the fact that for a 2-by-2 matrix A the value of $\operatorname{Tr} A^d$ can be expressed as a polynomial in $\operatorname{Tr} A$ and $\det A$. Since p does not divide the level we have

$$\begin{aligned} \operatorname{Tr} \overline{\rho_{g,\lambda'}}(\mathrm{Frob}_p) &= a_p(g) \pmod{\lambda'} \\ \det \overline{\rho_{g,\lambda'}}(\mathrm{Frob}_p) &= \varepsilon(p) p \pmod{\lambda'}, \end{aligned}$$

where $a_p(g)$ is the p-th coefficient in the Fourier expansion of g and ε is the character of g. Note that the right hand side for both these values is the reduction of an algebraic integer that is independent of λ'. Using these algebraic integers in the formula for $\operatorname{Tr} A^d$ we get the algebraic integer $a_{\mathfrak{p}}(g)$ from Remark 3.1.1. As mentioned in Section 3.2 these integers can automatically be computed in the framework [vL21a] by passing d as the argument `power` to `trace_of_frobenius`.

We use the method `eliminate_by_traces` explained in Section 3.3.1 on the curves $E_{1,\gamma}$ and $E_{2,\gamma}$ with their respective newforms. If we pass these curves as `FreyCurve`s the framework [vL21a] will automatically use the correct powers mentioned in the previous paragraph. Performing this elimination on all primes $\mathfrak{p} \nmid 30$ of characteristic $p < 30$ leaves us with 14 newforms of level 11520, 12 newforms of level 23040 and 7 newforms of level 15360, for which not all primes $l > 5$ could be eliminated.

The last step is to use both Frey curves simultaneously. This is known as a multi-Frey approach and was also used in [DF14], [BC12] and [Che12]. Instead of computing the sets $A_{\mathfrak{p}}(E_{1,\gamma})$ and $A_{\mathfrak{p}}(E_{2,\gamma})$ independently we now compute one set $A_{\mathfrak{p}} \subset \mathbb{Z}^2$ as discussed in Section 3.3.1. When performing this elimination on all primes $\mathfrak{p} \nmid 30$ of characteristic $p < 50$ we see all primes $l > 5$ can be eliminated. If a solution (a, b, c) with $\gcd(a, b) = 1$ to Equation (4.2) would exist for $l > 5$, then this would contradict Theorem 4.6.9. Therefore no such solution to Equation (4.2) can exist, proving Theorem 4.1.1 for $l > 5$ prime.

Remark 4.6.14. Most prime exponents $l > 5$ can already be eliminated by only looking at the curve $E_{2,\gamma}$ at more primes than considered here and using more restrictions on a and b. However it seems impossible to eliminate the case $l = 7$ in this way, hence the use of the multi-Frey curve approach.

Chapter 5

Explicitly determining perfect powers in several elliptic divisibility sequences

This chapter is joint work with Sander Dahmen. A modified version of it will be submitted for publication. The main contributions of the author of this dissertation include Subsection 5.2.1, Section 5.3, Section 5.4, and the computations done with the framework [vL21a] for the examples in Section 5.5. All code files mentioned in this chapter can be found in the `EDS` example directory.

Section 5.1

Introduction

Given a non-singular Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5.1}$$

with integral coefficients and a non-torsion point $P \in E(\mathbb{Q})$, one can use the group law on E to write

$$x(mP) = \frac{A_m}{B_m^2} \tag{5.2}$$

for any positive integer m, with $B_m > 0$ and $\gcd(A_m, B_m) = 1$. The sequence $(B_m)_{m\in\mathbb{Z}_{>0}}$ is known as an elliptic divisibility sequence. In particular, as is well known, for all natural numbers n, m it satisfies

$$n|m \Rightarrow B_n|B_m. \tag{5.3}$$

Some finiteness results have been achieved for perfect powers in elliptic divisibility sequences; see e.g. [ERS07] and [Rey12]. In particular, if E is a Mordell curve (so with j-invariant $j(E) = 0$) and $B_1 > 1$, then there are finitely many perfect powers in (B_m); see [Rey12, Theorem 1.2]. The method of proof includes a (regular) modular approach using elliptic curves over $\mathbb{Q}$.

Similarly, if E has j-invariant 1728 and $B_1 > 1$, then Dahmen and Reynolds study (in a preprint) again the finiteness of perfect powers in the corresponding sequence. In this case, a Frey $\mathbb{Q}$-curve is associated to the problem. Its field of definition is sometimes $\mathbb{Q}$, but 'generically' it is a quadratic number field. We do not strictly depend on their results, but our Frey $\mathbb{Q}$-curve construction is similar.

In the remainder of this chapter we focus on the $j = 1728$ case. The aim is to show that for many choices of E, P we can explicitly find a finite set S of primes such for all primes l not in S the associated elliptic divisibility sequence contains no l-th powers. We will work out several examples illustrating the power of the method. Our main Diophantine results are given in Section 5.5, namely Theorem 5.5.2, Theorem 5.5.6, as well as the results mentioned in Subsection 5.5.3. Most notably are cases (ii), (iii), and (viii) in Table 5.3 as no alternative approaches for these seem to be available in the literature. In principle, we believe that many more examples could be computed along similar lines of our approach.

In order to compute the levels of newforms associated with a Frey $\mathbb{Q}$-curve E, one needs to compute a particular twist of the curve. Given an abelian number field K over which E is completely defined and for which a splitting map factors over $G_{\mathbb{Q}}^K$, this twist can be computed from a map $\alpha : G_{\mathbb{Q}}^K \to K^*$ whose coboundary is a 2-cocycle $\left(G_{\mathbb{Q}}^K\right)^2 \to \{\pm 1\}$ associated with the Frey $\mathbb{Q}$-curve. In the literature a map $\alpha : G_{\mathbb{Q}}^K \to \mathcal{O}_K^*$ often suffices, but we shall show that this is not the case in the example corresponding to Theorem 5.5.6. We will demonstrate that we can instead take $\alpha : G_{\mathbb{Q}}^K \to \mathcal{O}_{K,S}^*$, where $\mathcal{O}_{K,S}^*$ is the ring of S-units for a non-empty finite set S.

Section 5.2

Associating a $\mathbb{Q}$-curve

Let D be a nonzero integer not divisible by a fourth power of a prime and consider the Weierstrass equation

$$E_D : y^2 = x^3 + Dx. \tag{5.4}$$

Note that $T = (0,0) \in E_D(\mathbb{Q})$ is a 2-torsion point. For any point $P \in E_D(\mathbb{Q})$ with $P \neq \mathcal{O}, T$ take $\hat{P} = T - P \in E_D(\mathbb{Q}) \setminus \{\mathcal{O}, T\}$. Since $P + \hat{P} + T = \mathcal{O}$, all of these points are on the line $y = \frac{y_P}{x_P}x$. Substituting this in the equation of E_D and comparing coefficients of x^2 tells us that

$$x_P + x_{\hat{P}} + 0 = \left(\frac{y_P}{x_P}\right)^2 = \frac{x_P^3 + Dx_P}{x_P^2} = x_P + \frac{D}{x_P},$$

hence $x_P x_{\hat{P}} = D$. If we write in lowest terms we get

$$P = \left(\frac{A}{B^2}, \frac{C}{B^3}\right) \text{ and } \hat{P} = \left(\frac{\hat{A}}{\hat{B}^2}, \frac{\hat{C}}{\hat{B}^3}\right),$$

with $A, B, C, \hat{A}, \hat{B}, \hat{C} \in \mathbb{Z}$, $\gcd(AC, B) = \gcd(\hat{A}\hat{C}, \hat{B}) = 1$ and $B, \hat{B} > 0$. This implies that $A\hat{A} = DB^2\hat{B}^2$. Since $\gcd(A, B) = \gcd(\hat{A}, \hat{B}) = 1$ there are $a, \hat{a} \in \mathbb{Z}$ such that $A = a\hat{B}^2$ and $\hat{A} = \hat{a}B^2$. Note that $D = a\hat{a}$, hence one can compute a and thus $\hat{a} = \frac{D}{a}$ easily from the fact that $\gcd(A, D) = |a| \gcd(\hat{B}^2, \hat{a}) = |a|$, noting that the sign of a must be the same as the sign of A. Now substituting the coordinates of P into the equation of E_D and multiplying by B^6 tells us that

$$C^2 = a^3\hat{B}^6 + a^2\hat{a}B^4\hat{B}^2.$$

Therefore $C = a\hat{B}w$ for some $w \in \mathbb{Z}$ and dividing the equation above by $a^2\hat{B}^2$ gives

$$w^2 = a\hat{B}^4 + \hat{a}B^4. \tag{5.5}$$

Note that in this equation B and $\hat{B}$ are coprime as $\gcd(B, \hat{B}) \mid \gcd(B, A) = 1$. Furthermore, substituting the coordinates of $\hat{P}$ into the equation for E_D gives rise to the same diophantine equation as $\hat{C} = \hat{B}^3 \frac{y_P}{x_P} x_{\hat{P}} = \hat{a}Bw$. For future reference, we note that actually $B, \hat{B}$, and w are pairwise coprime since also $\gcd(w, B) | \gcd(C, B) = 1$ and $\gcd(w, \hat{B}) | \gcd(\hat{C}, \hat{B}) = 1$.

The condition that B is an l-th power with $l > 1$ now leads to a so-called generalized Fermat equation of signature $(2, 4, 4l)$, hence also of signature $(2, 4, l)$. To the Fermat equation $y^2 - dx^4 = ez^l$ (for given nonzero integers d, e), we associate (basically as in [DU09]) the Frey $\mathbb{Q}$-curve

$$E_{d,x,y} : Y^2 = X^3 + 4\sqrt{d}xX^2 + 2(dx^2 + \sqrt{d}y)X. \tag{5.6}$$

We associate to (5.5) the $\mathbb{Q}$-curve above with $d = a$, $x = \hat{B} =: z$, and $y = w$, and for later reference a 'twisting parameter' γ (some algebraic integer), i.e.

$$E^\gamma_{a,z,w} : Y^2 = X^3 + 4\sqrt{a}z\gamma X^2 + 2\left(az^2 + \sqrt{a}w\right)\gamma^2 X. \tag{5.7}$$

This model has c_4-invariant

$$c^{\gamma}_{4,a,z,w} = -2^5\sqrt{a}\left(3w - 5\sqrt{a}z^2\right)\gamma^2$$

discriminant

$$\Delta^{\gamma}_{a,z,w} = -2^9\sqrt{a}^3\left(w - \sqrt{a}z^2\right)\left(w + \sqrt{a}z^2\right)^2\gamma^6,$$

and j-invariant

$$j_{a,z,w} = 2^6\frac{(3\,w - 5\,\sqrt{a}z^2)^3}{(w + \sqrt{a}z^2)^2(w - \sqrt{a}z^2)}.$$

Proposition 5.2.1. *The invariants $c^{\gamma}_{4,a,z,w}$ and $\Delta^{\gamma}_{a,z,w}$ are coprime outside all primes dividing $2\gamma a$.*

Proof. Suppose a finite prime $\mathfrak{p}$ divides $c^{\gamma}_{4,a,z,w}$ and $\Delta^{\gamma}_{a,z,w}$ but not $2\gamma a$, then $\mathfrak{p}$ should divide $z = \hat{B}$ and w, which are coprime. □

Corollary 5.2.2. *At all finite primes not dividing $2\gamma a$ the model $E^{\gamma}_{a,z,w}$ is minimal and has semi-stable (i.e. non-additive) reduction.*

Proposition 5.2.3. *Suppose B is divisible by a prime number p, with $p^3 \mid B$ if $p = 2$, then $j_{a,z,w}$ is not integral at primes above p. In particular $E^{\gamma}_{a,z,w}$ has potentially multiplicative reduction at such primes.*

Proof. Suppose that $p \mid B$ then we know that $p \nmid A = az^2$ and $p \nmid C = azw$. Since $\hat{a}B^4 = (w + \sqrt{a}z^2)(w - \sqrt{a}z^2)$ primes above p divide the denominator, but not the numerator of $j_{a,z,w}$ if $p \neq 2$.

When $p = 2$, let $\mathfrak{p}$ be a prime above 2 and suppose $\operatorname{ord}_{\mathfrak{p}} j_{a,z,w} \geq 0$. Writing this out gives

$$6\operatorname{ord}_{\mathfrak{p}} 2 + 3\operatorname{ord}_{\mathfrak{p}}(3\,w - 5\sqrt{a}z^2) \geq 2\operatorname{ord}_{\mathfrak{p}}(w + \sqrt{a}z^2) + \operatorname{ord}\mathfrak{p}(w - \sqrt{a}z^2). \quad (5.8)$$

If $\operatorname{ord}_{\mathfrak{p}}(w - \sqrt{a}z^2) > \operatorname{ord}_{\mathfrak{p}} 2$ then $\operatorname{ord}_{\mathfrak{p}}(3\,w - 5\sqrt{a}z^2) = \operatorname{ord}_{\mathfrak{p}}(w + \sqrt{a}z^2) = \operatorname{ord}_{\mathfrak{p}} 2$ and hence $\operatorname{ord}_{\mathfrak{p}}(w - \sqrt{a}z^2) = \operatorname{ord}_{\mathfrak{p}} 2\,(\operatorname{ord}_2 \hat{a} + 4\operatorname{ord}_2 B - 1)$. Substituting this in equation (5.8) gives us

$$9 \geq \operatorname{ord}_2 \hat{a} + 4\operatorname{ord}_2 B + 1,$$

contradicting $8 \mid B$. We thus have $\operatorname{ord}_{\mathfrak{p}}(w - \sqrt{a}z^2) = \operatorname{ord}_{\mathfrak{p}} 2$ and therefore we have that $\operatorname{ord}_{\mathfrak{p}}(w + \sqrt{a}z^2) = \operatorname{ord}_{\mathfrak{p}} 2\,(\operatorname{ord}_2 \hat{a} + 4\operatorname{ord}_2 B - 1) > 3\operatorname{ord}_{\mathfrak{p}} 2$. We thus find that

$$3\operatorname{ord}_{\mathfrak{p}}(3\,w - 5\sqrt{a}z^2) \geq \operatorname{ord}_{\mathfrak{p}} 2\,(2\operatorname{ord}_2 \hat{a} + 8\operatorname{ord}_2 B - 1) > 9\operatorname{ord}_{\mathfrak{p}} 2.$$

This contradicts that $3(w+\sqrt{a}z^2)-(3\,w-5\sqrt{a}z^2)=8w$ has valuation $3\operatorname{ord}_{\mathfrak{p}} 2$, completing the proof. □

Corollary 5.2.4. *If B is divisible by a prime number p, with $p^3 \mid B$ if $p=2$, then $E_{a,z,w}$ does not have complex multiplication.*

Proof. Follows directly from [Sil94, II, Theorem 6.1] □

Whenever the point P is not clear from the context, we will add an index P to the variables mentioned above, e.g. a_P, A_P, etc. If E_D has positive rank and $P \in E_D(\mathbb{Q})$ is a non-torsion point we will denote the variables associated to $P_m := mP$ by an index $m \in \mathbb{Z} \setminus \{0\}$, e.g. $a_m := a_{P_m}, A_m := A_{P_m}$, etc.

Subsection 5.2.1

a only depends on class modulo $[2]E_D(\mathbb{Q})$

We will now show that the value of a for a point only depends on its class modulo the image of the multiplication by 2 map. This will in particular show that the Frey $\mathbb{Q}$-curve associated with P_m ($m \in \mathbb{Z}\setminus\{0\}$, $P \in E_D(\mathbb{Q})$ non-torsion) only depends on the parity of m. Therefore, the construction (5.7) yields at most 2 distinct Frey $\mathbb{Q}$-curves up to twisting by γ (in the unknowns z and w) associated to an elliptic divisibility sequence.

Note that the short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & E_D[2] \arrow[r] & E_D(\overline{\mathbb{Q}}) \arrow[r, "{[2]}"] & E_D(\overline{\mathbb{Q}}) \arrow[r] & 1, \end{tikzcd}$$

induces a long exact sequence in Galois cohomology containing a map

$$\alpha : E_D(\mathbb{Q}) = H^0\left(G_{\mathbb{Q}}, E_D(\overline{\mathbb{Q}})\right) \to H^1\left(G_{\mathbb{Q}}, E_D[2]\right).$$

The kernel of this map is precisely the image of $[2] : E_D(\mathbb{Q}) \to E_D(\mathbb{Q})$, hence this map will be useful for proving things about points modulo this image. To work with the codomain of this map, we note that $E_D[2] = \{\mathcal{O}, T, T_{+1}, T_{-1}\}$, where

$$T_\delta = (\delta\sqrt{-D}, 0),$$

for a fixed choice of $\sqrt{-D}$.

For a fixed $[f] \in H^1(G_{\mathbb{Q}}, E_D[2])$ we can choose functions $f_\delta : G_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ such that

$$f(\sigma) = f_{+1}(\sigma)T_{+1} + f_{-1}(\sigma)T_{-1} \text{ for all } \sigma \in G_{\mathbb{Q}}.$$

Since f is a cocycle we find that $f(\sigma) + {}^{\sigma}f(\tau) = f(\sigma\tau)$ for all $\sigma, \tau \in G_{\mathbb{Q}}$, hence

$$\begin{cases} f_{+1}(\sigma) + f_{+1}(\tau) = f_{+1}(\sigma\tau) \text{ and } f_{-1}(\sigma) + f_{-1}(\tau) = f_{-1}(\sigma\tau) & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{-D})} \\ f_{+1}(\sigma) + f_{-1}(\tau) = f_{+1}(\sigma\tau) \text{ and } f_{-1}(\sigma) + f_{+1}(\tau) = f_{-1}(\sigma\tau) & \text{otherwise.} \end{cases}$$

This implies $f_\delta|_{G_{\mathbb{Q}(\sqrt{-D})}} \in \hom(G_{\mathbb{Q}(\sqrt{-D})}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Q}\left(\sqrt{-D}\right)^* / \left(\mathbb{Q}\left(\sqrt{-D}\right)^*\right)^2$, hence we can construct maps $\alpha_\delta : E_D(\mathbb{Q}) \to \mathbb{Q}\left(\sqrt{-D}\right)^* / \left(\mathbb{Q}\left(\sqrt{-D}\right)^*\right)^2$, by combining the map α with $[f] \mapsto f_\delta|G_{\mathbb{Q}(\sqrt{-D})}$. Note that the latter is well-defined as the relevant coboundaries are

$$\begin{cases} \partial\mathcal{O} = \partial T & = (\sigma \mapsto \mathcal{O}) \\ \partial T_{+1} = \partial T_{-1} & = \left(\sigma \mapsto \begin{cases} \mathcal{O} & \text{if } \sigma \in G_{\mathbb{Q}(\sqrt{-D})} \\ T & \text{otherwise} \end{cases}\right). \end{cases}$$

In case $-D$ is a square it is clear that the maps α_δ encode all information of the map α. In the case that there exists a $\sigma \in G_{\mathbb{Q}} \setminus G_{\mathbb{Q}(\sqrt{-D})}$ this remains true and in fact one of the maps α_δ becomes redundant. This can be seen as for any $\tau \in G_{\mathbb{Q}(\sqrt{-D})}$ we have

$$\begin{aligned} f_{-1}(\tau) &= f_{-1}(\tau\sigma^{-1}) - f_{-1}(\sigma^{-1}) = f_{+1}(\sigma\tau\sigma^{-1}) - f_{+1}(\sigma) - f_{-1}(\sigma^{-1}) \\ &= f_{+1}(\sigma\tau\sigma^{-1}) - f_{+1}(1) = f_{+1}(\sigma\tau\sigma^{-1}). \end{aligned}$$

Furthermore the value of f_{+1} at any element of $G_{\mathbb{Q}} \setminus G_{\mathbb{Q}(\sqrt{-D})}$ can be derived from $f_{+1}(\sigma)$. Since there exists a non-trivial coboundary in this case the exact value of $f_{+1}(\sigma)$ does not matter for the cohomology class $[f]$.

By making the maps $\alpha_\delta : E_D(\mathbb{Q}) \to \mathbb{Q}\left(\sqrt{-D}\right)^* / \left(\mathbb{Q}\left(\sqrt{-D}\right)^*\right)^2$ explicit we obtain the following result.

Proposition 5.2.5. *There exist homomorphisms*

$$\alpha_\delta : E_D(\mathbb{Q}) \to \mathbb{Q}\left(\sqrt{-D}\right)^* / \left(\mathbb{Q}\left(\sqrt{-D}\right)^*\right)^2$$

for $\delta \in \{\pm 1\}$ *such that the map*

$$(\alpha_{+1}, \alpha_{-1}) : E_D(\mathbb{Q}) \to \left(\mathbb{Q}\left(\sqrt{-D}\right)^* / \left(\mathbb{Q}\left(\sqrt{-D}\right)^*\right)^2\right)^2$$

has kernel $\{[2]P : P \in E_D(\mathbb{Q})\}$. *Explicitly these homomorphisms are given by*

$$\alpha_\delta(P) = \begin{cases} [x + \delta\sqrt{-D}] & \text{if } P = (x, y) \\ [1] & \text{if } P = \mathcal{O}. \end{cases}$$

Proof. The existence of these maps has already been proven using the map α. To make them explicit, note that α maps a point $P \in E_D(\mathbb{Q})$ to the class of $f : \sigma \mapsto {}^{\sigma}Q - Q$ for any $Q \in E_D(\overline{\mathbb{Q}})$ such that $[2]Q = P$.

Let $K = \mathbb{Q}(\sqrt{-D})$ and pick $\delta \in \{\pm 1\}$ and a point $P = (x, y) \in E_D(\mathbb{Q})$ arbitrary. Note that $\alpha_\delta(P) = [\gamma]$ for some $\gamma \in K^*$ such that

$$\begin{cases} \alpha(\sigma) \in \{\mathcal{O}, T_{-\delta}\} & \text{if } \sigma \in G_{K(\sqrt{\gamma})} \\ \alpha(\sigma) \in \{T, T_\delta\} & \text{if } \sigma \in G_K \setminus G_{K(\sqrt{\gamma})}. \end{cases}$$

All that remains to check is that in fact $\gamma = x + \delta\sqrt{-D}$ satisfies this condition.

Let $Q = (x_Q, y_Q) \in E_D(\overline{\mathbb{Q}})$ be a point such that $[2]Q = P$. The tangent line to E_D at Q is given by

$$Y = \frac{3x_Q^2 + D}{2y_Q}(X - x_Q) + y_Q.$$

By substituting this in the equation for E we get a cubic polynomial in X of which the roots are x and x_Q twice. Looking at the coefficient of X^2 this tells us that

$$2x_Q + x = \left(\frac{3x_Q^2 + D}{2y_Q}\right)^2 = \frac{9x_Q^4 + 6Dx_Q^2 + D^2}{4x_Q^3 + 4Dx_Q},$$

hence x_Q is a root of the polynomial

$$f(X) = X^4 - 4\,xX^3 - 2\,DX^2 - 4\,xDX + D^2.$$

Note that all four roots of this polynomial correspond to the x-coordinates of the four possible points Q, i.e. the x-coordinates of $Q, Q + T, Q + T_{+1}$, and $Q + T_{-1}$.

Now over the field $K(\sqrt{\gamma})$ the polynomial $f(X)$ splits as

$$f(X) = (X^2 - \omega X - \delta\sqrt{-D}\omega - D)(X^2 - \overline{\omega}X - \delta\sqrt{-D}\overline{\omega} - D)$$

where $\omega = 2x + 2\frac{y}{\sqrt{\gamma}}$ and $\overline{\omega} = 2x - \frac{y}{\sqrt{\gamma}}$. Assuming without loss of generality that x_Q is a root of the first factor, the other root of the first factor is $\omega - x_Q$, which we claim to be the x-coordinate of $Q + T_{-\delta}$. This would imply that

$$\begin{cases} {}^{\sigma}Q - Q \in \{\mathcal{O}, T_{-\delta}\} & \text{if } \sigma \in G_{K(\sqrt{\gamma})} \\ {}^{\sigma}Q - Q \in \{T, T_\delta\} & \text{if } \sigma \in G_K \setminus G_{K(\sqrt{\gamma})}, \end{cases}$$

as only $\sigma \notin G_{K(\sqrt{\gamma})}$ switch the factors of $f(X)$.

It thus remains to prove the claim that $\omega - x_Q$ is the x-coordinate of $Q + T_{-\delta}$. Note that the line through Q and $T_{-\delta}$ is given by

$$Y = \frac{y_Q}{x_Q + \delta\sqrt{-D}}(X + \delta\sqrt{-D}).$$

Doing the same substitution trick, we find that the x-coordinate of $Q + T_{-\delta}$ is

$$\begin{array}{ll} \beta & = \left(\frac{y_Q}{x_Q+\delta\sqrt{-D}}\right)^2 - x_Q + \delta\sqrt{-D} \\ & = \frac{x_Q(x_Q-\delta\sqrt{-D})}{x_Q+\delta\sqrt{-D}} - (x_Q - \delta\sqrt{-D}) \\ & = \frac{-\delta\sqrt{-D}(x_Q-\delta\sqrt{-D})}{x_Q+\delta\sqrt{-D}}. \end{array}$$

To see that this is the same as $\omega - x_Q$, note that

$$\begin{array}{ll} (\beta + x_Q - 2\,x)^2 & = \left(\frac{x_Q^2-D}{x_Q-\delta\sqrt{-D}} - 2\,x\right)^2 \\ & = \frac{x_Q^4-2Dx_Q^2+D^2}{(x_Q-\delta\sqrt{-D})^2} - 4\,x\frac{x_Q^2-D}{x_Q-\delta\sqrt{-D}} + 4\,x^2 \\ & = \frac{4\,xx_Q^3+4\,xDx_Q}{(x_Q-\delta\sqrt{-D})^2} - 4\,x\frac{x_Q^2-D}{x_Q-\delta\sqrt{-D}} + 4\,x^2 \\ & = 4\,x\frac{x_Q^2+\delta\sqrt{-D}x_Q-x_Q^2+D}{x_Q-\sqrt{-D}} + 4\,x^2 \\ & = 4\,x^2 - \delta\sqrt{-D}x = \left(\frac{y}{\sqrt{\gamma}}\right)^2. \end{array}$$

So for the right choice of $\sqrt{\gamma}$ we have $\beta + x_Q = \omega$.

□

Now we return to our premise. Suppose we have two points $P, Q \in E_D(\mathbb{Q})$ which have the same class modulo $[2]E_D(\mathbb{Q})$, but $a_P \neq a_Q$. Note first of all that

$$[a_P] = [A_P] = [x_P] = [y_p^2 x_P] = [x_P{+}D] = \begin{cases} [\alpha_{+1}(P)][\alpha_{-1}(P)] & \text{if } -D \text{ is a square} \\ [N(\alpha_{+1}(P))] & \text{otherwise,} \end{cases}$$

and similarly for $[a_Q]$. Therefore $[a_P] = [a_Q] \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ implying that we must have $|a_P| \neq |a_Q|$. Without loss of generality we may then assume that there is a prime number p such that

$$0 \leq \operatorname{ord}_p A_P < \min\{\operatorname{ord}_p A_Q, \operatorname{ord}_p D\}.$$

The fact that P and Q have the same class modulo $[2]E_D(\mathbb{Q})$ implies that $\alpha_{+1}(P) = \alpha_{+1}(Q)$. Note that $\alpha_{+1}(P)$ is the class of $x_P + \sqrt{-D}$ which is the same class as $A_P + B_P^2\sqrt{-D}$ and similarly $\alpha_{+1}(Q)$ is the class of $A_Q + B_Q^2\sqrt{-D}$. The classes being the same implies that

$$\left(A_P + B_P^2\sqrt{-D}\right)\left(A_Q + B_Q^2\sqrt{-D}\right) = \left(b + c\sqrt{-D}\right)^2,$$

for some $b, c \in \mathbb{Q}$. Since the left hand side is actually in the ring of integers of $\mathbb{Q}(\sqrt{-D})$ we can in fact say that $b, c \in \frac{1}{2}\mathbb{Z}$ with $b \notin \mathbb{Z} \iff c \notin \mathbb{Z}$. Writing out the equation in the case that $-D$ is not a square in $\mathbb{Z}$ gives us

$$\begin{aligned} A_P B_Q^2 + A_Q B_P^2 &= 2\,bc \text{ and} \\ A_P A_Q - D B_P^2 B_Q^2 &= b^2 - Dc^2. \end{aligned}$$

Since the left hand side of the first equation is an integer, we find that $b, c \in \mathbb{Z}$. Furthermore as $\operatorname{ord}_p A_Q > \operatorname{ord}_p A_P \geq 0$ we have $\operatorname{ord}_p B_Q = 0$ and the first equation tells us that

$$\operatorname{ord}_p A_P = \operatorname{ord}_p 2 + \operatorname{ord}_p b + \operatorname{ord}_p c.$$

This implies $\operatorname{ord}_p b \geq \frac{1}{2}\operatorname{ord}_p D > 0$ as otherwise b^2 would be the only term in the second equation with the smallest order of p. Note that $[a_P] = [a_Q] \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ implies that $\min\{\operatorname{ord}_p A_Q, \operatorname{ord}_p D\} - \operatorname{ord}_p A_P$ is a multiple of 2, so

$$\frac{1}{2}\operatorname{ord}_p D \leq \operatorname{ord}_p 2 + \operatorname{ord}_p b + \operatorname{ord}_p c = \operatorname{ord}_p A_P \leq \operatorname{ord}_p D - 2,$$

which would imply that $\operatorname{ord}_p D \geq 4$ contradicting one of our initial assumptions. Therefore indeed the value of a_P only depends on the class of P modulo $[2]E_D(\mathbb{Q})$ in case $-D$ is not a square.

In the case that $-D$ is a square $\min\{\operatorname{ord}_p A_Q, \operatorname{ord}_p D\} - \operatorname{ord}_p A_P$ is still a multiple of 2. Therefore we have $\operatorname{ord}_p A_Q \geq \operatorname{ord}_p D = 2$ and $\operatorname{ord}_p A_P = 0$. This implies that $\operatorname{ord}_p(A_P + B_P^2\sqrt{-D}) = 0$ and $\operatorname{ord}_p(A_Q + B_Q^2\sqrt{-D}) = 1$, but this contradicts the fact that their product should be a square. Therefore the result also holds when $-D$ is a square.

Section 5.3

Level lowering results

Since $E^{\gamma}_{a,z,w}(\mathbb{Q})$ is a $\mathbb{Q}$-curve, it follows from Theorem 2.1.9 and Theorem 2.1.10 that $E^{\gamma}_{a,z,w}$ is the quotient of the abelian variety A_f associated with some newform $f \in \mathcal{S}_2(N, \varepsilon)$. If a is a square and $\gamma \in \mathbb{Q}^*$, then we may assume f is rational with trivial character and level equal to the conductor of $E^{\gamma}_{a,z,w}$, as $E^{\gamma}_{a,z,w}$ is defined over $\mathbb{Q}$. In that case we will have that

$$\rho_{E,l} \cong \rho_{f,l} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_l)$$

for all prime numbers l. Otherwise the level and character can be determined by the theory in Section 2.8 and Section 2.9 when γ is chosen according to Corollary 2.7.8. Furthermore we then have that

$$\rho_{\beta,\lambda} \cong \rho_{f,l} : G_{\mathbb{Q}} \to \mathrm{GL}_2(L_\beta),$$

for a splitting map β for $c_{E^{\gamma}_{a,z,w}}$ and any prime λ of L_β.

In this section we will show that if B is an l-th power and $\lambda \mid l$ is a prime of the coefficient field of the newform f, then we can apply level lowering results to the mod λ representation $\overline{\rho_{f,\lambda}}$. First of all we will need that $\overline{\rho_{f,\lambda}}$ is absolutely irreducible. We can derive this from a corollary of Theorem 2.11.1 when a is not a square.

Proposition 5.3.1. *Let $P \in E_D(\mathbb{Q}) \setminus \{\mathcal{O}, T\}$ be a point such that $B_P \neq \pm 1$ is an l-th power with l an odd prime number and a_P not a square. Let f be a newform corresponding to an abelian variety of* GL$_2$*-type that arises from a splitting map for $E^{\gamma}_{a_P,z_P,w_P}$. For any prime $\lambda \mid l$ in the coefficient field of f, the Galois representation $\overline{\rho_{f,\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_l)$ is irreducible if either*

- *$l = 3$ and a is not the norm of an element in $\mathbb{Q}(\sqrt{-2})$;*
- *$l = 5$ and a is not the norm of an element in $\mathbb{Q}(\sqrt{-1})$;*
- *$l = 7$ or $l = 13$; or*
- *$l = 11$ or $l > 13$, and B_P is divisible by a prime number $p > 3$.*

Proof. Since $l \geq 3$ and $B_P \neq \pm 1$ there must be a prime $p \mid B$ satisfying the condition of Proposition 5.2.3. By Corollary 5.2.4 the curve $E^{\gamma}_{a_P,z_P,w_P}$ therefore does not have complex multiplication allowing the application of Theorem 2.11.1. The cases for $l = 3$ and $l = 5$ immediately follow. Since j_{a_P,z_P,w_P} is not integral, the case $l = 13$ is also clear. For the case $l = 7$ we still need to check two j-invariants, but by solving for which points P we have that j_{a_P,z_P,w_P} is one of the non-integral j-invariants listed we find that B_P is not a 7-th power. For the cases $l = 11$ and $l > 13$ the fact that a prime $p \mid B_P$ exists with $p > 3$ tells us we have potential multiplicative reduction at that prime. □

Now we show that, given irreducibility, we can apply level lowering results to the Galois representation $\overline{\rho_{f,\lambda}}$.

Proposition 5.3.2. *Let $P \in E_D(\mathbb{Q}) \setminus \{\mathcal{O}, T\}$ be a point such that $B_P \neq \pm 1$ is an l-th power with l an odd prime number. Suppose that $E = E^{\gamma}_{a_P, z_P, w_P}$ is defined over a number field K and that $f \in \mathcal{S}_2(N, \chi)$ is a newform such that*

$$\overline{\rho_{f,\lambda}}|_{G_K} \cong \overline{\rho_{E,l}} : G_K \to \mathrm{Aut}(E[l]) \cong \mathrm{GL}_2(\mathbb{F}_l),$$

for some prime $\lambda \mid l$ in the coefficient field of f. Let S be the set of prime numbers that ramify in K, divide $2D$, or divide the norm of γ. If $\overline{\rho_{f,\lambda}}$ is irreducible, then there exists a newform $g \in \mathcal{S}_2(\tilde{N}, \chi)$ and a prime $\lambda' \mid l$ in the coefficient field of g such that

$$\overline{\rho_{g,\lambda'}} \cong \overline{\rho_{f,\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_l}),$$

and $\tilde{N} = \prod_{p \in S} p^{\mathrm{ord}_p N}$.

Proof. For any prime number p not in S we know that p does not ramify in K, hence the ramification subgroup $I_p \subseteq G_{\mathbb{Q}}$ is a subgroup of G_K. This implies that $\overline{\rho_{f,\lambda}}|I_p \cong \overline{\rho_{E,l}}|I_p$. Note that E has good or multiplicative reduction at each prime $\mathfrak{p}$ above p by Corollary 5.2.2 and is also a minimal model at those primes. Furthermore the assumption that B_P is an l-th power shows that $l \mid \mathrm{ord}_{\mathfrak{p}} \Delta^{\gamma}_{a_P, z_P, w_P}$ as $p \nmid 2D$ and p also does not divide the norm of γ. It is well known that this implies that $\overline{\rho_{E,l}}|I_p$ is trivial when $p \neq l$ and finite flat if $p = l$.

The above results show that all primes $p \notin S$ do not show up in the Serre level of $\overline{\rho_{f,\lambda}}$. In case $l \notin S$ these results also show that the Serre weight is 2. As the character of $\overline{\rho_{f,\lambda}}$ is just the character of f, the result therefore follows from the proven Serre conjectures [KW09a, KW09b] in most cases. If not, the level lowering results required for the proof of Serre's conjectures can still be applied here to obtain the newform g. □

Section 5.4

The case $a = 1$

The case $a = 1$ is special as shown by the following result.

Proposition 5.4.1. *For any $P \in [2]E_D(\mathbb{Q}) \setminus \{\mathcal{O}\}$ we have $a_P = 1$.*

Proof. We use the homomorphisms $\alpha_\delta : E_D(\mathbb{Q}) \to \mathbb{Q}(\sqrt{-D})^*/(\mathbb{Q}(\sqrt{-D})^*)^2$ from Proposition 5.2.5. For any $P \in [2]E_D(\mathbb{Q})$ and $\delta \in \{\pm 1\}$ we know that $\alpha_\delta(P) = [1]$. Furthermore we have seen that

$$\mathbb{Q}^*/(\mathbb{Q}^*)^2 \ni [a_P] = \begin{cases} [\alpha_{+1}(P)][\alpha_{-1}(P)] & \text{if } -D \text{ is a square} \\ [N(\alpha_{+1}(P)] & \text{otherwise,} \end{cases}$$

so a_P is a square. We know that $\alpha_{+1}(P) = [A_P + B_P^2\sqrt{-D}]$, so $A_P + B_P^2\sqrt{-D}$ is a square in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$. We can write $A_P + B_P^2\sqrt{-D} = (b + c\sqrt{-D})^2$ with $b, c \in \frac{1}{2}\mathbb{Z}$ if $-D$ is not a square to find that

$$\begin{cases} A_P = b^2 - Dc^2 \\ B_P^2 = 2bc. \end{cases}$$

Since $b + c\sqrt{-D} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ we may assume that $b, c \in \mathbb{Z}$ from the second equation. Now any prime dividing a_P divides both A_P and D, hence therefore also b and thus B_P. Since $\gcd(A_P, B_P) = 1$ this shows us that $a_P = 1$ in this case.

If $-D$ is a square we know that $A_P + B_P^2\sqrt{-D} = b^2$ for some $b \in \mathbb{Z}$. Note that for any prime $p \mid a_P$ we have $p \nmid B_P$ and therefore

$$\operatorname{ord}_p A_P \geq \operatorname{ord}_p a_P \geq 2 > \frac{1}{2}\operatorname{ord}_p D = \operatorname{ord}_p(B_P^2\sqrt{-D})$$

by our assumptions on D. This implies that

$$2\operatorname{ord}_p b = \operatorname{ord}_p(A_P + B_P^2\sqrt{-D}) = \frac{1}{2}\operatorname{ord}_p D > 0,$$

which contradicts the previous equation. Therefore $a_P = 1$ also in this case. □

This result shows that for any elliptic divisibility sequence generated by P the curve $E_{1,z,w}^\gamma$ is the Frey curve corresponding to the points $P_{2m}, m \in \mathbb{Z}$. Note that the curve $E_{1,z,w}^\gamma$ is an elliptic curve defined over $\mathbb{Q}$ when $\gamma \in \mathbb{Q}^*$ and does not depend on D. We shall prove some general results about this curve here.

First we will try to find the twist $\gamma \in \mathbb{Q}^*$ such that the conductor of $E_{1,z,w}^\gamma$ is as small as possible. For this we may assume that γ is a squarefree integer. Note that if an odd prime p divides γ then $c_{4,1,z,w}^\gamma$ and $\Delta_{1,z,w}^\gamma$ are both divisible by p, but the model is still minimal as either $p^4 \nmid c_{4,1,z,w}^\gamma$ or $p^6 \nmid \Delta_{1,z,w}^\gamma$. So for an odd prime p the conductor exponent at p would be at least 2 if $p \mid \gamma$, whereas it would be 0 or 1 otherwise by Corollary 5.2.2. We therefore want $\gamma \in \{1, -1, 2, -2\}$.

Table 5.1 gives the possible conductor exponents at 2 for the curves $E^{\gamma}_{1,z,w}$ with $\gamma \in \{1, -1, 2, -2\}$. To compute these conductor exponents we used that the curve $E^{\gamma}_{1,z,w}$ is 2-isogenous over $\mathbb{Q}$ to the curve

$$\tilde{E}^{\gamma}_{1,z,w} : Y^2 = X^3 - 8\, z\gamma X^2 + 8\left(z^2 - w\right)\gamma^2 X.$$

Since isogenous curves have isomorphic l-adic Galois representations, their conductors are by definition the same. In the framework [vL21a] we can use this to perform the conductor computation on both curves simultaneously, and use the result from the one that finishes first for each pair z, w. The code to do this can be found in `a1conductors.rst`.

Remark 5.4.2. Note that the only assumption used to generate Table 5.1 is that 2 does not divide both z and w. When z and w correspond to a point on E_D we have that

$$(w + z^2)(w - z^2) = w^2 - z^4 = DB^4,$$

so we obtain further limitation based on the order of 2 in D and B. In particular if we assume B is an l-th power with $l > 1$ the cases with conductor exponents 2, 3, and 5 do not occur.

We will assume that whenever we use $E^{\gamma}_{1,z,w}$ from now on, γ is chosen such that the conductor exponent at 2 is as small as possible. Note that to do this γ might depend on the value of z and w modulo 2^8.

We will also show here that the Galois representations associated to the case $a = 1$ are irreducible.

Theorem 5.4.3. *For all prime numbers $l > 5$ and $\gamma \in \mathbb{Q}^*$ the mod l Galois representation $\overline{\rho_{E^{\gamma}_{1,z,w}, l}} : G_{\mathbb{Q}} \to \mathrm{Aut}(E^{\gamma}_{1,z,w}[l]) \cong \mathrm{GL}_2(\mathbb{F}_l)$ is irreducible.*

Proof. Note that $E_{1,z,w}$ has a rational 2-torsion point. If $\rho_l^{E^{\gamma}_{1,z,w}}$ would be reducible, then E would correspond to a non-cuspidal $\mathbb{Q}$-rational point on $X_0(2l)$. The well known deep fact that $X_0(2l)$ does not have such points for $l > 7$ (see e.g. [Dah08, Theorem 22-(ii)] for precise references) immediately proves the result for $l > 7$. For $l = 7$ we see if the j-invariants of points on $X_0(2l)$ can match $j_{1,z,w}$. Note that we have

$$j_{1,z,w} = 2^6 \frac{(3\,t - 5)^3}{(t-1)(t+1)^2},$$

after rewriting with $t = \frac{w}{z^2}$.

$\gamma = 1$	$\gamma = -1$	$\gamma = 2$	$\gamma = -2$	
8	8	8	8	if $\mathrm{ord}_2(w^2 - z^4) = 0$
7	7	7	7	if $\mathrm{ord}_2(w^2 - z^4) = 3$
4	3	6	6	if $w + z^2 \equiv 8 \pmod{32}$ and $z \equiv 1 \pmod 4$
3	4	6	6	if $w + z^2 \equiv 8 \pmod{32}$ and $z \equiv 3 \pmod 4$
2	4	6	6	if $w + z^2 \equiv 24 \pmod{32}$ and $z \equiv 1 \pmod 4$
4	2	6	6	if $w + z^2 \equiv 24 \pmod{32}$ and $z \equiv 3 \pmod 4$
6	6	4	2	if $w - z^2 \equiv 8 \pmod{32}$ and $z \equiv 1 \pmod 4$
6	6	2	4	if $w - z^2 \equiv 8 \pmod{32}$ and $z \equiv 3 \pmod 4$
6	6	3	4	if $w - z^2 \equiv 24 \pmod{32}$ and $z \equiv 1 \pmod 4$
6	6	4	3	if $w - z^2 \equiv 24 \pmod{32}$ and $z \equiv 3 \pmod 4$
5	5	6	6	if $\mathrm{ord}_2(w + z^2) = 4$
6	6	5	5	if $\mathrm{ord}_2(w - z^2) = 4$
3	4	6	6	if $\mathrm{ord}_2(w + z^2) = 5, 6$ and $z \equiv 1 \pmod 4$
4	3	6	6	if $\mathrm{ord}_2(w + z^2) = 5, 6$ and $z \equiv 3 \pmod 4$
6	6	4	3	if $\mathrm{ord}_2(w - z^2) = 5, 6$ and $z \equiv 1 \pmod 4$
6	6	3	4	if $\mathrm{ord}_2(w - z^2) = 5, 6$ and $z \equiv 3 \pmod 4$
0	4	6	6	if $\mathrm{ord}_2(w + z^2) = 7$ and $z \equiv 1 \pmod 4$
4	0	6	6	if $\mathrm{ord}_2(w + z^2) = 7$ and $z \equiv 3 \pmod 4$
6	6	4	0	if $\mathrm{ord}_2(w - z^2) = 7$ and $z \equiv 1 \pmod 4$
6	6	0	4	if $\mathrm{ord}_2(w - z^2) = 7$ and $z \equiv 3 \pmod 4$
1	4	6	6	if $\mathrm{ord}_2(w + z^2) \geq 8$ and $z \equiv 1 \pmod 4$
4	1	6	6	if $\mathrm{ord}_2(w + z^2) \geq 8$ and $z \equiv 3 \pmod 4$
6	6	4	1	if $\mathrm{ord}_2(w - z^2) \geq 8$ and $z \equiv 1 \pmod 4$
6	6	1	4	if $\mathrm{ord}_2(w - z^2) \geq 8$ and $z \equiv 3 \pmod 4$

Table 5.1: The conductor exponent of $E^\gamma_{1,z,w}$ at 2 for various values of γ.

A computation in Magma [BCP97] (see `irreducibility_a1.m` near the end) tells us that $X_0(14)$ is an elliptic curve with six $\mathbb{Q}$-rational points with j-invariants $\infty, -3375, 16\,581\,375$. If we equate these to $j_{1,z,w}$ we find $t = \pm 1, \pm\frac{65}{63}$. Since the denominator of t is a square the only option is $t = \pm 1$, which would give $z = \pm 1$ and $w = \pm 1$, meaning $B = 0$. This does not correspond to a point $P \in E_D(\mathbb{Q}) \setminus \{\mathcal{O}, T\}$. $\square$

We can extend Theorem 5.4.3 to $l = 3, 5$ for specific D as follows. First assume that the mod l Galois representation $\rho_l^{E^\gamma_{1,z,w}} : G_{\mathbb{Q}} \to \mathrm{Aut}(E^\gamma_{1,z,w}[l])$ is reducible, then $E^\gamma_{1,z,w}$ corresponds to a $\mathbb{Q}$-point on $X_0(l)$. Note that $X_0(l)$ is a rational curve for $l = 3, 5$ so we can parameterize it with a single parameter s. We let $j_l : X_0(l) \to X(1)$ be the j-invariant in which case we get that the curve $E^{\gamma}_{1,z,w}$ should correspond to a point on the curve

$$C_l : j_{1,z,w}(t) = j_l(s)$$

Computing this curve explicitly in Magma [BCP97] we see that it also is a rational curve, hence it has a parameterization. Parameterizing with respect to points $[x : y]$ on $\mathbb{P}^1$ we get that

$$\frac{w}{z^2} = t = \frac{w_l(x, y)}{z_l(x, y)}.$$

Since any point of $\mathbb{P}^1$ can be written with coprime integer coordinates, we thus know there are coprime $a, b \in \mathbb{Z}$ and some $c \in \mathbb{Q}^*$ such that

$$\begin{cases} cw & = w_l(a, b), \\ cz^2 & = z_l(a, b). \end{cases}$$

By rescaling we may assume w_l and z_l have integer coefficient in which case the denominator of c must be one as w and z^2 are coprime. Therefore we may also assume $c \in \mathbb{Z} \setminus \{0\}$.

From these equations it follows that

$$c^2 DB^4 = (cw)^2 - (cz^2)^2 = w_l(a, b)^2 - z_l(a, b)^2.$$

Computing the right hand side in Magma we actually see that

$$c^2 DB^4 = 2^8 c_1(a, b)^l c_2(a, b)^l c_3(a, b) c_4(a, b), \tag{5.9}$$

with c_1, c_2, c_3, c_4 all linear factors. By choosing a different parameterization of $\mathbb{P}^1$ we may assume that

$$\begin{aligned} c_1(a, b) & = a, \\ c_2(a, b) & = b, \\ c_3(a, b) & = a - b. \end{aligned}$$

Making this parameterization explicit in Magma we find that

$$c_4(a, b) = \begin{cases} a + 8\,b & \text{if } l = 3 \\ a + 4\,b & \text{if } l = 5. \end{cases}$$

Since a and b were coprime we can easily see that the c_i are pairwise coprime outside primes dividing $2\,l$. Therefore equation (5.9) implies that all the $c_i(a,b)$ must be fourth powers up to factors consisting of divisors of $2\,lc^2D$, i.e. we can write

$$c_i(a,b) = a_i b_i^4 \quad \text{with } a_i, b_i \in \mathbb{Z}.$$

Note that as c must divide the resultant of z_l and w_l there is only a finite list of possible (a_1, a_2, a_3, a_4). We can compute this list explicitly for a given D using Magma. For each choice of the a_i the linear relations between the c_i give us four generalized Fermat equations of signature $(4,4,4)$ that should be satisfied. Reaching a contradiction now follows by eliminating one such equation for each choice of a_i.

To eliminate Fermat equations we first check if they have local solutions over $\mathbb{Q}_2$, $\mathbb{Q}_3$, or $\mathbb{Q}_5$. If all four corresponding to a choice of the a_i do, we look at the quotient

$$\begin{aligned} \mathbb{P}^2 \supseteq \left\{AX^4 + BY^4 + CZ^4 = 0\right\} &\to \left\{Y^2Z = X^3 + \tfrac{BC}{A^2}XZ^2\right\} \subseteq \mathbb{P}^2 \\ [x:y:z] &\mapsto [By^2z : Bx^2y : -Az^3] \end{aligned}$$

and the other genus 1 quotients obtained by interchanging X, Y and Z. If one of these elliptic curves has rank 0 we can determine the solutions of the corresponding Fermat equation that map to its torsion points. This in turn gives us the possible values of a and b and hence the values of z, w for which the mod l representation may still be reducible. If we can do this for all remaining choices of a_i we thus get an explicit list of points on $E_D(\mathbb{Q})$ such that if $E_{1,z,w}^{\gamma}$ does not correspond to one of these points, then its mod l Galois representation is irreducible.

We did the above computation for some D that will be used in the examples below (see `irreducibility_a1.m`). The points for which we could not show that the mod l Galois representation is irreducible in this way, are listed in

D	$l = 3$	$l = 5$
-2	$\mathcal{O}$	$\mathcal{O}$
3	$\mathcal{O}$	$\mathcal{O}$, $(1, \pm 2)$, $\left(\frac{121}{9}, \pm\frac{1\,342}{27}\right)$
-17	$\mathcal{O}$	$\mathcal{O}$
125	$\mathcal{O}$, $\left(\frac{121}{4}, \frac{1\,419}{8}\right)$	$\mathcal{O}$

Table 5.2: Points on $E_D(\mathbb{Q})$ such that the mod l Galois representation of $E_{1,z,w}^{\gamma}$ is irreducible if it does not correspond to that point.

Table 5.2. The code written to do so can easily be reused to compute this for further values of D.

Section 5.5

Explicit examples

In this section we will make some choices of integers D and points $P_1 \in E_D(\mathbb{Q})$ for which we can prove the non-existence of l-th powers among the B_m with an explicit lower bound on the prime number l. We will use the requirements mentioned in the previous sections implicitly unless it is not clear they can be used.

Subsection 5.5.1

Example for $D = 125$

Take $D = 125$, then $E_D(\mathbb{Q})$ has rank 1 and $T = (0, 0)$ is the only non-trivial torsion point. Using SageMath we can compute that $E_D(\mathbb{Q})$ is generated by the points $P = \left(\frac{121}{4}, \frac{1419}{8}\right)$ and T. We have $a_P = 1$, so all non-zero multiples of P correspond to the Frey curve $E^{\gamma}_{1,z,w}$, where we choose γ as in the previous section.

The level of the newforms that remain after level lowering is the product of the 2-part and 5-part of the conductor of $E^{\gamma}_{1,z,w}$. The 2-part can be read of from Table 5.1, where we note that Remark 5.4.2 applies and $2 \mid B_{mP}$ for all $m \in \mathbb{Z} \setminus \{0\}$ by (5.3). We can compute that the conductor exponent at 5 is always 1, so the levels of the newforms after level lowering must be

$$\begin{cases} 5 & \text{if } w^2 - z^4 \equiv 2^8 \pmod{2^9} \\ 10 & \text{if } w^2 - z^4 \equiv 0 \pmod{2^9}. \end{cases}$$

Note that there are no newforms of level 5 or level 10, hence none of the B_{mP} with $m \in \mathbb{Z} \setminus \{0\}$ can be l-th powers for l an odd prime number.

There is another Frey curve associated with $D = 125$ as for any $m \in \mathbb{Z} \setminus \{0\}$ we have $a_{mP+T} = 125$. We will find the correct twist of the corresponding Frey $\mathbb{Q}$-curve $E^{\gamma}_{125,z,w}$ by studying $E_{125,z,w}$ first. Note that $E_{125,z,w}$ is completely defined over $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, but a splitting character is given by a character of conductor 20 and order 4. Therefore a complete definition field over which also a splitting map for $\xi_{E^{\gamma}_{125,z,w}}$ is defined is $K = \mathbb{Q}(\zeta_{40} + \zeta_{40}^{-1})$, the totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{40})$. We compute $c_{E_{125,z,w}}$ and c_β on $G^K_{\mathbb{Q}}$. We can use the isomorphism $(\mathbb{Z}/40\mathbb{Z})^* \cong G_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{40})}$ to identify $G_{\mathbb{Q}}^K$ with $(\mathbb{Z}/40\mathbb{Z})^* / \{\pm 1\}$, which we will use to denote elements of $G_{\mathbb{Q}}^K$ by representatives from $(\mathbb{Z}/40\mathbb{Z})^*$.

$c_{E_{125,z,w}}$	± 1	± 3	± 7	± 9	± 11	± 13	± 17	± 19
± 1	1	1	1	1	1	1	1	1
± 3	1	-2	-2	1	1	-2	-2	1
± 7	1	2	2	1	1	2	2	1
± 9	1	1	1	1	1	1	1	1
± 11	1	-1	-1	1	1	-1	-1	1
± 13	1	-2	-2	1	1	-2	-2	1
± 17	1	2	2	1	1	2	2	1
± 19	1	-1	-1	1	1	-1	-1	1

c_β	± 1	± 3	± 7	± 9	± 11	± 13	± 17	± 19
± 1	1	1	1	1	1	1	1	1
± 3	1	-2	2	1	1	2	-2	1
± 7	1	2	2	-1	-1	2	2	1
± 9	1	1	-1	-1	-1	-1	1	1
± 11	1	1	-1	-1	-1	-1	1	1
± 13	1	2	2	-1	-1	2	2	1
± 17	1	-2	2	1	1	2	-2	1
± 19	1	1	1	1	1	1	1	1

A simple computation shows us that the map $\alpha : G_{\mathbb{Q}}^K \to \mathcal{O}_K^*$ given by the table below has coboundary $c_{E_{125,z,w}} c_\beta^{-1}$.

σ	± 1, ± 19	± 3, ± 17	± 7, ± 13	± 9, ± 11
$\alpha(\sigma)$	1	$\zeta_{40}^{17} + \zeta_{40}^{-17}$	$(\zeta_{40} + \zeta_{40}^{-1})^{-1}$	$(\zeta_{40}^3 + \zeta_{40}^{-3})(\zeta_{40}^9 + \zeta_{40}^{-9})$

It is easy to verify that $\gamma = (\zeta_{40}^1 + \zeta_{40}^{-1})(\zeta_{40}^2 + \zeta_{40}^{-2})(\zeta_{40}^3 + \zeta_{40}^{-3})$ satisfies the equation ${}^\sigma\gamma = \alpha(\sigma)^2\gamma$ for all $\sigma \in G_{\mathbb{Q}}^K$, hence γ is the sought twist. Note that γ and thereby the twist $E_{125,z,w}^\gamma$ are defined over the field $K_0 = \mathbb{Q}(\zeta_{40}^2 + \zeta_{40}^{-2})$ which is the totally real subfield of $\mathbb{Q}(\zeta_{20})$. Some further checking shows that $E_{125,z,w}^\gamma$ is actually completely defined over this field, and the splitting map for $c_{E_{125,z,w}^\gamma}$ factors over $G_{\mathbb{Q}}^{K_0}$ as well.

We compute that the conductor of $E_{125,z,w}^\gamma$ is equal to

$$(64)\, \mathrm{Rad}_{10}\, \Delta_{125,z,w}^\gamma.$$

By computing all the splitting maps $\beta : G_{\mathbb{Q}}^{K_0} \to \overline{\mathbb{Q}}^*$ for $c_{E_{125,z,w}^{\gamma}}$ we find that the restriction of scalars $\mathrm{Res}_{\mathbb{Q}}^{K_0} E_{125,z,w}^{\gamma}$ must be isogenous to a product of two abelian varieties of GL_2-type. The levels of the associated newforms should be

$$\{1280\,\mathrm{Rad}_{10}(w^2 - 125z^4), 6400\,\mathrm{Rad}_{10}(w^2 - 125z^4)\},$$

where we can not a priori determine which level corresponds to which factor. After level lowering we thus obtain newforms of levels 1280 and 6400 which must be twists of one another. The characters of these newforms should be a character of conductor 20 and order 4.

The irreducibility of the mod l representations needed to perform level lowering is obtained from Corollary 5.3.1. For the cases $l = 3, 7, 13$ this is clear. For the cases $l = 11$, $l > 13$ we note that the only points $Q \in E_D(\mathbb{Q}) \setminus \{\mathcal{O}, T\}$ with B_Q not divisible by a prime number $p > 3$ are $\pm P$. For the case $l = 5$ we do not get irreducibility as 125 is the norm of $11 + 2\sqrt{-1}$.

Remark 5.5.1. One could try to use the j-invariant $j_5(x, y)$ presented in Theorem 2.11.1 to prove irreducibility of the mod l representation when $l = 5$. For this one would parameterize the $x, y \in \mathbb{Q}$ with $x^2 + y^2 = 125$ and find the solutions to $j_{125,z,w} = j_5(x, y)$. One will however find that there are infinitely many solutions to this equation.

When we compute the newforms of level 1280 and their twists of level 6400 we end up with 144 newforms. After comparing traces of Frobenius for the primes $p < 50$ with $p \neq 2, 5$ we find that all but 24 newforms can be a priori eliminated for all primes $l > 17$. All of the remaining newforms have coefficient field $\mathbb{Q}(\sqrt{-1})$ and most likely correspond to (pseudo) solutions (z, w). At the very least there will be a newform corresponding to the curve $E_{125,0,1}^{\gamma}$ which corresponds to the point T, so we can not eliminate all newforms without further assumptions.

If we look at the points $mP + T$ with m an odd integer, we note they are all the odd multiples of $P + T = \left(\frac{500}{121}, -\frac{32\,250}{1\,331}\right)$. By (5.3) we have that $11 \mid B_{mP+T}$ for all odd m. If we use this information when computing the traces of Frobenius at 11 we can actually eliminate all newforms for $l > 3$ and $l \neq 11$.

Combining these results we have thus proven the following result. All the computations to obtain this result can be found in `D125.rst`.

Theorem 5.5.2. *The sequence $B_m, m \in \mathbb{Z}_{>0}$ contains no l-th powers with l a prime number when*

- $P_1 = \left(\frac{121}{4}, \pm\frac{1419}{8}\right) \in E_{125}(\mathbb{Q})$ *and $l > 2$; or*
- $P_1 = \left(\frac{500}{121}, \pm\frac{32\,250}{1\,331}\right) \in E_{125}(\mathbb{Q})$ *and $l > 5$ with $l \neq 11$.*

Subsection 5.5.2

Example for $D = -17$

Take $D = -17$, then $E_D(\mathbb{Q})$ has rank 2 with $T = (0, 0)$ as the only non-trivial torsion point. With SageMath [Sag20] we can compute that there is a choice of generators

$$\begin{cases} P = & (-4, 2) \\ Q = & (-1, 4) \\ T = & (0, 0)\,, \end{cases}$$

for which $a_P = a_Q = -1$.

We first study the curve $E_{1,z,w}$, which corresponds to the points $mP + nQ$ with $m, n \in \mathbb{Z}$ and $m + n$ even. We use the twist $E^{\gamma}_{1,z,w}$ from Section 5.4 to get the lowest conductor. The level of the newforms after level lowering will consist of the 2-part and 17-part of this conductor. The 2-part can be read of from Table 5.1, where we apply Remark 5.4.2. Since the conductor exponent at 17 is always 1, we find that the level after level lowering is

$$\begin{cases} 2^8 \cdot 17 & \text{if } \operatorname{ord}_2(w^2 - z^4) = 0 \\ 17 & \text{if } \operatorname{ord}_2(w^2 - z^4) = 8 \\ 2 \cdot 17 & \text{if } \operatorname{ord}_2(w^2 - z^4) > 8. \end{cases}$$

We compute the newforms of these levels and compare traces of Frobenius for all prime numbers $p < 50$ that do not divide $2 \cdot 17$. This eliminates 25 of the 33 newforms of level $2^8 \cdot 17$ for all primes $l > 5$, but none of level 17 or $2 \cdot 17$. The non-eliminated newforms are all rational and the corresponding elliptic curves are geometrically isomorphic to the elliptic curves $E^{\gamma}_{1,z,w}$ corresponding to the points $P - Q$ and $Q - P$, and the pseudo solutions

$$(z, w) = (\pm 12, \pm 145), (\pm 15, \pm 353), (\pm 23, \pm 495).$$

Therefore they can not be eliminated without additional information.

Now look at the non-zero multiples P_m of the point

$$P_1 = 2P + 2Q = \left(\frac{3\,568\,321}{451\,584}, \frac{5\,750\,178\,337}{303\,464\,448} \right).$$

Note that B_1 is divisible by the primes 2, 3, and 7, so by (5.3) all B_m with $m \in \mathbb{Z}$ non-zero are. The fact that $2 \mid B_m$ immediately rules out all newforms of level $2^8 \cdot 17$. Comparing traces of Frobenius at 3 and 7 again using the restriction $3, 7 \mid B_m$ we can now eliminates all newforms for $l > 3$.

Next we study the Frey $\mathbb{Q}$-curve $E^{\gamma}_{-17,z,w}$ (see equation (5.7)) corresponding to points $mP + nQ + T$ with $m+n$ even that have an l-th power in their denominator.

We start with $\gamma = 1$ and find the correct twist later. The curve $E_{-17,z,w}$ is completely defined over $K = \mathbb{Q}(\sqrt{-17}, \sqrt{2})$. We compute that the trivial character could be a splitting character for $E_{-17,z,w}$, hence the square root of the degree map is a splitting map β for $\xi_{E_{-17,z,w}}$. We compute that $c_{E_{-17,z,w}}$ and c_β are given by

$c_{E_{-17,z,w}}$	1	σ_2	σ_{17}	$\sigma_2\sigma_{17}$
1	1	1	1	1
σ_2	1	2	1	2
σ_{17}	1	-1	1	-1
$\sigma_2\sigma_{17}$	1	-2	1	-2

and

c_β	1	σ_2	σ_{17}	$\sigma_2\sigma_{17}$
1	1	1	1	1
σ_2	1	2	1	2
σ_{17}	1	1	1	1
$\sigma_2\sigma_{17}$	1	2	1	2

,

where σ_2 and σ_{17} are generators of $G^K_{\mathbb{Q}(\sqrt{2})}$ and $G^K_{\mathbb{Q}(\sqrt{-17})}$ respectively. Note that the difference $c_{E_{-17,z,w}} c_\beta^{-1}$ can not be the coboundary of a map to $\mathbb{Q}^*$ as it is non-symmetric, hence a change of splitting map does not suffice. Instead we will have to find a twist γ for which we need a map $\alpha : G^K_{\mathbb{Q}} \to K^*$ with coboundary $c_{E_{-17,z,w}} c_\beta^{-1}$.

Using SageMath [Sag20] we can determine that $\mathcal{O}_K^* = \langle -1, \sqrt{2} - 1 \rangle$, so if α would be a map with codomain $\mathcal{O}_K^*$, we can write

$$\alpha(\sigma) = (-1)^{x(\sigma)} (\sqrt{2} - 1)^{y(\sigma)}$$

for some $x, y : G^K_{\mathbb{Q}} \to \mathbb{Z}$. Now we find that

$$\begin{aligned} 1 &= c_{E_{-17,z,w}} c_\beta^{-1}(\sigma_2, \sigma_{17}) = \alpha(\sigma_2)\ {}^{\sigma_2}\alpha(\sigma_{17})\, \alpha(\sigma_2\sigma_{17})^{-1} \\ &= (-1)^{x(\sigma_2) + x(\sigma_{17}) - x(\sigma_2\sigma_{17})}\, (\sqrt{2} - 1)^{y(\sigma_2) - y(\sigma_2\sigma_{17})}\ {}^{\sigma_2}(\sqrt{2} - 1)^{y(\sigma_{17})} \\ &\text{and} \\ -1 &= c_{E_{-17,z,w}} c_\beta^{-1}(\sigma_2, \sigma_{17}) = \alpha(\sigma_{17})\ {}^{\sigma_{17}}\alpha(\sigma_2)\, \alpha(\sigma_2\sigma_{17})^{-1} \\ &= (-1)^{x(\sigma_2) + x(\sigma_{17}) - x(\sigma_2\sigma_{17})}\, (\sqrt{2} - 1)^{y(\sigma_{17}) - y(\sigma_2\sigma_{17})}\ {}^{\sigma_{17}}(\sqrt{2} - 1)^{y(\sigma_2)}. \end{aligned}$$

Since ${}^{\sigma_2}(\sqrt{2} - 1) = \sqrt{2} - 1$ and $(\sqrt{2} - 1)\ {}^{\sigma_{17}}(\sqrt{2} - 1) = -1$ this gives us the linear system

$$\left\{ \begin{array}{llllll} x(\sigma_2) & +x(\sigma_{17}) & -x(\sigma_2\sigma_{17}) & & & \equiv 0 \pmod{2} \\ & & & y(\sigma_2) & +y(\sigma_{17}) \ -y(\sigma_2\sigma_{17}) & = 0 \\ x(\sigma_2) & +x(\sigma_{17}) & -x(\sigma_2\sigma_{17}) & +y(\sigma_2) & & \equiv 1 \pmod{2} \\ & & & -y(\sigma_2) & +y(\sigma_{17}) \ -y(\sigma_2\sigma_{17}) & = 0, \end{array} \right.$$

which is clearly inconsistent. Therefore there can be no map $\alpha : G_{\mathbb{Q}}^{K} \to \mathcal{O}_K^*$ with coboundary $c_{E_{-17,z,w}} c_\beta^{-1}$.

Now look at the map $\alpha : G_{\mathbb{Q}}^{K} \to K^*$ given by

$$\alpha(\sigma) = \begin{cases} 1 & \text{if } \sigma = 1 \\ -1 & \text{if } \sigma = \sigma_2 \\ \frac{1-3\sqrt{2}}{\sqrt{-17}} & \text{otherwise.} \end{cases}$$

A quick computation shows that the coboundary of this map is $c_{E_{-17,z,w}} c_\beta^{-1}$, and that $\gamma = 1 + 3\sqrt{2}$ satisfies ${}^\sigma\gamma = \alpha(\sigma)^2\gamma$ for all $\sigma \in G_{\mathbb{Q}}^{K}$.

Remark 5.5.3. Note that the set S given by Proposition 2.5.5 consists of all the primes above 7 and 17. Therefore the map α confirms the statement as its image is contained in $\mathcal{O}_{K,S}$. It also shows that in some cases we can choose S smaller than in Proposition 2.5.5 as in this case also S consisting of only the primes above 17 would suffice. Furthermore this example shows that also for Frey $\mathbb{Q}$-curves a non-empty S can be necessary.

Remark 5.5.4. Note that

$$1 - \sqrt{-17} = (1 + 3\sqrt{2}) \left(\frac{1}{\sqrt{2}} + \frac{3}{\sqrt{-17}} - \frac{1}{\sqrt{2}\sqrt{-17}} \right)^2,$$

so we could also take $\gamma = 1 - \sqrt{-17}$. The advantage of this is that $E_{-17,z,w}^{\gamma}$ remains defined over $\mathbb{Q}(\sqrt{-17})$ and in fact it is even completely defined over that field. The problem is that $1 - \sqrt{-17}$ is divisible by a prime above 3 in $\mathbb{Q}(\sqrt{-17})$. By Proposition 5.3.2 a 3 will appear in the level after level lowering, which most likely increases the dimension and thus computation time of the space of newforms.

The curve $E_{-17,z,w}^{\gamma}$ remains completely defined over K. The conductor of $E_{-17,z,w}^{\gamma}$ over K is

$$\begin{cases} \mathfrak{p}_2^{16}\,(17)\left(\mathrm{Rad}_{2\cdot 17}(w^2 + 17\,z^4)\right) & \text{if } 2 \mid w \\ \mathfrak{p}_2^{6}\,(17)\left(\mathrm{Rad}_{2\cdot 17}(w^2 + 17\,z^4)\right) & \text{if } 2 \nmid w. \end{cases}$$

Here $\mathfrak{p}_2$ is the unique prime of K above 2. The field generated by the values of β is $\mathbb{Q}(\sqrt{2})$. Since this is quadratic we know that $\mathrm{Res}_{\mathbb{Q}}^{K} E_{-17,z,w}^{\gamma}$ is a product of two $\mathbb{Q}$-simple abelian variety of GL_2-type. The levels of the associated newforms can be computed to be

$$\begin{cases} (2^8 \cdot 17^2 \cdot \mathrm{Rad}_{2\cdot 17}(w^2 + 17\,z^4), 2^8 \cdot 17^2 \cdot \mathrm{Rad}_{2\cdot 17}(w^2 + 17\,z^4)) & \text{if } 2 \mid w \\ (2^5 \cdot 17^2 \cdot \mathrm{Rad}_{2\cdot 17}(w^2 + 17\,z^4), 2^6 \cdot 17^2 \cdot \mathrm{Rad}_{2\cdot 17}(w^2 + 17\,z^4)) & \text{if } 2 \nmid w. \end{cases}$$

So after level lowering the lowest possible levels are $2^8 \cdot 17^2$ if $2 \mid w$ and $2^5 \cdot 17^2$ if $2 \nmid w$. Note that the character of these newforms is trivial as the splitting character for all splitting maps is trivial.

Note that we can apply level lowering when the corresponding mod l Galois representation is irreducible. This is the case for $l = 3, 5, 7, 13$ by Corollary 5.3.1. For $l = 11$ or $l > 13$ we need that the corresponding point $P \in E_D(\mathbb{Q}) \setminus \{\mathcal{O}, T\}$ has B_P divisible by a prime number $p > 3$. The points for which this is not the case can be computed to be

$$\left\{ \begin{array}{c} \pm P, \pm Q, \pm 2P, \pm 2Q, \pm P + T, \pm Q + T, \pm 2Q + T, \pm(P + Q), \\ \pm(P - Q), \pm(2P - 2Q), \pm(P - Q) + T, \pm(P - 2Q) + T \end{array} \right\}.$$

The only perfect powers among the B of these points are $B_{\pm 2P} = B_{\pm 2Q} = 2^2$ and $B_{\pm 2Q + T} = 3^2$. We may thus assume that for odd prime numbers l we have irreducibility.

Computing the newforms of these levels takes a few hours with Magma. Using the framework we find that by comparing traces at the primes

$$\{3, 5, 7, 11, 13, 19, 29, 31, 37, 41, 43, 47, 59, 67, 73, 97, 113\},$$

we can eliminate all but 10 newforms for all primes $l > 31$.

Remark 5.5.5. We have performed the elimination for all prime numbers below 200 besides 2 and 17, but the list given here includes the primes at which elimination actually happened.

The 10 newforms that remain all seem to have complex multiplication and coefficient field $\mathbb{Q}(\sqrt{2})$. They most likely correspond to values of (z, w) corresponding to (pseudo) solutions of the problem. For examples the point T corresponds to the curve $E^{\gamma}_{-17,0,1}$ which in turn corresponds to one of the newforms of level $2^5 \cdot 17^2$.

To avoid these (pseudo-)solutions we look at non-zero multiples P_m of the point $P_1 = P + Q + T$. Since $B_1 = 7$ (5.3) tells us all B_m are divisible by 7. Using this additional information when comparing traces of Frobenius at 7 allows us to eliminate all newforms for $l > 17$. This leads to the following asymptotic result. The code for all computations to obtain this result can be found in `Dm17.rst`.

Theorem 5.5.6. *The sequence B_m, $m \in \mathbb{Z}_{>0}$ contains no l-th powers with l a prime number when $P_1 = P + Q + T = \left(-\frac{153}{49}, \pm\frac{1632}{343}\right) \in E_{-17}(\mathbb{Q})$ and $l > 17$.*

Remark 5.5.7. Besides the methods described here, we also tried to eliminate the newforms for $l = 13$ and $l = 17$ by performing Kraus' method. This did not allow us to eliminate all newforms for these primes.

Subsection 5.5.3

Further examples

Using the framework one can easily compute further asymptotic results as in Theorem 5.5.2 and Theorem 5.5.6. We will not write this out in detail as the approach is very similar. Table 5.3 contains the results of the computations that were performed. The code for these computations can be found in `D125.rst`, `Dm17.rst`, `D3.rst`, and `Dm2.rst`.

case	D	$P_1 \in E_D(\mathbb{Q})$	l
(i)	125	$\left(\frac{121}{4}, \pm\frac{1\,419}{8}\right)$	$l > 2$
(ii)	125	$\left(\frac{500}{121}, \pm\frac{32\,250}{1\,331}\right)$	$l > 5$
(iii)	-17	$\left(-\frac{153}{49}, \pm\frac{1\,632}{343}\right)$	$l > 17$
(iv)	3	$\left(\frac{1}{4}, \pm\frac{7}{8}\right) = 2(3, \pm 6)$	$l > 2$
(v)	3	$\left(\frac{27}{121}, \pm\frac{1\,098}{1\,331}\right) = 3(3, \mp 6)$	$l > 17$
(vi)	-2	$\left(\frac{9}{4}, \pm\frac{21}{8}\right) = 2(-1, \mp 1)$	$l > 2$
(vii)	-2	$\left(-\frac{1}{169}, \pm\frac{239}{2197}\right) = 3(-1, \pm 1)$	$l > 2$
(viii)	-2	$\left(\frac{4\,651\,250}{1\,803\,649}, \pm\frac{8\,388\,283\,850}{2\,422\,300\,607}\right) = 5(-1, \mp 1) + (0,0)$	$l > 5$, $l \neq 79$
(ix)	-2	$\left(-\frac{8}{9}, \pm\frac{28}{27}\right) = 2(-1, \mp 1) + (0,0)$	$l > 3$

Table 5.3: Elliptic divisibility sequences with no l-th powers

Subsection 5.5.4

Small exponent values

While our main focus in this article is bounding prime exponents, a natural next step would be to determine all perfect powers in the elliptic divisibility sequences we consider. It follows immediately from [ERS07, Theorem 1.1] (dealing with any nonsingular Weierstrass equation over $\mathbb{Z}$) that for every integer $l > 1$, our main equation

$$B_m = v^l, \quad m, v \in \mathbb{Z}_{>0} \tag{5.10}$$

has only finitely many solutions. In particular, it suffices to restrict to prime exponents l. We note that this finiteness result is not effective, as it appeals to Faltings' finiteness theorem for rational points on curves of genus greater than one, amongst other things. Using the fact that our elliptic curves E_D

are of a rather special form (5.4), we will now discuss an independent, rather direct, reduction of solving (5.10) for a fixed integer $l > 1$ to finding $\mathbb{Q}$-rational points on finitely many hyperelliptic curves over $\mathbb{Q}$ of genus $2l - 1 > 1$ (or hyperelliptic quotients thereof of smaller genus). In general this approach would lead again, by Faltings' theorem, to an ineffective finiteness result for fixed exponents in (5.10). But in favourable cases it could fall within the scope of effective methods for determining rational points on (hyperelliptic) curves, though we shall not investigate this much in this chapter.

Fix some integer $l > 1$. For the construction, we start by recalling that (5.5), with $\hat{B} =: z$ and $B = B_m = v^l$, leads to a generalized Fermat equation of signature $(2, 4, 4l)$, namely

$$w^2 = az^4 + \hat{a}v^{4l}, \tag{5.11}$$

to be solved in pairwise coprime (positive) integers w, z, v. We remark that the sum of the reciprocals of the exponents satisfy $1/2 + 1/4 + 1/(4l) < 1$, so by [DG95, Theorem 2] there are only finitely many solutions, where once again the proof reduces the finiteness to Faltings' theorem. Now instead of considering (5.11) of signature $(2, 4, l)$, which leads to our Frey $\mathbb{Q}$-curve construction, we will consider it of signature $(2, 2, 4l)$, i.e., setting $u := z^2$, we get

$$w^2 = au^2 + \hat{a}v^{4l} \tag{5.12}$$

to be solved in pairwise coprime (positive) integers w, u, v. Since $1/2 + 1/2 + 1/(4l) > 1$, it is a *spherical* generalized Fermat equation, which yields that the solutions are given by finitely many parametrizations. More precisely, there exist finitely many, say r, triples of separable binary forms $F_i, G_i, H_i \in \mathbb{Z}[r, s]$ $(i = 1, 2, \ldots, r)$ of degrees $4l, 4l, 2$ respectively, satisfying $F_i^2 = aG_i^2 + \hat{a}H_i^{4l}$, and such that for any pairwise coprime integer solution (w, u, v) to (5.12) there exists an index i and coprime integers r, s such that $(F_i(r, s), G_i(r, s), H_i(r, s)) = (w, u, v)$. This means that a pairwise coprime solution (w, z, v) to the original equation (5.11) satisfies $z^2 = G_i(r, s)$ for some index i. Each of these equations defines a hyperelliptic curve

$$C_i : z^2 = G_i(r, s) \tag{5.13}$$

over $\mathbb{Q}$ in weighted projective space (of weights $1, 1, 2l$ for r, s, z respectively) of genus $2l - 1$ (since the G_i are separable). The C_i have some interesting quotients that might be helpful in determining the rational points $C_i(\mathbb{Q})$.

Example 5.5.8. We look at the elliptic divisibility sequence from Subsection 5.5.1, where $D = 125$ and we choose $P = (121/4, \pm 1419/8)$. We note that we have $a = 1$, and hence $\hat{a} = 125$, in (5.11) for solutions to (5.10). We can perform an elementary descent over $\mathbb{Z}$ to obtain sufficiently many hyperelliptic curves C_i as in (5.13) by rewriting (5.11) as $(w + z^2)(w - z^2) = 5^3 v^{4l}$. Recall that we have $2|B_m$. Hence $2|v$, which leads to $\gcd(w + z^2, w - z^2) = 2$. Without loss of generality we can and will assume $w > 0$, which now leads to

$$w + z^2 = 2c_2c_5\alpha^{4l}, \qquad w - z^2 = 2c_2'c_5'\beta^{4l}$$

for some $\alpha, \beta \in \mathbb{Z}$ and $\{c_2, c_2'\} = \{1, 2^{4l-2}\}, \{c_5, c_5'\} = \{1, 5^3\}$. Subtracting the second equation from the first and dividing by 2 yields equations for our hyperelliptic curves:

$$C_i : z^2 = c_2c_5\alpha^{4l} - c_2'c_5'\beta^{4l} \tag{5.14}$$

for $i = 1, 2, 3, 4$, say by choosing $(c_2, c_5) = (1, 1), (1, 5^3), (2^{4l-2}, 1), (2^{4l-2}, 5^3)$ respectively (which then also fixes the corresponding (c_2', c_5')).

As indicated by Theorem 5.5.2, the only (prime) exponent left to deal with is $l = 2$, so let us fix this value for the rest of this example. The hyperelliptic curves C_i are of genus 3 and one easily obtains that $C_2(\mathbb{Q}) = \emptyset$ by checking locally that $C_2(\mathbb{Q}_2) = \emptyset$. On all of the other 3 curves one can easily spot some $\mathbb{Q}$-rational point. All curves have genus 2 quotients, of which the jacobians all turn out to have rank 2, so that Chabauty-Coleman does not immediately apply to find all rational points. The equations invite some further descent, but we will not pursue determining $C_i(\mathbb{Q})$ for $i = 1, 3, 4$ further here.

As a final note, equations for the $l = 2$ case can also be obtained by considering (5.11) of signature $(2, 4, 2)$, whose solutions can again be parametrized. This leads to finitely many binary quartic forms $E_i \in \mathbb{Z}[s, t]$ such that solutions to the original equation are given by $v^4 = E_i(s, t)$, which define projective plane quartic curves.

Subsection 5.5.5

Alternative approaches for some examples

Consider any elliptic curve $E/\mathbb{Q}$ (in Weierstrass form with integral coefficients) and non-torsion point $P = (x, y) \in E(\mathbb{Q})$ with the denominator of x divisible by $p \in \{2, 3\}$. Reynolds associates in [Rey12] a Frey elliptic curve over $\mathbb{Q}$ (depending on p) to our Diophantine problem of interest (5.10). Together with Silverman's famous result on the existence of primitive divisors [Sil88] it is then shown that there exists an effective bound l_0 such that for all primes $l \geq l_0$ there are no solutions to (5.10); see Theorem 1.2 in *loc. cit.* (where again it is also noted that consequently (B_m) contains only finitely many perfect powers).

The cases (i), (iv), (vi), and (ix) from Table 5.3 fall in this category. The Frey curve mentioned above is actually associated to the elliptic divisibility subsequence for pP. As such, for cases (v) and (vii) from Table 5.3 there is also an alternative approach using Frey curves over $\mathbb{Q}$. This leaves cases (ii), (iii), and (viii) for which there does not seem to be alternative approaches available in the literature.

In the case that a is a positive non-square, the Frey curve $E_{a,z,w} = E^1_{a,z,w}$ is defined over a totally real field $\mathbb{Q}(\sqrt{a})$. As an alternative to the $\mathbb{Q}$-curve approach we could therefore use modularity of elliptic curves over totally real quadratic fields ([FLHS15]) and perform the modular method with the associated Hilbert modular forms. Furthermore one could try to combine the $\mathbb{Q}$-curve approach with this approach as a multi-Frey method.

We have tried to apply this Hilbert modular approach to some examples. In the case $a = D = 3$ this did not lead to any additional information. For larger D the levels of the Hilbert modular forms became too large to feasibly compute the corresponding newforms.

Chapter 6

Discussion

Throughout this dissertation we discussed how the modular method for Frey $\mathbb{Q}$-curves can be automated and how this automation has been implemented in the framework [vL21a]. We have also seen how this automation has successfully been used to prove some new Diophantine results in Chapter 4 and Chapter 5. Especially in Chapter 5 we saw how the framework [vL21a] can easily be applied to more examples of elliptic divisibility sequences. This shows the true potential of the framework [vL21a]: Given a Frey $\mathbb{Q}$-curve for a Diophantine equation, compute the conclusions that can be obtained from applying the modular method automatically.

Although the framework [vL21a] has been carefully put together, the coding of the various parts could still be prone to human error. Therefore the framework [vL21a] has repeatedly been tested using the various examples from the literature (see Table 3.1). Furthermore the implementation of Tate's algorithm from Chapter 1 has been checked by using random samples of 10 000 elliptic curves from the Cremona database as an input, as well as various elliptic curves over number fields. Also many functions and classes in the framework [vL21a] come with doctests that ensure these work as intended.

Future improvements to ensure the framework [vL21a] works as intended could include using Python3's typing module to type check functions. Another approach would be to verify the algorithms themselves, rather than their implementation, using a formal theorem prover such as Lean [dMKA$^+$15] or Coq [Coq20]. Note that to fully verify the correctness of the algorithms presented here would also require formal proofs of various arithmetic geometry results. A partial result might be feasible, especially considering the rapid growth in Lean's "mathlib" library [mC20], to which the author of this dissertation also made a small contribution.

As already mentioned in Section 1.7.2 there might be various optimizations for Tate's algorithm as implemented in the framework [vL21a]. As mentioned there a rewriting of the algorithm as presented in Section 1.1 to use checks of type 2 rather than type 1 (see Section 1.2) could lower the precision and thus computation time required, but would require a careful rethinking of the current approach. A more feasible speedup would be to implement $\mathfrak{p}$-adic trees (see Section 1.4) in a lower level language, which could also reduce its memory footprint.

In this dissertation we focused on Frey $\mathbb{Q}$-curves, but the framework [vL21a] is also capable of working with Frey curves over totally real fields and imaginary quadratic fields. As mentioned in Section 3.2 the method `newform_candidates` of such a Frey curve E/K actually computes the corresponding Hilbert or Bianchi modular forms, but one should note the correspondence is only conjectural if the field K is not totally real or of degree > 3. Nevertheless one can compute with the corresponding newforms and compare traces of Frobenius to find the result the modular method could (conjecturally) prove. This can also be applied to Frey $\mathbb{Q}$-curves that are defined over real quadratic fields such as discussed in Section 4.5 and Section 5.5.5, possibly even using a multi-Frey approach with both classical and Hilbert modular forms. The spaces of Hilbert modular forms in the examples in Chapter 4 and Chapter 5 were too big to do this, but this would be an interesting approach for new examples.

Besides utilising the additional functionality of the framework [vL21a] for new Diophantine problems, the functionality of the framework could also be further expanded. For example besides comparing traces of Frobenius one could include other methods for eliminating newforms, like image of inertia arguments or special properties related to complex multiplication. This could potentially take care of eliminating the newforms corresponding to (pseudo-)solutions in Section 5.5, as they seem to correspond to CM curves.

Ideally the framework [vL21a] would also be further automated. Theorem 2.11.1 and other irreducibility results could be implemented such that the framework [vL21a] automatically detects whether such results apply and prints which cases should be proved by hand otherwise. Another automation step would be to include various recipes for the construction of Frey curves from Diophantine equations, such that the user input does not have to include a Frey curve necessarily. A perfect framework would allow a user to input a Diophantine equation and automatically obtain the results the modular method could prove about it.

Summary

This dissertation discusses the modular method for Frey $\mathbb{Q}$-curves and applies this method to a few new Diophantine problems. In particular it focuses on how certain steps in the modular method can be automated, such that the entire process can easily be applied to a Diophantine equation. This includes both the theory to automate this process as well as an actual implementation as a Python package for SageMath [Sag20].

An important step in applying the modular method is the computation of the conductor of a Frey curve. A careful look at Tate's algorithm shows that the algorithm can also be applied to Frey curves, but in that case each step of the algorithm might have two distinct results based on the value of the parameters. By applying Hensel lifting and keeping track of the cases – in what we call $\mathfrak{p}$-adic trees – Chapter 1 demonstrates that Tate's algorithm can be automated for Frey curves to compute the conductor exponent at a prime.

The modularity of $\mathbb{Q}$-curves relates a classical newform to a $\mathbb{Q}$-curve through an abelian variety of GL_2-type. Chapter 2 discusses the theory behind this and explains how to compute the level and character of these newforms from this theory and the conductor computation from Chapter 1. This requires the computation of splitting maps, splitting characters, and the degree map, as well as a potential twist of the original curve, which can all be computed one from the other with some input data about isogenies of the $\mathbb{Q}$-curve. The chapter also establishes Galois representations associated with $\mathbb{Q}$-curves and shows how to compute the traces of Frobenius elements under these representations.

By applying this theory and level lowering results one can compute newforms associated with Frey $\mathbb{Q}$-curves of which the level does not depend on the particular value of the parameters anymore. Chapter 3 outlines this procedure and shows a few tactics to then eliminate newforms based on comparing their Galois representation with the corresponding Galois representation of the Frey $\mathbb{Q}$-curve.

Chapter 4 shows that the Diophantine equation $(x-y)^4 + x^4 + (x+y)^4 = z^n$ has no integer solutions (x, y, z, n) with $\gcd(x, y) = 1$ and $n > 1$. It is shown that a particular Hilbert modular approach seems unfeasible for this equation,

but that the automated $\mathbb{Q}$-curve approach works on the same Frey curves to show no solutions exist when $n > 5$ is prime. The cases where $n = 2, 3, 5$ are shown separately.

Chapter 5 considers perfect powers in elliptic divisibility sequences generated by $\mathbb{Q}$-points on an elliptic curve of j-invariant 1728. The automated approach is applied to various such examples to prove the non-existence of l-th powers with $l > l_0$ a prime number, and l_0 dependent on the sequence.

Acknowledgements

I would like to thank my supervisor, Sander Dahmen, for giving me the opportunity to do this PhD trajectory. I would also like to thank him for our weekly meetings in which he gave guidance and help during my PhD years. Thanks to him and my promotor, Rob de Jeu, for being the first to read my thesis and provide useful feedback.

I would like to thank some other people that were around during my PhD years at the VU. Thanks to Thomas for his sphere facts. Thanks to Patrick for being around on Friday nights although he finished his PhD already. Thanks to Ray for also being annoyed with the linear algebra book. Thanks to Eddie for being Eddie. Thanks to Chris for being a wizard. Thanks to Elena for being a great office mate in my first year. Thanks to Jan-David for teaching me how to play Go. Thanks to Gosse for being a Go opponent at my level. Thanks to Bente for allying with Russia. Thanks to Wouter for checking whether all my cupboards soft-closed. Thanks to Casper for sharing a huge office with me. Thanks to Pepijn for his sarcastic world view. Thanks to Niek for reminding us that climate change is an important issue. Thanks to Michael & Michael for reintroducing Magic at the VU. Thanks to Fabio for replacing me in the PhD council. Thanks to Ronen for inspiring me to create a PhD Dungeons & Dragons group. Also thanks to all the others for which I do not have a personal line, but whose company I enjoyed during lunch, cookie breaks, or Friday night drinks.

I would also like to thank my family and friends for the support they have given me throughout my PhD. I did not always find it easy to stay motivated, especially during the pandemic, but I am glad they provided listening ears and welcome distractions. Most of all I want to thank my Father in heaven, who always believed in me.

Appendix A

Proof of Theorem 2.9.8

In this appendix we will give the proof of Theorem 2.9.8. This will include some preliminary results. First we need the family of matrices

$$S_M^\lambda = \begin{bmatrix} M & \lambda \\ 0 & M \end{bmatrix} \text{ for } \lambda, M \in \mathbb{Z} \text{ and } M > 0.$$

Each matrix S_M^λ satisfies a useful property.

Lemma A.1. *For any matrix* $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z})$ *and* $M, \lambda, \mu \in \mathbb{Z}$ *with* $M > 0$ *we have that*

$$S_M^\lambda \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a + \mu \frac{c}{M} & b + \frac{1}{M}\left(\lambda d - \mu a - \lambda \mu \frac{c}{M}\right) \\ c & d - \mu \frac{c}{M} \end{bmatrix} S_M^\mu.$$

All matrices in this equation have integer coefficients if and only if

1. $M \mid c$*, and*
2. $\mu\left(a + \lambda \frac{c}{M}\right) \equiv d\lambda$ *(mod* M*).*

Furthermore for particular matrices we show equivalent conditions for which the conditions in Lemma A.1 are satisfied.

Lemma A.2. *Let* M *be a positive integer and* $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(M)$*. For any* $\lambda \in \mathbb{Z}$ *the following statements are equivalent*

1. *There exists a* $\mu \in \mathbb{Z}$ *such that*

$$\mu\left(a + \lambda \frac{c}{M}\right) \equiv d\lambda \quad (\text{mod } M). \tag{A.1}$$

2. *There exists a* $\mu \in \mathbb{Z}$*, unique modulo* M*, satisfying Equation* (A.1).

3. We have $\gcd\left(a + \lambda\frac{c}{M}, M\right) = 1$*.*

Proof. Note that any equation of the form $\alpha x \equiv \beta \pmod{M}$ has a solution $x \in \mathbb{Z}$ if and only if $\gcd(\alpha, M) \mid \beta$. The solution is unique modulo M if and only if $\gcd(\alpha, M) = 1$. Almost all equivalences are therefore clear and we only have to prove that $\delta = 1$ if $\delta = \gcd\left(a + \lambda\frac{c}{M}, M\right) \mid d\lambda$.

Note that $ad = 1 - bc \equiv 1 \pmod{M}$, hence a and d are units modulo M. Since $\delta \mid M$ by definition and assuming that $\delta \mid d\lambda$ we find that $\delta \mid \lambda$. We know that $\delta \mid a + \lambda\frac{c}{M}$ by definition, hence by the previous argument we have $\delta \mid a$, but a is coprime with M. Therefore we can conclude that $\delta = 1$ and finish the proof. □

Next we introduce $S = S_1^1$ and some operators on cuspforms. For this let $F \in \mathcal{S}_k(N, \varepsilon)$.

- For any 2-by-2 matrix

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

  with integer entries we define the modular form $F|_A$ by

  $$F|_A(\tau) = (\det A)^{k/2}\,(c\tau + d)^{-k}\,F(A\tau).$$

  Note that this operation satisfies $F|_{AB} = F|_A|_B$ for any $A, B \in M_2(\mathbb{Z})$.

- For any Dirichlet character χ of conductor M define

  $$F|_{\mathcal{R}_\chi} = \sum_{\mu \pmod{M}} \overline{\chi}(\mu) F|_{S_M^\mu}.$$

  This is well-defined as for any $\mu \equiv \mu' \pmod{M}$ we have that $\overline{\chi}(\mu) = \overline{\chi}(\mu')$ and $S_M^\mu = S^k S_M^{\mu'}$ for some $k \in \mathbb{Z}$, where we have $F|_S = F$ as $S \in \Gamma_1(N)$.

The operator $\mathcal{R}_\chi$ is special as

$$F|_{\mathcal{R}_\chi} = g(\overline{\chi})\,{}^\chi F,$$

where $g(\overline{\chi})$ is the Gauss sum of the complex conjugate $\overline{\chi}$ of χ, and ${}^\chi F$ is the twist of F by χ, as was noted on page 227 of [AL78]. This implies that to determine the level, character and degree of the newform ${}^\chi F$ we may as well look at the cuspform $F|_{\mathcal{R}_\chi}$.

We now have the ingredients to prove Theorem 2.9.8. First we prove part (1) in a more general context.

Proposition A.3. *Let $F \in \mathcal{S}_k\left(\Gamma_1\left(N\right), \varepsilon\right)$ and let χ be a Dirichlet character with conductor $M = \prod p_i^{e_i}$, with p_i distinct primes. If $\varepsilon\chi$ has conductor M', then the twist ${}^\chi F$ of F by χ is a cusp form of level $\tilde{N} = \operatorname{lcm}(N, \prod p_i^{e_i+1}, M'M)$ with character $\varepsilon\chi^2$ and weight k.*

Proof. Pick an arbitrary matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(\tilde{N})$. Note that a is a unit modulo M as $ad \equiv ad - bc = 1 \pmod{\tilde{N}}$, and that c/M is divisible by every prime dividing M. We thus find that $\gcd\left(a + \lambda\frac{c}{M}, M\right) = \gcd(a, M) = 1$ for each $\lambda \in \mathbb{Z}$ and thus each $\lambda \in \mathbb{Z}$ satisfies the equivalent conditions of Lemma A.2. Therefore for any $\lambda \pmod M$ there is a unique $\mu \pmod M$ such that we have $\mu\left(a + \lambda\frac{c}{M}\right) \equiv d\lambda \pmod M$. By Lemma A.1 we have a matrix $B_\lambda \in M_2(\mathbb{Z})$ such that $S_M^\lambda A = B_\lambda S_M^\mu$ for each such a pair λ and μ. Note furthermore that the map sending λ to a corresponding μ is a bijection, since for any μ the corresponding λ is the solution to $\lambda\left(d - \mu\frac{c}{M}\right) \equiv a\mu \pmod M$, which by an analoguous argument as that of Lemma A.2 is unique.

We thus find that

$$\begin{aligned}
F|_{\mathcal{R}_\chi}|_A &= \sum_{\lambda \pmod M} \overline{\chi}(\lambda) F|_{S_m^\lambda A} \\
&= \chi(d) \sum_{\lambda \pmod M} \overline{\chi}(d\lambda) F|_{B_\lambda S_m^\mu} \\
&= \chi(d) \sum_{\lambda \pmod M} \overline{\chi}\left(\mu\left(a + \lambda\frac{c}{M}\right)\right) \varepsilon\left(d - \mu\frac{c}{M}\right) F|_{S_m^\mu} \\
&= \chi(d) \sum_{\lambda \pmod M} \chi\left(d - \mu\frac{c}{M}\right) \varepsilon\left(d - \mu\frac{c}{M}\right) \overline{\chi}(\mu) F|_{S_m^\mu} \\
&= \chi(d) \sum_{\mu \pmod M} (\chi\varepsilon)\left(d - \mu\frac{c}{M}\right) \overline{\chi}(\mu) F|_{S_m^\mu} \\
&= (\varepsilon\chi^2)(d) \sum_{\mu \pmod M} \overline{\chi}(\mu) F|_{S_m^\mu} \quad = (\varepsilon\chi^2)(d) F|_{\mathcal{R}_\chi},
\end{aligned}$$

where we also used that

$$\left(a + \lambda\frac{c}{M}\right)\left(d - \mu\frac{c}{M}\right) = ad + \frac{c}{M}\left(\lambda d - \mu\left(a + \lambda\frac{c}{M}\right)\right) \equiv 1 \pmod M.$$

□

Proof of Theorem 2.9.8. Part 1) is just Proposition A.3 in this context.

For part 2), let $q'|M$ be any prime divisor and suppose that $F|_{\mathcal{R}_\chi}$ is of level $q^{\delta'}Mq'^{-1}$. Applying part 1) again shows that $F|_{\mathcal{R}_\chi}|_{\mathcal{R}_{\overline{\chi}}}$ is of level $q^{\delta'}Mq'^{-1}$. Note that this form differs from F by a constant, hence F must be of a level that divides both $q^{\delta'}Mq'^{-1}$ and N, but that would divide Nq'^{-1}. Since F is a newform this is a contradiction.

For part 3) first suppose that $F|_{\mathcal{R}_\chi}$ is of level $q^{\delta'-1}M$. By part 1) this implies that $F|_{\mathcal{R}_\chi}|_{\mathcal{R}_{\overline{\chi}}}$ is of level $q^{\delta''}M$, where

$$\delta'' = \max\{\delta'-1, \beta+1, \beta+\gamma\} = \max\{\delta-1, \max\{\beta+1, \beta+\gamma\}\}.$$

Note that this must be divisible by the level of F, hence $\delta \leq \delta''$ implying that $\delta \leq \max\{\beta+1, \beta+\gamma\}$. This proves that the level of $F|_{\mathcal{R}_\chi}$ is not $q^{\delta'-1}M$ if $\delta > \max\{\beta+1, \beta+\gamma\}$.

For the rest of the proof we may assume that $\gamma \geq 1$. Again we assume that $F|_{\mathcal{R}_\chi}$ is of level $q^{\delta'-1}M$ and do some calculation, wherein we will use the matrices

$$\begin{aligned} A_v &= \begin{bmatrix} 1 & 0 \\ vq^{\delta'-1}M & 1 \end{bmatrix} \\ B_{v,\mu} &= \begin{bmatrix} 1-\mu v q^{\delta'-\beta-1}M & q^{-\beta}\left(\lambda-\mu-\lambda\mu v q^{\delta'-\beta-1}M\right) \\ vq^{\delta'-1}M & 1+\lambda v q^{\delta'-\beta-1}M \end{bmatrix}, \end{aligned}$$

where $B_{v,\mu}$ is the matrix in Lemma A.1 such that $S^\lambda_{q^\beta}A_v = B_{v,\mu}S^\mu_{q^\beta}$. We get that

$$\begin{aligned} qF|_{\mathcal{R}_\chi} &= \sum_{v \pmod q} F|_{\mathcal{R}_\chi A_v} \\ &= \sum_{v \pmod q} \sum_{\lambda \pmod{q^\beta}} \overline{\chi}(\lambda) F|_{S^\lambda_{q^\beta}A_v} \\ &= \sum_{\substack{v,\lambda \\ q \,|\, 1+\lambda v q^{\delta'-\beta-1}M}} \overline{\chi}(\lambda) F|_{S^\lambda_{q^\beta}A_v} + \sum_{\substack{v,\lambda \\ q \,\nmid\, 1+\lambda v q^{\delta'-\beta-1}M}} \overline{\chi}(\lambda) F|_{S^\lambda_{q^\beta}A_v} \end{aligned}$$

Note that the matrix A_v in the second sum satisfies the conditions of Lemma A.2, hence we can apply Lemma A.1 and rewrite this sum as

$$\begin{aligned} \sum_{\substack{v,\lambda \\ q \,\nmid\, 1+\lambda v q^{\delta'-\beta-1}M}} \overline{\chi}(\lambda) F|_{S^\lambda_{q^\beta}A_v} &= \sum_{\substack{v,\mu \\ q \,\nmid\, 1-\mu v q^{\delta'-\beta-1}M}} \overline{\chi}(\mu)\chi(1-\mu v q^{\delta'-\beta-1}M) F|_{B_{v,\mu}S^\mu_{q^\beta}} \\ &= \sum_{\mu \pmod{q^\beta}} \overline{\chi}(\mu) \sum_{v \pmod q} (\varepsilon\chi)(1-\mu v q^{\delta'-\beta-1}M) F|_{S^\mu_{q^\beta}}. \end{aligned}$$

Here we have returned to the sum over all μ and all v, since for any combination of μ and v with $q \mid 1 - \mu v q^{\delta'-\beta-1}M$ we have that $\chi(1 - \mu v q^{\delta'-\beta-1}M) = 0$. Since $\delta \leq \max\{\beta+1, \beta+\gamma\}$ we know that $\delta' = \max\{\beta+1, \beta+\gamma\}$. As $\gamma \geq 1$ this implies that

$$\sum_{v \pmod q} (\varepsilon\chi)(1 - \mu v q^{\delta'-\beta-1}M) = \sum_{v \pmod q} (\varepsilon_q\chi)(1 - \mu v q^{\gamma-1}M).$$

Note that in the latter sum the values at which $\varepsilon_q\chi$ is computed are those in the kernel of the map $(\mathbb{Z}/q^\gamma\mathbb{Z})^* \to \left(\mathbb{Z}/q^{\gamma-1}\mathbb{Z}\right)^*$. Note that as $\varepsilon_q\chi$ has conductor q^γ it must map this kernel to a non-trivial subgroup, hence the sum sums (possibly multiple times) over a non-trivial subgroup of roots of unity. Such sums are zero, giving us the result we want in this case.

What thus remains is the sum

$$\sum_{\substack{v,\lambda \\ q \,\mid\, 1+\lambda v q^{\delta'-\beta-1}M}} \overline{\chi}(\lambda) F|_{S^\lambda_{q^\beta} A_v},$$

which we claim to be zero in both the remaining cases, leading to the necessary contradiction to prove 3b) and 3c). If we are in case b this is obvious, since we then have $\delta' > \beta + 1$, hence $1 + \lambda v q^{\delta'-\beta-1}M \equiv 1 \pmod q$.

What remains is case 3c), in which case $\alpha = \beta = \gamma = \delta = 1$ and hence $\delta' = 2$. In this case we know that if $q \mid 1 + \lambda v q^{\delta'-\beta-1}M = 1 + \lambda v M$ then

$$S^\lambda_{q^\beta} A_v = \begin{bmatrix} 1+\lambda v M & \lambda \\ vN & q \end{bmatrix} \begin{bmatrix} q & 0 \\ 0 & 1 \end{bmatrix}.$$

The left matrix on the right hand side is of the special form mentioned in Proposition 1.1 in [AL78], hence we can rewrite the sum as

$$\begin{aligned} \sum_{\substack{v,\lambda \\ q \,\mid\, 1+\lambda v M}} \overline{\chi}(\lambda) F|_{S^\lambda_{q^\beta} A_v} &= \sum_{\substack{v,\lambda \\ q \,\mid\, 1+\lambda v M}} \overline{\chi}(\lambda)\overline{\varepsilon_q}(\lambda)\overline{\varepsilon_M}\left(\frac{1+\lambda v M}{q}\right) F|_W \\ &= \left(\sum_{\substack{v,\lambda \\ q \,\mid\, 1+\lambda v M}} \overline{\chi\varepsilon_q}(\lambda) \right) \varepsilon_M\,(q)\, F|_W, \end{aligned}$$

where

$$W = W_q \begin{bmatrix} q & 0 \\ 0 & 1 \end{bmatrix}.$$

for $W_q = W_Q$ the matrix as in Proposition 1.1 of [AL78] and where we use that

$$q\frac{1 + \lambda M}{q} = 1 + \lambda M \equiv 1 \pmod{M},$$

so $\frac{1+\lambda M}{q} \equiv q^{-1}$ modulo M. Note that the remaining sum sums over all λ modulo q exactly once, and since $\overline{\chi \varepsilon_q}$ has conductor q^γ with $\gamma = 1$ the result is zero as needed. This completes the proof. □

Bibliography

[AL78] A. O. L. Atkin and Wen Ch'ing Winnie Li. Twists of newforms and pseudo-eigenvalues of W-operators. *Inventiones Mathematicae*, 48(3):221–243, 1978.

[AM04] Alejandro Adem and R. James Milgram. *Cohomology of Finite Groups.* Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[AP19] Alejandro Argáez-García and Vandita Patel. On perfect powers that are sums of cubes of a three term arithmetic progression. *Journal of Combinatorics and Number Theory*, 10(3):147–160, 2019.

[BC12] Michael A. Bennett and Imin Chen. Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$. *Algebra & Number Theory*, 6(4):707–730, 2012.

[BCDY14] Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani. On the equation $a^3 + b^{3n} = c^2$. *Acta Arithmetica*, 163(4):327–343, 2014.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BMS08] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. A multi-Frey approach to some multi-parameter families of diophantine equations. *Canadian Journal of Mathematics*, 60(3):491–519, 2008.

[BPS16] Michael A. Bennett, Vandita Patel, and Samir Siksek. Superelliptic equations arising from sums of consecutive powers. *Acta Arithmetica*, 172(4):377–393, 2016.

[Car89] Henri Carayol. Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires. *Duke Mathematical Journal*, 59(3):785 – 801, 1989.

[Che10] Imin Chen. On the equation $a^2 + b^{2p} = c^5$. *Acta Arithmetica*, 143(4):345–375, 2010.

[Che12] Imin Chen. On the equations $a^2 - 2b^6 = c^p$ and $a^2 - 2 = c^p$. *LMS Journal of Computation and Mathematics*, 15:158–171, 2012.

[Coq20] The Coq Development Team. The Coq Proof Assistant, version 8.11.0. `https://doi.org/10.5281/zenodo.3744225`, January 2020.

[Dah08] Sander R. Dahmen. *Classical and modular methods applied to Diophantine equations*. PhD thesis, Universiteit Utrecht, 2008.

[Dar93] Henri Darmon. The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$. *International Mathematics Research Notices*, 1993(10):263–274, 05 1993.

[DD15] Tim Dokchitser and Vladimir Dokchitser. Local invariants of isogenous elliptic curves. *Transactions of the American Mathematical Society*, 367(6):4339–4358, 2015.

[DF14] Luis Dieulefait and Nuno Freitas. The Fermat-type equations $x^5 + y^5 = 2z^p$ or $3z^p$ solved through $\mathbb{Q}$-curves. *Mathematics of Computation*, 83(286):917–933, 2014.

[DG95] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *The Bulletin of the London Mathematical Society*, 27(6):513–543, 1995.

[Dia97] Fred Diamond. The refined conjecture of Serre. In *Elliptic Curves, Modular Forms & Fermat's Last Theorem (Hong Kong)*, pages 172–186. International Press, second edition, 1997.

[DM97] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's last theorem. *Journal für die Reine und Angewandte Mathematik*, 490:81–100, 1997.

[dMKA$^+$15] Leonardo Mendonça de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn, and Jakob von Raumer. The Lean theorem prover (system description). In Amy P. Felty and Aart Middeldorp, editors, *Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany,* *August 1-7, 2015, Proceedings*, volume 9195 of *Lecture Notes in Computer Science*, pages 378–388. Springer, 2015. `https://leanprover.github.io/`.

[DNS20] Maarten Derickx, Filip Najman, and Samir Siksek. Elliptic curves over totally real cubic fields are modular. *Algebra & Number Theory*, 14(7):1791–1800, 2020.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, 2005.

[DU09] Luis Dieulefait and Jorge Jiménez Urroz. Solving Fermat-type equations via modular $\mathbb{Q}$-curves over polyquadratic fields. *Journal für die Reine und Angewandte Mathematik*, 633:183–195, 2009.

[Ell04] Jordan S. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *American Journal of Mathematics*, 126(4):763–787, 2004.

[ERS07] Graham Everest, Jonathan Reynolds, and Shaun Stevens. On the denominators of rational points on elliptic curves. *Bulletin of the London Mathematical Society*, 39(5):762–770, 2007.

[FLHS15] Nuno Freitas, Bao V. Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular. *Inventiones Mathematicae*, 201(1):159–206, 2015.

[FS15] Nuno Freitas and Samir Siksek. The asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields. *Compositio Mathematica*, 151(8):1395–1415, 2015.

[Kou19] Angelos Koutsianas. On the solutions of the Diophantine equation $(x-d)^2 + x^2 + (x+d)^2 = y^n$ for d a prime power. *arXiv e-prints*, May 2019.

[KP18] Angelos Koutsianas and Vandita Patel. Perfect powers that are sums of squares in a three term arithmetic progression. *International Journal of Number Theory*, 14(10):2729–2735, 2018.

[Kra98] Alain Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experimental Mathematics*, 7(1):1–13, 1998.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (I). *Inventiones Mathematicae*, 178(3):485–504, 2009.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (II). *Inventiones Mathematicae*, 178(3):505–586, 2009.

[mC20] The mathlib Community. The Lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP 2020, page 367–381, New York, NY, USA, 2020. Association for Computing Machinery.

[Mil72] J. S. Milne. On the arithmetic of abelian varieties. *Inventiones Mathematicae*, 17:177–190, 1972.

[Pap93] I. Papadopoulos. Néron classification of elliptic curves where the residual characteristics equal 2 or 3. *Journal of Number Theory*, 44(2):119 – 152, 1993.

[Pat18] Vandita Patel. Perfect powers that are sums of consecutive squares. *Mathematical Reports of the Academy of Science. The Royal Society of Canada*, 40(2):33–38, 2018.

[PS17] Vandita Patel and Samir Siksek. On powers that are sums of consecutive like powers. *Research in Number Theory*, 3:Art. 2, 7, 2017.

[Que00] Jordi Quer. $\mathbb{Q}$-curves and abelian varieties of GL_2-type. *Proceedings of the London Mathematical Society. Third Series*, 81(2):285–317, 2000.

[Que01] Jordi Quer. Embedding problems over abelian groups and an application to elliptic curves. *Journal of Algebra*, 237(1):186–202, 2001.

[Rey12] Jonathan Reynolds. Perfect powers in elliptic divisibility sequences. *Journal of Number Theory*, 132(5):998–1015, 2012.

[Rib90] Kenneth A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Inventiones Mathematicae*, 100(1):431–476, 1990.

[Rib94] Kenneth A. Ribet. Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In *Motives (Seattle, WA, 1991)*, volume 55.2 of *Proceedings of Symposia in Pure Mathematics*, pages 639–676. American Mathematical Society, Providence, RI, 1994.

[Rib04] Kenneth A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Modular Curves and Abelian Varieties*, volume 224 of *Progress in Mathematics*. Birkhäuser, Basel, 2004.

[Sag20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.1)*, 2020. `http://www.sagemath.org`.

[Shi71] Goro Shimura. On elliptic curves with complex multiplication as factors of the jacobians of modular function fields. *Nagoya Mathematical Journal*, 43:199–208, 1971.

[Sil88] Joseph H. Silverman. Wieferich's criterion and the *abc*-conjecture. *Journal of Number Theory*, 30(2):226–237, 1988.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[SW93] Thomas R. Shemanske and Lynne H. Walling. Twists of Hilbert modular forms. *Transactions of the American Mathematical Society*, 338(1):375–403, 1993.

[vL21a] Joey M. van Langen. Modular Method SageMath Package. `https://github.com/jmvlangen/modular-method-package`, 2021.

[vL21b] Joey M. van Langen. On the sum of fourth powers in arithmetic progression. *International Journal of Number Theory*, 17(01):191–221, 2021.

[Wei82] André Weil. *Adeles and algebraic groups*, volume 23 of *Progress in Mathematics*. Birkhäuser, Boston, Mass., 1982. With appendices by M. Demazure and Takashi Ono.

[Zha14] Zhongfeng Zhang. On the Diophantine equation $(x-1)^k+x^k+(x+1)^k = y^n$. *Publicationes Mathematicae Debrecen*, 85(1-2):93–100, 2014.

[Zha17] Zhongfeng Zhang. On the Diophantine equation $(x-d)^4+x^4+(x+d)^4 = y^n$. *International Journal of Number Theory*, 13(9):2229–2243, 2017.

Cover art: Remco Wetzels