UNIVERSITY OF AMSTERDAM

MSC MATHEMATICS

MASTER THESIS

The Symplectic Method for solving Diophantine Equations

Author:
Mike Daas

Supervisor:
dr. S. Dahmen

Examination date:
June 18, 2020

Korteweg-de Vries Institute for
Mathematics

Abstract

This thesis discusses the *modular method* and explores the different ways in which it can be applied to solve Diophantine equations. In particular, the *symplectic method* will be discussed in detail and illustrated through myriad examples. We introduce the theory of *modular forms* and the modular method is explained before proving two *symplectic theorems* and discussing their applications, in particular the solutions to the equation $x^3 + y^3 = z^\ell$ for primes $\ell \equiv 2 \pmod 3$. We proceed to discuss more strategies to solve certain Diophantine problems and consider generalisations of the symplectic method to more general number fields. We conclude with a list of newly found applications of the symplectic method, solving Diophantine equations of varying signatures with two degrees of freedom in their coefficients for at least half the primes in most cases.

Title: The Symplectic Method for solving Diophantine Equations
Author: Mike Daas, dutchmikedaas@gmail.com, 10999892
Supervisor: dr. S. Dahmen
Second Examiner: dr. A. Kret
Examination date: June 18, 2020

Korteweg-de Vries Institute for Mathematics
University of Amsterdam
Science Park 105-107, 1098 XG Amsterdam
`http://kdvi.uva.nl`

Contents

Introduction

Though not as old as number theory itself, this tale has captured the imagination of many a young aspiring mathematician. A tale well known among, but not limited to, mathematicians of all ages. Not long after his death in 1665, the son of the famous mathematician Pierre de Fermat found his father's notes, scribbled on the pages of a copy of *Diophantus*. In a seemingly nondescript corner of the book, he found written on the old, worn pages a remark by his father, reading that he had found a marvellous proof of the fact that for any integer $n > 2$ there could be no three positive integers a, b and c satisfying $a^n + b^n = c^n$. Sadly, Fermat was known to often omit the actual proofs of his claims and even after many centuries of arduous attempts, a proper proof of this statement, that had nevertheless held strong against any and all attempts of finding a counterexample, continued to elude the world's mathematical community. Even though Fermat had actually written down his proof for the exponent $n = 4$, it took even more notable figures like Euler, Legendre, Dirichlet and Lebesgue to prove the theorem for other small values of n. It is generally assumed that Fermat did, in fact, not have a proof of his conjecture when he jotted down that remark in the margins of his book. The problem remained open and unsolved until the final decade of the foregone millennium, when it took some of the greatest minds in contemporary mathematics and some of the most modern techniques to finally settle this problem once and for all.

Ever since the proof of the *modularity theorem* that started with the famous major breakthrough by Andrew Wiles and Richard Taylor in 1994 and was completed no sooner than the year 1999 due to the admirable work of Taylor, Diamond, Conrad and Breuil, mathematicians around the world have been pushing the limits of the so-called *modular method* to solve ever greater families of Diophantine equations with varying exponents. The underlying theory of this method, in short, is the following.

Given a rational *elliptic curve*, we can for every prime ℓ associate to it a mod-ℓ representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ induced by the action of this group on the ℓ-torsion module $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. By combining all ℓ^k-torsion points into a single module, called the *Tate module*, one can even construct an ℓ-adic representation. On the other side of the story, we have *modular forms*, which are, in short, functions $f : \mathbb{H} \to \mathbb{C}$, where $\mathbb{H}$ denotes the complex upper half plane, that transform nicely when acted upon by certain subgroups $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, and in addition satisfy certain growth conditions. These seemingly analytic objects are, as the modularity theorem testifies, very closely related to elliptic curves and therefore intriguingly algebraic in nature. Depending on the subgroup Γ that defines our modular form, every such function comes with the notion of a *level*. We will mostly concern ourselves with quite special modular forms, called *newforms*. These are normalised eigenfunctions of all the *Hecke operators*, consisting of T_n for all $n \in \mathbb{N}$, which act on the space of modular forms with respect to the group $\Gamma_0(N)$. The

road to get there is a bit longer in this case, but it turns out that for newforms, which we will briefly assume to be rational for simplicity of the exposition, we can also define mod-ℓ and ℓ-adic representations for every prime ℓ.

To solve Fermat's equation, the idea had risen to take a hypothetical counterexample to the theorem and to construct a very clever elliptic curve using these elusive numbers. The modularity theorem mentioned above proves that it is possible to associate to this elliptic curve a seemingly completely different object, a newform, such that their ℓ-adic representations are isomorphic for every prime ℓ. The idea to tackle Fermat's equation requires another intricate result, however; Ribet's *level lowering* theorem. This roughly states that, given a newform and some prime ℓ, we can, under some fairly mild conditions, find another newform of a much lower level that has an isomorphic mod-ℓ representation. In case of Fermat's Last Theorem, executing this procedure will leave us with the existence of a newform at the extraordinarily low level of 2. It can be shown however, using more elementary means, that such objects cannot exist, yielding a contradiction. Hence Fermat's equation cannot have any solutions; end of proof.

It turns out that the equation defining Fermat's Last Theorem is not the only one that allows for the construction of a cunningly chosen elliptic curve. However, it is not hard to see the limitations of the proof sketched above. Of course, at a great many levels, newforms do exist. In fact, there is just a finite list of levels at which newforms do not exist, meaning that these cases are generally quite rare. If the above way to arrive at a contradiction would have been the only one, then one would be justified in concluding that the modular method is nothing than an accidental quirk. It turns out, however, that it is not.

Namely, after applying the modularity theorem and the level lowering theorem, still some relations between the original elliptic curve and the modular form must hold; their mod-ℓ representations must be isomorphic. Now, a newform can be written $f = \sum_{n=1}^{\infty} a_n(f) q^n$ where $q = \exp(2\pi i z/N)$, where N denotes the level of the newform. Defining for any prime p and elliptic curve E the quantity $a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p)$, where $\tilde{E}$ denotes the reduction of E at p, it turns out that, when solving an equation with prime exponent ℓ, it must almost always hold that either $a_p(E) \equiv a_p(f) \pmod{\ell}$ or $\pm(p+1) \equiv a_p(f) \pmod{\ell}$. Even when there exist newforms at the level that we ended up at, sometimes a quick computer program can verify that neither of these relations can be satisfied in our current situation, hence yielding a contradiction. This method is often referred to as *comparing traces of Frobenius*, because the quantities $a_p(E)$ and $a_p(f)$ are the traces of the image of the Frobenius elements for the prime p under the mod-ℓ representations of the absolute Galois group $G_{\mathbb{Q}}$, which are assumed to be isomorphic by the level-lowering theorem. This is an especially powerful method when the newform f is *irrational*, meaning that not all $a_n(f)$ are integers. It therefore follows that the modular method can be very powerful even when there are newforms at the level that we end up at.

It follows that for large exponents the modular method can mostly be hampered in its way towards a contradiction when the newforms at the level we find ourselves at, are rational. There is another possible way to arrive at a contradiction, and that is when the newforms in question have *complex multiplication*. This concept is most easily un-

derstood when applying the modularity theorem again to our newform, getting back a rational elliptic curve F. If we started our argument with the elliptic curve E and prime exponent ℓ, it follows that E and F must have isomorphic mod-ℓ representations. An elliptic curve is said to have complex multiplication if its endomorphism ring is isomorphic to an order in an imaginary quadratic number field, instead of to $\mathbb{Z}$. Galois representations of elliptic curves *with* complex multiplication are known to have a particularly small image. Many years of hard work have been put into attempts to prove *Serre's uniformity conjecture*, stating that for all primes $\ell > \ell_0$ for some prime ℓ_0, the mod-ℓ representation of $G_{\mathbb{Q}}$ associated to an elliptic curve *without* complex multiplication is surjective. In general it is believed that $\ell_0 = 37$ should be sufficient. Even though Serre's uniformity conjecture is still an open problem, the partial resolutions published hitherto are often sufficient to still arrive at a contradiction when applying the modular method.

Another method comes from examining the order of the image of the *inertia subgroup* for some prime p under the mod-ℓ representations and can also sometimes be used to arrive at a contradiction. Namely, it turns out that this order being divisible by ℓ is often strongly related to the elliptic curves having *potentially good reduction* at p or not, and sometimes these reduction types can differ, possibly yielding a contradiction. Potentially good reduction is a notion that is most conveniently characterised by $\nu_p(j(E)) \geqslant 0$, where j denotes the j-invariant of an elliptic curve.

A different approach to the sport that is solving Diophantine equations, is the main topic of this thesis: the *symplectic method*. This intriguing approach has in recent years enjoyed many great advances. It promises, and has already yielded, numerous interesting and strong results. Its core concept is fairly simple. For each prime ℓ, there exists a natural pairing, called the *Weil pairing*, on the ℓ-torsion group of any elliptic curve E, denoted $e_{E,\ell} : E[\ell] \times E[\ell] \to \mathbb{F}_\ell$. This pairing is defined by computing the determinant of the change of basis matrix that maps a preferred basis onto the two torsion-points considered. It is easy to see when a basis is preferred when working over the complex numbers, for then we can distinguish the quotient of the numbers being in $\mathbb{H}$ or not. We call such preferred bases *symplectic*. Now an isomorphism of p-torsion modules can either preserve the Weil-pairing up to a scalar multiple, or not. If it does, we call the isomorphism *symplectic*, otherwise it is said to be *anti-symplectic*. The idea is to determine the symplectic type of the isomorphism in different ways and to compare these outcomes to each other. More precisely, we can often determine the symplectic type of the isomorphism by examining the situation locally at a single prime. Should the outcomes of distinct primes differ, we will have found our desired contradiction.

This thesis discusses the proofs of two such local symplectic criteria. One criterium states that if p is a prime of *multiplicative reduction* for both elliptic curves E and F, then $E[\ell]$ and $F[\ell]$, when isomorphic, are symplectically isomorphic if and only if $\nu_p(\Delta(E))$ and $\nu_p(\Delta(F))$ differ by a square modulo ℓ, where Δ denotes the discriminant of an elliptic curve. This very versatile proposition can be used independently as many times as there are primes of multiplicative reduction, sometimes yielding contradictions for certain residue classes modulo ℓ. Nowadays there are many symplectic criteria available that examine the situation of potentially good reduction at a certain prime p. We

treat the proof of one of these criteria in detail, dealing with a certain case for potentially good reduction at the prime 2. This theorem was first introduced in a paper that used it to show that the generalised Fermat equation $x^3 + y^3 = z^\ell$ has no non-trivial primitive integral solutions for primes $\ell \equiv 2 \pmod 3$ and $\ell \geqslant 17$. More precisely, albeit more technically, the used theorem assumes that two elliptic curves E and F have isomorphic ℓ-torsion and both have potentially good reduction at 2, satisfying additionally the property that the Galois group of $L/\mathbb{Q}_2^{un}$, where L denotes the minimal extension of the maximal unramified extension $\mathbb{Q}_2^{un}$ of the 2-adic numbers where the elliptic curves achieve their good reduction, is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$. It then follows that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic when 2 is a square mod ℓ. In the case that 2 is not a square mod ℓ, they are symplectically isomorphic if and only if $v_2(\Delta(E)) \equiv v_2(\Delta(F)) \pmod 3$. One immediately recognises the very specific nature of these symplectic criteria for potentially good reduction, so it is not hard to imagine there being myriad other proven statements dealing with similar, yet slightly different situations.

Using the criteria proved as of today, we investigated some novel examples of applications of the symplectic method to large families of Diophantine equations. For instance, the equations

$$x^\ell + 2^\alpha y^\ell + 3^k z^\ell = 0, \quad 3^k x^\ell + 2^\alpha y^\ell = z^2 \quad \text{and} \quad x^\ell + 2^\alpha 3^k y^\ell = z^2$$

are shown to have no non-trivial primitive integral solutions for almost every choice of positive integers α and k for at least half the prime exponents ℓ, aside for some small exceptional solutions. We also study the slightly smaller families of equations

$$5^k x^\ell + 4y^\ell = z^2, \quad x^\ell + 4 \cdot 5^k y^\ell = z^2, \quad 2^k x^\ell + 9y^\ell = z^3 \quad \text{and} \quad x^\ell + 2^k \cdot 9y^\ell = z^3$$

and show that they have no non-trivial primitive integral solutions for a positive density of the primes ℓ for almost all choices of α and k. A limitation of the symplectic method is that it can never arrive at a contradiction for all primes, only for a certain positive density of primes.

The reason for restricting our attention to prime exponents is very straightforward; if an equation has no solutions with exponent ℓ, then also not for any exponent n for which $\ell \mid n$. Therefore, to show the non-existence of solutions to an equation for all exponents, it suffices to consider primes. However, it can often occur that for certain primes, small ones in particular, the methods to arrive at a contradiction fail, and sometimes solutions do actually exist. Among all odd primes, this problem is most common for the prime $\ell = 3$. To solve the equation for all exponents in such an event, one is forced to say something about exponent ℓ^2. We thus briefly explore the possibilities of level lowering modulo *prime powers*, in particular the number 9. We further describe a more general approach to solving Diophantine equations while working not over just the rationals, but over totally real number fields instead. This so-called *Hilbert modular method* is still an active area of research and promises a great many interesting applications. We also briefly touch on the possibilities of the symplectic method when working over number fields greater than $\mathbb{Q}$, and explore how the symplectic criteria proved earlier generalise to this setting.

Acknowledgements

I would like to thank my supervisor dr. Sander Dahmen for introducing me to the modular method, for his useful explanations and suggestions which helped shape the vast majority of this thesis and for his advice and support during my process of finding a suitable PhD-position. This piece of writing would not have turned out the same if it wasn't for his indispensable contributions. I would also like to thank the second examiner dr. Arno Kret for taking the time to read through this lengthy thesis, and Wouter Rienks for his continued moral support. Lastly I would like to thank dr. Nuno Freitas for his invaluable contributions to the field and for his answering two of my emails with questions about his work on such short notice.

1 Newforms

We begin by introducing the theory of *modular forms* and we will be working towards defining special modular forms, called *newforms*, in particular. Large parts of this chapter contain information that was extracted from [16] and locally we will refer more precisely. Many proofs will not be discussed in detail. For a comprehensive treatment of the theory of modular forms we again refer the reader to the majority of the book [16], but for our purposes, the discussions below will suffice.

This chapter, and the rest of the thesis for that matter, will expect the reader to be familiar with the theory of elliptic curves. Still, where necessary we will refer to [42] and [41] to provide the reader with further reference.

1.1 Modular forms for $\mathbf{SL}_2(\mathbb{Z})$

Modular forms for $\mathrm{SL}_2(\mathbb{Z})$ are, roughly speaking, holomorphic functions on the complex upper half plane

$$\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\}$$

that satisfy a growth condition and a certain transformation rule when acted upon by the group $\mathrm{SL}_2(\mathbb{Z})$. Recall that

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

This group acts on $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ via general linear transformations by defining

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{az + b}{cz + d}$$

for all $z \in \hat{\mathbb{C}}$ with the usual conventions for arithmetic with ∞. It can be verified through direct calculation that this indeed defines a group action of $\mathrm{SL}_2(\mathbb{Z})$ on $\hat{\mathbb{C}}$. For brevity we will denote

$$j_\alpha(z) = cz + d \quad \text{for any} \quad \alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Q}).$$

The equality $\mathrm{im}(\alpha(z)) = \det(\alpha)\mathrm{im}(z)/|j_\alpha(z)|^2$ can be verified through direct computation and shows that $\mathrm{SL}_2(\mathbb{Z})$ even acts on $\mathcal{H}$. The following operator is central to the whole theory of modular forms.

Definition 1.1. Let $\alpha \in \mathrm{GL}_2(\mathbb{Q})$, $k \in \mathbb{Z}$ and $f : \mathcal{H} \to \mathbb{C}$. Then we define the *weight* k *operator* $[\alpha]_k$ by

$$(f[\alpha]_k)(z) = \det(\alpha)^k j_\alpha(z)^{-k} f(\alpha(z)).$$

The following lemma can be verified through direct computation.

Lemma 1.2. *Let* $\alpha_1, \alpha_2 \in \mathrm{GL}_2(\mathbb{Q})$ *and* $k \in \mathbb{Z}$. *Then* $[\alpha_1]_k[\alpha_2]_k = [\alpha_1\alpha_2]_k$.

Definition 1.3. Let $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function satisfying $f(z+1) = f(z)$. Then we can write that $f(z) = g(e^{2\pi i z})$ for some $g : \{z \in \mathbb{C} \mid 0 < |z| < 1\} \to \mathbb{C}$. We then say that f is *holomorphic at* ∞ if g can be holomorphically extended to the origin. In that case, g has a Fourier expansion around 0, and thus

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n \quad \text{where} \quad q = e^{2\pi i z},$$

for some $a_n(f) \in \mathbb{C}$. These numbers are called the *Fourier coefficients* of f.

From complex analysis we know that whenever we can continue g continuously to 0, it will immediately be holomorphic as well. This has the following quick corollary.

Lemma 1.4. *Let* $f : \mathcal{H} \to \mathbb{C}$ *satisfy* $f(z+1) = f(z)$ *for all* $z \in \mathcal{H}$. *If* $\lim_{\mathrm{im}(z)\to\infty} f(z)$ *exists, then* f *is holomorphic at* ∞.

We are now ready to define modular forms.

Definition 1.5. A *modular form* with respect to $\mathrm{SL}_2(\mathbb{Z})$ of weight $k \in \mathbb{Z}$ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ satisfying

$$f[\gamma]_k = f \quad \text{for all} \quad \gamma \in \mathrm{SL}_2(\mathbb{Z})$$

and such that f is holomorphic at ∞. The set of modular forms with respect to $\mathrm{SL}_2(\mathbb{Z})$ of weight k has a natural $\mathbb{C}$-vector space structure and we denote this vector space by $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$.

Remark 1.6. Since $\mathrm{SL}_2(\mathbb{Z})$ contains the matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

we see that any modular form f of weight k satisfies $f(z+1) = f(z)$ and $f(-1/z) = z^k f(z)$, so that the definition of holomorphicity at ∞ applies to f. In fact, the above two matrices can be checked to generate the group $\mathrm{SL}_2(\mathbb{Z})$, so that by Lemma 1.2, the above two conditions combined with being holomorphic at ∞ are sufficient to conclude that a holomorphic map $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k with respect to $\mathrm{SL}_2(\mathbb{Z})$.

Remark 1.7. If we let I denote the 2×2 identity matrix, then the fact that $-I \in \mathrm{SL}_2(\mathbb{Z})$ implies that for any weight k modular form f with respect to $\mathrm{SL}_2(\mathbb{Z})$ it must hold that $f(z) = (-1)^k f(z)$. It follows immediately that if k is odd, we must have $f = 0$.

Remark 1.8. At first glance, this seems to be quite a strange definition. It is imperative, however, to keep in mind that this definition is very closely related to the characterisation of complex elliptic curves. Namely, using the association $\tau \mapsto (\mathbb{Z} + \tau\mathbb{Z})$, the moduli space of complex elliptic curves is given by $SL_2(\mathbb{Z}) \setminus \mathbb{H}$, so a modular form of weight zero can be viewed as a holomorphic map from the moduli space of complex elliptic curves to the complex numbers. For higher weights the modular form cannot quite be defined on this moduli space, because it is not constant on homothetic lattices, but instead it transforms with a fixed power of the multiplying constant. Still, it turns out that these seemingly analytic objects have great algebraic structure, which is part of why they are so interesting to study.

Example 1.9. One of the most elementary nontrivial examples of an even weight $k > 2$ modular form with respect to $SL_2(\mathbb{Z})$ is the Eisenstein series,

$$E_k(z) = \sum_{a,b \in \mathbb{Z} \setminus \{(0,0)\}} (a + bz)^{-k}.$$

This sum converges uniformly on any compact subset of $\mathcal{H}$ and as a result, it can easily be seen to satisfy $E_k(z+1) = E_k(z)$ and $E_k(-1/z) = z^k E_k(z)$. To find the limit of $E_k(z)$ when $\mathrm{im}(z) \to \infty$ for even k, by uniform convergence we may add the limits of every term in the sum. For $b \neq 0$ these limits vanish and for $b = 0$ the terms are constant and sum to $2\zeta(k)$, where ζ denotes the Riemann zeta function. Hence the limit exists and thus E_k is a modular form of weight k. We have also calculated that $a_0(E_k) = 2\zeta(k)$. $\triangle$

There is a subset of the complete set of modular forms of a given weight that is of particular interest, namely those for which $\lim_{\mathrm{im}(z)\to\infty} f(z) = 0$.

Definition 1.10. A modular form f for $SL_2(\mathbb{Z})$ of weight k is called a *cusp form* if $a_0(f) = 0$. We denote the $\mathbb{C}$-vector space of cusp forms of weight k by $\mathcal{S}_k(SL_2(\mathbb{Z}))$, which is a subspace of $\mathcal{M}_k(SL_2(\mathbb{Z}))$.

1.2 Congruence subgroups

Now that we know what modular forms with respect to $SL_2(\mathbb{Z})$ are, we can generalise the notions of the previous section to explore a greater class of functions. Namely, it turns out that often it is necessary and useful to consider holomorphic functions on the upper half plane which we only demand to transform nicely when acted upon by a certain subgroup of the full modular group $SL_2(\mathbb{Z})$.

Definition 1.11. Let $N \in \mathbb{N}$ be a positive integer. Then we define the following groups:

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\};$$

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \pmod{N} \right\};$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

We say a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma(N) \subset \Gamma$ for some positive integer N. The smallest N that satisfies that condition is called the *level* of Γ. We remark that we have the inclusions $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$, and so $\Gamma_1(N)$ and $\Gamma_0(N)$ are also congruence subgroups. It is not hard to show that they are both of level N.

The observant reader may notice that our previous definition of holomorphicity at ∞ does not work for maps that might not be $\mathbb{Z}$-periodic. However, every congruence subgroup Γ contains the matrix

$$\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$$

for some minimal $h \in \mathbb{N}$, since

$$\begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix} \in \Gamma(N) \subset \Gamma.$$

This motivates the following definition.

Definition 1.12. Let $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic map satisfying $f(z+h) = f(z)$ for all $z \in \mathcal{H}$ for some $h \in \mathbb{N}$. Then we can write $f = g(e^{2\pi i z/h})$ and we say that f is *holomorphic at infinity* when g extends holomorphically to 0. In particular we obtain a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q_h^n \quad \text{where} \quad q_h = e^{2\pi i z/h}.$$

Definition 1.13. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. A *modular form* of weight $k \in \mathbb{Z}$ with respect to Γ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ satisfying

$$f[\gamma]_k = f \quad \text{for all} \quad \gamma \in \Gamma$$

and such that for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ we have that $f[\alpha]_k$ is holomorphic at ∞. The set of modular forms with respect to Γ of weight k has a natural $\mathbb{C}$-vector space structure and we denote this vector space by $\mathcal{M}_k(\Gamma)$.

Remark 1.14. If $-I \notin \Gamma$, our previous argument showing that modular forms of odd weight do not exist, no longer applies. In fact, such modular forms do actually exist in general. We also note that our first definition of modular forms with respect to $\mathrm{SL}_2(\mathbb{Z})$ coincides with the above, because in that case, $f[\alpha]_k = f$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Example 1.15. An easy way to obtain a modular form with respect to $\Gamma_0(N)$ that is not necessarily a modular form with respect to $\mathrm{SL}_2(\mathbb{Z})$, is to take any modular form $f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ and to consider $f(Nz)$. Then we have for all $\gamma \in \Gamma_0(N)$ that

$$f(N\gamma(z)) = f\left(\frac{aNz + bN}{cz + d}\right) = f\left(\frac{a(Nz) + bN}{(c/N)(Nz) + d}\right) = j_\gamma(Nz)^{-k} f(Nz),$$

where we used that $N \mid c$ and that f is weight k invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. It can also be checked that $f(Nz)[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, and so $f(Nz)$ is indeed a modular form with respect to $\Gamma_0(N)$. It is not hard to see that this method generalises to lift modular forms from level M to level N, provided that $M \mid N$. $\triangle$

Definition 1.16. A modular form f of weight k with respect to Γ is called a *cusp form* if $a_0(f[\alpha]_k) = 0$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. We denote the vector space of cusp forms of weight k with respect to Γ by $\mathcal{S}_k(\Gamma)$.

We present the following fact without a detailed proof, for introducing all the necessary tools would take us too far afield.

Theorem 1.17. *For any congruence group Γ and weight k, the vector spaces $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$ are finite dimensional.*

There are multiple ways to prove the above statement. One such approach is outlined in Chapter 3 of [16]. There one first finds an expression for the genus of the *modular curve* $X(\Gamma)$ in terms of the number of *elliptic points*; that is, the complex numbers with a stabilizer under the Γ-action containing some element different from $\pm I$. Then one defines *automorphic forms* of weight k and *meromorphic differentials* of degree $2k$ and shows that there exists an isomorphism of vector spaces relating these objects for fixed k. One then uses the Riemann-Roch theorem on the modular curve to obtain explicit dimension formulas for $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$ for even k, showing in particular that those dimensions are finite. These methods can then be refined to also obtain formulas for odd k. The modular curve and meromorphic differentials will be briefly discussed again later in this chapter.

A different approach is outlined by Serre in Chapter 7 of [37]. He first examines the $\mathrm{SL}_2(\mathbb{Z})$ case, for which we know that there are no modular forms of odd weight. Denoting $\rho = e^{2\pi i/3}$, his method is based on the so-called *valence formula*, which is given by

$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_\rho(f) + \sum_{\substack{p \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \\ p \neq i,\rho}} \nu_p(f) = \frac{k}{12},$$

where $f \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) \setminus \{0\}$ and $\nu_p(f)$ denotes the order of vanishing of f in the point p. We remark that by the $\mathrm{SL}_2(\mathbb{Z})$-invariance of f, this order of vanishing is well-defined for a given orbit. The reason that i and ρ have special roles in the above equation is that they are the elliptic points for the action of $\mathrm{SL}_2(\mathbb{Z})$. We further remark that Serre uses a different convention for the weight, namely exactly half our convention, so that his formula ends with $k/6$ instead of $k/12$.

From Serre's equation, it follows immediately that if $k < 0$, there are no non-zero modular forms with respect to $\mathrm{SL}_2(\mathbb{Z})$, as the left hand side is non-negative. One also sees that it is impossible to make $1/6$ on the left hand side, showing that there are no modular forms for $\mathrm{SL}_2(\mathbb{Z})$ of weight 2. There is only one way to write $2/6$, $3/6$, $4/6$ and $5/6$ using terms from the left hand side and since we know that the Eisenstein series exist for these weights, it follows that $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ has dimension 1 for $k = 4, 6, 8, 10$. Since $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ has codimension at most 1 in $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$, as it is the kernel of the evaluation at ∞ map, the fact that Eisenstein series of even weight are not cusp forms proves that the codimension is exactly 1 for all even $k \geqslant 4$. Consequently, there are no cusp forms of weights $k = 4, 6, 8, 10$. Then Serre gives a cusp form of weight 12, commonly written as Δ, multiplying by which provides an isomorphism

$\mathcal{M}_{k-12}(SL_2(\mathbb{Z})) \to \mathcal{S}_k(SL_2(\mathbb{Z}))$, which then by induction yields dimension formulas for each $\mathcal{M}_k(SL_2(\mathbb{Z}))$.

These results can be extended to arbitrary Γ as follows. Again using Δ one can show that any $f \in M_k(SL_2(\mathbb{Z}))$ at ∞ having order at least the dimension of the vector space it lives in, must be identically zero. In particular this shows that a modular form of weight k with respect to $SL_2(\mathbb{Z})$ is uniquely determined by its first $\dim(M_k(SL_2(\mathbb{Z}))$ Fourier coefficients. Then one can transform some $f \in M_k(\Gamma)$ into a function $F \in M_{kn}(SL_2(\mathbb{Z})$ by taking a product over $f[\gamma_i]$, where $\{\gamma_i\}_{i=1,\dots,n}$ denotes a set of coset representatives of the subgroup $\Gamma/\{\pm 1\}$ inside $SL_2(\mathbb{Z})/\{\pm 1\}$. Then if f has an order at ∞ that is too large, since $f \mid F$ it will imply that $F = 0$ and so also $f = 0$. It then follows quickly that also $\dim(M_k(\Gamma))$ is finite as well.

1.3 Hecke operators

Aside from the *weight* k *operator* $[\alpha]_k$ that was used to define modular forms, we can define a different type of operator that acts on the modular forms with respect to the congruence subgroup $\Gamma_0(N)$, which will be most important for our purposes. We must start with a technical lemma, the proof of which can be found in Section 5.2 of [16].

Lemma 1.18. *Let* p *be a prime number, let* $N \in \mathbb{N}$ *and consider*

$$\alpha = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \in GL_2(\mathbb{Q}).$$

Define for all $0 \leqslant j \leqslant p-1$ *the matrices*

$$\beta_j = \begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix} \quad \textit{and} \quad \beta_\infty = \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix},$$

if $p \nmid N$. *Then we have that*

$$\Gamma_0(N)\alpha\Gamma_0(N) = \bigsqcup_{j=0}^{p-1} \Gamma_0(N)\beta_j \quad \textit{if} \quad p \mid N$$

and

$$\Gamma_0(N)\alpha\Gamma_0(N) = \Gamma_0(N)\beta_\infty \sqcup \bigsqcup_{j=0}^{p-1} \Gamma_0(N)\beta_j \quad \textit{if} \quad p \nmid N.$$

Definition 1.19. Let p be a prime number, $k, N \in \mathbb{N}$ and $f \in \mathcal{M}_k(\Gamma_0(N))$. We define the operator T_p by

$$T_p f = \sum_{j=0}^{p-1} f[\beta_j]_k \quad \text{if} \quad p \mid N,$$

and

$$T_p f = f[\beta_\infty]_k + \sum_{j=0}^{p-1} f[\beta_j]_k \quad \text{if} \quad p \nmid N.$$

Remark 1.20. To motivate the above definition, recall the interpretation of modular forms for $SL_2(\mathbb{Z})$ of maps that, up to scalars to the power k, map isomorphism classes of complex elliptic curves, which are quotients of $\mathbb{C}$ by a lattice, to complex numbers. In that language, $T_p f$ evaluated at a lattice Λ can be defined as summing over the outcomes of all the lattices in which Λ has index p. This equivalence is not obvious from the definitions, but it is true nonetheless.

Proposition 1.21. *The Hecke operator T_p maps $\mathcal{M}_k(\Gamma_0(N))$ to itself.*

Proof. Let $f \in \mathcal{M}_k(\Gamma_0(N))$ and $\gamma \in \Gamma_0(N)$. Write B for the set of coset representatives that we obtained from Lemma 1.18. Then using the above definition, we compute that

$$T_p f[\gamma]_k = \sum_{b \in B} f[b]_k[\gamma]_k = \sum_{b \in B} f[b\gamma]_k.$$

We claim that if b and $b'\gamma$ represent the same coset of $\Gamma_0(N)\backslash\Gamma_0(N)\alpha\Gamma_0(N)$, we have that $f[b]_k = f[b'\gamma]_k$. To see this, write $b = \sigma_1\alpha\sigma_2$ and $b'\gamma = \tau_1\alpha\tau_2$ for certain $\sigma_1, \sigma_2, \tau_1, \tau_2 \in \Gamma_0(N)$. Then the fact that $\Gamma_0(N)b = \Gamma_0(N)b'\gamma$ translates to $\Gamma_0(N)\alpha\tau_2 = \Gamma_0(N)\alpha\sigma_2$. But if $\epsilon\alpha\tau_2 = \alpha\sigma_2$ for some $\epsilon \in \Gamma_0(N)$, then we find for any $f \in \mathcal{M}_k(\Gamma_0(N))$ that

$$f[b]_k = f[\sigma_1]_k[\alpha\sigma_2]_k = f[\epsilon\alpha\tau_2]_k = f[\alpha\tau_2]_k = f[\tau_1\alpha\tau_2]_k = f[b'\gamma]_k,$$

where we used that f is invariant under the actions of $\sigma_1, \epsilon, \tau_1 \in \Gamma_0(N)$. This proves our claim. Now, the set $\{b\gamma \mid b \in B\}$ is again a set of coset representatives, since $\gamma \in \Gamma_0(N)$. So by the claim,

$$\sum_{b \in B} f[b\gamma]_k = \sum_{b \in B} f[b]_k = T_p f,$$

which concludes the proof. □

Remark 1.22. It is important to remark here that with a slightly different β_∞, as given in Proposition 5.2.1 in [16] and the subsequent paragraph, the above operators can be shown to also act on the space $\mathcal{M}(\Gamma_1(N))$. Furthermore, there is a second set of operators acting on the space $\mathcal{M}_k(\Gamma_1(N))$. They rely on the observation that

$$\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^* : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d \pmod N$$

descends to an isomorphism $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$. This can be used to show that for any $d \in \mathbb{Z}$ we have a well-defined *diamond operator* $\langle d\rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$ by

$$\langle d\rangle f = \begin{cases} 0 & \text{if } \gcd(d, N) > 1; \\ f[\gamma]_k & \text{if } \gcd(d, N) = 1, \quad \text{where} \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N). \end{cases}$$

The subspace $\mathcal{M}_k(\Gamma_0(N)) \subset \mathcal{M}_k(\Gamma_1(N))$ is precisely the subspace of modular forms that are fixed by all diamond operators.

Definition 1.23. Let p be a prime number and $r \geqslant 2$ an integer. Then on the space $\mathcal{M}_k(\Gamma_0(N))$ we inductively define

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} T_{p^{r-2}},$$

using the convention that $T_1 = \mathrm{id}$. For any $n = \prod p_i^{e_i}$, we define

$$T_n = \prod T_{p_i^{e_i}}.$$

These form the *Hecke operators*. Since the T_p are linear operators, because $[\alpha]_k$ is linear for every $\alpha \in \mathrm{GL}_2(\mathbb{Q})$, it follows that all T_n are linear operators as well. It is not hard to show that these operators take cusp forms to cusp forms, so that we have constructed a set of linear operators on both $\mathcal{M}_k(\Gamma_0(N))$ and $\mathcal{S}_k(\Gamma_0(N))$.

Remark 1.24. Again, the above definition warrants a short justification. It turns out that if f is a normalised, meaning $a_1(f) = 1$, eigen-cuspform for all the T_p operators, then the eigenvalue of f for T_p is simply given by its p-th Fourier coefficient $a_p(f)$. The above inductive definition is crafted in such a way that this fact will extend to all the natural numbers. This will be discussed again later.

Remark 1.25. We remark that in the more general case of $\mathcal{M}_k(\Gamma_1(N))$ the definition of T_{p^r} has to be adjusted to

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}.$$

Theorem 1.26. *For any two positive integers m and n, the operators T_n and T_m commute.*

The proof relies on the claim that T_p and T_q commute for any two primes p and q. It will then follow by induction that T_{p^r} and T_{q^s} will commute for all $r, s \in \mathbb{N}$, and so also T_n and T_m for all $n, m \in \mathbb{N}$. The proof of the claim is technical and relies on explicit descriptions of the operators T_p and T_q in terms of the Fourier coefficients of f. We refer the reader to Proposition 5.2.4 of [16] for the proof.

Remark 1.27. It is worth noting that the T_p operators also commute with all the diamond operators, and that the diamond operators commute with each other as well.

1.4 $\mathcal{S}_k(\Gamma)$ as inner product space

In this section it will finally become apparent why we are particularly interested in cusp forms, rather than modular forms in general. Namely, we can define a natural inner product on the space of all cusp forms via an integral that would not converge for every pair of two modular forms, but which will converge when we restrict our view to cusp forms.

Definition 1.28. The *hyperbolic measure* $d\mu$ on $\mathcal{H}$ is defined by

$$d\mu(z) = \frac{dx\, dy}{y^2}, \quad \text{where} \quad z = x + iy, \;\; x, y \in \mathbb{R}.$$

It can be checked that $d\mu$ is invariant under the action of $SL_2(\mathbb{Z})$. Since the functions we are interested in are weight k invariant under the action of a congruence subgroup Γ, should we desire to define an inner product using an integral, it makes sense to integrate over a set of points representing each Γ-orbit exactly, or almost exactly, once. The following lemma will tell us what such a set approximately looks like and is proved in Section 2.3 from [16].

Lemma 1.29. *Any $z \in \mathcal{H}$ is mapped to the set*

$$\mathcal{D} = \{z \in \mathcal{H} \mid \mathrm{Re}(z) \leqslant 1/2,\ |z| \geqslant 1\}$$

by some element from $SL_2(\mathbb{Z})$. This element is almost always *unique; that is, uniqueness fails only on a set of measure zero on the boundary of $\mathcal{D}$. More generally, let Γ be a congruence subgroup. Suppose that $SL_2(\mathbb{Z}) = \bigsqcup\{\pm I\}\Gamma\gamma_j$ for a certain set $\{\gamma_j\} \subset SL_2(\mathbb{Z})$. Then any $z \in \mathcal{H}$ is mapped to the set*

$$\bigsqcup_j \gamma_j \mathcal{D}$$

by an element from Γ. This element is unique away from a set of measure zero.

Definition 1.30. Let $f, g \in \mathcal{S}_k(\Gamma)$ be cusp forms where Γ a congruence subgroup and $\{\gamma_j\}$ is as above. Then we define the *Petersson inner product* by

$$\langle f, g\rangle = \frac{1}{V_\Gamma} \sum_j \int_{\mathcal{D}} f(\gamma_j(z))\overline{g(\gamma_j(z))}(\mathrm{im}(\gamma_j(z)))^k \, d\mu.$$

Here V_Γ is a number chosen so that the above expression evaluates to 1 when the integrand is replaced by the constant function 1.

Remark 1.31. It is easy to check that $f(z)\overline{g(z)}(\mathrm{im}(z))^k$ is Γ-invariant, using an identity from the first page of this chapter. This can be used to show that the above definition is independent of the representatives $\{\gamma_j\}$ chosen and thus well-defined. It can be shown that this integral converges whenever the integrand is bounded. The fact that both f and g are cusp forms ensures that $f(z)\overline{g(z)}(\mathrm{im}(z))^k$ is bounded, and hence the convergence of the integral follows.

Remark 1.32. Write $Y(\Gamma)$ for the set of orbits of the action of Γ on $\mathcal{H}$, which has, with some care, a topology induced by charts from $\mathbb{C}$. It is possible to compactify $Y(\Gamma)$ to form an object $X(\Gamma)$ by adding the Γ orbits of $\mathbb{Q} \cup \{\infty\}$. This has the structure of a compact Riemann surface and it is therefore more natural to view the above definition of the inner product as integrating over $X(\Gamma)$. This is called the *modular curve* with respect to Γ. A complete description of the elaborate construction of $X(\Gamma)$ can be found in Chapter 2 of [16], and it is not a short read. We will need this again later.

Recall that the *adjoint* of a linear endomorphism A of an inner product space V is given by the linear endomorphism A^* that satisfies $\langle Av, w\rangle = \langle v, A^*w\rangle$ for all $v, w \in V$. It turns out that the Hecke operators have particularly nice adjoints.

Theorem 1.33. *Let p be a prime number and $N \in \mathbb{N}$ such that $p \nmid N$. Then on the space $\mathcal{S}(\Gamma_0(N))$ the Hecke operator T_p is self-dual.*

The proof of the above statement is quite lengthy and technical. We will refer the interested reader to Theorem 5.5.3 of [16] for the details. The core of the argument consists of showing that for $\Gamma \subset \Gamma'$ a normal subgroup and $\alpha \in \Gamma'$, we have that $[\alpha]_k^* = [\det(\alpha)\alpha^{-1}]_k$. After that, it is mainly bookkeeping.

Recall that a linear endomorphism is called *normal* when it commutes with its adjoint.

Corollary 1.34. *For any $n, N \in \mathbb{N}$ coprime, the operator T_n acting on $\mathcal{S}(\Gamma_0(N))$ is normal. Hence by the spectral theorem, there exists an orthogonal basis of $\mathcal{S}_k(\Gamma_0(N))$ consisting of simultaneous eigenfunctions for all the T_n.*

This is a major step towards the definition of newforms, which, as we will see shortly, are certain normalised eigenforms for every Hecke operator. The above theorem guarantees the existence of such simultaneous eigenforms.

Remark 1.35. We again note that with the help of the diamond operators the above theorems generalise to the space $\mathcal{S}(\Gamma_1(N))$. There T_p will no longer quite be self-dual, but it will satisfy $T_p^* = \langle p \rangle^{-1} T_p$. Because T_p and $\langle p \rangle$ commute, the latter result generalises without any problems to $\mathcal{S}(\Gamma_1(N))$.

1.5 Newforms

Recall Example 1.15. There we established a non-trivial way of lifting modular forms from a level M to a level N, provided that $M \mid N$. It can be verified that that construction restricts to cusp forms, yielding a non-trivial, injective map $\mathcal{S}_k(\Gamma_0(M)) \to \mathcal{S}_k(\Gamma_0(N))$. Explicitly, if we let $d = N/M$ and

$$\alpha_d = \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix},$$

then the map described in the example is up to a scalar multiple given by the operator $[\alpha_d]_k$. We remark that the trivial way of mapping $\mathcal{S}_k(\Gamma_0(M))$ to $\mathcal{S}_k(\Gamma_0(N))$ is to observe that if $M \mid N$, we have that $\mathcal{S}_k(\Gamma_0(M)) \subset \mathcal{S}_k(\Gamma_0(N))$, as the latter set requires weight k invariance for fewer matrices. Now one can wonder which modular forms of a given level N can be written as such lifts from a suitable lower level, and which cannot.

Definition 1.36. Let p be a prime number and $N \in \mathbb{N}$ such that $p \mid N$. Then we define the map

$$i_p : \mathcal{S}_k(\Gamma_0(N/p))^2 \to \mathcal{S}_k(\Gamma_0(N)) \colon (f, g) \mapsto f + g[\alpha_p]_k.$$

Then we define the space of *oldforms* by

$$\mathcal{S}_k(\Gamma_0(N))^{\text{old}} = \sum_{p \mid N} \text{Image}(i_p).$$

Naturally, the space of *newforms* is defined as

$$\mathcal{S}_k(\Gamma_0(N))^{\text{new}} = \mathcal{S}_k(\Gamma_0(N))^{\text{old},\perp}.$$

Proposition 1.37. *All Hecke operators map $S_k(\Gamma_0(N))^{\text{old}}$ to itself and $S_k(\Gamma_0(N))^{\text{new}}$ to itself. As a result, both $S_k(\Gamma_0(N))^{\text{old}}$ and $S_k(\Gamma_0(N))^{\text{new}}$ have orthogonal bases consisting of eigenfunctions for all T_n for all n* coprime to N.

Proof. (Sketch) One can show that for each prime $p \mid N$,

$$i_p(T_{p'}f, T_{p'}g) = T_{p'}i_p(f, g),$$

where $p' \neq p$ is a prime. Note that the operators act differently depending on the level of the modular form they are acting on. The above equality can be verified through an extensive computation. The operator T_p can be checked individually. Hence the oldforms are stable under the action of all Hecke operators. Now if $\gcd(n, N) = 1$, since each T_n is self-adjoint, from this it follows immediately that also the newforms are preserved under the Hecke operators. If n and N share factors, the argument requires a more precise version of Theorem 1.33, which can be found at the very end of Section 5.5 of [16]. □

These results about the existence of bases consisting of eigenfunctions for a lot of operators, motivate the following definition.

Definition 1.38. A *newform* is a function $f \in S_k(\Gamma_0(N))^{\text{new}}$ that is an eigenfunction of *all* T_n and such that $a_1(f) = 1$.

The following result shows why we were allowed to remove the restriction on n and to allow it to share factors with N.

Proposition 1.39. *Suppose that $f \in S_k(\Gamma_0(N))^{\text{new}}$ is an eigenfunction for all T_n for all n coprime to N. Then f is an eigenfunction for T_n for all $n \in \mathbb{N}$. We also have $a_1(f) \neq 0$, so f may be normalised to be a newform. Lastly, for such normalised f, the eigenvalues of f for the operators T_n are precisely given by $a_n(f)$.*

Proof. (*Sketch*) The proof in part relies on the explicit description of the operator T_n in terms of the Fourier coefficients of f, as given in Proposition 5.2.2 in [16]. In this case, it gives us that $a_1(T_n f) = a_n(f)$ for all $n \in \mathbb{Z}$. Hence since f is an eigenform for many T_n, if $a_1(f) = 0$, then $a_n(f) = 0$ for all n coprime to N. A result called the *main lemma*, proved as Theorem 5.7.1 in [16], then tells us that f is actually an oldform; a contradiction. So f can be normalised, which we will now assume. Using the same reasoning, the function $g = T_n f - a_n(f)f$ is again a newform, but by construction it has $a_1(g) = 0$, contradicting the fact that g can be normalised if $g \neq 0$. Hence we must have that $T_n f = a_n(f)f$. □

Corollary 1.40. *The set of newforms in $S_k(\Gamma_0(N))^{\text{new}}$ forms an orthogonal basis.*

This is what we have been working towards for the entirety of this chapter. What we have constructed is a finite dimensional vector space, $S_k(\Gamma_0(N))^{\text{new}}$, along with a set of special operators; the Hecke operators. What the above corollary says, is that this space, rather remarkably, has a preferred basis to work with. A basis consisting of so-called

newforms, which are normalised eigenfunctions for all the Hecke operators that are mutually orthogonal in the Petersson inner product. This leaves us with a space with a lot of structure, and even more so when we restrict our attention to weight 2 forms.

Remark 1.41. All the results presented above can be generalised to the space $S_k(\Gamma_1(N))$, but for our purposes this will not be important.

1.6 Algebraic integers

Finally, we will examine some properties of the Fourier coefficients of a normalised eigenform of weight 2 specifically. Namely, it turns out that these are not just any arbitrary complex numbers, but they are actually algebraic integers. In fact, an even stronger result holds: all the Fourier coefficients of a given normalised eigenform are contained in a *finite* extension of $\mathbb{Q}$; that is, a number field. To establish these results, we will need to introduce a new object, called the *Jacobian*, and show that the operators T_p act nicely on these suitable finitely generated subspaces. Then since the Fourier coefficients of a normalised eigenform are part of the spectrum of the T_p by Proposition 1.39, this will give us the information we need. For a more detailed account of the forthcoming theory we refer the reader to Chapter 6 of [16].

Let X be any compact Riemann surface. Write $\Omega^1_{\text{hol}}(X)$ for the space of holomorphic differentials on X, formally defined by gluing sets of compatible differentials on suitable coordinate charts from $\mathbb{C}$ to X. To obtain a notion of integrating a differential from a point x to a point x', we need to take into account integrating over a loop, which does not necessarily have to vanish. Let g be the genus of X. Then adopting the parlance of Section 6.1 in [16], we can think of X as a complex sphere with g *handles*. Consider loops $A_1, \dots, A_g$ longitudinally around each handle and loops $B_1, \dots, B_g$ latitudinally around each handle. Then it can be shown that integration over any loop in X can be expressed as the linear combination of integrating over all the A_i, B_i. We define

$$H_1(X, \mathbb{Z}) = \bigoplus_{i=1}^{g} \mathbb{Z} \int_{A_i} \oplus \bigoplus_{i=1}^{g} \mathbb{Z} \int_{B_i} \cong \mathbb{Z}^{2g}.$$

One can show that we can express the dual space of $\Omega^1_{\text{hol}}(X)$ as

$$\Omega^1_{\text{hol}}(X)^* = \bigoplus_{i=1}^{g} \mathbb{R} \int_{A_i} \oplus \bigoplus_{i=1}^{g} \mathbb{R} \int_{B_i}.$$

Now recall the modular curve $X(\Gamma_0(N))$ from Remark 1.32, which is often denoted $X_0(N)$.

Definition 1.42. We define the *Jacobian* of $X_0(N)$ to be

$$J_0(N) = \Omega^1_{\text{hol}}(X_0(N))^* / H_1(X_0(N), \mathbb{Z}).$$

The following proposition makes it clear why weight 2 cusp forms are especially interesting.

Proposition 1.43. *There is a natural isomorphism between* $\Omega^1_{\mathrm{hol}}(X_0(N))$ *and* $\mathcal{S}_2(\Gamma_0(N))$.

Proof. (*Sketch*) We have a natural projection $\pi : \mathcal{H} \to X_0(N)$. Via coordinate charts this defines a pullback $\pi^* : \Omega^1_{\mathrm{hol}}(X_0(N)) \to \Omega^1(\mathcal{H}) = \{f\,dz \mid f \text{ is holomorphic on } \mathcal{H}\}$. Any form $f\,dz$ in the image of this pullback comes from an object on $X_0(N)$ and thus must be invariant under the action of $\Gamma_0(N)$ itself. But since for $\gamma \in \Gamma_0(N)$ we have, remarking that its derivative satisfies $\gamma'(z) = j_\gamma(z)^{-2}$,

$$\gamma^*(f\,dz) = f(\gamma(z))\gamma'(z)\,dz = j_\gamma(z)^{-2} f(\gamma(z))\,dz = f[\gamma]_2(z)\,dz,$$

we see that the image of π^* consists of forms $f\,dz$ with $f \in \mathcal{M}_2(\Gamma_0(N))$, briefly ignoring holomorphicity at ∞. It can be shown that f is even a cusp form. Conversely, such forms can via charts be lifted to a differential form on $X_0(N)$, establishing the bijection. □

We observe that since any Hecke operator T_n acts on $\mathcal{S}_2(\Gamma_0(N))$, we have a natural action on the dual space of $\mathcal{S}_2(\Gamma_0(N))$. Namely, for any functional ϕ, we set $T_n \cdot \phi := \phi(T_n(-))$. By the above theorem this action directly translates to an action on the space of differentials. Now we can state a very fundamental result.

Proposition 1.44. *Let* n *be a positive integer. Then the action of* $T_n : \mathcal{S}_2(\Gamma_0(N))^* \to \mathcal{S}_2(\Gamma_0(N))^*$ *descends to a map* $J_0(N) \to J_0(N)$. *In particular, this means that* T_n *acts on* $H_1(X_0(N), \mathbb{Z})$.

Proving the above statement is a lot of work and we opt to refer the reader to Sections 6.1, 6.2 and 6.3 of [16] for the full proof. Now we will be able to derive our number theoretically interesting results.

Proposition 1.45. *Let* $f \in \mathcal{S}_2(\Gamma_0(N))$ *be a normalised eigenform. Then each of its Fourier coefficients is an algebraic integer.*

Proof. Recall from Proposition 1.44 that the weight 2 Hecke operators T_p act for any prime p on $H_1(X_0(N), \mathbb{Z})$, which is a finitely generated abelian group. Let μ_p be its minimal polynomial as a linear operator on $H_1(X_0(N), \mathbb{Z})$, so μ_p will have integral coefficients. Now since T_p is $\mathbb{C}$-linear and since $\mathcal{S}_2(\Gamma_0(N))^*$ is just the $\mathbb{R}$-linearisation of $H_1(X(N), \mathbb{Z})$, we find that μ_p is even the minimal polynomial of T_p on all of $\mathcal{S}_2(\Gamma_0(N))^*$, and so also of T_p on $\mathcal{S}_2(\Gamma_0(N))$. Thus the eigenvalues of T_p must be zeroes of μ_p, making them algebraic integers. The result for general T_n follows readily. □

Definition 1.46. Let $N \in \mathbb{N}$. Then we define the *Hecke algebra* over $\mathbb{Z}$ acting on $\mathcal{S}_2(\Gamma_0(N))$ by

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\{T_n \mid n \in \mathbb{N}\}].$$

We remark that even though the Hecke algebras are distinct for different levels, the number N is often omitted from the notation. Now we can prove our big result.

Theorem 1.47. *Let* $f \in \mathcal{S}_2(\Gamma_0(N))$ *be a normalised eigenform. Then* $K_f = \mathbb{Q}(a_1(f), a_2(f), \ldots)$ *is a* number field, *called the number field of* f.

Proof. Recall that $\mathbb{T}_{\mathbb{Z}}$ acts on $H_1(X_0(N), \mathbb{Z})$, which is a finitely generated abelian group. Hence $\mathbb{T}_{\mathbb{Z}}$, viewed as a subring of $\mathrm{End}(H_1(X_0(N), \mathbb{Z}))$, is a finitely generated abelian group as well. Now we consider the map $\mathbb{T}_{\mathbb{Z}} \to \mathbb{C}$ that picks out the eigenvalue of f for a given operator $T \in \mathbb{T}_{\mathbb{Z}}$. Its image is equal to $\mathbb{Z}[a_1(f), a_2(f), \ldots]$. Hence this must be a finitely generated abelian group as well and so it must be contained in a finite field extension of $\mathbb{Q}$; that is, a number field. □

We conclude the chapter with one last result that shows that it does not matter in what way we embed the number field K_f into $\mathbb{C}$, as one would expect. Namely, we can now think of the Fourier coefficients of f as not being complex numbers, but as living in an abstract number field K_f. We will not treat the proof, but it can be found as Theorem 6.5.4 in [16].

Proposition 1.48. *Let f be a normalised eigenform of weight 2 with respect to $\Gamma_0(N)$ with number field K_f. Let $\sigma : K_f \to \mathbb{C}$ be any embedding. Then*

$$f^{\sigma} = \sum_{n=1}^{\infty} \sigma(a_n(f)) q^n$$

is again a normalised eigenform of weight 2 with respect to $\Gamma_0(N)$. If f was a newform, then f^{σ} is also a newform.

Remark 1.49. As has been noted numerous times before, all the above results generalise to the space $S_2(\Gamma_1(N))$, though it is worth observing that the Hecke algebra will be defined to be generated not only by the T_n operators, but also by the diamond operators. In fact, with the proper preparation, it is actually most natural to prove the above results in this more general setting first, and then specialising to the congruence subgroup $\Gamma_0(N)$ later.

2 The symplectic method

In this chapter we will outline the basics about the way that the modular method for solving Diophantine equations works in practice and we will list the theorems it relies on. We will explore the limitations of these theorems and focus on proving two *symplectic* criteria that can help to complete the argument when applying the modular method. We give a more complete overview of the history of the symplectic method at the beginning of Section 2.4, along with details about how we will discuss and use this method in the later sections.

Everything is very closely related to *Galois representations*, which are (continuous) representations of the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, or in some cases $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ for some prime ℓ. It turns out that certain degree 2 representations are induced by elliptic curves and by modular forms. Describing the way in which these induced representations relate is the core of the *modularity theorem*, arguably one of the greatest theorems in number theory. It is this theorem, combined with a few other very powerful results, that will allow us to solve certain equations.

In what follows, *newforms of level* N will always be normalised eigenforms in the space $\mathcal{S}_2(\Gamma_0(N))^{\mathrm{new}}$.

2.1 Galois representations

First we will concern us with the way an elliptic curve $E/\mathbb{Q}$ induces a degree 2 Galois representation. We first need to define a special invariant of E.

Definition 2.1. Let $E/\mathbb{Q}$ be an elliptic curve and consider a minimal model of E, with minimal discriminant $\Delta_{\min}$. Then we define the *conductor* N of E to be the number

$$N = \prod_{p \mid \Delta_{\min}} p^{f_p + \delta_p} \quad \text{where} \quad f_p = \begin{cases} 1 & \text{if } E \text{ has multiplicative reduction at } p; \\ 2 & \text{if } E \text{ has additive reduction at } p, \end{cases}$$

and where $\delta_p = 0$ for $p \geqslant 5$. The precise values of δ_2 and δ_3 can be computed using Tate's algorithm, which is described in Section IV.9 in [41].

We recall the following result, the proof of which is elementary by examining the dual isogeny of the multiplication by m map, as explained in Section III.6 from [42].

Proposition 2.2. *Let E be a rational elliptic curve and let $m \in \mathbb{N}$. Write $E[m]$ for the subgroup of m-torsion points of E over $\overline{\mathbb{Q}}$. Then $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.*

We claim that $E[m]$ is a $G_{\mathbb{Q}}$-module. To see this, let $\sigma \in G_{\mathbb{Q}}$ and recall that every torsion point of E is contained in $\overline{\mathbb{Q}}$. The addition of points on E is defined over $\mathbb{Q}$ and hence commutes with the action of σ. It follows that σ maps m torsion to m torsion compatibly with the group structure, making $E[m]$ indeed a $G_{\mathbb{Q}}$-module. In fact, this justifies the following definition.

Definition 2.3. Let $E/\mathbb{Q}$ be an elliptic curve and let ℓ be a prime number. Then we have a representation

$$\rho_E^{\ell} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_{\ell}),$$

which is induced by the action of the absolute Galois group on $E[\ell]$.

We can also define a slightly more intricate representation, that will allow us to work in characteristic zero instead of characteristic ℓ. We can write down a projective system

$$E[\ell] \leftarrow E[\ell^2] \leftarrow E[\ell^3] \leftarrow \dots,$$

where the maps are all given by multiplication by ℓ.

Definition 2.4. For any prime ℓ, define the *Tate module* of E by the inverse limit

$$Ta_{\ell}(E) = \varprojlim_n E[\ell^n].$$

Explicitly, the Tate module consists of sequences of points $(P_1, P_2, \dots)$ such that $P_n \in E[\ell^n]$ and $\ell P_{n+1} = P_n$ for all $n \in \mathbb{N}$. By the above theorem we see that we have a non-canonical isomorphism $Ta_{\ell}(E) \cong \mathbb{Z}_{\ell}^2$, where $\mathbb{Z}_{\ell}$ denotes the ℓ-adic integers. Observe that the absolute Galois group $G_{\mathbb{Q}}$ acts on the Tate module, because it acts on each $E[\ell^n]$ compatibly. Thus we have a homomorphism

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(Ta_{\ell}(E)) \cong GL_2(\mathbb{Z}_{\ell}) \subset GL_2(\mathbb{Q}_{\ell}),$$

that is, a degree 2 representation of $G_{\mathbb{Q}}$. Now we will need a few definitions from algebraic number theory. More details can be found in Section 9.3 of [16].

Definition 2.5. Let p be a prime number and let $\mathfrak{p}$ be a prime ideal of $\overline{\mathbb{Z}}$ lying over p. Write $D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$. Then $D_{\mathfrak{p}}$ acts on $\overline{\mathbb{Z}}/\mathfrak{p} \cong \overline{\mathbb{F}}_p$ and can be shown to surject onto $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Then we write $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$ for any element that maps to the Frobenius element of $\overline{\mathbb{F}}_p$, which is only defined up to an element from the *inertia* subgroup $I_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} \mid \sigma(x) \equiv x \pmod{\mathfrak{p}}\}$.

Definition 2.6. Let ρ be a representation of $G_{\mathbb{Q}}$. Then we say that ρ is *unramified* over a prime number p if for any prime ideal $\mathfrak{p} \subset \overline{\mathbb{Z}}$ we have that $I_{\mathfrak{p}} \subset \ker(\rho)$. Consequently, if ρ is unramified at p, the image $\rho(\mathrm{Frob}_{\mathfrak{p}})$ is well defined.

Recall that for any elliptic curve $E/\mathbb{Q}$ and any prime number p we can write down a minimal model of its reduction $\tilde{E}$ over $\mathbb{F}_p$. We let $\#\tilde{E}(\mathbb{F}_p)$ denote the number of points of $\tilde{E}$ over $\mathbb{F}_p$ including the point at infinity, and we use it to define the quantity

$$a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

Theorem 2.7. *Let E be a rational elliptic curve with conductor N and let ℓ and p be distinct prime numbers such that $p \nmid N$. Then $\rho_{E,\ell}$ is unramified at p. Let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any prime ideal lying over p. Then the equation*

$$x^2 - a_p(E)x + p = 0$$

is the characteristic equation of $\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$. Lastly, $\rho_{E,\ell}$ is irreducible.

The first two statements in the above theorem are not difficult to prove and can be found as Theorem 9.4.1 in [16]. The fact that $\rho_{E,\ell}$ is irreducible is much more difficult to show, but we will not need it in this thesis.

Remark 2.8. We remark that the above theorem gives us that in particular

$$\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})) = a_p(E) \quad \text{and} \quad \det(\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})) = p.$$

Now it turns out that we can arrive at a similar result starting from a newform f of level N instead of an elliptic curve E, but the road to get there is a bit longer and it can be found in Section 9.5 of [16]. First one must define for some prime number ℓ an action of $G_\mathbb{Q}$ on the ℓ^n-torsion of the Picard group of $X_0(N)$, yielding a $2g$-dimensional Galois representation by taking inverse limits as above, where g is the genus of $X_0(N)$, that is unramified at all primes different from ℓ and not dividing N. This representation does not involve the newform yet, but we will use it to define the object $A_f = J_0(N)/I_f J_0(N)$, where $I_f = \{T \in \mathbb{T}_\mathbb{Z} \mid Tf = 0\}$. One can define a map from the ℓ^n-torsion of the Picard group to the ℓ^n-torsion of A_f compatible with the representation, thus yielding a representation on the inverse limit of the $A_f[\ell^n]$. Tensoring this module over $\mathbb{Q}$ gives the object $V_\ell(A_f)$, which can be shown to be a free module over $K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} K_{f,\lambda}$ of rank 2, where λ is a prime ideal in the ring of integers $\mathcal{O}_f$ lying over ℓ and $K_{f,\lambda}$ denotes the inverse limit of the rings $\mathcal{O}_f/\lambda^n$. The following is Theorem 9.5.4 in [16].

Theorem 2.9. *Let f be a newform of level N. Let K_f be its number field, ℓ a prime number and λ a prime of K_f lying over ℓ. Then there exists a Galois representation*

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

that is unramified at every prime $p \nmid N$ different from ℓ. For any prime $\mathfrak{p} \subset \overline{\mathbb{Z}}$ lying over p, the characteristic equation of $\rho_{f,\lambda}(\mathrm{Frob}_\mathfrak{p})$ is given by

$$x^2 - a_p(f)x + p = 0.$$

Remark 2.10. We specialise to the case that f is a *rational* normalised eigenform; that is, $K_f = \mathbb{Q}$ and we suppose that f is a newform with respect to $\Gamma_0(N)$. Then the above theorem simplifies to the sole case $\lambda = (\ell)$ and we obtain a representation

$$\rho_{f,\ell} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$$

with the properties that

$$\mathrm{tr}(\rho_{f,\ell}(\mathrm{Frob}_\mathfrak{p})) = a_p(f) \quad \text{and} \quad \det(\rho_{f,\ell}(\mathrm{Frob}_\mathfrak{p})) = p.$$

This should remind the reader very much of Theorem 2.7. In fact, it is precisely these similarities that inspired the *modularity theorem*, which stood as a conjecture for a very long time until it was finally proved in the nineties.

To conclude this section, we also construct a Galois representation over a finite field that arises from a newform $f \in S_2(\Gamma_0(N))$. Even though $\rho_{f,\ell}$ maps to $GL_2(K_{f,\lambda})$, Proposition 9.3.5 from [16] shows that $\rho_{f,\ell}$ is equivalent to a representation with integral coefficients; that is, with its image contained in $GL_2(\mathcal{O}_{f,\lambda})$. Reducing this representation modulo λ yields

$$\rho_f^\lambda \colon G_\mathbb{Q} \to GL_2(\mathcal{O}_{f,\lambda}/\lambda\mathcal{O}_{f,\lambda}) \cong GL_2(\mathcal{O}_f/\lambda\mathcal{O}_f).$$

If the residue field degree of λ happens to be one, it follows that this defines a representation on $GL_2(\mathbb{F}_\ell)$, but since the representation need not be surjective, this is not a necessary condition. One may wonder when the representations induced by elliptic curves and modular forms coincide. This question lies at the core of some of the theorems in the next section.

2.2 Big theorems

This section lists some of the big results that allow us to apply the modular method. This first result is not too difficult and follows from the work done to establish dimension formulas in Chapter 3 of [16].

Proposition 2.11. *There exist no newforms of level at most 10. Furthermore, there also exist no newforms at the levels* 12, 13, 16, 18, 22, 25, 28 *and* 60. *At all other levels newforms do exist.*

The above proposition can sometimes be used to quickly arrive at a contradiction when applying the modular method to a Diophantine equation. Next we state the huge theorem that was hinted at near the end of the previous section. The first proof of this was given in [8], where it is Theorem A.

Theorem 2.12. *Let* $E/\mathbb{Q}$ *be an elliptic curve with conductor* N. *Then there exists some rational newform* f *with respect to the group* $\Gamma_0(N)$ *of level* N *such that for every prime number* ℓ, *there exists an equivalence of representations* $\rho_{E,\ell} \sim \rho_{f,\ell}$.

This result is known as the *modularity theorem* and its proof is far beyond the scope of this thesis. Conversely, the *Eichler-Shimura construction* allows for the association of an elliptic curve of conductor N to any rational newform for the group $\Gamma_0(N)$. This construction can be found in Section 6.6 of [16]. As is stated in Section 3 of [40], by showing that isogenous elliptic curves yield equivalent Galois representations, this has the following corollary.

Corollary 2.13. *For any positive integer* N *there is a bijection between isogeny classes of elliptic curves of conductor* N *and rational newforms with respect to* $\Gamma_0(N)$ *of level* N.

Remark 2.14. Should we compare the characteristic polynomials of the images of Frob_p under $\rho_{E,\ell}$ and $\rho_{f,\ell}$, we find that for all $p \nmid \ell N$ it holds that

$$a_p(E) = a_p(f).$$

As discussed in Section 8.8 in [16], it can be refined to show that this is enough to conclude that the above equality holds for all primes p. Hence given an elliptic curve, we know precisely what the Fourier coefficients of the claimed newform f in the above theorem must be. The association from a newform to an elliptic curve is not quite so easy to describe.

The following theorem concerns itself with mod-ℓ representations, instead of ℓ-adic representations.

Theorem 2.15. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and minimal discriminant $\Delta_{\min}$. Let $\ell \geqslant 3$ be a prime number such that ρ_E^ℓ is irreducible. Define*

$$N_\ell = N \Big/ \prod_{p \| N,\ \ell | \nu_p(\Delta_{\min})} p.$$

Then there exists a newform f of level N_ℓ such that we have an isomorphism of representations $\rho_E^\ell \sim \rho_f^\lambda$ for a suitable prime ideal $\lambda \subset \mathcal{O}_f$.

This result is known as *Ribet's Level Lowering Theorem* and its proof will not be treated here, but can in greater generality be found as Theorem 1.1 in [34]. There is an equivalent condition to ρ_E^ℓ being irreducible, which is not so hard to prove but will be very useful. Recall that an ℓ-isogeny of an elliptic curve is an isogeny of degree ℓ.

Proposition 2.16. *Let $E/\mathbb{Q}$ be an elliptic curve and ℓ a prime number. Then ρ_E^ℓ is irreducible if and only if E does not admit any rational isogenies of degree ℓ.*

Proof. First suppose that ρ_E^ℓ is reducible; that is, we have an invariant subspace $C \subset E[\ell]$, which is also a subgroup. Then E/C is again an elliptic curve, so the projection map $E \to E/C$ is separable and so has degree $\#\ker = |C| = \ell$. Since C is fixed by the Galois action, this isogeny can be defined over $\mathbb{Q}$. We refer the reader to III.4.12 and III.4.13 in [42] for the details. On the other hand, suppose that some rational isogeny $E \to F$ has degree ℓ, so that its kernel is a subgroup C of order ℓ in E. Now since the isogeny was rational, C is fixed under the Galois action, yielding an invariant subspace and thus making the representation reducible. □

Fortunately, there are results available that give us easy to check conditions which imply that an elliptic curve has no ℓ-isogenies. This will make it much easier to apply the level lowering theorem. Recall the j-invariant $j(E)$ of an elliptic curve E.

Definition 2.17. Let $E/\mathbb{Q}$ be an elliptic curve. Then we say that E is *semistable* if E has either good or multiplicative reduction at every prime.

Theorem 2.18. *Let $E/\mathbb{Q}$ be an elliptic curve and let $\ell \geqslant 5$ be a prime number.*

- *If $\#E(\mathbb{Q})[2] = 4$ and E is semistable, then E has no ℓ-isogenies.*
- *If $\ell \geqslant 17$ and $j(E) \notin \mathbb{Z}[1/2]$, then E has no ℓ-isogenies.*

We also opt to not treat the proof of the above theorem, but the first statement is Proposition 6 in [36] and the second is Corollary 4.4 in [33].

2.3 Examples of the modular method

We will now outline how the ideas and theorems from the previous section, combined with the ingenious notion of a *Frey curve*, can work together to solve the problem of Fermat's Last Theorem. First we take a brief moment to establish some terminology.

Definition 2.19. An integral solution (x, y, z) to a *ternary equation* of *signature* (p, q, r) of the form

$$Ax^p + By^q + Cz^r = 0$$

for some non-zero integers A, B and C and some positive integers p, q and r, is called

- *non-trivial* if $xyz \neq 0$;
- *primitive* if in addition Ax, By and Cz are pairwise coprime.

We will now work out the example of Fermat's Last Theorem thoroughly, for it is the most influential and famous example of its kind.

Theorem 2.20. *Let x, y and z be integers satisfying*

$$x^n + y^n + z^n = 0$$

for some integer $n \geqslant 2$. Then $xyz = 0$.

Proof. Due to the formulation of the theorem, the statement is trivial for even n. Of course, for the classic formulation of Fermat's Last Theorem one still has to consider the famous argument by infinite descent to solve the equation for $n = 4$. Now the case $n = 3$ can be solved by working in the ring $\mathbb{Z}[\zeta_3]$. Hence we may reduce to the case where $n = \ell \geqslant 5$ is a prime. The main trick is to define an elliptic curve using a supposed non-trivial solution to the equation, namely

$$E\colon Y^2 = X(X - x^\ell)(X + y^\ell).$$

Since the equation is homogeneous we may assume that x, y and z are pairwise coprime. Therefore precisely one of them is even, so we assume that $2 \mid y$. We may also assume that $x^\ell \equiv -1 \pmod 4$, for if not, we consider the solution $(-x, -y, -z)$. Now we have the following lemma, the proof of which can be found in Appendix A.

Lemma 2.21. *The elliptic curve defined above has the properties that*

$$\Delta_{\min} = (xyz)^{2\ell}/2^8 \quad \textit{and} \quad N = \operatorname{rad}(xyz).$$

Now we can prove Fermat's Last Theorem. We calculate N_ℓ by remarking that for all primes $p \mid N$ we have that $\ell \mid v_p(\Delta) = 2\ell$, but for the case $p = 2$. Namely, then $\ell \nmid v_2(\Delta) = 2\ell - 8$. Thus it follows that $N_\ell = 2$. Thus if E has no ℓ-isogenies, we may conclude from Theorem 2.15 that E has its mod-ℓ representation isomorphic to that of a newform of level 2. However, Proposition 2.11 tells us that such newforms do not exist, yielding a contradiction. To prove this absence of ℓ-isogenies, we invoke Theorem 2.18. We can clearly see that $E(\mathbb{Q})[2] = \{O, (0,0), (x^\ell, 0), (-y^\ell, 0)\}$ and since the conductor N is square free, we see that E has at most multiplicative reduction at every prime, showing that E is semistable. Hence Theorem 2.18 may be applied. □

This second example will show that the idea of a Frey curve is not just a one-hit-wonder, but can actually be applied to many different problems. We will prove the following theorem that has been previously shown as a special case of Theorem 1 in [39].

Theorem 2.22. *Let $\ell \geqslant 17$ a prime number. Then the equation*

$$x^2 = y^\ell + 4z^\ell$$

has no non-trivial primitive solutions for which z is odd.

Indeed, the idea will again be to define a suitable Frey curve. Thus, suppose that the above theorem is not true and consider a non-trivial primitive integral solution (x, y, z) to the equation $x^2 = y^\ell + 4z^\ell$ with z odd. Then we consider the elliptic curve

$$E\colon Y^2 = X(X^2 + 2xX + y^\ell), \text{ which satisfies } \Delta = 256(y^2z)^\ell \text{ and } j(E) = \frac{2^{12}(4x^2 - 3y^\ell)^3}{\Delta}.$$

Since x, y and $4z$ do not share any factors by assumption, both x and y will be odd. By considering $-x$ if necessary, we may assume that $x \equiv -1 \pmod 4$. We have the following lemma, the proof of which can again be found in Appendix A.

Lemma 2.23. *The elliptic curve defined above has the properties that*

$$\Delta_{\min} = \Delta \quad \textit{and} \quad N = \begin{cases} 4\mathrm{rad}(yz) & \textit{if } z^\ell \equiv -1 \pmod 4; \\ 16\mathrm{rad}(yz) & \textit{if } z^\ell \equiv 1 \pmod 4. \end{cases}$$

This allows us to complete the proof. Similar to the Fermat case, we see that $N_\ell = 4$ or $N_\ell = 16$, depending on the case which we are in. But by Proposition 2.11, newforms of these levels do not exist, so if Theorem 2.15 may be applied, we arrive at a contradiction. Since the elliptic curve can have additive reduction at 2, it is not semistable. Thus we rely on the second criterion in Theorem 2.18. To show that $j(E) \notin \mathbb{Z}[1/2]$, we suppose that y has an odd prime factor p. Then $p \mid \Delta$, but p does not divide the numerator in the expression for $j(E)$. Hence $j(E) \notin \mathbb{Z}[1/2]$. We may thus reduce to the case that $y = \pm 1$, so that $x^2 = \pm 1 + 4z^\ell$. Then we find that

$$j(E) = \frac{2^{12}(4x^2 \mp 3)^3}{256z^\ell} = \frac{16(4x^2 \mp 3)^3}{(x^2 \mp 1)} = 64\frac{(a \pm 1)^3}{a},$$

where $a = 4(x^2 \mp 1) = 16z^\ell$. If $j(E) \in \mathbb{Z}[1/2]$, one sees that a can only have factors of 2. But z is odd and so $a = \pm 16$, which is easily seen to be impossible. This concludes the proof. □

Remark 2.24. Perhaps a better way to show that $j(E) \notin \mathbb{Z}[1/2]$ might have been to remark that any odd prime p dividing either y or z will divide the conductor of E exactly once. Thus E has multiplicative reduction at p, so that $v_\ell(\Delta) > 0$, but c_4 is not divisible by p. Hence $v_\ell(j(E)) < 0$ and $j(E) \notin \mathbb{Z}[1/2]$. The cases where $y, z = \pm 1$ are quickly ruled out.

2.4 A symplectic criterion

In the previous two examples we got very lucky; using Ribet's level lowering theorem we were able to argue that a hypothetical solution to the equation of interest would imply the existence of a newform of a particular level, yielding a contradiction by observing that such newforms do not exist. In general, we cannot expect to be so lucky, for, as Proposition 2.11 shows, at all but finitely many levels, newforms actually do exist. The *symplectic method* gives us a way of arriving at a contradiction even when newforms do exist at the level that our argument has brought us.

In short, the symplectic method comes down to the following. When applying the modular method, after invoking the level lowering theorem using a Frey curve E, we obtain a newform f at some low level. If f is rational, it in turn corresponds to a rational elliptic curve F with small conductor such that $\rho_F^\ell \sim \rho_E^\ell$, which is equivalent to saying that $E[\ell]$ and $F[\ell]$ are isomorphic $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. Since these spaces are both isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$, the isomorphism between them must be a linear map. If we fix bases on both sides, it has a determinant that scales quadratically when we scale the isomorphism. One may thus wonder whether or not this determinant is a square modulo ℓ or not; that is, what is the *symplectic type* of the isomorphism.

It turns out that this is a very interesting question, and one that can often be answered using just the local information at one small prime at which the two elliptic curves have interesting reduction. The earliest known example of such a *symplectic* theorem is from the year 1992, when Kraus and Oesterlé showed in [31] a result, Proposition 2.31 in this thesis, that allows to determine the symplectic type of the isomorphism if the two considered elliptic curves E and F have a shared prime of good reduction. We give the full proof of this result in this section. In the year 2002, with the modularity theorem proved, in [25] the authors Kraus and Halberstadt showcased, among some other techniques, the usefulness of the symplectic theorem proved in [31] when solving Diophantine equations using the modular method. Among many other examples, they showed the result stated in Section 2.5 of this thesis on the equation $x^\ell + 3y^\ell + 5z^\ell = 0$.

For some time the symplectic method was not developed much further, until fairly recently most notably Freitas and Kraus regained interest in this topic. In [18], Freitas gave a novel symplectic criterion, Theorem 2.39 in this thesis, that allows to determine the symplectic type of the isomorphism when both elliptic curves have *potentially good* reduction at the prime 2, satisfying some additional assumptions. We give a full proof of this theorem in Section 2.6 of this thesis and in Sections 2.7 and 2.8 we explore some of its applications and how it can be used in unison with Proposition 2.31 to show the non-existence of primitive solutions to certain equations. Very important is the application given by Freitas in the same article that first proved this criterion, that shows that the equation $x^3 + y^3 = z^\ell$ does not have any non-trivial primitive integral solutions when the exponent satisfies $\ell \equiv 2 \pmod 3$.

Kraus and Freitas have been expanding the set of different symplectic criteria ever since, finding satisfying results for varying reduction types at varying primes and under varying additional assumptions. An overview of the current state of affairs is given in Section 4 of [20], where all currently known symplectic criteria are listed. At the start

of Chapter 4 we state a few of these results and sketch their proofs. In the remainder we use them, along with the criteria discussed in this chapter, to analyse numerous families of Diophantine equations and we show the non-existence of non-trivial primitive integral solutions for a positive density of the primes in each case.

It should be noted that more methods that can help with the modular method are available, for instance *comparing traces of Frobenius*, dealing with curves with *complex multiplication* and examining the *image of inertia*. These methods will be explained in more detail in the next chapter, as we will first focus on the symplectic method. Still, for all the upcoming statements that we will prove using the symplectic method, it was checked that none of these other methods were sufficient, thus ensuring its necessity.

The first applications of the symplectic method come down to the following result, first given in [25] as Lemme 1.6.

Theorem 2.25. *Let $E/\mathbb{Q}$ be an elliptic curve and ℓ be a prime number. Let $F/\mathbb{Q}$ be an elliptic curve such that $\rho_E^\ell \sim \rho_F^\ell$. Let p and q be distinct primes different from ℓ such that both E and F have multiplicative reduction at p and q. Further suppose that none of $v_p(\Delta_{\min}(E))$, $v_p(\Delta_{\min}(F))$, $v_q(\Delta_{\min}(E))$ and $v_q(\Delta_{\min}(F))$ are divisible by ℓ. Then*

$$\frac{v_p(\Delta_{\min}(E))v_q(\Delta_{\min}(E))}{v_p(\Delta_{\min}(F))v_q(\Delta_{\min}(F))} \quad \textit{is a square modulo } \ell.$$

Of course we could have simply written the expression in the theorem as a product instead of a quotient, because that doesn't change it being a square modulo ℓ. However, as we will see momentarily, writing it this way emphasises that this expression originates from comparing two quotients. In this section we will be working towards proving this theorem. In order to understand where this result comes from, we will first need a definition.

Definition 2.26. Let N be a positive integer and fix a primitive N-th root of unity ζ_N. Now let $E/\mathbb{Q}$ be an elliptic curve. Suppose that $E(\mathbb{C}) \cong \mathbb{C}/(w_1\mathbb{Z} \oplus w_2\mathbb{Z})$ with $w_1/w_2 \in \mathcal{H}$, so that $(w_1/N, w_2/N)$ is a basis for $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$. Then for any $P, Q \in E[N]$ there exists some $\gamma \in (\mathbb{Z}/N\mathbb{Z})^{2\times 2}$ such that

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} w_1/N \\ w_2/N \end{pmatrix}.$$

We then define the *Weil-pairing* to be

$$e_{E,N}(P, Q) = \zeta_N^{\det(\gamma)}.$$

Because any other ordered basis (w_1', w_2') for the lattice $w_1\mathbb{Z} + w_2\mathbb{Z}$ with $w_1'/w_2' \in \mathcal{H}$ is obtained from (w_1, w_2) by the action of an element of $SL_2(\mathbb{Z})$ on the lattice, the above definition is independent of the choice of basis.

Remark 2.27. We note that there is also a purely algebraic definition that omits the passage to the field $\mathbb{C}$, which can be found in Section III.8 in [42]. However, we will

only need the definition for $\mathbb{C}$, as we will only be working over ℓ-adic fields in the forthcoming, which can be embedded into $\mathbb{C}$. For the sake of completion, we will state the general definition here regardless.

Let $P, Q \in E[N]$. Proposition III.3.5 in [42] gives us the existence of some f in the function field of E with divisor equal to $N \cdot P - N \cdot O$, where $O \in E$ denotes the unit element. Denoting by ϕ^* the pullback of a morphism ϕ, there also exists a function g in the function field with divisor $[N]^*P - [N]^*O$, so that by looking at their divisors, we have the equality $f \circ [N] = g^N$ up to a scalar, which we choose to be 1. Now observe that

$$g(X+Q)^N = f(N(X+Q)) = f(NX) = g(X)^N.$$

So the function $g(X+Q)/g(X)$ can only take values in N-th roots of unity and by its continuity it must be constant. One defines

$$e_{E,N}(P,Q) = g(X+Q)/g(X)$$

for some X such that the expression on the right makes sense.

It can be shown that these definitions coincide if one chooses ζ_N in the first definition for the Weil-pairing to agree with the image of $e_{E,N}(w_1/N, w_2/N)$ in the second definition. Namely, the Weil-pairing can for both definitions be shown to be alternating and bilinear; see for instance Section 1.3 in [16] and III.8 in [42]. Identifying $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$, $w_1/N = e_1$ and $w_2/N = e_2$, the image of $e_{E,N}(e_1, e_2)$ then fixes $e_{E,N}(ke_1, e_2)$ and so $e_{E,N}(ke_1, k'e_2)$ by bilinearity. Because it is alternating, we also know $e_{E,N}(k'e_2, k'e_2) = 1$ and combining these last two yields again by bilinearity the image of $e_{E,N}(P, k'e_2)$ for all $P \in E[N]$. Using this same argument again we find that $e_{E,N}(P,Q)$ is completely determined for all $P, Q \in E[N]$, proving the claim.

It turns out that the Weil pairing behaves very well with respect to isogenies, as is shown in Proposition III.8.2 in [42]. We will only need this result later, but we will state it here for convenience.

Proposition 2.28. *Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves and write $\hat{\phi}$ for its dual isogeny. Then we have for all positive integers N and $P \in E_1[N]$, $Q \in E_2[N]$ that*

$$e_{E_1,N}(P, \hat{\phi}(Q)) = e_{E_2,N}(\phi(P), Q).$$

Because $\hat{\phi} = \phi^{-1}$ for $\phi \in \mathrm{Aut}(E)$, it follows that automorphisms respect the Weil pairing.

Now let ℓ be a prime and recall that $\rho_F^\ell \sim \rho_E^\ell$ if and only if $E[\ell]$ and $F[\ell]$ are isomorphic $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, generally called *Galois modules*. From now on we will restrict our view to prime torsion. The following lemma tells us what happens to the Weil pairing under an isomorphism between Galois modules.

Lemma 2.29. *Let E and F be elliptic curves over $\mathbb{Q}$ and let ℓ be a prime number such that there exists an isomorphism of Galois modules $\varphi : E[\ell] \to F[\ell]$. Then there exists some non-zero number $r(\varphi) \in \mathbb{F}_\ell$ such that $e_{F,\ell}(\varphi(P), \varphi(Q)) = e_{E,\ell}(P,Q)^{r(\varphi)}$ for all $P, Q \in E[\ell]$. Furthermore, for any non-zero $a \in \mathbb{F}_\ell$, we have $r(a\varphi) = a^2 r(\varphi)$.*

Proof. Write $(w_1/\ell, w_2/\ell)$ for an ordered basis as in the definition of the Weil-pairing for E. Then $(\varphi(w_1/\ell), \varphi(w_2/\ell))$ must be a basis for $F[\ell]$. We observe that since $E[\ell], F[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, we may regard $\varphi \in \mathrm{Aut}(\mathbb{F}_\ell^2) = \mathrm{GL}_2(\mathbb{F}_\ell)$. So if

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} w_1/\ell \\ w_2/\ell \end{pmatrix}, \quad \text{then} \quad \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} = \gamma \begin{pmatrix} \varphi(w_1/\ell) \\ \varphi(w_2/\ell) \end{pmatrix} = \gamma\gamma' \begin{pmatrix} w_1'/\ell \\ w_2'/\ell \end{pmatrix},$$

where γ' is the basis transformation between $(\varphi(w_1/\ell), \varphi(w_2/\ell))$ and $(w_1'/\ell, w_2'/\ell)$, where $F(\mathbb{C}) \cong \mathbb{C}/(w_1'\mathbb{Z} \oplus w_2'\mathbb{Z})$ with $w_1'/w_2' \in \mathcal{H}$. It now follows immediately from the definition that $r(\varphi) = \det(\gamma')$. For the second part, we observe that if we multiply the isomorphism φ by some constant a, the change of basis map γ' will be multiplied with a as well. Then it follows that $r(a\varphi) = \det(a\gamma') = a^2\det(\gamma') = a^2 r(\varphi)$, which concludes the proof. □

One may wonder whether or not the isomorphism between the Galois modules preserves the Weil pairing, or at least up to a scalar multiple. This gives rise to the following definition.

Definition 2.30. Let E and F be elliptic curves over $\mathbb{Q}$ and let ℓ be a prime number. Then an ordered basis (P, Q) for $E[\ell]$ is called *symplectic* if $e_{E,\ell}(P, Q) = \zeta_\ell$. Now suppose that there exists some $\varphi : E[\ell] \to F[\ell]$ that is an isomorphism of Galois modules. Then we say φ is a *symplectic* isomorphism if $r(\varphi)$ is a square modulo ℓ. If $r(\varphi)$ is not a square, we say that φ is *anti-symplectic*.

This is the language that Theorem 2.25 is hiding. Namely, it turns out that it is a natural corollary of the following statement about symplectic isomorphisms. This proposition was first proved in [31] as Proposition 2.

Proposition 2.31. *Let $E/\mathbb{Q}$ be an elliptic curve and let p and ℓ be distinct prime numbers. Let $F/\mathbb{Q}$ be an elliptic curve such that $E[\ell]$ and $F[\ell]$ are isomorphic Galois modules and suppose that both E and F have multiplicative reduction at p. Further suppose that neither $v_p(\Delta_{\min}(E))$ nor $v_p(\Delta_{\min}(F))$ is divisible by ℓ. Then $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if $v_p(\Delta_{\min}(E))$ and $v_p(\Delta_{\min}(F))$ differ by a square modulo ℓ.*

Assuming this proposition, the proof of Theorem 2.25 is almost trivial. Namely, in the case that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic, then both $v_p(\Delta_{\min}(E))/v_p(\Delta_{\min}(F))$ and $v_q(\Delta_{\min}(E))/v_q(\Delta_{\min}(F))$ are squares modulo ℓ, and thus so will their product be. In the case that $E[\ell]$ and $F[\ell]$ are in fact anti-symplectically isomorphic, then both of $v_p(\Delta_{\min}(E))/v_p(\Delta_{\min}(F))$ and $v_q(\Delta_{\min}(E))/v_q(\Delta_{\min}(F))$ are non-squares modulo ℓ. But then by the multiplicativity of the Legendre symbol, their product will in fact again be a square, concluding the proof.

Now what remains to be done is proving Proposition 2.31. However, we will first need a bit of theory about elliptic curves over local fields in order to carry out the proof. Recall that a field k is called *complete* when it comes with a multiplicative norm with respect to which it is complete; that is, every Cauchy sequence in k converges to an element in k. For every field k with such a norm, there exists a field $k' \supset k$ with an

extension of the norm map such that k' is complete. There even exists a smallest such k', meaning that it embeds into any other field with the properties above. This makes k' unique up to isometric isomorphism and it is generally referred to as the *completion* of the field k.

A *local* field is a field k with a discrete valuation $\nu : K \to \mathbb{Z}$. We let $R = \{x \in K \mid \nu(x) \geqslant 0\}$ denote its ring of integers and we define a *uniformiser* to be an element $\pi \in K$ such that $\nu(\pi) = 1$. If the cardinality q of the residue field $R/(\pi)$ is finite, we have a natural multiplicative norm by defining $|x| = q^{-\nu(x)}$. Clearly the ℓ-adic numbers and its algebraic extensions are local fields for every prime ℓ.

As a motivation for the forthcoming ideas, recall that over the complex numbers any elliptic curve can be written as $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ for some $\tau \in \mathcal{H}$. Applying the exponential map gives us an isomorphism $E(\mathbb{C}) \cong \mathbb{C}^\times/q^{\mathbb{Z}}$, where $q = e^{2\pi i\tau} \in \{z \in \mathbb{C} \mid |z| < 1\}$ and $q^{\mathbb{Z}} = \{q^n \mid n \in \mathbb{Z}\}$. The following result is a slight generalisation of Theorem V.3.1 in [41], which is mostly proved in Sections V.3 and V.4. All discriminants appearing in the remainder of this section will be minimal.

Theorem 2.32. *Let k be a complete local field with norm $\|\cdot\|$ and let $q \in k^\times$ so that $\|q\| < 1$. Then there exists an elliptic curve E_q over k such that $E_q(\overline{k}) \cong \overline{k}^\times/q^{\mathbb{Z}}$ as $\mathrm{Gal}(\overline{k}/k)$-modules, and it has the property that $\|\Delta(E_q)\| = \|q\| < 1$ and $\|j(E_q)\| = \|q^{-1}\| > 1$.*

The curve E_q above is known as a *Tate curve*. Now a natural question would be to ask which elliptic curves over k can be realised by a quotient $\overline{k}^\times/q^{\mathbb{Z}}$ for some $q \in k$ with $\|q\| < 1$. Fortunately, Theorem 5.3 in [41] has an answer to this question, the proof of which spans most of Section V.5. The following Theorem is slightly more general than what is proved there.

Theorem 2.33. *Let k be a complete local field with norm $\|\cdot\|$ and let E be an elliptic curve over k. Suppose that $\|j(E)\| > 1$. Then there exists some $q \in k^\times$ with $\|q\| < 1$ such that $E(\overline{k}) \cong \overline{k}^\times/q^{\mathbb{Z}}$ as $\mathrm{Gal}(\overline{k}/L)$-modules for some field L that is unramified over k of degree at most 2.*

Now we are finally fully equipped to tackle the proof of Proposition 2.31.

Proof. (of Proposition 2.31) We will first have to do some preparation, and after that the equivalence will follow quite easily. Consider the maximal unramified extension of $\mathbb{Q}_p$, which is given by adjoining all n-th roots of unity for all n coprime to p, and let k be its completion. Then in particular k will contain all ℓ-th roots of unity and both E and F will have multiplicative reduction at p over k, as Proposition III.5.4 of [42] tells us that unramified extensions preserve reduction type. It then follows that $\|j\| = \|c_4\|^3/\|\Delta\| = 1/\|\Delta\| > 1$ for both E and F. Hence from Theorem 2.33 we may conclude that there exist $q_E, q_F \in k$ with the properties that $\nu_p(q_E) = \nu_p(\Delta(E))$ and $\nu_p(q_F) = \nu_p(\Delta(F))$ and

$$E(\overline{k}) \cong \overline{k}^\times/q_E^{\mathbb{Z}} \quad \text{and} \quad F(\overline{k}) \cong \overline{k}^\times/q_F^{\mathbb{Z}},$$

as $\mathrm{Gal}(\overline{k}/L)$-modules for some unramified extension L of k of degree at most 2. But since k was maximal unramified, we must have $k = L$ and so we have an isomorphism of $\mathrm{Gal}(\overline{k}/k)$-modules. Let $\varphi : E(\overline{\mathbb{Q}})[\ell] \to F(\overline{\mathbb{Q}})[\ell]$ be the assumed isomorphism of Galois modules. Then we observe that all the ℓ-torsion points of E are defined over $\overline{\mathbb{Q}}$, and so $\mathrm{Gal}(\overline{k}/\overline{\mathbb{Q}})$ acts trivially on the ℓ-torsion points of E. Thus any embedding $\overline{\mathbb{Q}} \to \overline{k}$ induces an isomorphism $\psi : E(\overline{k})[\ell] \to F(\overline{k})[\ell]$ of $\mathrm{Gal}(\overline{k}/k)$-modules. Because they are given by the same matrix, φ is symplectic precisely when ψ is symplectic.

Since we assumed that ℓ does not divide $\nu_p(\Delta(E))$ or $\nu_p(\Delta(F))$, we may choose integers n, m such that $\nu_p(\Delta(F)) = n\nu_p(\Delta(E)) + m\ell$, with $\ell \nmid n$. Let γ_E be an ℓ-th root of q_E in $\overline{k}$. Now observe that by construction $\nu_p(q_F/(q_E^n p^{m\ell})) = 0$. Now we consider the polynomial $X^\ell - [q_F/(q_E^n p^{m\ell})]$ over k, with discriminant $\ell^\ell [q_F/(q_E^n p^{m\ell})]^{\ell-1}$. Since p does not divide the discriminant, adding a zero α to k would yield an unramified extension of k. But by maximality of k, we must thus have $\alpha \in k$. Hence there exists some $\alpha \in k$ such that $\alpha^\ell = q_F/(q_E^n p^{m\ell})$. Then the element $\gamma_F = \gamma_E^n p^m \alpha \in \overline{k}$ is quickly seen to be an ℓ-th root of q_F.

Now Proposition 2.2 gives us that $E(\overline{k})[\ell]$ and $F(\overline{k})[\ell]$ are both isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. Write ζ for a primitive ℓ-th root of unity in k, such that $(\zeta q_E^{\mathbb{Z}}, \gamma_E q_E^{\mathbb{Z}})$ is a symplectic basis for the ℓ-torsion of E. To see that this is possible, observe that for any given basis of $\mathbb{F}_\ell^2$ and any other basis (v, w) of $\mathbb{F}_\ell^2$, there exists a scalar $a \in \mathbb{F}_\ell$ such that the matrix representing the basis change to (v, aw) has unit determinant. Applying this to a given symplectic basis and $v = \gamma_E$ and w an arbitrary primitive ℓ-th root of unity in k, the result follows. By a similar argument we may also choose α in such a way that $(\zeta q_F^{\mathbb{Z}}, \gamma_F q_F^{\mathbb{Z}})$ is a symplectic basis for the ℓ-torsion of F.

We remark that in both cases, the subspace spanned by ζ is fixed under the action of $\mathrm{Gal}(\overline{k}/k)$, because we chose $\zeta \in k$. Since $\psi : E(\overline{k})[\ell] \to F(\overline{k})[\ell]$ was an isomorphism of $\mathrm{Gal}(\overline{k}/k)$-modules, we must have

$$\psi = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

in the bases chosen above. Now let $\sigma \in \mathrm{Gal}(\overline{k}/k)$ be an element that satisfies $\sigma(\gamma_E) = \zeta\gamma_E$. Then we have by construction that

$$\sigma(\gamma_F) = \sigma(\gamma_E^n p^m \alpha) = \sigma(\gamma_E)^n p^m \alpha = \zeta^n \gamma_E^n p^m \alpha = \zeta^n \gamma_F.$$

Now ψ must commute with the action of σ, again because it is an isomorphism of $\mathrm{Gal}(\overline{k}/k)$-modules. Writing the action of σ out in terms of matrices, we find that

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

and thus by looking at the top-left entry, we conclude that $a \equiv nd \pmod{\ell}$. Then since $(\zeta q_E^{\mathbb{Z}}, \gamma_E q_E^{\mathbb{Z}})$ and $(\zeta q_F^{\mathbb{Z}}, \gamma_F q_F^{\mathbb{Z}})$ were symplectic bases, we can now compute that for $P, Q \in E(\overline{k})[\ell]$ we have

$$e_{F,p}(\psi(P), \psi(Q)) = e_{E,p}(P, Q)^{\det(\psi)} = e_{E,p}(P, Q)^{nd^2}.$$

Now the proposition will follow easily. We observe that $v_p(\Delta(F)) \equiv n v_p(\Delta(E)) \pmod{\ell}$, so $v_p(\Delta(E))$ and $v_p(\Delta(F))$ differ by a square mod ℓ if and only if n is a square. But then the exponent nd^2 is also a square, making the isomorphism ψ and thus also φ symplectic. Conversely, if the isomorphism φ is symplectic, then also ψ and so nd^2 is a square mod ℓ. Hence n is a square mod ℓ, which concludes the proof. □

2.5 An application of the symplectic method

The idea is that Theorem 2.25 allows us to sometimes conclude that a certain equation has no non-trivial solutions. An example of this will be outlined below. This result was first proved as part of Proposition 2.2 in [25].

Theorem 2.34. *Let $\ell \geqslant 5$ be a prime such that $12 \nmid \ell - 1$. Then any integers (x, y, z) satisfying*

$$x^\ell + 3y^\ell + 5z^\ell = 0$$

for which y is even, must satisfy $x = y = z = 0$.

Remark 2.35. The condition $\ell \geqslant 5$ will appear naturally in the proof. Now, it is trivial to see that the theorem still holds for $\ell = 2$. However, it is worth remarking that the theorem will fail to hold for $\ell = 3$, since $(x, y, z) = (2, -1, -1)$ is easily seen to be a solution in that case and so are scalar multiples. A second family of solutions is given by $(x, y, z) = (4, 13, -11)$. In fact, using the function EllipticCurve in Magma [7] with the first solution, we see that this curve is isomorphic to the elliptic curve $y^2 + y = x^3 - 1519$. Using the function RankBounds in Magma we see that this curve has rank 1 over $\mathbb{Q}$, meaning that there will be infinitely many families of solutions.

The remainder of this section will treat the proof of the above theorem. Unsurprisingly, it starts once more by defining a certain elliptic curve using a solution to the above equation such that $xyz \neq 0$. We may consider a solution such that x, $3y$ and $5z$ are pairwise coprime. As before, we may also assume that $x^\ell \equiv -1 \pmod{4}$. Then we consider the Frey curve

$$E\colon Y^2 = X(X - x^\ell)(X + 3y^\ell).$$

This should remind the reader of the curve we defined when proving Fermat's Last Theorem. It might therefore not come as a surprise that the following lemma holds, the proof of which can be found in Appendix A.

Lemma 2.36. *Let E be the elliptic curve as above. Then we have that*

$$\Delta_{\min}(E) = (15)^2(xyz)^{2\ell}/2^8 \quad \text{and} \quad N_E = \operatorname{rad}(15xyz).$$

The above shows that E has at most multiplicative reduction at every prime, making it semistable. Now it also has full rational 2-torsion, so that by Theorem 2.18 we obtain that E has no ℓ-isogenies. In this case we have that $N_\ell = 30$. It turns out that there exists a unique newform f at level 30, so we have not arrived at our contradiction yet.

Using a computer algebra system, for instance the software Magma [7] and the function EllipticCurve, we may carry out the association $f \mapsto F$ to obtain the explicit curve

$$F\colon Y^2 + XY + Y = X^3 + X + 2, \quad \text{with} \quad \Delta(F) = -2160 = -2^4 \cdot 3^3 \cdot 5 \quad \text{and} \quad N_F = 30.$$

In order to apply Theorem 2.25, we must determine what the reduction of F is modulo the primes 2, 3 and 5. To that end, we can compute that $c_4(F) = -71$ and we note that none of these primes divide $c_4(F)$, making the reduction multiplicative. Because at least one of x, y and z must be even, E also has multiplicative reduction at these primes.

Now we can apply Theorem 2.25 to each of the pairs of primes $(2,3)$, $(2,5)$ and $(3,5)$ to obtain that all of

$$\frac{(2\ell v_2(xyz) - 8)(2\ell v_3(xyz) + 2)}{4 \cdot 3}, \quad \frac{(2\ell v_2(xyz) - 8)(2\ell v_5(xyz) + 2)}{4 \cdot 1}$$
$$\text{and} \quad \frac{(2\ell v_3(xyz) + 2)(2\ell v_5(xyz) + 2)}{3 \cdot 1}$$

must be squares modulo $\ell \geqslant 5$. These expressions may be simplified to

$$\frac{-16}{12} = \frac{-4}{3}, \quad \frac{-16}{4} = -4, \quad \text{and} \quad \frac{4}{3},$$

which must all be squares modulo ℓ. We can see that if the latter two are squares, so will the first one, so we may disregard it. We know that $4 \cdot 3^{-1}$ is a square modulo ℓ precisely when 3 is, and that happens precisely when $\ell \equiv \pm 1 \pmod{12}$. We also know that -4 is a square precisely when -1 is, and so we obtain that $\ell \equiv 1 \pmod 4$. Combined we find that $\ell \equiv 1 \pmod{12}$, but this was the precise case we excluded from the theorem. Hence we arrive at a contradiction. □

2.6 Another symplectic criterion

Using the fact that ℓ-torsion modules, when isomorphic, can be symplectically or anti-symplectically isomorphic, it is possible to derive more useful results, different from Theorem 2.25. The main result of this section was first proved in [18], where it was used to show that the equation $x^3 + y^3 = z^\ell$ has no non-trivial primitive solutions for $\ell \equiv 2 \pmod 3$. Shortly after, this theorem was also used to show that $3x^\ell + 8y^\ell + 21z^\ell = 0$ and $3x^\ell + 4y^\ell + 5z^\ell = 0$ have no non-trivial solutions when ℓ falls in certain residue classes modulo 24. The details of the final statement just mentioned will be proved in the next section, whereas we will examine the equation $x^3 + y^3 = z^\ell$ in the section thereafter.

We first need a quick definition.

Definition 2.37. Let k be a local field as in Section 2.4 and let E/k be an elliptic curve. Then we say that E has *potentially good reduction* if there exists a finite field extension L/k such that E/L has good reduction.

The following proposition makes the above an easy property to verify. The proof can be found as Proposition VII.5.5 in [42].

Proposition 2.38. *Let E/k be an elliptic curve over a complete local field k with valuation map v. Then E has potentially good reduction if and only if $v(j(E)) \geqslant 0$.*

In particular the above result will hold for elliptic curves over the local field $\mathbb{Q}_p$ for any prime number p, because they are complete with respect to their respective p-adic norms. For k a local field, E/k an elliptic curve and ℓ a prime number, we write $k(E[\ell])$ for the extension of k obtained by adjoining to k all the x and y coordinates of points in $E[\ell] \subset \overline{k}$. If E has potentially good reduction at ℓ, the *criterion of Néron-Ogg-Shafarevich* can be used to show that $k(E[\ell])/k$ is an extension of k making the reduction good. Recall that the maximal unramified extension of $\mathbb{Q}_p$, denoted $\mathbb{Q}_p^{un}$, is obtained by adjoining all the primitive n-th roots of unity for all n coprime to p. For an elliptic curve E over $\mathbb{Q}_p$ with potentially good reduction, one can even show that for any $\ell \geqslant 3$, the field $L = \mathbb{Q}_p^{un}(E[\ell])$ is the minimal extension of $\mathbb{Q}_p^{un}$ at which E achieves good reduction, see for instance Corollary 3 in [38]. This explains why L is often referred to as the *semistability defect*.

We now state the main result of this section, first proved in [18] as Theorem 4.

Theorem 2.39. *Let ℓ be an odd prime and let $E/\mathbb{Q}_2$ and $E'/\mathbb{Q}_2$ be elliptic curves with potentially good reduction at 2. Write $L = \mathbb{Q}_2^{un}(E[\ell])$ and $L' = \mathbb{Q}_2^{un}(E'[\ell])$. Suppose that $L = L'$ and that $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$. Then $E[p]$ and $E'[p]$ are isomorphic $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules for all odd primes p. Moreover, if 2 is a square mod ℓ, they are symplectically isomorphic. Otherwise they are symplectically isomorphic if and only if $v_2(\Delta_{\min}(E)) \equiv v_2(\Delta_{\min}(E')) \pmod 3$.*

The proof of this statement will require a lot of work, which we will split in a number of different lemmas. First we explore a possible issue with Theorem 2.39. Suppose that we have proved a symplectic isomorphism of $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules, and by definition of L this implies symplectically isomorphic $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2^{un})$-modules. If we would want to use Theorem 2.39 in unison with the result from Proposition 2.31, we need symplectically isomorphic $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-modules. Fortunately, we have the following result from [25], where it can be found as Lemme A.4.

Proposition 2.40. *Let E and E' be elliptic curves over a field k and let L/k be an algebraic field extension. Let $\ell \neq \mathrm{char}(k)$ be a prime number and suppose that $E[\ell]$ and $E'[\ell]$ are isomorphic $\mathrm{Gal}(\overline{k}/k)$-modules. Suppose further that the image of $\mathrm{Gal}(\overline{L}/L)$ in $\mathrm{GL}(E[\ell])$ is non-abelian. Then if $E[\ell]$ and $E'[\ell]$ are symplectically isomorphic $\mathrm{Gal}(\overline{L}/L)$-modules, then they are also symplectically isomorphic $\mathrm{Gal}(\overline{k}/k)$-modules.*

Proof. Let $\varphi : E[\ell] \to E'[\ell]$ be a symplectic isomorphism of $\mathrm{Gal}(\overline{L}/L)$-modules and $\psi : E[\ell] \to E'[\ell]$ an isomorphism of $\mathrm{Gal}(\overline{k}/k)$-modules. It then follows that $\psi^{-1} \circ \varphi$ is an automorphism of the $\mathrm{Gal}(\overline{L}/L)$-module $E[\ell]$. In terms of matrices, it follows that the matrix of $\psi^{-1} \circ \varphi$ commutes with the image of $\mathrm{Gal}(\overline{L}/L)$ in $\mathrm{GL}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$. We show that this forces $\psi^{-1} \circ \varphi = \lambda\,\mathrm{id}$ for some $\lambda \in \mathbb{F}_\ell$, so that $\varphi = \lambda\psi$, making ψ also symplectic and concluding the proof.

To prove the claim, let M denote the matrix of $\psi^{-1} \circ \varphi$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$. If M is not a multiple of the identity, we can find some vector v that is not an eigenvector of M. Hence $\{v, Mv\}$ is a basis for $\mathbb{F}_\ell^2$. If A is any matrix that commutes with M, then if we

write $Av = av + bMv = (a\,\mathrm{id} + bM)v$ for some $a, b \in \mathbb{F}_\ell$, it follows that $AMv = MAv = M(a\,\mathrm{id} + bM)v = (a\,\mathrm{id} + bM)Mv$. We see that the matrices A and $a\,\mathrm{id} + bM$ agree on a basis, making them equal. Hence we conclude that all the elements that commute with M are given by $\{a\,\mathrm{id} + bM \mid a, b \in \mathbb{F}_\ell\}$. All these elements commute, but it contains the image of $\mathrm{Gal}(\overline{L}/L)$ in $\mathrm{GL}(E[\ell])$, which was assumed to be non-abelian. This is a contradiction, proving our claim. □

Remark 2.41. We observe that the exact same argument as in the previous lemma can be used to show that if we are in the situation from Theorem 2.39 and $E[\ell]$ and $F[\ell]$ are isomorphic Galois modules, then they cannot be both symplectically isomorphic and anti-symplectically isomorphic.

With these concerns out of the way, we will focus on the proof of Theorem 2.39. In the end, the computational criteria will rely on the following rather technical result about the explicit groups in question. It will immediately show the significance and origin of 2 being a square modulo ℓ or not.

Lemma 2.42. *Let ℓ be an odd prime and let $G = \mathrm{GL}_2(\mathbb{F}_\ell)$. Let $H \subset \mathrm{SL}_2(\mathbb{F}_\ell) \subset G$ be a subgroup satisfying $H \cong \mathrm{SL}_2(\mathbb{F}_3)$. Then we have*

$$N_G(H)/Z(G) \cong \mathrm{Aut}(H) \cong S_4,$$

where $N_G(H) = \{g \in G \mid gH = Hg\}$ is the normaliser, $Z(G) = \{\lambda\,\mathrm{id} \mid \lambda \in \mathbb{F}_\ell\}$ is the centre and $\mathrm{Aut}(H)$ is the automorphism group of H. The first isomorphism is given by conjugation. Moreover, if 2 is a square modulo ℓ, then all elements from $N_G(H)$ have square determinant modulo ℓ. Otherwise, the matrices with square determinant modulo ℓ correspond to the subgroup of $\mathrm{Aut}(H)$ isomorphic to A_4, which consists of precisely the inner automorphisms.

The proof can be found as Lemma 3 in [18] and it is purely by elementary considerations and manipulations in these explicit finite groups. We will also need the following lemmas before we can get started with the proof of Theorem 2.39.

Lemma 2.43. *Let E and E' be elliptic curves over $\mathbb{Q}_2$ and write $\overline{E}$ and $\overline{E}'$ for the elliptic curves over $\overline{\mathbb{F}}_2$ obtained by reducing E/L and E'/L. Then we have natural injective homomorphisms $\psi : \mathrm{Aut}(\overline{E}) \to \mathrm{SL}(\overline{E}[\ell]) \subset \mathrm{GL}(\overline{E}[\ell])$ and $\psi' : \mathrm{Aut}(\overline{E}') \to \mathrm{SL}(\overline{E}'[\ell]) \subset \mathrm{GL}(\overline{E}'[\ell])$.*

Proof. Clearly automorphisms map ℓ-torsion to ℓ-torsion. To see that ψ and ψ' map to the determinant 1 matrices, we recall Proposition 2.28. Automorphisms preserve the Weil-pairing, and so must map a symplectic basis for the ℓ-torsion to a symplectic basis. In particular it follows that the determinant of this transformation must be equal to 1. To see that ψ and ψ' are injective, we recall that automorphisms of elliptic curves, when embedded into $\mathbb{P}^2_k$ for k the (algebraically closed) field over which we are working, extend uniquely to automorphisms of the whole of $\mathbb{P}^2_k$. This is because automorphisms of elliptic curves are given by suitable substitutions of the form $x' = u^2x + a$ and $y' = u^3y + bx + c$, so that any automorphism of E indeed extends as the map $(1 : x : y) \to (1 : u^2x + a : u^3y + bx + c)$. Now for all odd primes ℓ we can choose four points of $E[\ell]$,

no four of which lie on a line. Since automorphisms of $\mathbb{P}^2_k$ are uniquely determined by their images of four such points, it follows that any automorphism fixing these points must be equal to the identity, making the action faithful. □

Lemma 2.44. *Continuing with the notation from above, we also have injective homomorphisms* $\gamma_E : \mathrm{Gal}(L/\mathbb{Q}_2^{un}) \to \mathrm{Aut}(\overline{E})$ *and* $\gamma_{E'} : \mathrm{Gal}(L/\mathbb{Q}_2^{un}) \to \mathrm{Aut}(\overline{E}')$ *induced by the action of* $\mathrm{Gal}(L/\mathbb{Q}_2)$ *on* L*, and thus on the points of* E *and* E'*. Let* $\rho_{E,\ell}$ *be the Galois representation on* $E[\ell]$ *of* $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$ *induced by* E *and write* $\varphi : E \to \overline{E}$ *for the reduction morphism. Then for all* $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_2^{un})$ *we have that*

$$\varphi \circ \rho_{E,\ell}(\sigma) = \psi(\gamma_E(\sigma)) \circ \varphi.$$

Proof. We only sketch the proof. One approach is outlined in the text above Corollary 2 in Section 2 of [38], where it is shown that for any abelian variety with potentially good reduction, the inertia group, which can be shown to be isomorphic to $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$, acts faithfully on the Tate module T_ℓ. Because one can show that $\mathrm{Aut}(T_\ell) \cong \mathrm{Aut}(\overline{E})$, the injectivity of γ_E follows. A more direct approach is taken in Section 16 of [20]. Here it is shown via direct computations and explicit Weierstrass transformations precisely how an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_2^{un})$ induces an automorphism of $\overline{E}$. It is then verified by hand that the equality $\varphi \circ \rho_{E,\ell}(\sigma) = \psi(\gamma_E(\sigma)) \circ \varphi$ holds for this definition of γ_E. It then follows immediately that γ_E is a homomorphism. Its injectivity will then follow from the observation that $\rho_{E,\ell} : \mathrm{Gal}(L/\mathbb{Q}_2^{un}) \to \mathrm{GL}(E[\ell])$ is injective by the definition of $L = \mathrm{Gal}(\mathbb{Q}_2^{un}(E[\ell])/\mathbb{Q}_2^{un})$ and because $\ell \neq 2$, the reduction map φ is injective on the ℓ-torsion by Proposition VII.3.1 from [42]. Hence the right hand side describes an injective morphism, and so the left hand side must as well, forcing γ_E to be injective. □

Lemma 2.45. *Under the conditions of Theorem 2.39,* $\psi \circ \gamma_E$ *and* $\psi' \circ \gamma_{E'}$ *are isomorphic representations of* $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$*.*

Proof. We assumed that $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$, and so using Lemma 2.44, we find that $|\mathrm{Aut}(\overline{E})| \geqslant |\mathrm{SL}_2(\mathbb{F}_3)| = 24$. From a slight refinement of Theorem III.10.1 in [42] it then follows that $\mathrm{Aut}(\overline{E}) \cong \mathrm{SL}_2(\mathbb{F}_3)$, making both γ_E and $\gamma_{E'}$ isomorphisms of groups. Now Theorem III.10.1 from [42] also tells us that we must have $j(\overline{E}) = 0$, and similarly $j(\overline{E}') = 0$. Since their j-invariants coincide, it follows that $\overline{E}$ and $\overline{E}'$ are isomorphic over $\overline{\mathbb{F}}_2$. Thus we may assume that both E/L and E'/L reduce to the same $\overline{E}$, also identifying $\psi = \psi'$. So it follows that

$$\psi(\gamma_E(\mathrm{Gal}(L/\mathbb{Q}_2^{un}))) = \psi(\gamma_{E'}(\mathrm{Gal}(L/\mathbb{Q}_2^{un}))) = \psi(\mathrm{Aut}(\overline{E})) \subset \mathrm{SL}(\overline{E}[\ell]) \cong \mathrm{SL}_2(\mathbb{F}_\ell).$$

Since γ_E, $\gamma_{E'}$ were isomorphisms and ψ is an isomorphism onto its image, it follows that there must be some $\alpha \in \mathrm{Aut}(\psi(\mathrm{Aut}(E)))$ such that $\psi \circ \gamma_E = \alpha \circ \psi \circ \gamma_{E'}$. But then by Lemma 2.42 we find some $g \in N_G(\mathrm{Aut}(\overline{E}))$ such that $\alpha(x) = gxg^{-1}$ for all $x \in \psi(\mathrm{Aut}(E))$. Combining these two last assertions shows that g intertwines $\psi \circ \gamma_E$ and $\psi \circ \gamma_{E'}$, as desired. □

Corollary 2.46. *Consider the situation as in Theorem 2.39. Then* $E[\ell]$ *and* $E'[\ell]$ *are isomorphic* $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$*-modules.*

Proof. We note that φ is an isomorphism between $\mathbb{F}_\ell$-vector spaces $E(L)[\ell]$ and $\overline{E}(\overline{\mathbb{F}}_2)[\ell]$, and similarly φ' is an isomorphism between $E'(L)[\ell]$ and $\overline{E}'(\overline{\mathbb{F}}_2)[\ell]$. By Lemma 2.44, φ and φ' are intertwiners, and so it follows that $E[\ell]$ and $E'[\ell]$ are isomorphic $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules if and only if $\psi \circ \gamma_E$ and $\psi' \circ \gamma_{E'}$ are isomorphic representations of $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$. This is Lemma 2.45. □

Proposition 2.47. *Again consider the situation as in Theorem 2.39 and suppose that 2 is a square mod ℓ. Then $E[\ell]$ and $E'[\ell]$ are symplectically isomorphic $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules.*

Proof. As in the proof of Lemma 2.45, we may assume that both E and E' reduce to the same curve $\overline{E}$ over $\overline{\mathbb{F}}_2$. We fix a symplectic basis for $\overline{E}[\ell]$ and let M_g be the matrix that represents the intertwiner g of $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules that we constructed in the proof of Lemma 2.45. Since φ and φ' were isomorphisms between the $\mathbb{F}_\ell$-vector spaces $E[\ell]$ respectively $E'[\ell]$ and $\overline{E}[\ell]$, we may lift this fixed basis to both $E[\ell]$ and $E'[\ell]$. It is not hard to see that these lifted bases are again symplectic, so that both φ and φ' act as the identity matrix in these bases. Then in terms of matrices we see that Lemma 2.44 turns into

$$\rho_{E,\ell}(\sigma) = \psi(\gamma_E(\sigma)) = M_g \psi(\gamma_{E'}(\sigma)) M_g^{-1} = M_g \rho_{E',\ell}(\sigma) M_g^{-1}.$$

Hence M_g represents a morphism between $E[\ell]$ and $E'[\ell]$ of $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules, which is symplectic if and only if $\det(M_g)$ is a square mod p. If 2 is a square mod p, it follows from Lemma 2.42 that M_g indeed has square determinant mod p, proving the claim. □

We have only the case where 2 is not a square left to examine. Again, we will need a few smaller results to get us going. This first result explains the appearance of the prime 3 in Theorem 2.39.

Lemma 2.48. *Let ℓ be a prime number such that 2 is not a square mod ℓ. Then $E[\ell]$ and $E'[\ell]$ are symplectically isomorphic $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules precisely when $E[3]$ and $E'[3]$ are symplectically isomorphic $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules.*

Proof. We remark that from the previous proof, it can even be concluded that $E[\ell]$ and $E'[\ell]$ are symplectically isomorphic *if and only if* M_g has square determinant. Namely, $E[\ell]$ and $E[\ell']$ cannot be both symplectically and anti-symplectically isomorphic. As remarked before, this is seen by precisely the same argument as in the proof of Proposition 2.40, because in this case, the image of $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$ in $\mathrm{GL}(E[\ell])$ is indeed non-abelian.

By Lemma 2.42, M_g has square determinant precisely when $\alpha \in A_4 \subset S_4 \cong \mathrm{Aut}(H)$ is an inner automorphism. We can repeat all the above arguments with the prime 3 instead of ℓ with the map $\psi_3 : \mathrm{Aut}(\overline{E}) \to \mathrm{SL}(\overline{E}[3]) \subset \mathrm{GL}(\overline{E}[3])$ to find some $\alpha_3 \in \mathrm{Aut}(H)$ such that $\psi_3 \circ \gamma_E = \alpha_3 \circ \psi_3 \circ \gamma_{E'}$. Thus we have

$$(\psi^{-1} \circ \alpha \circ \psi) \circ \gamma_{E'} = \gamma_E = (\psi_3^{-1} \circ \alpha_3 \circ \psi_3) \circ \gamma_{E'}.$$

But since both γ_E and $\gamma_{E'}$ were surjective, we conclude that $\psi^{-1} \circ \alpha \circ \psi = \psi_3^{-1} \circ \alpha_3 \circ \psi_3$. Hence α and α_3 differ only by some conjugation. Thus α will be inner precisely when

α_3 is inner and since 2 is not a square modulo 3, this is equivalent to $E[3]$ and $E'[3]$ being symplectically isomorphic. □

Lemma 2.49. *Let* $L_3 \subset L$ *be an extension of* $\mathbb{Q}_2^{un}$ *of degree 8. Then* E *and* E' *both have a 3-torsion point defined over* L_3.

Proof. Since $[L : \mathbb{Q}_2^{un}] = |\mathrm{Gal}(L/\mathbb{Q}_2^{un})| = |SL_2(\mathbb{F}_3)| = 24$ and $[L_3 : \mathrm{Gal}(L/\mathbb{Q}_2^{un})] = 8$, it follows that $[L : L_3] = 24/8 = 3$. Because the 2-Sylow subgroup in $SL_2(\mathbb{F}_3)$ is normal, we must have $\mathrm{Gal}(L/L_3) \cong \mathbb{Z}/3\mathbb{Z} \subset \mathrm{Gal}(L/\mathbb{Q}_2^{un})$. Thus in particular $\gamma_E(\mathrm{Gal}(L/L_3))$ and $\gamma_{E'}(\mathrm{Gal}(L/L_3))$ are subgroups of order 3 in $\mathrm{Aut}(\overline{E})$, and so $\psi(\gamma_E(\mathrm{Gal}(L/L_3)))$ and $\psi(\gamma_{E'}(\mathrm{Gal}(L/L_3)))$ are order 3 subgroups of $SL_2(\mathbb{F}_3)$. This group contains precisely 8 elements of order 3, which come in two different conjugacy classes, represented by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

We observe that if we write a generator for $\psi(\gamma_E(\mathrm{Gal}(L/L_3)))$ in a symplectic basis, conjugating with an element from $SL_2(\mathbb{F}_3)$ expresses this matrix in a different, but still symplectic, basis. Hence we may choose a symplectic basis in which the group is generated by one of the above two matrices. But this means that the first basis vector is left invariant under the action of $\mathrm{Gal}(L/L_3)$, and so this must be a 3-torsion point of E defined over L_3. We can repeat this argument for E'. □

Lemma 2.50. *Let* σ *be a generator of* $\mathrm{Gal}(L/L_3) \cong \mathbb{Z}/3\mathbb{Z}$. *Then* $E[3]$ *and* $E'[3]$ *are symplectically isomorphic if and only if* $\gamma_E(\sigma) = \gamma_{E'}(\sigma)$.

Proof. We remark that the two possible generators in the above proof generate the same group, so we may assume that the groups $\psi(\gamma_E(\mathrm{Gal}(L/L_3)))$ and $\psi(\gamma_{E'}(\mathrm{Gal}(L/L_3)))$ coincide in $SL_2(\mathbb{F}_3)$, say both equal to $\Sigma = \langle \psi(\gamma_E(\sigma)) \rangle$. Hence it follows that the matrix equality $\psi(\gamma_E(\sigma)) = M_g \psi(\gamma_{E'}(\sigma)) M_g^{-1}$ implies that M_g is in the normaliser of Σ in $GL_2(\mathbb{F}_3)$. It can be verified by hand that the matrices in the centraliser of Σ are precisely the matrices in the normaliser of Σ with square determinant. Since we had seen before that $E[3]$ and $E'[3]$ are symplectically isomorphic precisely when M_g has square determinant, from the above it follows that this is equivalent to M_g being in the centraliser of Σ. This happens precisely when $\psi(\gamma_E(\sigma)) = \psi(\gamma_{E'}(\sigma))$ and since ψ was injective, this happens precisely when $\gamma_E(\sigma) = \gamma_{E'}(\sigma)$. □

This final part of the proof is adapted from Appendix A in [25].

Proof. (*of Theorem 2.39*) Given Proposition 2.47, we are left to complete the proof of the case in which 2 is not a square modulo ℓ. Since $j(\overline{E}) = 0$ and we work in characteristic 2, Proposition A.1.1 from [42] tells us that we can write

$$\overline{E} : y^2 + a_3 y = x^3 + a_4 x + a_6 \quad \text{where} \quad a_3, a_4, a_6 \in \overline{\mathbb{F}}_2.$$

Recall that $\gamma_E(\sigma)$ and $\gamma_{E'}(\sigma)$ are both elements of order 3 in $\mathrm{Aut}(\overline{E})$ that generate the same subgroup of $\mathrm{Aut}(\overline{E})$ of order 3. Thus we have $\gamma_E(\sigma) = \gamma_{E'}(\sigma)^{\pm 1}$.

Automorphisms of $\overline{E}$ are of the form $(x, y) \to (u^2x + s^2, u^3y + u^2sx + t)$ where $u^3 = 1$ and $s, t \in \overline{\mathbb{F}}_2$ satisfy some equations; see Proposition A.2 in [42]. Since there are precisely 8 automorphisms satisfying $u = 1$ and these form a subgroup, we see that $\gamma_E(\sigma)$ and $\gamma_{E'}(\sigma)$, having order 3 in $\mathrm{Aut}(\overline{E})$, cannot have $u = 1$. It is not hard to see that we have a character $\chi : \mathrm{Aut}(\overline{E}) \to \mathbb{F}_3$, sending an automorphism to its value of u. By the above, it also follows that χ restricts to an isomorphism on the subgroup generated by $\gamma_E(\sigma)$ and $\gamma_{E'}(\sigma)$. We claim that for a suitable primitive cube root of unity ω, we have

$$\chi(\gamma_E(\sigma)) = \omega^{v_2(\Delta_{\min}(E))} \quad \text{and} \quad \chi(\gamma_{E'}(\sigma)) = \omega^{v_2(\Delta_{\min}(E'))}.$$

If we can show this claim, it would follow that the images of $\gamma_E(\sigma)$ and $\gamma_{E'}(\sigma)$ coincide precisely when $v_2(\Delta(E))$ and $v_2(\Delta(E'))$ agree mod 3. Since χ restricted to an isomorphism, this would happen precisely when $\gamma_E(\sigma)$ and $\gamma_{E'}(\sigma)$ themselves coincide. Tracing back through all the previous lemmas, this would prove Theorem 2.39.

We give a sketch of the proof of this claim and refer the reader to appendix A of [25] for the details. Using the result from Lemma 2.49, we can also write E as

$$y^2 + axy + by = x^3$$

for some $a, b \in \mathbb{Q}_2^{un}$ such that $b = 2^\alpha$ for some $\alpha \in \{1, 2\}$. Then we have $\Delta = b^3(a^3 - 27b)$ and so $v_2(\Delta(E)) = 4\alpha$. If we let z be a cube root of 2, we can show that $L = L_3(z)$ and if $u = z^\alpha$, the substitution $(x, y) = (u^2x, u^3y)$ makes the above equation minimal over L. With these equations for E one can show that $\sigma(u)/u = \chi(\gamma_E(\sigma))$. If we write ω for the primitive cube root of unity such that $\sigma(z) = \omega z$, then on the other hand, the quotient $\sigma(u)/u$ equals ω^α. It then follows that $\chi(\gamma_E(\sigma)) = \omega^\alpha = \omega^{4\alpha} = \omega^{v_2(\Delta(E))}$, which would conclude the proof. □

2.7 Another application of the symplectic method

Before we start with our example, we take a moment to reflect on the condition that appeared in Theorem 2.39; namely, that $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$, or as it turns out, equivalently, that it has order 24. One can imagine that in general it might not be so easy to determine the Galois group of this rather abstract field extension. Fortunately, the hard work has been done for us already by Kraus in [28]. He provides us with very elaborate tables that allow us to decide for a given elliptic curve what the order of the group $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$ is, purely in terms of the discriminant and c_4. The following proposition is only a small subset of all his criteria.

Proposition 2.51. *Let $E/\mathbb{Q}_2$ be an elliptic curve with minimal discriminant Δ and recall the quantity c_4. Suppose that E has potentially good reduction and let $L/\mathbb{Q}_2^{un}$ be the minimal extension of good reduction. Then $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$ if any of the following holds:*

- $v_2(\Delta) = 4$ *and* $v_2(c_4) = 5$.
- $v_2(\Delta) = 8$ *and* $v_2(c_4) = 4$ *and* $\Delta/2^8 \equiv 1 \pmod 4$.

- $v_2(\Delta) = 10$ *and* $v_2(c_4) = 4$.

Now we are ready to use the two symplectic theorems that we have proved so far to show the non-existence of solutions to certain twisted Fermat equations. As an example, we prove the following theorem that was first shown in [19] as Theorem 2.

Theorem 2.52. *Let ℓ be a prime number satisfying either*

$$\ell \equiv 5 \pmod 8 \quad \textit{or} \quad \ell \equiv 19 \pmod{24}.$$

Then the equation

$$3x^\ell + 4y^\ell + 5z^\ell = 0$$

has no non-trivial integral solutions.

The remainder of this section will be devoted to proving the above theorem. We suppose there exists such a primitive non-trivial solution (x, y, z). Then it follows that x and z are odd and because $\ell > 2$ we may assume without loss of generality that $x^\ell \equiv -1 \pmod 4$. Consider the elliptic curve

$$E\colon Y^2 = X(X - 3x^\ell)(X + 4y^\ell).$$

Again, a Frey curve in the same vein as in the proofs of Theorem 2.20 and Theorem 2.34. A careful consideration of Tate's algorithm as outlined in the proof of Lemma 2.36, will yield the following result, also proved in Appendix A.

Lemma 2.53. *Let E be the elliptic curve as above. Then we have that*

$$\Delta_{\min}(E) = 2^8(15)^2(xyz)^{2\ell} \quad \textit{and} \quad N_E = 4\,\mathrm{rad}(30xyz) \quad \textit{if } y \textit{ is odd,}$$

and

$$\Delta_{\min}(E) = (15)^2(xyz)^{2\ell}/2^4 \quad \textit{and} \quad N_E = \mathrm{rad}(30xyz) \quad \textit{if } y \textit{ is even.}$$

A quick way to see that E has no ℓ-isogenies is to observe that the conductor tells us that E has multiplicative reduction at 3 and 5. As in Remark 2.24, the result that $j(E) \notin \mathbb{Z}[1/2]$ follows for $\ell \geqslant 17$. In fact, in Lemme 4 of [29] it is shown that this will actually hold true for all $\ell \geqslant 5$. We will briefly touch on this topic again in Section 4.2.

Now we may apply Theorem 2.15 to find newforms of the levels

$$N_\ell = 120 \quad \text{if } y \text{ is odd, and} \quad N_\ell = 30 \quad \text{if } y \text{ is even,}$$

such that $\rho_E^\ell \sim \rho_f^\ell$. Now there exists a unique newform of level 30, and there even exist two distinct newforms of level 120. We must tackle both of these cases separately.

First suppose that y even. The modular form of level 30 is the same as in the proof of Theorem 2.34. We can repeat the same argument using Theorem 2.25 to find that all of

$$\frac{-4\cdot 2}{4\cdot 3}, \quad \frac{-4\cdot 2}{4\cdot 1} \quad \text{and} \quad \frac{2\cdot 2}{3\cdot 1}$$

must be squares modulo p. This readily reduces to both -2 and 3 being squares modulo p. The first happens precisely when $p \equiv 1, 3 \pmod 8$ and the second precisely when $p \equiv 1, 11 \pmod{12}$. Combined this only holds for $p \equiv 1, 11 \pmod{24}$.

Now suppose that y is odd. Then one can use the function EllipticCurve in Magma [7] to find that the two possible newforms of level 120 correspond to the elliptic curves

$$F_1 \colon Y^2 = X^3 + X^2 - 15X + 18 \quad \text{with} \quad \Delta(F_1) = 2^4 \cdot 3^2 \cdot 5 \quad \text{and} \quad c_4(F_1) = 2^5 \cdot 23,$$

and

$$F_2 \colon Y^2 = X^3 + X^2 + 4X \quad \text{with} \quad \Delta(F_2) = -2^8 \cdot 3 \cdot 5 \quad \text{and} \quad c_4(F_2) = -2^4 \cdot 11.$$

We also compute that

$$\Delta(E) = 2^8(15)^2(xyz)^{2\ell} \quad \text{and} \quad c_4(E) = 16\left(36x^\ell y^\ell + (3x^\ell - 4y^\ell)^2\right).$$

In order to be able to apply Theorem 2.39, we must check that the above three elliptic curves have potentially good reduction at 2. Using Lemma 2.38, it suffices to check that $v_2(j) \geqslant 0$, or equivalently, that $3v_2(c_4) \geqslant v_2(\Delta)$. For F_1 and F_2 this is immediately verified. For E, we remark that since we assumed x, y and z to be odd, we have $v_2(\Delta(E)) = 8$ and $v_2(c_4(E)) = 4$, once more satisfying our constraint.

In addition we must check that we have $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$. To this end, we will invoke Proposition 2.51. For the curve F_1 we can use the first case of the proposition, For F_2 and E we can use the second case, after remarking that indeed $-15 \equiv 1 \pmod 4$ and that $\Delta_E/2^8 = (15(xyz)^\ell)^2 \equiv 1 \pmod 4$, as it is the square of an odd number.

If $\rho_{F_1}^\ell \sim \rho_E^\ell$, we know that $E[\ell]$ and $F_1[\ell]$ are isomorphic Galois modules. Hence it follows immediately that their considered extensions of good reduction coincide, because these are obtained by adjoining all the coordinates of the ℓ-torsion points of the elliptic curves. The argument for the F_2-case is identical. This shows that we are in the position to apply Theorem 2.39. We remark that we could have also used this argument to conclude that some of the above Galois groups were isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$, but it is good to see that Kraus's criteria withstand this test.

Suppose that 2 is not a square modulo ℓ. We will split two cases.

First suppose that $\rho_E^\ell \sim \rho_{F_1}^\ell$. Using Theorem 2.39 and the observation that $v_2(\Delta(E)) = 8 \not\equiv 4 = v_2(\Delta(F_1)) \pmod 3$, we may conclude that $E[\ell]$ and $F_1[\ell]$ are isomorphic, but not symplectically isomorphic $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules. If they were symplectically isomorphic $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-modules, then by restriction certainly also symplectically isomorphic $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$-modules, so this is not the case. We observe that since the prime 3 occurs only once in the conductor of both E and F_1, these elliptic curves have multiplicative reduction at 3. Thus we may apply Proposition 2.31, from which it follows that $v_3(\Delta(E)) = 2 + 2\ell v_3(xyz) \equiv 2 \pmod \ell$ and $v_3(\Delta(F)) = 2$ cannot differ by a square modulo ℓ. But they do; a contradiction.

Now suppose that $\rho_E^\ell \sim \rho_{F_2}^\ell$. Using Theorem 2.39 and the facts that $v_2(\Delta(E)) = 8 = v_2(\Delta(F_2))$, we may conclude that $E[\ell]$ and $F_2[\ell]$ *are* symplectically isomorphic Galois modules. Using Proposition 2.40, noting that indeed the image of $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$ under

ρ_E^ℓ is non-abelian, it follows that they are also symplectically isomorphic $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-modules. Note that since the prime 5 occurs only once in the conductor of both E and F_2, these elliptic curves have multiplicative reduction at 5. Thus we may apply Proposition 2.31, from which it follows that $v_5(\Delta(E)) = 2 + 2\ell v_5(xyz) \equiv 2 \pmod{\ell}$ and $v_5(\Delta(F)) = 1$ must differ by a square modulo ℓ. But we assumed that 2 is not a square mod ℓ; a contradiction.

We conclude that 2 must be a square mod ℓ, which means that $\ell \equiv 1, 7 \pmod 8$. Combining this result for the even y case, we conclude that the equation can only have non-trivial solutions if either $\ell \equiv 1, 11 \pmod{24}$ or $\ell \equiv 1, 7 \pmod 8$. One readily checks that precisely the primes as specified in the theorem fall outside both of these families. Hence for these primes, no non-trivial solutions can exist. □

2.8 The equation $x^3 + y^3 = z^\ell$

A very impressive application of the symplectic method was demonstrated in [18] as Theorem 3, where the generalised Fermat equation $x^3 + y^3 = z^\ell$ is solved for half the primes ℓ. To be precise, it shows that this equation does not have any non-trivial primitive solutions for $\ell \equiv 2 \pmod 3$ where $\ell \geqslant 17$. It is conjectured that this equation has no non-trivial primitive solutions for any odd prime number ℓ, but this has not been shown yet, as of today.

Theorem 2.54. *Let $\ell \geqslant 17$ be a prime number with $\ell \equiv 2 \pmod 3$. Suppose (x, y, z) are pairwise coprime integers satisfying*

$$x^3 + y^3 = z^\ell.$$

Then $xyz = 0$.

Remark 2.55. For $\ell = 2$ this equation does admit non-trivial solutions. For instance, consider $(x, y, z) = (1, 2, 3)$. In fact, in this case parametrisations for all solutions can be found, as described in Section 14.3.1 in [11]. It is also worth noting that more partial results have been established; for instance, in Theorem 1 of [10] it is shown with clever use of quadratic reciprocity over number fields that the equation $x^3 + y^3 = z^\ell$ does not have non-trivial primitive solutions for a set of primes of density approximately 0.628 given by congruence conditions. It should also be noted that in Section 3.3.2 in [12] the above equation is shown to have no solutions for $\ell \in \{5, 7, 11, 13\}$.

First we will follow some of the theory built by Kraus in [30]. It all begins with another Frey curve, so we will again suppose that we have a non-trivial, primitive solution (x, y, z). Observe that we may assume without loss of generality that y is odd, and so xz is even. We consider the curve

$$E : Y^2 = X^3 + 3xyX + x^3 - y^3, \quad \text{with} \quad c_4 = -2^4 \cdot 3^2 \cdot xy \quad \text{and} \quad \Delta = -2^4 \cdot 3^3 \cdot z^{2\ell}.$$

To compute the conductor, we need to distinguish a fair number of cases. We opt to not write out the details here, as they can be found in the proof of Lemme 4.1 in [30]. For

convenience, we will write R for the product of all primes at least 5 that divide z, as the interesting differences will only involve the primes 2 and 3.

Lemma 2.56. *Suppose that z is even and $y \equiv -1 \pmod 4$. Then*

$$N_E = 2 \cdot 3^2 \cdot R.$$

If z is odd and $y \equiv 1 \pmod 4$, then the Weierstrass equation for E is minimal and

$$N_E = \begin{cases} 2^3 \cdot 3^2 \cdot R & \text{if } v_2(x) = 1; \\ 2^2 \cdot 3^2 \cdot R & \text{if } v_2(x) \geqslant 2. \end{cases}$$

Now in order to be able to apply the level-lowering results, we must check that E does not have any ℓ-isogenies. We will use Theorem 2.18, which tells us that it suffices to show that $j(E) \notin \mathbb{Z}[1/2]$. But because we have

$$j(E) = \frac{c_4^3}{\Delta} = \frac{2^8 \cdot 3^3 \cdot x^3 y^3}{z^{2\ell}},$$

it follows immediately that $z = 2^k$ for some $k \geqslant 0$. If $k = 0$, then we observe that $x^3 + y^3 = 1$ only has trivial solutions. If $k \geqslant 1$, we observe both x and y must be odd, so that that the equation

$$(x + y)(x^2 - xy + y^2) = x^3 + y^3 = 2^{k\ell}$$

contains an even and an odd factor. We thus see that $x^2 - xy + y^2 = 1$, but this again only has trivial solutions and $x = y = \pm 1$, quickly proving the claim. Hence we may apply the level lowering theorem. We will split the rest of the proof into a few different lemmas.

Lemma 2.57. *Consider the situation as in Theorem 2.54 for a general prime $\ell \geqslant 17$. Then z is odd.*

Proof. If z is even, then we may assume without loss of generality that $y \equiv -1 \pmod 4$. But then the level lowering result gives us a newform of level 18. However, Proposition 2.11 tells us that such newforms do not exist; a contradiction. □

We conclude that z is odd and in this case we will assume without loss of generality that $y \equiv 1 \pmod 4$.

Lemma 2.58. *Consider the situation as in Theorem 2.54. Then $v_2(x) = 1$.*

We postpone the proof of this result to the next chapter, Example 3.12 to be precise, because it deals with elliptic curves having complex multiplication, which we will discuss in detail later. For now, we will assume this result and move on.

Lemma 2.59. *Consider the situation as in Theorem 2.54. Then $3 \mid z$.*

Again, we will prove this result later because it deals with arguments involving the *image of inertia*. The proof we will give in Example 3.14 will be similar to the proof given in [30] of Théorème 6.1c.

This is the point from where the original article [30] by Kraus could not proceed. With the help of Theorem 2.39, we can continue the proof by following Section 2 of [18].

Proof. (*of Theorem 2.54*)

It follows that we need only examine the case where $v_2(x) = 1$ and $3 \mid z$. From the level lowering results we obtain a newform of level 72, of which there exists only one, and which corresponds to the elliptic curve

$$F : Y^2 = X^3 + 6X - 7.$$

We note that the *quadratic twist* of F by -3 is given by

$$F' : Y^2 = X^3 + 5X + 189, \quad \text{with minimal model} \quad F' : Y^2 = X^3 - X^2 + X,$$

as can be found by executing Tate's algorithm in its entirety for the prime 3. We have that $\Delta_{\min}(F') = -2^4 \cdot 3$ and $c_4(F') = -2^5$ and $N_{F'} = 24$. Let E' denote the quadratic twist of E by -3. Since twisting curves is functorial, see for example Section X.5 in [42], it follows that $\rho^{\ell}_{E'} \sim \rho^{\ell}_{F'}$.

We want to use Theorem 2.39. We see that since $v_2(\Delta(F')) = 4$ and $v_2(c_4(F')) = 5$, the curve F' has potentially good reduction at 2 and Proposition 2.51 gives us that $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{un}}) \cong \mathrm{SL}_2(\mathbb{F}_3)$. If we can show that E' also has potentially good reduction at 2, we will be in the position to apply Theorem 2.39. To see this, we explicitly observe that

$$E' : Y^2 = X^3 + 27xyX - 27(x^3 - y^3), \quad \text{with} \quad c_4 = -2^4 \cdot 3^4 \cdot xy \quad \text{and} \quad \Delta = -2^4 \cdot 3^9 \cdot z^{2\ell}.$$

Because z is odd, indeed we have that $v_2(c_4(E')) = 4 + v_2(xy) = 5$ and $v_2(\Delta(E')) = 4$. These values are identical to those of F', showing everything we need.

Now we advance to using the theorem. Since we have $v_2(\Delta(E')) < 12$, it follows that $v_2(\Delta_{\min}(E')) = v_2(\Delta(E')) = 4$. Since also $v_2(\Delta(F')) = 4$, it follows from Theorem 2.39 that $E'[\ell]$ and $F'[\ell]$ are symplectically isomorphic $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{un}})$-modules. By Proposition 2.40 they are even symplectically isomorphic $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-modules.

Since 3 divides $N_{F'}$ precisely once, the reduction of F' at the prime 3 is multiplicative; this was the sole purpose of the twisting that we did. In order to obtain information about E' at the prime 3, we recall that $3 \mid z$, so also $3 \nmid xy$. Then Tate's algorithm will tell us that the equation for E' is not minimal. Hence we may apply a change of variables to obtain a model for E' satisfying $v_3(c_4) = 4 - 4 = 0$ and $v_3(\Delta) = -3 + 2v_\ell(z)$. Now the Weierstrass equation must be minimal at the prime 3, since $v_3(c_4)$ cannot be lowered any further. We conclude that $v_3(\Delta_{\min}(E')) = -3 + 2\ell v_3(z) \equiv -3 \pmod{\ell}$. It also follows that $N_{E'} = 2^3 \cdot 3 \cdot R$, making the reduction multiplicative. Thus we may apply Proposition 2.31 for the prime 3 to conclude that $v_3(\Delta_{\min}(E'))$ and $v_3(\Delta_{\min}(E')) = 1$ must differ by a square modulo ℓ. We conclude from the above that -3 must be a square mod ℓ. However, this contradicts $\ell \equiv 2 \pmod 3$. □

3 More methods to solve equations

The symplectic method can be very useful to tackle problems, in case one finds oneself on a level at which newforms do exist when applying the modular method. However, it should be stressed that there is a more elementary method available that will sometimes do the trick, without having to resort to the subtle art of the symplectic type of isomorphisms. We discuss this approach, called *comparing traces of Frobenius*, along with the results about *complex multiplication* and a result coming from the *image of inertia*. Then some generalisations of the modular method and some symplectic theorems are considered, before moving on to newly found applications of the symplectic method in the next chapter.

3.1 Comparing traces of Frobenius

A very elementary corollary to the theory described at the beginning of the previous chapter is the following.

Proposition 3.1. *Let* E *and* F *be elliptic curves over* $\mathbb{Q}$ *and let* ℓ *be a prime number. Suppose that* $E[\ell]$ *and* $F[\ell]$ *are isomorphic Galois modules and let* p *be any prime at which* E *and* F *both have good reduction. Then we have*

$$a_p(E) \equiv a_p(F) \pmod{\ell}, \quad \textit{or equivalently,} \quad \#\tilde{E}(\mathbb{F}_p) \equiv \#\tilde{F}(\mathbb{F}_p) \pmod{\ell}.$$

Proof. For $p \neq \ell$ this follows almost immediately from Theorem 2.7. Namely, since $E[\ell]$ and $F[\ell]$ are isomorphic Galois modules, we have an equivalence of representations ρ_E^ℓ and ρ_F^ℓ. Additionally, for primes ℓ as considered above, we have that $\mathrm{tr}(\rho_E^\ell(\mathrm{Frob}_\mathfrak{p})) = a_p(E)$ and $\mathrm{tr}(\rho_F^\ell(\mathrm{Frob}_\mathfrak{p})) = a_p(F)$. As the character is invariant under equivalence of representations, the claim follows. The proof for $\ell = p$ is more intricate and can be found in [31] in the proof of Proposition 3. □

The following result is also proved in detail in [31] when proving Proposition 3. It allows us to use the same ideas as above, but then in the case that one of the two curves has multiplicative reduction at some prime.

Proposition 3.2. *Let* E *and* F *be elliptic curves over* $\mathbb{Q}$ *and let* ℓ *be a prime number. Suppose that* $E[\ell]$ *and* $F[\ell]$ *are isomorphic Galois modules and let* p *be any prime at which* E *has multiplicative reduction and* F *has good reduction. Then we have*

$$a_p(F) \equiv \pm(p+1) \pmod{\ell}.$$

Proof. We sketch the proof. By considering Tate curves, one can find a subspace of $E[\ell]$ on which the image of $\mathrm{Frob}_\mathfrak{p}$ acts as multiplication by $a_p(E)$, making it an eigenvalue. We note that $a_p(E) = \pm 1$, because the reduction is multiplicative. Because the mod ℓ representations of E and F are assumed to be isomorphic, it follows that $a_p(E)$ is also an eigenvalue of $\rho_F^\ell(\mathrm{Frob}_\mathfrak{p})$ and thus it must be a zero of its characteristic polynomial. We find that $a_p(E)^2 - a_p(E)a_p(F) + p \equiv 0 \pmod{\ell}$ and using $a_p(E) = \pm 1$, it follows that $\pm a_p(F) \equiv p + 1 \pmod{\ell}$, as claimed. □

These results can be used in a very naive way to sometimes very quickly arrive at a contradiction, solving an equation for almost all primes at once.

Example 3.3. Suppose that we are trying to solve the equation

$$x^\ell + y^\ell + 13^k z^\ell = 0$$

for some integer $k \geqslant 0$ and some prime $\ell > 7$. Then we may immediately reduce to $\ell \nmid k$, because we know how to solve Fermat's Last Theorem. One considers a primitive solution to the equation and we let

$$E : Y^2 = X(X - x^\ell)(X + y^\ell).$$

Since E is semistable and has full rational 2-torsion, Theorem 2.18 tells us that the level lowering theorem applies. From the recipe in Section 4 of [29] we obtain a newform at level $2 \cdot 13 = 26$. There are two modular forms at this level, corresponding to the elliptic curves

$$F_1 : Y^2 + XY + Y = X^3 - 5X - 8 \quad \text{and} \quad F_2 : Y^2 + XY + Y = X^3 - X^2 - 3X + 3.$$

Now the idea is that our initial elliptic curve E is an elliptic curve of a very particular type; namely, it has full rational 2-torsion. Suppose that, after level lowering, we are to compare E to an elliptic curve F that does not have a rational 2-torsion point. It could happen that we find a prime at which F does not have a 2-torsion point. But then we find that all the possibilities for $\#\tilde{E}(\mathbb{F}_p)$ are even, whereas $\#\tilde{F}(\mathbb{F}_p)$ need not be. But these numbers must agree modulo ℓ, yielding only very few possibilities for ℓ. Of course, this is all under the assumption that both E and F have good reduction at p.

Now, we observe that both F_1 and F_2 have good reduction at 3. Then using the functions written in SageMath [43] in Appendix B, we obtain that $\#\tilde{F}_i(\mathbb{F}_3) \in \{3, 7\}$ whereas the only possibility for E is that $\#\tilde{E}(\mathbb{F}_3) = 4$, assuming good reduction. Namely, we must have $E \pmod 3 : Y^2 = X(X+1)(X+2)$ to avoid being singular. So if E has good reduction at 3, these numbers must agree mod ℓ. However, $\ell > 7$ and so this cannot happen.

It follows that E must have multiplicative reduction at 3. Applying Proposition 3.2 and observing that $\pm a_3(F_i) \in \{-1, 1, -3, 3\}$, we find that one of these numbers must be equal to $3 + 1 = 4 \pmod{\ell}$. Again, since $\ell > 7$, this cannot happen. Hence no non-trivial solutions can exist and we have solved the equation. △

Remark 3.4. An attempt to solve the equation for all primes ℓ, since $\ell = 2$ clearly gives no non-zero solutions, is thus reduced to considering $\ell \in \{3, 5, 7\}$.

For $\ell = 3$ there are many solutions, provided $3 \nmid k$, which is taken care off by Fermat. Namely, using the function EllipticCurve in Magma [7] with the solution $(1, -1, 0)$ we see that the genus 1 curves

$$x^3 + y^3 + 13z^3 = 0 \quad \text{and} \quad x^3 + y^3 + 169z^3 = 0$$

are isomorphic to the elliptic curves

$$Y^2 + Y = X^3 - 1141 \quad \text{and} \quad Y^2 + Y = X^3 - 192787$$

respectively. Using the function RankBounds we can determine that these elliptic curves both have rank 1 and are torsion free. A quick search for solutions yields that the smallest families of solutions other than $(1, -1, 0)$ are given by $(2, 7, -3)$ and $(7, 2, -3)$ in the first case, and $(7, -8, 1)$ and $(-8, 7, 1)$ in the second case. Because the ranks of the curves are 1, there will be infinitely many more families of solutions.

To deal with $\ell = 5$, closely observing traces of Frobenius at 3 using our code in SageMath [43], yields that E can only have isomorphic 5-torsion modules with F_1. Next we remark that $x^5 \equiv 0, \pm 1 \pmod{11}$ and so in the case of good reduction, we must have $E : Y^2 = X(X+1)(X-1) \pmod{11}$ so that $\#\tilde{E}(\mathbb{F}_{11}) = 12$. However, $\#\tilde{F}_1(\mathbb{F}_{11}) = 6$ and so we would find $12 \equiv 6 \pmod 5$, a contradiction. The other case is E having multiplicative reduction at 11, but then $a_{11}(F_1) = \pm 6$ which is not equal to $12 \pmod 5$. We conclude that no non-trivial solutions can exist in this case.

If $\ell = 7$, then by closely looking at the traces modulo 3, any supposed non-trivial solution to the equation will yield an isomorphism of ρ_E^7 and $\rho_{F_2}^7$. But F_2 has a rational 7-torsion point and so $\rho_{F_2}^7$ will not be irreducible. However, ρ_E^7 is irreducible and so this also cannot happen.

As a final concluding remark we note that this solves the equation $x^n + y^n + 13^k z^n = 0$ for all integers n, except for n a power of three. We will return to the question what can be said about $n = 9$ in Section 3.4.

We conclude with a more computationally practical way to combine the above propositions into one fairly easy to implement criterion, as given in [40] as Proposition 9.1.

Proposition 3.5. *Let $E/\mathbb{Q}$ and $F/\mathbb{Q}$ be elliptic curves such that $E[\ell]$ and $F[\ell]$ are isomorphic Galois modules for some odd prime ℓ. Let p be a prime number at which F has good reduction and E has at most multiplicative reduction, such that E has no p-torsion point. Then for any number $t \mid \#\tilde{E}(\mathbb{Q})_{\text{tors}}$, define*

$$S_p = \left\{ a \in \mathbb{Z} \;\middle|\; |a| \leqslant 2\sqrt{p},\ \ a \equiv p + 1 \pmod t \right\}.$$

Then

$$\ell \;\Big|\; \left((p+1)^2 - a_p(F)^2\right) \prod_{a \in S_p} (a - a_p(F)).$$

Proof. From the assumption on p, we are either in the situation of Proposition 3.1 or Proposition 3.2. In the second case, ℓ must divide $(p+1)^2 - a_p(F)^2$, proving the claim. In the other case, it suffices to show that $a_p(E) \in S_\ell$. To see this, we observe that because E has good reduction modulo p, the torsion away from p injects into the reduction modulo p, see for example Proposition 3.1 in Section VII.3 in [42]. This is the complete torsion by assumption. Hence $\#\tilde{E}(\mathbb{F}_p) \equiv 0 \pmod{t}$ and so $a_p(E) \equiv p+1 \pmod{t}$. The fact that $|a_p(E)| \leqslant 2\sqrt{p}$ is nothing but the Hasse-Weil bound, as can be found as Theorem 1.1 in Section VI.1 in [42]. □

If we can find a prime number for which the right hand side is non-zero, we obtain a bound for the prime ℓ, solving our equation for all but finitely many primes. This method is very likely to succeed when the torsion structure of F is vastly different from what can be observed from that of E.

Remark 3.6. We note that this method can be generalised to irrational newforms f with number field $K_f \supsetneq \mathbb{Q}$, as outlined in Section 9 in [40], by replacing all factors on the right hand side by their norms in the field extension $K_f/\mathbb{Q}$. Then for any prime p for which $a_p(f)$ is irrational, the appropriately modified version of the right hand side of the above equation will be non-zero and so we obtain a bound for the prime ℓ. Therefore it is generally a good thing to end up at a level with many irrational newforms, for the equation can always be solved for sufficiently large primes using this method. The rational newforms are therefore the hardest to deal with, and it explains why they are the focus of the symplectic theorems discussed in the previous chapter.

3.2 Complex multiplication

Recall that if K is an imaginary quadratic number field with ring of integers $\mathcal{O}_K$, an *order* in K is a subring of the form $\mathbb{Z} + f\mathcal{O}_K$ for some positive integer f. Further recall that an elliptic curve E is said to have *complex multiplication* with respect to an order R in an imaginary quadratic field K if $\mathrm{End}(E) \cong R$. It can happen that the elliptic curve we end up with after applying the level lowering theorem has complex multiplication. This can often give us a lot of information and can make it markedly easier to solve the equation. We will first need some definitions.

Definition 3.7. Let ℓ be an odd prime and let $H \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be a subgroup.

- If H is a maximal abelian subgroup that is diagonalisable over $\overline{\mathbb{F}}_\ell$, then H is called a *Cartan subgroup*.
- If H is a Cartan subgroup that is diagonalisable over $\mathbb{F}_\ell$, then H is called a *split* Cartan subgroup. Otherwise, H is called a *non-split* Cartan subgroup.

It begins with the following observation. A very detailed description of all the possible images of the mod-ℓ representations of the rational curves with complex multiplication is given in Proposition 1.14, 1.15 and 1.16 of [44], but we will only need the following.

Proposition 3.8. *Let $F/\mathbb{Q}$ be an elliptic curve with complex multiplication with respect to an order in the number field K and let ℓ be a prime number that is unramified in K. Then:*

- *If ℓ splits in K, the image of ρ_F^ℓ is contained in the normaliser of a split Cartan subgroup.*
- *If ℓ does not split in K, the image of ρ_F^ℓ is contained in the normaliser of a non-split Cartan subgroup.*

Proof. We view $F(\mathbb{C}) = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ where, because F is assumed to have complex multiplication, τ satisfies the relation $f\tau^2 = x\tau + y$ for some $f, x, y \in \mathbb{Z}$ with $f > 0$ minimal. We then know that $\mathrm{End}(F) = \mathbb{Z}[f\tau]$. It is then not hard to see that for any $\sigma \in G_{\mathbb{Q}}$ and $a + bf\tau \in \mathrm{End}(F)$ we have that $\sigma(a + bf\tau)\sigma^{-1} = a + bf\sigma(\tau) \in \mathrm{End}(F)$. We conclude that the image of the Galois representation is contained in the normaliser of the image of $\mathrm{End}(F)$ when viewing its action on $F[\ell]$.

It thus remains to show that the image of $\mathrm{End}(F)$ is given by a (non)-split Cartan subgroup. We can explicitly write out in the natural basis $\{1/\ell, \tau/\ell\}$, that

$$a + bf\tau \text{ acts as } \begin{pmatrix} a & by \\ bf & bx + a \end{pmatrix}.$$

This matrix has a characteristic polynomial equal to

$$\lambda^2 - (bx + 2a)\lambda + a(bx + a) - b^2fy = 0$$

and hence it will have its eigenvalues in $\mathbb{F}_\ell$ if and only if its discriminant, which nicely works out to $b^2(x^2 + 4fy)$, is a square. Hence the eigenvalues of the matrix are in $\mathbb{F}_\ell$ precisely when $x^2 + 4fy$ is a square in $\mathbb{F}_\ell$, which is easily seen to be equivalent to ℓ splitting in $\mathbb{Z}[\tau]$.

So if ℓ does not split in $\mathbb{Z}[\tau]$, it follows that all these matrices have two distinct eigenvalues, not in $\mathbb{F}_\ell$, making them diagonalisable but not over $\mathbb{F}_\ell$. Since $\mathrm{End}(F)$ is abelian, clearly its image is also abelian. Its maximality follows from a counting argument, knowing that non-split Cartan subgroups always have an order equal to $\ell^2 - 1$, and the above image, when excluding zero, has that same order.

If ℓ does split in $\mathbb{Z}$, then the eigenvalues of all matrices are in $\mathbb{F}_\ell$. Then all matrices are diagonalisable because from the analysis above we may conclude that the eigenvalues are distinct provided that ℓ is unramified in K. The rest of the proof is similar to the above. □

Now one might wonder whether or not the converse also holds. For if so, we would have an inordinate amount of information if, after level lowering, we would end up at a curve with complex multiplication. If we could conclude that E must also have had complex multiplication, then we would find that $j(E)$ would have had to have been an integer, severely restricting any prime factors occurring in the numbers comprising an assumed primitive solution to the considered equation. Sadly, it turns out that this is not quite the case, but we can get very close thanks to the following theorems. Most of these were inspired by a problem called *Serre's uniformity problem*, which conjectures

that there exists some prime ℓ_0 such that for any prime $\ell > \ell_0$ and elliptic curve $E/\mathbb{Q}$ without complex multiplication, the representation ρ_E^ℓ is surjective. It is generally believed that $\ell_0 = 37$ suffices, but even though a lot of progress has been made, it remains an open problem to this day.

The first result of the following theorem was shown for the most part in Corollary 1.2 in [5], with the special case of $\ell = 13$ being dealt with in Theorem 1.1 in [1] using very involved and modern techniques. The second statement in the below theorem was first shown in a weaker form as Theorem 8.1 in [14] and was later strengthened in [32] as Theorem 1.4.

Theorem 3.9. *Let $E/\mathbb{Q}$ be an elliptic curve and let $\ell \geqslant 11$ be a prime number.*

- *If the image of ρ_E^ℓ is contained in the normaliser of a split Cartan subgroup, then E must have complex multiplication.*
- *If the image of ρ_E^ℓ is contained in the normaliser of a non-split Cartan subgroup and E has a rational r-isogeny for some $r \in \{2, 3, 5, 7, 13\}$, then it holds that $j(E) \in \mathbb{Z}$.*

This often means that if we end up at an elliptic curve with complex multiplication, both when ℓ splits in K or not, we obtain some very powerful additional information. This is illustrated with the examples below.

Example 3.10. We analyse the equation

$$x^\ell + 2^\alpha y^\ell + z^\ell = 0$$

for primes $\ell \geqslant 5$ and $\alpha \geqslant 0$ an integer. Again, $\alpha = 0$ has been treated before. Considering a primitive solution, so x, $2y$ and z are coprime, we construct the elliptic curve

$$E : Y^2 = (X - x^\ell)(X + 2^\alpha y^\ell).$$

By Tate's algorithm, we find that $N_E = 2^\beta \mathrm{rad}_2(xyz)$, where rad_2 denotes the radical of a number ignoring the prime 2 and β depends on α. It turns out, using the recipe in Section 4 of [29], that we may apply the level lowering result to end up at level 1, 2, 4 or 8, unless $\alpha = 1$ and y is odd, when we will end up at the level 32. By Proposition 2.11 we may thus restrict our attention to this case, which gives us the elliptic curve

$$F : Y^2 = X^3 + 4X,$$

which has complex multiplication by the ring $\mathbb{Z}[i]$. We now assume that $\ell \geqslant 11$. It is a classical result that an odd prime ℓ splits in $\mathbb{Z}[i]$ if and only if $\ell \equiv 1 \pmod 4$. So if $\ell \equiv 1 \pmod 4$, then the image of ρ_F^ℓ will be contained in the normaliser of a split Cartan subgroup, and hence also the image of ρ_E^ℓ. Then by Theorem 3.9 it follows that E must have complex multiplication, and so in particular $j(E) \in \mathbb{Z}$. If $\ell \equiv -1 \pmod 4$, then we find that the image of ρ_E^ℓ is contained in the normaliser of a non-split Cartan subgroup. It again follows from Theorem 3.9 that $j(E) \in \mathbb{Z}$, because E has a 2-torsion point. So it follows that

$$j(E) = 2^6 \frac{(x^{2\ell} + 2x^\ell y^\ell + 4y^{2\ell})^3}{(xyz)^{2\ell}} \in \mathbb{Z}.$$

Since x and y are coprime, no prime factor of x will divide the numerator, so $x = \pm 1$. Similarly, we must have $y = \pm 1$ and so also $z = \pm 1$, yielding just the solutions $(\pm 1, \mp 1, \pm 1)$. △

Remark 3.11. One may wonder what happens for the primes $\ell \in \{3, 5, 7\}$, which were excluded from the above proof. In that case it is actually possible to show by "elementary" means that the equation has no non-trivial integral solutions. For $\ell = 3$ this can be shown similarly to Euler's proof of Fermat's Last Theorem for exponent 3. The cases of $\ell = 5$ and $\ell = 7$ are somewhat more involved and were solved by Dirichlet and Dénes respectively, as can be found in [15]. It follows that for no exponent $n \geqslant 2$, the equation $x^n + 2y^n + z^n = 0$ has a solution other than $(x, y, z) = (\pm 1, \mp 1, \pm 1)$.

Example 3.12. We can now also treat the proof of Lemma 2.58, analogous to the proof by Kraus of Théorème 6.1b in [30]. Recall, there we considered a primitive solution to the equation $x^3 + y^3 = z^\ell$ for which $\ell \equiv 2 \pmod 3$ was a prime with $\ell \geqslant 17$ and if $v_2(x) \geqslant 2$, after level lowering we end up with a newform f of level 36 such that $\rho_E^\ell \sim \rho_f^\ell$. This newform is unique and corresponds to the elliptic curve $E' : Y^2 = X^3 + 1$. It has complex multiplication with the order $\mathbb{Z}[\zeta_3]$, where ζ_3 denotes a primitive cube root of unity. From elementary number theory it follows that any $\ell \equiv 2 \pmod 3$ does not split in $\mathbb{Z}[\zeta_3]$ and so by Proposition 3.8, the image of the Galois representation $\rho_{E'}^\ell$, is contained in the normaliser of a non-split Cartan subgroup, and thus so must be the image of ρ_E^ℓ. Since $(x - y, 0)$ is a rational 2-torsion point of E, Theorem 3.9 gives us that $j(E) \in \mathbb{Z}$. This means that z must be ± 1, which is easily seen to be impossible. △

3.3 Image of inertia

We conclude our treatment of different methods that can help complete the argument when applying the modular method by briefly discussing the argument based on the *image of inertia*. Recall the inertia subgroup I_p from Definition 2.5 for any prime p. Suppose that we have two rational elliptic curves E and F such that for some prime ℓ we have an isomorphism $E[\ell] \cong F[\ell]$, so the representations ρ_E^ℓ and ρ_F^ℓ are equivalent. Then certainly it follows that $\#\rho_E^\ell(I_p) = \#\rho_F^\ell(I_p)$. It turns out that the cardinality of this image is dependent on the elliptic curve having potentially good reduction at p or not. The following result is Proposition 55 in [12].

Proposition 3.13. *Let E and F be rational elliptic curves and let $\ell \geqslant 5$ and p be distinct prime numbers. Suppose that E has potentially good reduction at p, that F does not have potentially good reduction at p and that $\ell \nmid v_p(j(F))$. Then the representations ρ_E^ℓ and ρ_F^ℓ are not equivalent.*

Proof. (*sketch*) As argued below Theorem 2 in [38] in greater generality, $\rho_E^\ell(I_p)$ is isomorphic to the Galois group $\mathrm{Gal}(\mathbb{Q}_p^{un}(E[\ell])/\mathbb{Q}_p^{un})$. By combining all the results in [28], it follows that the degree of this extension can only be divisible by 2 and 3, so in particular $\ell \nmid \#\rho_E^\ell(I_p)$. On the other hand, the assumption that $\ell \nmid v_p(j(F))$ ensures that we can use Proposition V.6.1 in [41], which gives us an element in the inertia group whose image under ρ_F^ℓ has order precisely ℓ. Hence $\ell \mid \#\rho_F^\ell(I_p)$, so in particular $\#\rho_E^\ell(I_p) \neq \#\rho_F^\ell(I_p)$. This proves the claim. □

This proposition allows us to sometimes arrive at a contradiction, as the following example illustrates. It follows the original proof by Kraus in [30] of Théorème 6.1c.

Example 3.14. Recall the situation from Theorem 2.54; we will now prove Lemma 2.59. We had constructed a Frey curve E with j-invariant

$$j(E) = \frac{2^8 \cdot 3^3 \cdot x^3 y^3}{z^{2\ell}},$$

and because we had already shown that z is odd and that $v_2(x) = 1$, after level lowering we end up with the elliptic curve

$$F : Y^2 = X^3 + 6X - 7$$

with conductor 72 and j-invariant equal to $j(F) = 2^{11}/3$ that satisfies the property that ρ_E^ℓ and ρ_F^ℓ are equivalent representations. If $3 \nmid z$ we see that $v_3(j(E)) > 0$ and so E has potentially good reduction at 3. On the other hand, $v_3(j(F)) = -1$ and so F does not have potentially good reduction at 3. Because $\ell \neq 3$ and $\ell \nmid -1$, the above proposition gives an immediate contradiction, showing the claim. △

3.4 Level lowering modulo 9

It turns out that level lowering results are not purely restricted to prime exponents. When solving a Diophantine equation of the form $Ax^\ell + By^\ell + Cz^\ell = 0$, it often happens that for small odd prime exponents there actually are non-trivial solutions. This happens especially for the prime $\ell = 3$. Should one desire to solve such an equation for more exponents than just those that are prime, it would be natural to wonder whether or not there is a technique available to show the non-existence of solutions to the equation with exponent 9. To state a special case of the theorem that sometimes enables us to do this, we will first need a definition.

Definition 3.15. Let ℓ be an odd prime number and let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ be a representation of the group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Write $\ell^* = (-1)^{(\ell-1)/2}\ell$.

- We say that ρ is *absolutely irreducible* if it is irreducible over $\overline{\mathbb{F}}_\ell$.
- We say that ρ is *strongly irreducible* if $\rho|_{G_{\mathbb{Q}(\sqrt{\ell^*})}}$ is absolutely irreducible.

As for irreducibility of the mod-ℓ representations in general, it can be difficult to determine which case we are in. Fortunately, there are some results available that show that sometimes strong irreducibility is not that different from plain irreducibility. The first result follows from the proof of Proposition 2 in [17] and the second is Corollary 11 in [13].

Proposition 3.16. *Let $E/\mathbb{Q}$ be an elliptic curve and let ℓ be an odd prime.*

- *If $\ell \geqslant 5$ and E does not have additive reduction at ℓ, then ρ_E^ℓ is strongly irreducible if and only if it is irreducible.*

- *If $\ell = 3$ and E has full rational 2-torsion, then ρ_E^3 is strongly irreducible if and only if it is irreducible.*

The following is Proposition 13 in [13].

Corollary 3.17. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose there exists a prime $p \equiv 1 \pmod 3$ at which E has good reduction with the property that $3 \mid a_p(E)$. Then ρ_E^3 is strongly irreducible.*

Proof. By the above it suffices to show that ρ_E^3 is irreducible, and hence it suffices to show that E does not have a rational 3-isogeny. One can show that this happens precisely if E or the quadratic twist of E by -1, say E', has a 3-torsion point. Because $a_p(E') = -a_p(E)$, from this is follows that $3 \mid \#\tilde{E}(\mathbb{F}_p) = p + 1 - a_p(E)$ or $3 \mid \#\tilde{E}'(\mathbb{F}_p) = p + 1 + a_p(E)$. In other words, $a_p(E) \equiv \pm(1+p) \pmod 3$. But since $p \equiv 1 \pmod 3$, it follows that $3 \nmid a_p(E)$. This contradicts our assumption. □

It is generally not easy to prove the irreducibility of the mod-3 representation. Therefore, most of the time we can only do so much, as the following example illustrates.

Example 3.18. We return to a primitive solution to the equation studied in Example 3.3,

$$x^9 + y^9 + 13^k z^9 = 0,$$

for some integer $0 < k < 9$ with $3 \nmid k$. We still consider

$$E : Y^2 = X(X - x^9)(X + y^9)$$

and we note that $\Delta_{\min}(E) = 2^{-8} \cdot 13^{2k} \cdot (xyz)^{18}$ and $N_E = 2\mathrm{rad}(13xyz)$. Imagine that we want to apply the level lowering theorem modulo 3. To this end, we must show that ρ_E^3 is irreducible. To use Corollary 3.17, we must assume that E has good reduction at either 7 or 19. Namely, using our SageMath [43] code, we see that for the elliptic curve E as above, it must hold that $\#\tilde{E}(\mathbb{F}_7) = 8$ and so $a_7(E) = 0$. Similarly, it must hold that $\#\tilde{E}(\mathbb{F}_{19}) = 20$ and so $a_{19}(E) = 0$. Hence assuming good reduction at one of these primes, it follows that ρ_E^3 must be irreducible. We found no primes other than 7 and 19 that could help us show irreducibility.

We may then apply the level lowering theorem to arrive at level 26, finding our two curves F_1 and F_2 as possible candidates again. However, F_1 has a rational 3-torsion point, and so $\rho_{F_1}^3$ will not be irreducible. It would immediately follow that F_2 is the only possible curve that we would still have to deal with. We are left to compare traces of Frobenius using our SageMath [43] code in Appendix B. If we assume that E has good reduction at 7, then the isomorphism $\rho_E^3 \sim \rho_{F_2}^3$ gives us that $\#\tilde{E}(\mathbb{F}_7) \equiv \#\tilde{F}_2(\mathbb{F}_7) \pmod 3$. However, computing this yields that $8 \equiv 7 \pmod 3$, a contradiction. Similarly, good reduction modulo 19 would imply that $20 \equiv \#\tilde{F}_2(\mathbb{F}_7) = 21 \pmod 3$, again a contradiction. We conclude that any solution as considered above must satisfy $7 \cdot 19 \mid xyz$. The author suspects there to be no non-trivial solutions in general, but failed to show this with the current methods available. △

Remark 3.19. It follows from the above example that the criteria as provided above can be insufficient when there exists a global solution involving a zero. Namely, the solution $(1,-1,0)$ will work for exponent 9 as well as for exponent 3 and it hence prevents us from ever using the above proposition in full generality, because multiplicative reduction at any prime is possible. Proving the irreducibility of the mod-3 representation is therefore generally quite difficult.

To state the main theorem of this section, we note that even for prime powers, we obtain representations

$$\rho_E^{\ell^r} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell^r\mathbb{Z})$$

and in Section 1 of [17] it is explained that for prime ideals lying over ℓ in the number field $\mathcal{O}_f$ corresponding to a newform f, we also have

$$\rho_f^{\lambda^r} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_f/\lambda^r).$$

The following is a special case of a more general theorem proved first as Theorem 2 in [13].

Theorem 3.20. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N. Define*

$$M = \prod_{\substack{p \mid \Delta(E) \\ 9 \mid \nu_p(\Delta(E))}} p \quad \textit{and} \quad N_0 = N/M.$$

and suppose that $\gcd(M, N_0) = 1$. Further suppose that $3 \nmid \nu_p(\Delta(E))$ for all primes $p \mid N_0$ and that $9 \nmid N$. Lastly suppose that ρ_E^3 is a strongly irreducible Galois representation and that there exists a unique pair (f, λ) consisting of a newform f of level N_0 and some unramified prime ideal $\lambda \subset \mathcal{O}_f$ lying over 3 such that $\rho_E^3 \cong \rho_f^\lambda$. Then it follows that $\rho_E^9 \cong \rho_f^{\lambda^2}$. In particular, for all $p \nmid 3N$ we have

$$a_p(f) \equiv a_p(E) \pmod{\lambda}^2$$

and if $p \nmid 3N_0$ and $p \mid N$, then

$$a_p(f) \equiv \pm(1+p) \pmod{\lambda}^2.$$

It took many hours of manpower to find an example of the usefulness of the above theorem that was not already listed in the original article that proved it.

Example 3.21. We study the equation

$$x^9 + 8y^9 + 7^5 z^9 = 0.$$

We consider a non-trivial primitive solution to the above and the elliptic curve

$$E : Y^2 = X(X - x^9)(X + 8y^9).$$

Now, this elliptic curve has the property that $\Delta_E = (14)^{10}(xyz)^{18}$ and if y is odd, then $N_E = 8 \cdot 7\mathrm{rad}_{2,7}(xyz)$. To apply the above theorem, we find that $M = \mathrm{rad}_{2,7}(xyz)$ and so

$N_0 = N/M = 56$. Indeed M and N_0 are coprime and we see that $3 \nmid v_p(\Delta)$ for $p = 2, 7$, and $9 \nmid N$. In order to proceed, we must show that ρ_E^3 is strongly irreducible.

We use Proposition 3.17 with the prime $p = 37$. Namely, for this prime we observe that E must have good reduction. To see this, recall that multiplicative reduction can only occur when one of x, y and z is divisible by 37. However, modulo 37 the equation reduces to

$$x^9 + 8y^9 + 9z^9 \equiv 0 \pmod{37}$$

and it turns out that none of 8, 9 and $8 \cdot 9^{-1} \equiv 5$ are ninth powers modulo 37, therefore excluding this as an option. Using our SageMath [43] code, carefully using all the information available, reveals that we must have $\#\tilde{E}(\mathbb{F}_{37}) \in \{32, 44\}$ and so $a_{37}(E) \in \{-6, 6\}$. It follows that $a_{37}(E)$ must be divisible by 3, and since $37 \equiv 1 \pmod 3$, we conclude that ρ_E^3 is strongly irreducible.

If y is even, then the level lowering result will put us at level 14, where a single class of elliptic curves resides. However, the elliptic curve has a rational 3-torsion point, and therefore its mod-3 representation will not be irreducible. We arrive at a contradiction.

If y is odd, then we apply the level lowering result modulo 3 to end up at level 56. There exists a unique newform of this level, corresponding to the elliptic curve

$$F : Y^2 = X^3 + X + 2.$$

We cannot hope to arrive at a contradiction by comparing traces of Frobenius modulo 3, for there are actually solutions when one changes the exponent in the equation to 3. For example, $(2, -1, 0)$ describes an obvious family of solutions, and $(28, -77, 6)$ and $(77, -7, -3)$ are some additional, less obvious solutions. As we have done before, we can transform this equation into an elliptic curve which turns out to have rank 1. Therefore we indeed expect many families of solutions. The question is of course whether or not any of these families survive when we increase the exponent to 9.

Indeed, there exists a unique pair $(F, (3))$ at level 56 such that $\rho_E^3 \cong \rho_F^3$. Therefore Theorem 3.20 may be applied and it follows that even $\rho_E^9 \cong \rho_F^9$. We examine the situation at the prime 19, where the equation reduces to

$$x^9 + 8(y^9 - z^9) \equiv 0 \pmod{19}.$$

Since $x^9, y^9, z^9 \in \{-1, 0, 1\} \pmod{19}$, it is not hard to see that from this it follows that $19 \mid x$. Therefore E has multiplicative reduction at 19, whereas F has good reduction. It follows from the theorem, using $a_{19}(F) = 19 + 1 - 12 = 8$, that

$$8 \equiv \pm 20 \pmod{9}.$$

This is a contradiction. We conclude that there can be no solutions, hence solving the equation. It should again be noted that this would not have yielded a contradiction modulo 3, because indeed $8 \equiv 20 \pmod 3$. △

Remark 3.22. What killed the lion's share of our attempts at finding examples illustrating the use of the above theorem, was the existence of local obstructions for small

primes. For primes $1 \pmod 9$ in particular, it is fairly common that for some prime p, the equation $Ax^9 + By^9 + Cz^9 \equiv 0 \pmod p$ only has the trivial solution $(0,0,0)$, yielding a contradiction by the assumed coprimality of x, y and z. The general Hasse-Weil bound says that for a smooth projective plane curve C with genus g, it holds that

$$|\#C(\mathbb{F}_p) - (p+1)| \leqslant 2g\sqrt{p}.$$

Using Plückers Formula, we can compute that the degree 9 plane curve given by the zero set of $x^9 + 8y^9 + 7^5z^9$ has genus $7 \cdot 8/2 = 28$. Therefore we can only have local obstructions, corresponding to $\#C(\mathbb{F}_p) = 1$, as long as $p \leqslant 56\sqrt{p}$, so $p \leqslant 3136$. To be sure about the non-existence of local obstructions, it thus suffices to check all primes up to that bound for local solutions. This was checked with the aid of SageMath [43] with code that can be found in Appendix B, and indeed no local obstructions were found. This once again shows the necessity of the level lowering modulo 9.

Remark 3.23. One may wonder what happens to the equation $x^\ell + 8y^\ell + 7^5z^\ell = 0$ for prime exponents $\ell \geqslant 7$, noting that for $\ell = 5$ we reduce to Example 3.10. If y is even, then applying the modular method puts us at level 14, with a single isogeny class of elliptic curves, say G. Comparing traces of Frobenius using the SageMath [43] code in Appendix B, we find that if E has good reduction at 5, then $\#\tilde{E}(\mathbb{F}_5) \in \{4, 8\}$, whereas $\#G(\mathbb{F}_5) = 6$. These cannot agree modulo ℓ, and similarly, if E has multiplicative reduction, then $0 = \pm a_5(G) \equiv 5 + 1 \pmod \ell$, again a contradiction for $\ell \geqslant 7$.

If y is odd, we again find ourselves at level 56. It turns out that then comparing traces of Frobenius of images of inertia will get us nowhere, and since we have no complex multiplication, we are left to consider the symplectic method. Both E and F have additive reduction at 2 and multiplicative reduction at 7. Considering the additive reduction first, a glance at Proposition 2.51 reveals that with $v_2(\Delta_F) = 8$, $v_2(c_4(F)) = 4$ and $\Delta_F/2^8 = -7 \equiv 1 \pmod 4$, we find that $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{un}}) \cong \mathrm{SL}_2(\mathbb{F}_3)$. Similarly, we have $v_2(\Delta_E) = 10$ and $v_2(c_4(E)) = 4$ which gives the same result. Looking at Theorem 2.39 it follows that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if 2 is a square mod ℓ, using that 8 and 10 disagree modulo 3. On the other hand, using the multiplicative reduction at 7 and the facts that $v_7(\Delta_E) = 10$ and $v_7(\Delta_F) = 1$, we find by Proposition 2.31 that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if 10 is a square modulo ℓ. Combining these results yields a contradiction when 5 is not a square modulo ℓ. We conclude that for $\ell \equiv 2, 3 \pmod 5$ with $\ell \geqslant 5$, this equation can have no solutions. Additionally, we have shown that any solution must have y odd. As of now, we cannot determine any more results.

3.5 The Hilbert modular method

One may wonder whether or not the modular method can be applied to solve equations over general number fields, instead of just the field of rationals. Alternatively, it may be that to a certain equation one can attach a Frey curve that cannot be defined over $\mathbb{Q}$, but instead only over some number field. We will give a very minimalistic sketch of the *Hilbert modular method* that can be used when encountering one of the above situations.

First, one would need a modularity theorem for number fields greater than the rationals, and because of this we opt to restrict our view to totally real fields. It is sensible that this theorem should contain a notion of elliptic curves over the number field K in question, but it is not immediately clear what the appropriate generalisation of the rational newform should be. The answer turns out to be the following, and a more in depth treatment can be found in Chapter 1 of [9]. In the following, $\mathcal{O}_K$ will denote the ring of integers of the number field K.

Given a totally real number field K of degree m over $\mathbb{Q}$, we can list its m real embeddings $(\sigma_1, \ldots, \sigma_m)$. These induce a map $\mathrm{SL}_2(\mathcal{O}_K) \to \mathrm{SL}_2(\mathbb{R})^m$, by sending a matrix γ to $(\sigma_1(\gamma), \ldots, \sigma_m(\gamma))$. This induces an action of $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathcal{H}^m$.

Recall the definition of $j(\gamma, z)$ for 2×2 matrices γ and complex numbers z.

Definition 3.24. For each ideal $I \subset \mathcal{O}_K$ we define the *principal congruence subgroup* as

$$\Gamma_K(I) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{I} \right\} \subset \mathrm{SL}_2(\mathcal{O}_K).$$

A *congruence subgroup* is a subgroup $\Gamma \subset \mathrm{SL}_2(\mathcal{O}_K)$ that contains $\Gamma_K(I)$ for some ideal I. The largest possible such I defines the *level* of Γ.

Definition 3.25. A *Hilbert modular form* of degree m and *parallel weight* 2 of level I is a holomorphic function $f : \mathcal{H}^m \to \mathbb{C}$ satisfying

$$f(\gamma z) = f(z) \cdot \prod_{i=1}^{m} j(\sigma_i(\gamma), z_i)^2$$

for all $z = (z_1, \ldots, z_m) \in \mathcal{H}^m$ and all $\gamma \in \Gamma$, where Γ is of level I. Only for $m = 1$ we must additionally impose the conditions about holomorphicity at the cusps as outlined in Chapter 1.

Remark 3.26. The reason that we need not concern ourselves with holomorphicity at the cusps for $m > 1$ is that, rather remarkably, such conditions are automatically satisfied for holomorphic functions satisfying the transformation property given above. This is called *Koecher's principle* and can be found as Theorem 1.20 in [9].

We remark that the conductor of an elliptic curve over a number field is now an *ideal* in $\mathcal{O}_K$, with a definition very similar to that over $\mathbb{Q}$. The way to construct a Galois representation from an elliptic curve over a number field K is also completely analogous to what we did for elliptic curves over $\mathbb{Q}$. Again, we will not discuss the details here, as they can be found in Section II.1 and II.2 in [4], but we also have a theory of Hecke operators and eigenforms for Hilbert modular forms, and so we can also talk about *Hilbert newforms*. We define $\mathbb{Q}_f$ to be the field obtained by adjoining all eigenvalues of the Hilbert newform f for all the Hecke operators to the field of rationals. It is also possible to associate ℓ-adic representations for every prime number ℓ to a Hilbert modular form with respect to the obvious generalisation of the congruence subgroup $\Gamma_0(I)$ for an ideal I.

From now on we will follow the brief summary of the method provided in Sections 1 and 2 in [23]. The modularity theorem 2.12 was a huge achievement, and it has turned out that, recalling the struggle to prove it over $\mathbb{Q}$, generalising it to other number fields is not an easy task. The following theorem summarises some of the most recent results and was originally proved in [21] as Theorem 1 and Theorem 5.

Theorem 3.27. *For a totally real field* K*, there exist, up to isomorphism over* $\overline{K}$*, as most finitely many elliptic curves that are* not *modular, i.e. for which there exists no Hilbert newform for which the* ℓ*-adic representations agree for every prime* ℓ*. If* K *is real quadratic, then every elliptic curve over* K *is modular.*

Indeed, the conductor of an elliptic curve and the level of its associated modular form must agree. Now the natural question to ask is whether or not there is also a result that conversely says that every Hilbert modular form can be associated with an elliptic curve with the right conductor. This also is in its full generality but merely a conjecture, known as the Eichler-Shimura Conjecture, but some partial results for this have been established, including the following, which is actually a special case of a more general result originally derived from the results by Hida in [26] in Section 2 of [6].

Theorem 3.28. *Let* K *be a totally real number field and* f *a Hilbert modular form of parallel weight 2 of level* I *such that* $\mathbb{Q}_f = \mathbb{Q}$*. Suppose that there exists a prime* q *such that* $v_q(I) = 1$*. Then there exists an elliptic curve* E *over* K *with conductor* I *such that the* ℓ*-adic representations of* f *and* E *agree for all primes* ℓ*.*

Next, one would like to have some kind of level lowering theorem for Hilbert modular forms. This is given by the following theorem, first given in [23] as Theorem 7, by combining many previously shown results together. These kinds of theorems are truly the backbone of the modular method.

Theorem 3.29. *Let* K *be a totally real field,* E/K *an elliptic curve of conductor* I *and* p *a prime number. Define*

$$I_p = I \Big/ \prod_{\substack{q \mid I \\ p \mid v_q(\Delta(E))}} q,$$

where $\Delta(E)$ *should always be taken to be of a minimal model locally at* q*. Suppose that the prime* p *satisfies* $p \geqslant 5$*, the ramification index for all* $\mathfrak{P} \mid p$ *is smaller than* $p - 1$*, and* $\mathbb{Q}(\zeta_p)^+ \not\subset K$*. Suppose further that* E *is modular,* ρ_E^p *is irreducible,* E *does not have additive reduction at any* $\mathfrak{P} \mid p$ *and lastly* $p \mid v_{\mathfrak{P}}(\Delta(E))$ *for any* $\mathfrak{P} \mid p$*. Then there exists a Hilbert newform of parallel weight 2 at level* I_p *and a prime ideal* $\mathfrak{Q} \mid p$ *in the ring of integers of* $\mathbb{Q}_f$ *such that* $\rho_E^p \sim \rho_f^{\mathfrak{Q}}$*.*

Using the above results, one should be able to verify all conditions from the above theorem, except for the irreducibility of the mod-p representation. Fortunately, we also have the following result, first given as Theorem 2 in [24].

Theorem 3.30. *Let* K *be a totally real Galois extension of* $\mathbb{Q}$*. Then there exists an explicit constant* C_K *with the property that for all* $p > C_K$ *and all elliptic curves* E/K *with the property that* E *does not have additive reduction at any* $\mathfrak{P} \mid p$*, the representation* ρ_E^p *is irreducible.*

This concludes our very brief discussion of the Hilbert modular method. It is not our desire to explore this topic very deeply and thoroughly, as is reflected by the concision of the above treatment, but we will merely use the understanding of a partially working modular method to be conducted over totally real number fields to proceed. This motivates the importance of the topic to be treated in the next section, which will be the last before jumping to our newly found examples of applications of the symplectic method over the rationals in Chapter 4.

3.6 The symplectic method over number fields

We generalise the symplectic criteria proved in the previous chapter to more general number fields. For the first, we will make use of the generality of the concept of Tate curves, which, as in the proof over the rationals, will do most of the work for us. We closely mimic the proof of Proposition 2.31.

Theorem 3.31. *Let K be a number field and let E/K be an elliptic curve. Let ℓ be a prime number and let $\mathfrak{P} \subset \mathcal{O}_K$ be a prime ideal lying over an* unramified *prime $p \neq \ell$. Let F/K be an elliptic curve such that $E[\ell]$ and $F[\ell]$ are isomorphic $\mathrm{Gal}(\overline{K}/K)$-modules and suppose that both E and F have multiplicative reduction at $\mathfrak{P}$. Further suppose that neither $v_{\mathfrak{P}}(\Delta_{\min}(E))$ nor $v_{\mathfrak{P}}(\Delta_{\min}(F))$ is divisible by ℓ. Then $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if $v_{\mathfrak{P}}(\Delta_{\min}(E))$ and $v_{\mathfrak{P}}(\Delta_{\min}(F))$ differ by a square modulo ℓ.*

Proof. Instead of working over the p-adic numbers, we now consider

$$K_{\mathfrak{P}} = \mathrm{Frac}\big(\varprojlim_n \mathcal{O}_K/\mathfrak{P}^n\mathcal{O}_K\big).$$

Let k be the completion of the maximal unramified extension of $K_{\mathfrak{P}}$. Note that our assumption of p being unramified, implies that $K_{\mathfrak{P}}/\mathbb{Q}_p$ is unramified also. Hence k contains all n-th roots of unity for all n coprime to p. Then in particular k will contain all ℓ-th roots of unity and because the extension is unramified, both E and F will still have multiplicative reduction at $\mathfrak{P}$ over k. Again it follows that $\|j\| > 1$ for both E and F. Hence by Theorem 2.33 we may conclude that there exist $q_E, q_F \in k$ with the properties that $v_{\mathfrak{P}}(q_E) = v_{\mathfrak{P}}(\Delta(E))$ and $v_{\mathfrak{P}}(q_F) = v_{\mathfrak{P}}(\Delta(F))$ and

$$E(\overline{k}) \cong \overline{k}^*/q_E^{\mathbb{Z}} \quad \text{and} \quad F(\overline{k}) \cong \overline{k}^*/q_F^{\mathbb{Z}},$$

as $\mathrm{Gal}(\overline{k}/k)$-modules, again using that k was maximally unramified. In parallel to our previous proof, if $\varphi : E(\overline{\mathbb{Q}})[\ell] \to F(\overline{\mathbb{Q}})[\ell]$ is the assumed isomorphism of $\mathrm{Gal}(\overline{K}/K)$-modules, then any embedding $\overline{K} \to \overline{k}$ induces an isomorphism $\psi : E(\overline{k})[\ell] \to F(\overline{k})[\ell]$ of $\mathrm{Gal}(\overline{k}/k)$-modules. Clearly φ is symplectic precisely when ψ is symplectic.

The rest of the proof is almost completely analogous to the proof of Proposition 2.31, as it just deals with 2×2-matrices and $\mathfrak{P}$-valuations. □

We see that passing to the maximal unramified extension basically nullified the complications caused by the introduction of the general number field. Therefore the above

seems to be a potentially powerful result to aid in the process of solving the equations with elliptic curves defined over number fields. Recall that the proof of Theorem 2.39 also made use of the maximal unramified extension and algebraic closures, so that most of the proof will carry over to more general number fields, just as above. For convenience, and with regards to the previous section, we will specialise to quadratic extensions.

Theorem 3.32. *Let* K *be a quadratic extension of* $\mathbb{Q}_2$ *in which 2 splits completely. Let* v *denote its valuation and let* ℓ *be a prime number. Let* E/K *and* E'/K *be elliptic curves with potentially good reduction. Write* $L = \mathbb{Q}_2^{un}(E[\ell])$ *and* $L' = \mathbb{Q}_2^{un}(E'[\ell])$. *Suppose that* $L = L'$ *and that* $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$.

Then $E[\mathfrak{p}]$ *and* $E'[\mathfrak{p}]$ *are isomorphic* $\mathrm{Gal}(L/\mathbb{Q}_2^{un})$*-modules for all odd primes* $\mathfrak{p}$. *Moreover, if 2 is a square modulo* ℓ*, they are symplectically isomorphic. Otherwise they are symplectically isomorphic if and only if* $v(\Delta_{\min}(E)) \equiv v(\Delta_{\min}(E')) \pmod 3$.

Proof. We begin by observing that $K \subset \mathbb{Q}_2^{un}$ by our assumptions. Note that Lemma 2.42 was just a group theoretic tool, that the proof of Lemma 2.43 is independent of the base field and Lemma 2.44 is shown in the text above Corollary 2 in Section 2 of [38] in similar generality. Reducing at a uniformiser still gives residue field $\mathbb{F}_2$ and so the proof of Lemma 2.45 will still hold as well. The subsequent corollary remains valid and so does the proof of the case that 2 is a square modulo ℓ. Similarly, we need not touch the proofs of Lemma 2.48 and Lemma 2.49, as they do not rely on the base field in question. The last reduction before the final stretch is also still valid. Now to assure ourselves that the arguments given in Appendix A from [25] may still be applied to our current situation, we remark that Proposition A.2 is already stated for more general local fields, so we need only check that the conditions from the theorem still apply. We find that only the assumption that 3 is a square modulo ℓ is not satisfied, but as was already noted at the end of Section 3 in [18], by examining the proof, we find that that assumption is only used to reduce the general theorem to the case that E has a 3-torsion point defined over K. Fortunately, by Lemma 2.49, we are already in that situation. This completes the proof. □

Taking $K/\mathbb{Q}$ to be real quadratic satisfying a few other conditions depending on the equation thus makes the symplectic method a potentially powerful tool to help solve equations over fields greater than $\mathbb{Q}$ using the Hilbert modular method. Because examples of the this method and other methods dealing with elliptic curves over number fields quickly become very technical, we opt to conclude our brief exploration of possible generalisations of the symplectic method here. In the final chapter we will again return to the rational numbers and we will discuss a great number of new examples in detail.

4 New results

In the following few sections we will prove a number of different statements about families of twisted Fermat equations of varying signatures. First we will consider the signature (ℓ, ℓ, ℓ), then $(\ell, \ell, 2)$ and finally $(\ell, \ell, 3)$. For each of the theorems that we are about to prove, we checked using the computer software SageMath [43] that we could not obtain any general information by comparing traces of Frobenius for any prime of good reduction smaller than 100, making it unlikely that any greater prime would. The code and the results of the programs are found in Appendix B. Furthermore, none of the elliptic curves that we are to compare our Frey curve with have complex multiplication, unless specified otherwise. For none of the examples below, Proposition 3.13 about the image of inertia could be applied. Namely, in each case, the conductors of the Frey curves show that these curves have multiplicative reduction at primes for which the j-invariants of the curves obtained after level lowering have negative valuation, and thus not potentially good reduction.

The goal of this investigation was to find new applications of the symplectic method, solving families of equations as general as possible. Therefore we avoided situations where the classical approaches could be applied to the best of our abilities. Before we present the new results, however, we will first need to expand our set of symplectic criteria in order to be a little more versatile when applying the method.

4.1 More symplectic theorems

Our presentation of the symplectic method in Chapter 2 was far from comprehensive. Aside from Proposition 2.31 and Theorem 2.39, there are more symplectic criteria available. To be more specific, especially in the case of potentially good reduction at a given small prime, there are a lot of different theorems available in the literature to help us determine the symplectic type of the isomorphism. We let $L = \mathbb{Q}_p^{un}(E[\ell])$ for some odd prime ℓ be the semistability defect of an elliptic curve $E/\mathbb{Q}_p$ with potentially good reduction as in Chapter 2. There we considered the case that $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$, but one can imagine that this is far from always the case. Sometimes one has potentially good reduction at a prime different from 2, or sometimes the degree of the minimal extension of good reduction is not maximal. In Section 4 in [20] all currently known symplectic criteria are systematically listed. We will now list and elaborate on the theorems that we will need in the forthcoming sections. The following result is Theorem 1 in [20].

Theorem 4.1. *Let* $p \equiv 2 \pmod 3$ *be a prime number and let* E *and* F *be elliptic curves over* $\mathbb{Q}_p$ *with potentially good reduction at* p*. Suppose that we have* $\mathrm{Gal}(L/\mathbb{Q}_p^{un}) \cong \mathbb{Z}/3\mathbb{Z}$ *and that*

$E[\ell]$ *and* $F[\ell]$ *are isomorphic Galois modules for some prime* $\ell \geqslant 5$ *different from* p. *Set* $t = 1$ *if exactly one of* E *and* F *has a 3-torsion point defined over* $\mathbb{Q}_p$ *and* $t = 0$ *otherwise. Set* $r = 0$ *if* $v_p(\Delta_{\min}(E)) \equiv v_p(\Delta_{\min}(F)) \pmod 3$ *and* $r = 1$ *otherwise. Then*

$$E[\ell] \text{ and } F[\ell] \text{ are symplectically isomorphic if and only if } \left(\frac{p}{\ell}\right)^r \left(\frac{3}{\ell}\right)^t = 1.$$

Remark 4.2. The scrutinous reader may be concerned about the commutative nature of the group $\mathbb{Z}/3\mathbb{Z}$, possibly making it so that Proposition 2.40 need not be able to be applied alongside the above theorem. However, fortunately in Section 4 in [20] most results are about symplectically isomorphic $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-modules, including the above. This means that it can still be compared to Proposition 2.31, and we will make use of this fact later.

We briefly sketch the idea of the proof. One can consider the matrices N, A, N', A' corresponding to the two generators of $\mathrm{Gal}(L/\mathbb{Q}_p^{\mathrm{un}})$ acting on the ℓ-torsion for both elliptic curves. Recall the definition of γ_E as presented in Lemma 2.44. Similar to what is sketched in the final stretch of the proof of Theorem 2.39, we can express $\gamma_E(\sigma)$ explicitly in terms of the valuation $v_p(\Delta_E)$. This valuation also determines to some extent the existence of a 3-torsion point over $\mathbb{Q}_p$. Combining all this information appropriately, one can choose symplectic bases such that $N = N'$ and $A^{\pm 1} = A'$, where the sign depends on the value of r. One then proceeds to show that the matrix that represents the isomorphism of ℓ-torsion modules, or a matrix closely related to it, has to be contained in the centralisers of both A and N, but by group theory one can show that only scalar matrices can occur in such an intersection. All of these matrices have determinant a square modulo ℓ, yielding results about the symplecticity of the isomorphism.

In order to aid the reader with applying this result, in Theorem 2 of [20] the authors provide fairly elementary criteria that help decide whether or not an elliptic curve with the properties as assumed in the above theorem actually has a 3-torsion point defined over $\mathbb{Q}_p$ or not. A subset of these criteria for the prime $p = 2$, catered to our needs, is presented in the proposition below.

Proposition 4.3. *Let* $E/\mathbb{Q}_2$ *be an elliptic curve with potentially good reduction at 2 and with* $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{un}}) \cong \mathbb{Z}/3\mathbb{Z}$. *Suppose that either*

- $(v_2(c_4(E)), v_2(c_6(E)), v_2(\Delta(E))) = (4, 6, 8)$ *and* $c_4(E)/2^4 \equiv 21 \pmod{32}$ *and* $c_6(E)/2^6 \equiv 11 \pmod{16}$;
- $(v_2(c_4(E)), v_2(c_6(E)), v_2(\Delta(E))) = (\geqslant 6, 5, 4)$ *and* $c_6(E)/2^5 \equiv 5 \pmod 8$.

Then E *has a 3-torsion point defined over* $\mathbb{Q}_2$.

The proof of these criteria is not particularly deep and can be obtained by carefully writing everything out. This is done in Section 13.2 in [20].

Now we turn to perhaps the most natural case to consider after having proved Theorem 2.39. Namely, the next largest possible degree of minimal extension of good reduction at the prime 2 is the case that $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{un}}) \cong H_8$, where H_8 denotes the quaternion group. The following result is Theorem 7 and a special case of Theorem 8 in [20].

Theorem 4.4. *Let* E *and* F *be elliptic curves over* $\mathbb{Q}_2$ *with potentially good reduction at 2. Suppose that* $E[\ell]$ *and* $F[\ell]$ *are isomorphic Galois modules for a certain prime* $\ell \geqslant 3$ *and suppose that* $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong H_8$. *Then* $E[\ell]$ *and* $F[\ell]$ *cannot be simultaneously symplectically and anti-symplectically isomorphic. If 2 is a square modulo* ℓ, *then they are symplectically isomorphic.*

If 2 is not a square modulo ℓ, *then suppose further that both* E *and* F *have precisely five factors of 2 in their conductors and both satisfy* $(\nu_2(c_4), \nu_2(c_6), \nu_2(\Delta)) = (4, \geqslant 7, 6)$ *and* $c_4/2^4 \equiv -1 \pmod 4$. *Then* $E[\ell]$ *and* $F[\ell]$ *are symplectically isomorphic.*

The proof of most of the above theorem is very similar to that of Theorem 2.39 and can be found partly in the proof of Theorem 4.6 in [22] and for the case that 2 is not a square modulo ℓ, in Section 30 of [20]. It starts with a different group theoretical lemma, stating that for $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ and $H \subset G$ a subgroup isomorphic to H_8, we have

$$N_G(H)/Z(G) \cong \mathrm{Aut}(H) \cong S_4$$

and that all the matrices in $N_G(H)$ have square determinant if 2 is a square modulo ℓ, and if not, only those corresponding to the inner automorphisms. After that, all arguments starting at Lemma 2.43 and ending at Lemma 2.48 can be copied almost verbatim. It is shown in Section 30 of [20] that the conditions in the above theorem imply that the number of factors of 2 in the conductors of E and F must agree. To then determine when $\overline{E}[3]$ and $\overline{F}[3]$ are symplectically isomorphic if 2 is not a square modulo ℓ, for each of the values of $\nu_2(N_E) = \nu_2(N_F)$ the authors determined all possibilities for the triples $(\nu_2(c_4), \nu_2(c_6), \nu_2(\Delta))$ and showed that after a change of coordinates, the residual curves could only fall into finitely many different classes. They then checked all possible pairs for symplecticity with the aid of a computer. What is stated in the theorem is a small part of the outcome of that endeavour, as in the forthcoming we will only apply this theorem when working with elliptic curves with five factors of 2 in their conductors.

Lastly, we turn to what some might argue to have truly been the most natural case to consider after proving Theorem 2.39, namely that of the second largest possible degree of minimal extension of good reduction for any prime; $\mathrm{Gal}(L/\mathbb{Q}_3^{un}) \cong \mathrm{Dic}_{12}$, where Dic_{12} denotes the dicyclic group of order 12. The following is Theorem 10 and a bit of Theorem 11 from [20].

Theorem 4.5. *Let* E *and* F *be elliptic curves over* $\mathbb{Q}_3$ *with potentially good reduction at 3. Suppose that* $E[\ell]$ *and* $F[\ell]$ *are isomorphic Galois modules for some prime* $\ell \geqslant 5$ *and suppose further that* $\mathrm{Gal}(L/\mathbb{Q}_3^{un}) \cong \mathrm{Dic}_{12}$. *Then* $E[\ell]$ *and* $F[\ell]$ *are not simultaneously symplectically and anti-symplectically isomorphic. If* 3 *is a square modulo* ℓ, *then* $E[\ell]$ *and* $F[\ell]$ *are symplectically isomorphic.*

If 3 *is not a square modulo* ℓ, *suppose further that the conductors of both* E *and* F *have precisely three factors of 3. Then* $E[\ell]$ *and* $F[\ell]$ *are symplectically isomorphic if and only if* $\nu_3(\Delta_E) \equiv \nu_3(\Delta_F) \pmod 4$.

The proof of this theorem is again very similar to that of the other two local symplectic criteria with a large degree of minimal extension of good reduction that we have

proved so far. The most notable changes for the first part are that we are working over $\mathbb{Q}_3$ instead of $\mathbb{Q}_2$. In the second part we reduce to checking whether or not $E[5]$ and $F[5]$ are symplectically isomorphic, because 5 is the smallest prime for which 3 is not a square.

Remark 4.6. A very important detail to observe is that all the symplectic theorems have one property in common; they all contain a statement of the form: "if α is a square modulo ℓ, then $E[\ell]$ and $F[\ell]$ are symplectically isomorphic." No matter how many different symplectic criteria for potentially good reduction we combine, we will always find some residue class of primes for which all those α's are squares mod ℓ, yielding symplectically isomorphic ℓ-torsion. Even combining it with Proposition 2.31 will not be able to result in a contradiction for all primes, for the same reason. Therefore, with the symplectic criteria currently available, it is *not* possible to solve an equation completely for all primes ℓ. In theory the density of the primes for which we can solve the equation can be arbitrarily close to 1, but it can never quite reach that number. One will always need some additional information or tricks in order to deal with the remaining primes. This is a severe limitation of the symplectic method.

We conclude this section by extending the list of criteria in [28] to perfectly suit our needs in the forthcoming. This will help us determine the order of the semistability defect in all the considered examples.

Proposition 4.7. *Let $E/\mathbb{Q}_p$ be an elliptic curve with minimal discriminant Δ and recall the quantity c_4. Denote $G = \mathrm{Gal}(L/\mathbb{Q}_p^{\mathrm{un}})$ with L defined as before. Then if $p = 2$, we have:*

- *if $v_2(\Delta) = 8$ and $v_2(c_4) = 4$ and additionally $\Delta/2^8 \equiv c_6/2^{v_2(c_6)} \equiv -1 \pmod 4$, then $G \cong \mathbb{Z}/3\mathbb{Z}$.*
- *if $v_2(\Delta) = 4$ and $v_2(c_4) \geqslant 6$ and additionally $c_6/2^{v_2(c_6)} \equiv 1 \pmod 4$, then $G \cong \mathbb{Z}/3\mathbb{Z}$.*
- *if $v_2(\Delta) = 6$ and $v_2(c_4) = 4$, then $G \cong H_8$.*

If $p = 3$ then

- *if $v_3(\Delta) = 9$ and $v_3(c_6) = 6$ and additionally $\Delta/3^9 \not\equiv 2, 4 \pmod 9$, then $G \cong \mathrm{Dic}_{12}$.*
- *if $v_3(\Delta) = 3$ and $v_3(c_6) = 3$ and additionally $\Delta/3^3 \not\equiv 2, 4 \pmod 9$, then $G \cong \mathrm{Dic}_{12}$.*

4.2 A theorem of signature (ℓ, ℓ, ℓ)

We will prove the following theorem, which the author has not been able to find in any of the literature. Much like the examples in Chapter 2, it will make use of both the symplectic criteria that we had proved there, but also some new ones from the previous section. We will consider an infinite family of twisted Fermat equations with two parameters and say something meaningful about almost every case. We will heavily rely on the results from Section 14 in [40]; when we cite this source in this section, we always refer to Section 14.1.

Theorem 4.8. *Let $k, \alpha \geqslant 0$ be integers and $\ell \geqslant 5$ a prime. Then the equation*

$$x^\ell + 2^\alpha y^\ell + 3^k z^\ell = 0$$

has no nontrivial solutions if

- $\alpha = 0$ *or* $\alpha > 3$.
- $k = 0$ *and* $\alpha \neq 1$, *where the exceptional case has the solutions* $(\pm n, \mp n, \pm n)$.
- $\alpha \in \{1, 2, 3\}$ *and* y *is even.*
- $\alpha \in \{1, 2\}$ *and* ℓ *is such that* k *is not a square modulo* ℓ.
- $\alpha = 3$ *and* ℓ *is such that* $2k$ *is not a square modulo* ℓ.

Proof. To establish this theorem, we will split a great many cases. The solution for $k = 0$ was already described in Example 3.10. Consider a non-trivial primitive solution to the above equation. Assume without loss of generality that $x^\ell \equiv -1 \pmod 4$. We consider the elliptic curve

$$E : Y^2 = X(X - x^\ell)(X + 2^\alpha y^\ell).$$

From [40] it follows that the conductor of E is of the form $2^\beta \mathrm{rad}_2(2^\alpha 3^k xyz)$, where $\beta \in \{0, 1, 3, 5\}$ depends on α and y. Here rad_2 indicates the radical of the number, ignoring the prime 2. In particular we see that 3 divides the conductor of E precisely once, making the reduction there multiplicative. By Remark 2.24 it then follows that $j(E) \notin \mathbb{Z}[1/2]$ and so we find that E has no ℓ-isogenies for $\ell \geqslant 17$.

In fact, we can go as far down as $\ell \geqslant 5$ by following the reasoning in Lemme 4 in [29]. Namely, it follows from the conductor that E can only have additive reduction at the prime 2, which it only has when $\alpha \in \{1, 2, 3\}$ and y is odd. For all other α, the curve E must hence be semistable and so by Theorem 2.18 we may conclude that ρ_E^ℓ is irreducible. In the remaining cases, we will show in the remainder of the proof that the group $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{un}})$ will either be isomorphic to H_8 or to $\mathrm{SL}_2(\mathbb{F}_3)$. In particular, this group is non-abelian and thus non-cyclic in each case. Then Proposition 23(b) from [35] shows that ρ_E^ℓ is irreducible for all $\ell \geqslant 5$. Hence the level lowering theorem applies in each case. We may now continue the proof.

First suppose that $\alpha = 4$. Then according to [40], E corresponds to a newform of level $\mathrm{rad}_2(2^\alpha 3^k) = 3$, but these do not exist. Similarly, if $\alpha = 0$ or $\alpha \geqslant 5$, then E corresponds to a newform of level $2\mathrm{rad}_2(2^\alpha 3^k) = 6$, but these do not exist either.

It remains to consider $\alpha \in \{1, 2, 3\}$. If y is even, then Section 14 in [40] tells us that E corresponds to a newform of level $2\mathrm{rad}_2(2^\alpha 3^k) = 6$, which do not exist. We thus need only concern us with the case that y is odd. We remark that for $\ell \mid k$, the statements that remain to be proved are vacuous, so we may assume that $\ell \nmid k$.

The case $\alpha = 1$: Here [40] gives that E gives rise to a newform of level $2^5 \mathrm{rad}_2(2^\alpha 3^k) = 96$. There exist two newforms of this level, and they correspond to the elliptic curves

$$F_1 : Y^2 = X^3 - X^2 - 2X \quad \text{and} \quad F_2 : Y^2 = X^3 + X^2 - 2X$$

These elliptic curves are quadratic twists by -1 and hence have the exact same discriminant, j-invariant and conductor, namely

$$\Delta = 2^6 \cdot 3^2, \quad \text{and} \quad c_4 = 2^4 \cdot 7.$$

We will drop the subscript in the following. It is easy to see that F has potentially good reduction at 2, because $v_2(j(F)) \geqslant 0$. We want to make use of this potentially good reduction, which we remark E has as well because $c_4(E) = 16(x^{2\ell} + 2x^\ell y^\ell + 4y^{2\ell})$ has precisely 4 factors of two, whereas $\Delta_E = 2^6 3^{2k}(xyz)^{2\ell}$ has only 6. Now Proposition 4.7 tell us that $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong H_8$, where H_8 denotes the quaternion group. Theorem 4.4 then tells us that if 2 is a square mod ℓ, then $E[\ell]$ and $F[\ell]$ are symplectically isomorphic. Now, the difficult case is to decide what happens when 2 is not a square mod ℓ. We remark that both E and F have 5 factors of 2 in their conductors. We compute that

$$c_6(E) = 2^6(x^{3\ell} + 3x^{2\ell}y^\ell - 6x^\ell y^{2\ell} - 8y^{3\ell}) \quad \text{and} \quad c_6(F) = 2^7 \cdot 5.$$

and since x and y are assumed to be odd, it follows that in both cases, c_6 has at least 7 factors of 2. Now, $c_4(F)/2^4 = 7 \equiv -1 \pmod 4$ and in addition

$$c_4(E)/2^4 = x^{2\ell} + 2x^\ell y^\ell + 4y^{2\ell} \equiv 1 + 2x^\ell y^\ell \equiv -1 \pmod 4,$$

where we use that $2x^\ell y^\ell \equiv 2 \pmod 4$. Therefore Theorem 4.4 tells us that also in this case, $E[\ell]$ and $F[\ell]$ are symplectically isomorphic, making them symplectically isomorphic in every case.

It is easy to see that E and F have multiplicative reduction at 3. Therefore Proposition 2.31 gives us that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if $v_3(\Delta_E) \equiv 2k \pmod \ell$ and $v_3(\Delta_{F_i}) = 2$ differ by a square modulo ℓ; that is, k is a square modulo ℓ. Combined with the above, we find a contradiction when k is not a square modulo ℓ.

The case $\alpha = 2$: We may apply Theorem 2.15 to obtain a newform of level 24. There exists only one such newform, and it corresponds to the elliptic curve

$$F : Y^2 = X^3 - X^2 - 4X + 4, \quad \text{with} \quad \Delta = 2^8 \cdot 3^2.$$

It is easy to compute that F has potentially good reduction at 2. One can compute that

$$\Delta_{E,\min} = 2^8 3^{2k}(xyz)^{2\ell} \quad \text{and} \quad c_4(E) = 16(x^{2\ell} + 4x^\ell y^\ell + 16y^{2\ell}).$$

Therefore $v_2(\Delta_E) = 8$ and $v_2(c_4(E)) = 4$. Thus $v_2(j(E)) = 4 > 0$ and thus E also has potentially good reduction. Since the ℓ-torsion modules of these curves are isomorphic, their minimal extensions of good reduction agree. Now we observe that $v_2(\Delta_F) = 8$ and $v_2(c_4(F)) = 4$ and $\Delta_F/2^8 = 9 \equiv 1 \pmod 4$, and so Proposition 2.51 gives us that $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$. Similarly, $v_2(\Delta_E) = 8$ and $v_2(c_4(E)) = 4$ and so Proposition 2.51 applies once more, noting that $(3^k(xyz)^\ell)^2 \equiv 1 \pmod 4$ since all of x, y and z are odd. Now we are in the position to apply Theorem 2.39 to find that, since $v_2(\Delta_E) = v_2(\Delta_F)$, the ℓ-torsion modules of E and F are symplectically isomorphic. We remark that both elliptic curves have multiplicative reduction at 3. Now Proposition 2.31 gives us that

$v_3(\Delta_E) \equiv 2k \pmod{\ell}$ and $v_3(\Delta_F) = 2$ differ by a square modulo ℓ. This again means that k is a square modulo ℓ.

The case $\alpha = 3$: We may apply Theorem 2.15 again to find the same elliptic curve F with conductor 24. As before, we find that Theorem 2.39 applies. Again Proposition 2.51 yields that also $v_2(\Delta_E) = 10$ and $v_2(c_4(E)) = 4$ together give $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \cong \mathrm{SL}_2(\mathbb{F}_3)$. However, now we have that $v_2(\Delta_E) = 10$, which is not equivalent to $v_2(\Delta_F) = 8$ modulo 3. Therefore we find that the ℓ-torsion modules are symplectically isomorphic if and only if 2 is a square mod ℓ. On the other hand, Proposition 2.31 still gives us that they are symplectically isomorphic if and only if k is a square mod ℓ. This means that it cannot happen that 2 and k have distinct Legendre symbols. □

Remark 4.9. The reader may wonder if this same method can be used to derive very similar results for the equation

$$x^\ell + y^\ell + 2^\alpha \cdot 3^k z^\ell = 0.$$

The problem is that we no longer know the parity of z in a primitive solution, meaning that E need not have potentially good reduction at 2 if z is even. Restricting our view to odd z, the same argument as above can actually be applied. We do note that this does not affect the first two claims from the above theorem, which still hold in this case.

Remark 4.10. It is important to remark here that in Corollaire 1 in [29], Kraus showed that for any prime p that is not of the form $2^n \pm 1$, it holds that the equation $x^\ell + 2^\alpha y^\ell + p^k z^\ell = 0$ has no solutions for primes ℓ exceeding a certain numerical bound, dependent only on p. This result would have been much stronger than the above theorem, had it not been for the fact that $3 = 2^2 - 1$ is of the forbidden form. Théorème 1 in that same paper gives a contradiction for sufficiently large primes ℓ should the curves at level 24 and 96 not have had full rational 2-torsion, but it turns out that they do. Therefore, the symplectic method really is the only way known to the author to arrive at the results stated and proved above.

4.3 Theorems of signature $(\ell, \ell, 2)$

Fortunately, [40] provides detailed recipes for more signatures than just (ℓ, ℓ, ℓ). We next turn to a different type of twisted Fermat equation, using a set of Frey curves with properties originally described in Section 2 of [2]. When we cite [40] in this section, we will always refer to Section 14.2.

Theorem 4.11. *Let* $k > 0$ *be an integer and* $\ell \equiv \pm 1 \pmod{24}$ *a prime number. Then the equation*

$$5^k x^\ell + 4y^\ell = z^2$$

has no nontrivial primitive solutions for ℓ *such that* k *is not a square modulo* ℓ*, apart from*

$$5^1 \cdot 1^\ell + 4 \cdot 1^\ell = (\pm 3)^2, \quad 5^1 \cdot 1^\ell + 4 \cdot (-1)^\ell = (\pm 1)^2, \quad \textit{and} \quad 5^3 \cdot 1^\ell + 4 \cdot (-1)^\ell = (\pm 11)^2.$$

Proof. As always, suppose that we have a non-trivial and primitive solution, meaning that $5x$, $2y$ and z are pairwise coprime. We need to distinguish two different cases. First suppose that y is even and assume without loss of generality that $z \equiv 1 \pmod 4$. We may again assume that $\ell \nmid k$ and we consider the elliptic curve

$$E : Y^2 + XY = X^3 + \frac{z-1}{4}X^2 + \frac{y^\ell}{16}X.$$

Note that $\ell \geqslant 7$ is assured by our conditions on ℓ. Then [40] tells us that if $xy \neq \pm 1$, one can show that E corresponds via the level lowering theorem to a newform of level $N_\ell = \operatorname{rad}(5^k \cdot 4) = 10$. However, newforms of this level do not exist.

Now suppose that y is odd, and then assume without loss of generality that $z \equiv -y \pmod 4$. We consider the elliptic curve

$$E : Y^2 = X^3 + zX^2 + y^\ell X, \quad \text{with} \quad \Delta_E = 2^4 5^k (xy^2)^\ell.$$

We once more need to distinguish two cases. If $y \equiv 1 \pmod 4$, then [40] tells us that if $xy \neq \pm 1$, then E corresponds to a newform of level $N_\ell = 2^2 \cdot \operatorname{rad}(5^k \cdot 4) = 40$. There exists a unique newform of level 40, and it corresponds to the elliptic curve

$$F : Y^2 = X^3 - 7X - 6 \quad \text{with} \quad \Delta_F = 2^8 \cdot 5^2 \quad \text{and} \quad c_4(F) = 2^4 \cdot 3 \cdot 7.$$

We see that F has potentially good reduction at 2. We must show that E does so too. We can see that $c_4(E) = 16(-3y^\ell + z^2)$ and since all of x, y and z are assumed to be odd, we see that $v_2(\Delta_E) = 4$ and using that $y, z^2 \equiv 1 \pmod 4$, we also see that $v_2(c_4(E)) = 5$, showing potentially good reduction at 2. Now Proposition 2.51 gives us that E satisfies $\operatorname{Gal}(L/\mathbb{Q}_2^{\mathrm{un}}) \cong \mathrm{SL}_2(\mathbb{F}_3)$ and similarly also F. We may thus apply Theorem 2.39 and using the fact that $v_2(\Delta_E)$ and $v_2(\Delta_F)$ disagree mod 3, we find that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if 2 is a square mod ℓ. On the other hand, clearly F has multiplicative reduction at 5 and to see that E has multiplicative reduction there as well, we either remark that since $z^2 \equiv 4y^\ell \pmod 5$ it follows that $-3y^\ell + z^2 \equiv y^\ell \not\equiv 0 \pmod 5$, or we invoke [40] to observe that $N_E = 4 \operatorname{rad}(10xy)$, which indeed has precisely one factor of 5. Now we may apply Proposition 2.31 to find that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if k and 2 differ by a square modulo ℓ. We conclude that k must be a square modulo ℓ.

The remaining case is that $y \equiv -1 \pmod 4$. According to [40], we now have $N_\ell = 2 \operatorname{rad}(5^k \cdot 4) = 20$. Once more, there exists a unique newform of level 20, and it corresponds to the elliptic curve

$$G : Y^2 = X^3 + X^2 + 4X + 4 \quad \text{with} \quad \Delta_G = -2^8 \cdot 5^2 \quad \text{and} \quad c_4(G) = -2^4 \cdot 11.$$

We readily see that G has potentially good reduction at 2, but a complication is that, according to Proposition 4.7, because $\Delta_G/2^8 \equiv -1 \pmod 4$ and $c_6(G)/2^6 = -37 \equiv -1 \pmod 4$, we have that $\operatorname{Gal}(L/\mathbb{Q}_2^{\mathrm{un}}) \cong \mathbb{Z}/3\mathbb{Z}$. Now E also still has potentially good reduction at 2, and $v_2(\Delta_E) = 4$. Because also $v_2(c_4(E)) = 4 + v_2(-3y^\ell + z^2) \geqslant 6$ by our assumption $y \equiv -1 \pmod 4$, and

$$c_6(E) = 32z(9y^\ell - 2z^2), \quad \text{so that} \quad c_6(E)/2^5 = z(9y^\ell - 2z^2) \equiv z(-9-2) \equiv 1 \pmod 4,$$

where we used that we assumed a while back that $z \equiv -y \equiv 1 \pmod 4$, it again follows from Proposition 4.7 that we obtain a semistability defect of order 3.

We use the symplectic criterion Theorem 4.1 that applies to our situation. To this end, we need to invoke Proposition 4.3 that tells us whether or not E and G have a 3-torsion point defined over $\mathbb{Q}_2$. Carefully considering that theorem, we conclude that G does have such a point and E has it precisely when $c_6(E)/2^5 \equiv 5 \pmod 8$, so when $z(y-2) \equiv 5 \pmod 8$, which happens precisely when $y \equiv -z \pmod 8$. Then we see from Theorem 1 that:

- If $8 \mid y + z$, then $E[\ell]$ and $G[\ell]$ are symplectically isomorphic.
- If $8 \nmid y + z$, then $E[\ell]$ and $G[\ell]$ are symplectically isomorphic if and only if 3 is a square modulo ℓ.

On the other hand, since both E and G have multiplicative reduction at 5, it follows that $E[\ell]$ and $G[\ell]$ are symplectically isomorphic if and only if $v_5(\Delta_E) \equiv k \pmod \ell$ and $v_5(\Delta_G) = 2$ differ by a square mod ℓ. In the first case we get a contradiction if $2k$ is not a square mod ℓ and in the second case if $6k$ is not a square mod ℓ. The assumptions from the theorem yield a contradiction in each of our cases, because for $\ell \equiv \pm 1 \pmod{24}$, both 2 and 3 are squares mod ℓ.

Now all that remains to be done is to deal with the cases that $xy = \pm 1$. Suppose first that $x = -1$. Then reducing the equation mod 4 yields $-1 \equiv -5^k \equiv z^2 \pmod 4$, but this cannot happen. Therefore $x = 1$. We split cases. If $y = 1$, we have $5^k + 4 = z^2$, and so $5^k = (z+2)(z-2)$. However, $\gcd(z+2, z-2) \mid 4$ and hence it must be 1. Thus $z+2$ and $z-2$ must both be powers of 5, forcing $z = \pm 3$ and so $k = 1$. If $y = -1$, we must solve $5^k = z^2 + 4$. Working in $\mathbb{Z}[i]$, we find that $(1-2i)^k(1+2i)^k = 5^k = (z+2i)(z-2i)$. Again, since $\gcd(z+2i, z-2i) \mid 4$, it must be 1. Hence $z + 2i = i^n(1+2i)^k$ for some n, implying that either $(1+2i)^k$ has either its real or imaginary part equal to 2. These both grow exponentially, so it would not be hard to show that this forces $k = 1$ or $k = 3$. These correspond to $z = \pm 1$ or $z = \pm 11$ respectively. □

Remark 4.12. It may be interesting to briefly elaborate on the fact that we may take our prime ℓ in the above theorem as low as 7, instead of the safer lower bound of 17. In the proof of Corollary 3.1 in [2], the argument is roughly as follows. If the mod-ℓ Galois representation is reducible, then we must have a rational $\mathbb{Q}$-isogeny of degree ℓ. Now, by the very strong results from Theorem 1 in [33], this can only happen for a very specific set of primes. But because E even has a rational 2-torsion point, namely $(0,0)$, it has a Galois-invariant subgroup of order 2ℓ and hence a rational 2ℓ-isogeny. It turns out that this cannot occur for $\ell \geqslant 17$. For $7 \leqslant \ell \leqslant 13$ it could happen, but only for curves with complex multiplication. However, it is easy to see that if $xy \neq 1$, then E has multiplicative reduction at any prime that divides xy and so it cannot have complex multiplication, for then its j-invariant would have been an integer.

Theorem 4.13. *Let $k > 0$ be an integer and $\ell \equiv \pm 1 \pmod{24}$. Then the equation*

$$x^\ell + 4 \cdot 5^k y^\ell = z^2$$

has no nontrivial primitive solutions for ℓ such that k is not a square modulo ℓ.

Proof. The proof is exactly the same as the above theorem, but now we begin with a solution for which x, $10y$ and z are pairwise coprime. The case for even y is analogous with the curve

$$E : Y^2 + XY = X^3 + \frac{z-1}{4}X^2 + \frac{5^k y^\ell}{16}X.$$

For odd y we consider the curve

$$E : Y^2 = X^3 + zX^2 + 5^k y^\ell X, \quad \text{with} \quad \Delta_E = 2^4 5^{2k}(xy^2)^\ell.$$

Because $5^k \equiv 1 \pmod 4$, all arguments are analogous up to the point where we invoke Proposition 2.31, because now $v_5(\Delta_E) \equiv 2k \pmod \ell$. Therefore if $y \equiv 1 \pmod 4$, we find that the ℓ-torsion modules are symplectically isomorphic if and only if k is a square modulo ℓ, which on the other hand happens precisely if 2 is a square modulo ℓ. If $y \equiv -1 \pmod 4$, then $E[\ell]$ and $G[\ell]$ are either symplectically isomorphic or only symplectically isomorphic if 3 is a square mod ℓ. Again, since we assume 2 and 3 to be squares mod ℓ, we obtain a contradiction with our assumptions in each case.

Now we must only still analyse the cases that $xy = \pm 1$. If $x = -1$, then modulo 4 the equation reduces to $-1 \equiv z^2$, which has no solutions. Hence $x = 1$ and so $\pm 4 \cdot 5^k = z^2 - 1$. Writing $z = 2w + 1$ yields $\pm 5^k = w(w+1)$, so that w and $w+1$ must both be powers of 5. However, this clearly cannot happen. □

Remark 4.14. We remark that in both the above theorems, the case $k = 0$, yielding the equation

$$x^\ell + 4y^\ell = z^2,$$

will after level lowering end up at a level not exceeding 8, hence yielding no solutions for any $\ell \geqslant 7$. For $\ell = 5$ there actually is a solution for which $xyz \neq 0$, which is given by $2^5 + 4 \cdot 1^5 = 6^2$. For $\ell = 3$, we found 15 pairs of non-trivial solutions, two small examples of which are given by $2^3 + 4 \cdot (-1)^3 = 2^2$ and $(-2)^3 + 4 \cdot 3^3 = 10^2$. The author suspects the $\ell = 5$ case especially to be quite difficult to solve generally.

We found another, slightly more general example of a result that can be proved using the symplectic method with signature $(\ell, \ell, 2)$.

Theorem 4.15. *Let $k, \alpha > 0$ be integers and $\ell \geqslant 7$ a prime. Then the equation*

$$3^k x^\ell + 2^\alpha y^\ell = z^2$$

has no nontrivial primitive solutions if

- *$\alpha \in \{2, 5\}$ and ℓ is such that k is not a square modulo ℓ;*
- *$\alpha = 4$ and ℓ is such that $2k$ is not a square modulo ℓ;*
- *$\alpha \geqslant 6$ and $xy \neq 1$,*

with the exceptions of

$$3^1 \cdot (-1)^\ell + 2^2 \cdot 1^\ell = (\pm 1)^2, \;\; 3^2 \cdot 1^\ell + 2^4 \cdot 1^\ell = (\pm 5)^2 \;\; \textit{and} \;\; 3^4 \cdot 1^\ell + 2^5 \cdot (-1)^\ell = (\pm 7)^2.$$

Proof. As before, we consider a primitive solution such that $3x$, $2y$ and z are pairwise coprime. If y is even, we may assume that $z \equiv 1 \pmod 4$ and we consider the elliptic curve

$$E : Y^2 + XY = X^3 + \frac{z-1}{4}X^2 + 2^{\alpha-6}y^\ell X.$$

According to [40], this elliptic curve corresponds to a newform of level $\mathrm{rad}(3^k \cdot 2^\alpha) = 6$, but this does not exist. The proof for $\alpha \geqslant 6$ is completely analogous, but this will require the restriction that $xy \neq 1$. Thus we restrict our attention to odd y. We consider under suitable assumptions on $z \pmod 4$ the elliptic curve

$$E : Y^2 = X^3 + zX + 2^{\alpha-2}y^\ell X.$$

We then have that

$$\Delta_E = 2^{2\alpha}3^k(xy^2)^\ell \quad \text{and} \quad c_4(E) = 16(-3 \cdot 2^{\alpha-2}y^\ell + z^2).$$

The case $\alpha = 2$: We split cases once more. If $y \equiv -1 \pmod 4$, then [40] tells us that if $xy \neq 1$, we find that E corresponds to a newform of level $2\mathrm{rad}(3^k \cdot 2^2) = 12$, but these do not exist. If $y \equiv 1 \pmod 4$, then [40] tells us that if $xy \neq 1$, we find that E corresponds to a newform of level $2^2 \cdot \mathrm{rad}(3^k \cdot 2^2) = 24$. As we have seen before, this corresponds to the elliptic curve

$$F : Y^2 = X^3 - X^2 - 4X + 4, \quad \text{with} \quad \Delta = 2^8 \cdot 3^2.$$

We know that F has potentially good reduction at 2, multiplicative reduction at 3 and satisfies $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{un}}) \cong \mathrm{SL}_2(\mathbb{F}_3)$. Since $\alpha = 2$ we have $v_2(\Delta_E) = 4$ and $v_2(c_4(E)) = 4 + v_2(-3y^\ell + z^2) = 5$ and hence the same holds for E. We may apply Theorem 2.39 to conclude that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if 2 is a square mod ℓ. A glance at the conductor of E in [40] reveals that E has multiplicative reduction at 3 and so does F. Hence Proposition 2.31 gives us that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if k and 2 differ by a square modulo ℓ, a contradiction if k is not a square.

Now the case that $xy = \pm 1$ remains to be examined. If $x = 1$, then reducing the equation mod 8 yields a contradiction, so $x = -1$. Now the left hand side tends to be negative, so it is easily seen to only have $z = \pm 1$ and $k = 1$ as a solution.

The case $\alpha \in \{4, 5\}$: Now [40] tells us that if $xy \neq 1$, then again E corresponds with an elliptic curve of level $2^2 \cdot \mathrm{rad}(3^k \cdot 2^\alpha) = 24$, which is again F. We compute that $v_2(\Delta_E) = 8$ or 10 and $v_2(c_4(E)) = 4$. Using Proposition 2.51, observing that $3^k(xy^2)^\ell \equiv 3^k x^\ell \equiv z^2 \equiv 1 \pmod 4$, we are again in the position of Theorem 2.39. If $\alpha = 4$, then $v_2(\Delta_E) = v_2(\Delta_F)$ and so we conclude that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic. Since 3 is still a shared multiplicative prime, it follows that k and 2 differ by a square mod ℓ. If $\alpha = 5$, then the argument is the same as in the case that $\alpha = 2$.

To tackle $xy = \pm 1$, we observe that if $x = -1$, the left hand side tends to be negative, whereas the right hand side is not. One can check all finite number of exceptions to find no further solutions. We conclude that $x = 1$. Reducing modulo 4 gives us that $3^k \equiv z^2 \equiv 1 \pmod 4$ and so k must be even. Therefore 3^k is a perfect square and so ± 16 and ± 32 respectively must be the differences between two squares, $z^2 - 3^k$. Checking all finitely many possibilities, we find $z = \pm 5$ and $k = 2$ if $\alpha = 4$ and $z = \pm 7$ and $k = 4$ if $\alpha = 5$. □

Theorem 4.16. *Let $k, \alpha > 0$ be integers and $\ell \geqslant 7$ a prime. Then the equation*

$$x^\ell + 2^\alpha 3^k y^\ell = z^2$$

has no nontrivial primitive solutions if

- $\alpha \in \{2, 5\}$ *and ℓ is such that $2k$ is not a square modulo ℓ;*
- $\alpha = 4$ *and ℓ is such that k is not a square modulo ℓ;*
- $\alpha \geqslant 6$,

with the exceptions of

$$1^\ell + 2^4 \cdot 3^1 \cdot 1^\ell = (\pm 7)^2 \quad \textit{and} \quad 1^\ell + 2^5 \cdot 3^2 \cdot 1^\ell = (\pm 17)^2.$$

Proof. Unsurprisingly, the proof is very similar to that of the above theorem, but now we consider a solution for which x, $6y$ and z are pairwise coprime. The cases for even y and $y \equiv -3^k \pmod 4$ are similar and all the remaining cases for $\alpha \in \{2, 4, 5\}$ will again leave us at level 24, using

$$E : Y^2 = X^3 + zX + 2^{\alpha-2} 3^k y^\ell X.$$

The discriminant of E equals $2^{2\alpha} 3^{2k} (xy^2)^\ell$ and $c_4(E) = 16(2^{\alpha-2} \cdot 3^{k+1} y^\ell + z^2)$. For $\alpha = 2$, this gives $\nu_2(\Delta_E) = 4$ and $\nu_2(c_4(E)) = 4 + \nu_2(-3^{k+1} y^\ell + z^2) = 5$, where we need that $y \equiv 3^k \pmod 4$. So we are neatly in the situation in which Theorem 2.39 may be applied. Combined with the multiplicative reduction at 3 that the conductor gives us, we may conclude that $E[\ell]$ and $F[\ell]$ are symplectically isomorphic if and only if 2 is a square mod ℓ, but also if and only if k is a square mod ℓ. For $\alpha = 4$ we have $\nu_2(\Delta_E) = 8$ and $\nu_2(c_4(E)) = 4$ and since $\Delta/2^8 = 3^{2k}(xy^2)^\ell \equiv 1 \pmod 4$ because $x^\ell \equiv z^2 \equiv 1 \pmod 4$, we find that we are again in the situation to apply Theorem 2.39. This time combining it with Proposition 2.31 yields that k is a square mod ℓ. For $\alpha = 5$ we have that $\nu_2(\Delta_5) = 10$ and $\nu_2(c_4(E)) = 4$ and from then the argument is the same as in the case $\alpha = 2$.

To handle the cases that $xy = \pm 1$, we first remark that in all cases, $y = -1$ yields a negative left hand side whereas the right hand side is positive. Therefore $y = 1$ and looking mod 4 gives that also $x = 1$. Writing $z = 2w + 1$, we can now rewrite the equation to $2^{\alpha-2} 3^k = w(w+1)$. Because w and $w+1$ are coprime, one must be a power of 2 and the other must be a power of 3. We must thus solve the equation $|3^k - 2^{\alpha-2}| =$

1. This is merely an exercise in elementary number theory; consider $3^k - 2^{\alpha-2} = -1$ and observe that reducing modulo 3 gives that α is even. Hence $3^k = 2^{\alpha-2} - 1 = (A-1)(A+1)$ for some integer A. So $A-1$ and $A+1$ must both be powers of three; it follows that $A = 2$ and so $\alpha = 4$, $k = 1$ and $z = \pm 7$. The other case is $3^k - 2^{\alpha-2} = 1$ and observe that $\alpha = 2$ yields no solution, and we do not consider $\alpha = 3$. Now reducing the equation modulo 4 yields that k is even, and so $2^{\alpha-2} = 3^k - 1 = (B+1)(B-1)$ for some integer B. So $B-1$ and $B+1$ must both be powers of 2, and we find $B = 3$, so $k = 2$, $\alpha = 5$ and $z = \pm 17$. This completely solves the equation for $xy = \pm 1$. □

Also in the above two theorems we may examine the cases $\alpha = 0$ or $k = 0$ separately. This turns out to be surprisingly intricate.

Theorem 4.17. *Let $k, \alpha > 0$ and let $\ell \geqslant 7$ be a prime number. Then the equation*

$$3^k x^\ell + y^\ell = z^2$$

has no non-trivial primitive solutions if ℓ is such that $2k$ is not a square modulo ℓ except for

$$3^1 \cdot 1^\ell + 1^\ell = (\pm 2)^2.$$

Furthermore, the equation

$$x^\ell + 2^\alpha y^\ell = z^2$$

has no non-trivial solutions if $\alpha \notin \{1, 3\}$. For $\alpha = 3$ and $\ell \geqslant 11$ the only solution is given by

$$1^\ell + 2^3 \cdot 1^\ell = (\pm 3)^2.$$

Proof. Consider the first equation. If either x or y is even, it quickly follows from the recipe that we find no non-trivial primitive solutions for $\ell \geqslant 7$ because there are no newforms of level 6. If they are both odd however, then we may assume that $y \equiv -1 \pmod 4$ and so after considering the elliptic curve

$$E : Y^2 = X^3 + 2zX^2 + y^\ell X \quad \text{with} \quad \Delta_E = 2^6 3^k (xy^2)^\ell \quad \text{and} \quad N_E = 2^5 \cdot \mathrm{rad}(3xy).$$

the recipe leaves us at level $2^5 \cdot 3 = 96$ provided that $xy \neq 1$. We have encountered this level before, and it contains two different elliptic curves, F_1 and F_2, which are quadratic twists of each other by -1, and both satisfy $\Delta = 2^6 \cdot 3^2$ and $c_4 = 2^4 \cdot 7$. Because

$$c_4(E) = -48 \cdot y^\ell + 64z^2$$

has precisely 4 factors of two, E will have potentially good reduction at 2. Looking at Proposition 4.7, we find that both E and F have $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{un}}) \cong H_8$, again dropping the subscript of F for convenience. Now Theorem 4.4 tells us that if 2 is a square modulo ℓ, then their ℓ-torsion modules are symplectically isomorphic. Now note that both E and F have precisely 5 factors of 2 in their conductors, 6 in their discriminants, 4 in their values of c_4 and because

$$c_6(E) = 64(9y^\ell z - 16z^3)$$

has at least 7, as z must be even, and so does F. It thus follows from Theorem 4.4 that if 2 is not a square modulo ℓ, then the ℓ-torsion modules are symplectically isomorphic if and only if $c_4/16 \equiv -1 \pmod 4$ for both of the curves. For F this is the case, and for E we have $c_4/16 \equiv -3y^\ell \equiv -1 \pmod 4$, because a while back we assumed $y \equiv -1 \pmod 4$. It follows that in this case they are also symplectically isomorphic.

Now we observe that both curves also have multiplicative reduction at 3, and that $v_3(\Delta_F) = 2$ and $v_3(\Delta_E) \equiv k \pmod \ell$. It thus follows from Proposition 2.31 that $2k$ must be a square modulo ℓ.

If $xy = \pm 1$ we are to solve $\pm 3^k \pm 1 = z^2$. To ensure the left hand side is positive, the first sign must be a plus. The equation $3^k - 1 = z^2$ is solved by looking modulo 3, and $3^k = (z-1)(z+1)$ is solved by noting that $\gcd(z-1, z+1) | 2$ and so $z = \pm 2$ is the only solution.

Now for the second equation, we consider a non-trivial, primitive solution and observe that if $\alpha \notin \{1, 3\}$, the level at which we end up after applying the recipe will not exceed 8, yielding an immediate contradiction. We more closely inspect the case $\alpha = 3$, for the other case leaves us few options to proceed. In that case we use the elliptic curve

$$E : Y^2 = X^3 + zX^2 + 2y^\ell X$$

to end up at level 32, another level we have encountered before. It contains the curve $F : Y^2 = X^3 + 4X$ which has complex multiplication with the ring $\mathbb{Z}[i]$.

If $\ell \equiv 1 \pmod 4$, it follows that the image of ρ_F^ℓ is contained in the normaliser of a split Cartan subgroup, and hence by Theorem 3.9 if $\ell \geqslant 11$ it follows that E must have complex multiplication. Similarly, if $\ell \equiv -1 \pmod 4$ and $\ell \geqslant 11$, since E has a 2-torsion point, it also follows that $j(E) \in \mathbb{Z}$. The recipe gives us that $N_E = 2^4 \operatorname{rad}(2xy)$ and in order to prevent multiplicative reduction at a certain prime, it follows that x and y can only have 2 as a prime factor. But x is odd as the solution is primitive and so $x = \pm 1$. The equation reduces to

$$\pm 1 + 8 \cdot y^\ell = z^2,$$

but the case of $x = -1$ is solved by looking modulo 4 and the case of $x = 1$ is solved by observing that $\gcd(z-1, z+1) = 2$, quickly yielding $y = \pm 1$ too.

It remains to find the solutions for $xy = \pm 1$. By looking at the sign $\pm 1 - 2^\alpha = z^2$ cannot happen, and $-1 + 2^\alpha = z^2$ yields $\alpha \leqslant 1$ by looking modulo 4. We solve $2^\alpha = (z-1)(z+1)$ similar as before to find only $\alpha = 3$ and $z = \pm 3$ as a solution. □

Remark 4.18. Somewhat uncomfortably, the above techniques were not enough to solve the case of $\alpha = 3$ for $\ell = 7$, meaning that the question about non-trivial solutions to the equation

$$x^7 + 8y^7 = z^2$$

is still very much open. A quick search with Mathematica [27] yielded no non-trivial solutions apart from the ones already listed in the theorem for $|x|, |y|, |z| \leqslant 200$. Yet comparing traces of Frobenius seemed to yield no contradictions. We invite the reader to try to tackle this equation themselves, though the author suspects this may be fairly tricky to settle.

4.4 A theorem of signature $(\ell, \ell, 3)$

In this last section, we use the final recipe described in [40] to prove another novel theorem using the symplectic method. Originally this Frey curve was described in Section 2 of [3]. When we cite [40] in this section, we will always refer to Section 14.3.

Theorem 4.19. *Let $k > 0$ be a positive integer and $\ell \equiv \pm 1 \pmod{12}$ a prime number. Then the equations*

$$2^k x^\ell + 9y^\ell = z^3 \quad \textit{and} \quad x^\ell + 2^k \cdot 9y^\ell = z^3$$

have no non-trivial primitive solutions for ℓ such that k is not a square modulo ℓ, except for

$$2^3 \cdot 1^\ell + 9 \cdot (-1)^\ell = (-1)^3 \quad \textit{and} \quad 2^3 \cdot (-1)^\ell + 9 \cdot 1^\ell = 1^3$$

for the first equation. There are no exceptions for the second equation.

Proof. One final time, we consider a non-trivial and primitive solution to either of the above equations, meaning that $2x$, $3y$ and z are pairwise coprime in the first case, and that x, $6y$ and z are pairwise coprime in the second case. We consider the curves

$$E_1 : Y^2 + 3zXY + 9y^\ell Y = X^3 \quad \text{and} \quad E_2 : Y^2 + 3zXY + 2^k \cdot 9y^\ell Y = X^3$$

respectively. Then [40] tells us that if $xy \neq 1$, the level lowering theorem applies. We split two cases. If $3 \mid y$, then for both equations we arrive at a newform of level $\mathrm{rad}_3(2^k \cdot 9) \cdot 1^2 \cdot 3 = 6$, but no newforms of this level exist, yielding an immediate contradiction.

If $3 \nmid y$, then [40] gives us that we arrive at a newform of level $\mathrm{rad}_3(2^k \cdot 9) \cdot 1^2 \cdot 3^3 = 54$. There exist precisely two such newforms, and they correspond to the elliptic curves

$$F_1 : Y^2 + XY = X^3 - X^2 + 12X + 8 \quad \text{with} \quad \Delta(F_1) = -2^3 \cdot 3^9 \quad \text{and} \quad c_4(F_1) = -3^4 \cdot 7$$

and

$$F_2 : Y^2 + XY + Y = X^3 - X^2 + X - 1 \quad \text{with} \quad \Delta(F_2) = -2^3 \cdot 3^3 \quad \text{and} \quad c_4(F_2) = -3^2 \cdot 7.$$

We see that both curves have potentially good reduction at 3. To proceed, we show that E has the same property. Namely, in [3] it is computed that

$$\Delta(E_1) = 3^9 \cdot 2^k (xy^3)^\ell \quad \text{and} \quad c_4(E_1) = 3^4 z(2^k x^\ell + y^\ell)$$

and in the other case

$$\Delta(E_2) = 3^9 \cdot 2^{3k} (xy^3)^\ell \quad \text{and} \quad c_4(E_2) = 3^4 z(x^\ell + 2^k y^\ell).$$

We conclude that $v_3(\Delta(E_i)) = 9$ and $v_3(c_4(E_i)) \geqslant 4$, so that both E_1 and E_2 have potentially good reduction at 3.

In order to proceed, we must determine the order of the extension $\mathrm{Gal}(L/\mathbb{Q}_3^{\mathrm{un}})$. We turn to Proposition 4.7 and after close examination of the criteria given there, we find

with some calculations that both F_1 and F_2 must have an extension of order 12, falling precisely in the first and second category for the prime 3 respectively. Hence we may apply Theorem 4.5 to continue.

We find that $E_i[\ell]$ and $F_j[\ell]$ are symplectically isomorphic when 3 is a square mod ℓ. Now, the slightly more involved case is to check what happens when 3 is not a square mod ℓ. Looking at Theorem 4.5, we find that F_1, E_1 and E_2 are in a different case from F_2. Therefore, without information about the case which we are in, we cannot conclusively determine the symplectic type of the isomorphism if 3 is not a square mod ℓ.

Now we observe that all curves considered have multiplicative reduction at 2. For E_1 this follows from the assumption that y is odd, and for E_2 this follows from the assumption that x is odd. Now we note that $v_2(\Delta(F_i) = 3$ and $v_2(\Delta(E_1)) \equiv k \pmod{\ell}$ and $v_2(\Delta(E_3)) \equiv 3k \pmod{\ell}$, and so by Proposition 2.31 we find that $E_1[\ell]$ and $F_i[\ell]$ are symplectically isomorphic if and only if 3 and k differ by a square modulo ℓ, and $E_2[\ell]$ and $F_i[\ell]$ are symplectically isomorphic exactly when 3 and $3k$ differ by a square modulo ℓ.

Now we observe that our assumption on ℓ implies that 3 is a square modulo ℓ, yielding that the ℓ-torsion modules of E_i and F_j must be symplectically isomorphic, and hence in all cases yielding that k must be a square modulo ℓ.

Now it remains to discuss the case that $xy = \pm 1$. By flipping the sign of z, we may assume that $x = 1$ and $y = \pm 1$. To solve $2^k \pm 9 = z^3$, we reduce modulo 9 to observe that since $z^3 \in \{-1, 0, -1\} \pmod 9$, it must follow that $3 \mid k$. Hence 9 must be expressed as the difference between two cubes, which can clearly only be obtained with 8 and -1, or with -8 and 1. We find only the solution $k = 3$ and $z = -1$. To solve $1 \pm 9 \cdot 2^k = z^3$, we remark that z must be odd. Now we rewrite it as $\pm 9 \cdot 2^k = (z-1)(z^2+z+1)$ and since the second factor is odd, we must have that $z^2 + z + 1 \mid 9$. It follows that $z \in \{-2, -1, 0, 1\}$, yielding no solutions. □

Remark 4.20. It is again interesting to argue why ℓ in the above theorem was allowed to be as low as 5. In [3], the argument is roughly the same as in the $(\ell, \ell, 2)$-case. If the mod-ℓ Galois representation is reducible, then we must have a rational $\mathbb{Q}$-isogeny of degree ℓ, and combining it with the rational 3-torsion point, namely $(0, 0)$, we even find a rational 3ℓ-isogeny. It turns out that this cannot occur for $\ell \geqslant 11$. For $\ell = 5, 7$ it could happen, but only a finite list of possible elliptic curves. Looking at the coefficients we are working with, it is clear that these cases cannot occur in the theorem above.

Remark 4.21. In the proof of the above theorem we did not check whether for each E_i the degree of the extension $\mathrm{Gal}(L/\mathbb{Q}_3^{un})$ agreed with the degree we found for both F_i. According to Proposition 4.7, this would only have been the case if

$$2^k(xy^3)^\ell \equiv y^\ell z^3 \not\equiv 2, 4 \pmod 9 \quad \text{respectively} \quad 2^{3k}(xy^3)^\ell \not\equiv 2, 4 \pmod 9.$$

Hence we would also have arrived at a contradiction in the case that the above condition would not hold. This time, our assumptions on x, y and z did not guarantee this congruence to be satisfied, as was usually the case. It is merely an extremely marginal

strengthening, but an important remark nonetheless. The author has yet to find a situation in which considerations such as these can lead to more impressive contradictions and results. Although it seems to be a very rare occurrence, it seems to be a possibly promising way to deal with some very special cases nonetheless.

Remark 4.22. It may again be interesting to also consider the case that $k = 0$ in the above theorem, thus studying the equation

$$x^\ell + 9y^\ell = z^3.$$

Considering a non-trivial, primitive solution to the above equation and the elliptic curve

$$E : Y^2 + 3zXY + 9y^\ell Y = X^3,$$

provided that $xy \neq 1$ we may apply the level lowering theorem to end up at the level 3 if $3 \mid y$ and at level 27 if $3 \nmid y$. The former immediately gives us a contradiction, but at the second level there exists a unique elliptic curve,

$$F : Y^2 + Y = X^3 - 7,$$

which has complex multiplication by the ring $\mathbb{Z}[\zeta_3]$, where ζ_3 denotes a primitive cube root of unity. Now E has a rational 3-torsion point, so that from Theorem 3.9 we may conclude that E must have integral j-invariant for all $\ell \geqslant 11$. Because $N_E = 27\,\mathrm{rad}_3(xy)$ and $3 \nmid x$ because the solution is assumed to be primitive, in order to prevent multiplicative reduction it follows that $x = \pm 1$ and y must be a power of 3. It then follows that $z^3 \pm 1$ must be a power of three and so both $z \pm 1$ and $z^2 \mp z + 1$ must be powers of 3 as well. But if $3 \mid z \pm 1$, then $z^2 \mp z + 1 \equiv 3 \pmod 9$, yielding no solutions but for $z = \pm 2$. Hence the only solutions for $\ell \geqslant 11$ are given by

$$(\pm 1)^\ell + 9 \cdot (\mp 1)^\ell = (\mp 2)^3.$$

Again one may wonder what happens with the equation for $p = 7$; that is,

$$x^7 + 9y^7 = z^3.$$

Again, comparing traces of Frobenius does not seem to be enough to settle the question. A computer search with Mathematica [27] yielded no non-trivial solutions for $|x|, |y|, |z| \leqslant 500$ either, except for those already listed above. It seems likely that there are no further solutions, but a proof of that has yet to be found.

Appendix A: Calculating some conductors

In this appendix some explicit applications of Tate's algorithm can be found, which is a crucial step in any application of the modular method. The precise value of the conductor of the elliptic curve must be meticulously calculated, for most, if not all, arguments will make use of this exact value. We calculate the conductors in the order in which they appear in Chapter 2. Tate's algorithm can be found in section IV.9 in [41].

We first turn to Fermat's Last Theorem. Recall that we could assume that $\ell \geqslant 5$ and that we had a primitive solution to $x^\ell + y^\ell + z^\ell = 0$ for which $2 \mid y$ and $x^\ell \equiv -1 \pmod 4$. We considered the curve

$$E\colon Y^2 = X(X - x^\ell)(X + y^\ell).$$

Lemma 2.21. *The elliptic curve defined above has the properties that*

$$\Delta_{\min} = (xyz)^{2\ell}/2^8 \quad \textit{and} \quad N = \operatorname{rad}(xyz).$$

Proof. We apply Tate's algorithm. Given the Weierstrass equation as above, we can calculate using the usual formulas that $\Delta = 16(xyz)^{2\ell}$. Thus we must apply the algorithm by Tate for all primes dividing x, y or z. Let $q \mid x$. Since $E \pmod q\colon Y^2 = X(X + y^\ell)$, the singular point is at the origin and since the quantity $b_2 = 4(y^\ell - x^\ell)$ is not divisible by $q \neq 2$, we conclude by step 2 of the algorithm that $v_q(\Delta_{\min}) = v_q(\Delta) = 2\ell$, that $f_q = 1$ and that E has multiplicative reduction at q. The case that $q \mid y$ goes analogously, provided that $q \neq 2$. For $q \mid z$, we observe that since $x^\ell \equiv -y^\ell \pmod q$, it follows from the equation that $X = x^\ell$ is a double zero of the equation mod q, and so the singular point is $(x^\ell, 0)$ modulo q. Translating this point to the origin yields $E\colon Y^2 = X^2(X + x^\ell) \pmod q$ and thus the same result holds as for the odd primes dividing x and y.

Now we must finally handle the prime 2. Moving beyond step 2 in the algorithm, it follows quickly that we must skip all the way ahead to step 6. There it tells us to make the substitution $y' = y + x$, so that we obtain

$$E\colon Y^2 + 2XY = X^3 + (y^\ell - x^\ell - 1)X^2 - (xy)^\ell X.$$

The algorithm tells us to consider the polynomial $P(T) = T^3 + \frac{1}{2}(y^\ell - x^\ell - 1)T^2 - \frac{1}{4}(xy)^\ell \equiv T^3 \pmod 2$. The second coefficient vanishes because we assumed $x^\ell \equiv -1 \pmod 4$ and the final coefficient because $2 \mid y$ and $\ell \geqslant 5$. This polynomial has a triple root and so we move on to further steps, where we quickly reach step 11, which tells us that the equation was not minimal. We can thus make a change of variables to obtain

$$E\colon Y^2 + XY = X^3 + \frac{y^\ell - x^\ell - 1}{4}X^2 - \frac{(xy)^\ell}{16}X,$$

and we remark that this equation has integer coefficients by all our assumptions. The discriminant loses twelve factors of 2, so that $\Delta = (xyz)^{2\ell}/2^8$. Now when we arrive at step 2 for this equation, we see that $b_2 = 1 + (y^\ell - x^\ell - 1) \equiv 1 \pmod 2$, terminating the algorithm and yielding $f_2 = 1$. Thus for all primes $q \mid xyz$ we have $f_q = 1$, proving $N = \operatorname{rad}(xyz)$. □

Now we turn to the second example of the modular method. Given a primitive solution (x, y, z) to the equation $x^2 = y^\ell + 4z^\ell$, we consider the elliptic curve

$$E\colon Y^2 = X(X + 2xX + y^\ell), \text{ which satisfies } \Delta = 256(y^2z)^\ell.$$

We assume y to be odd. Since y and z do not share any factors, neither will they share any with x, which must be odd. By considering $-x$ if necessary, we may assume that $x \equiv -1 \pmod 4$.

Lemma 2.23. *The elliptic curve defined above has the properties that*

$$\Delta_{\min} = \Delta \quad \textit{and} \quad N = \begin{cases} 4\operatorname{rad}(yz) & \textit{if } z^\ell \equiv -1 \pmod 4; \\ 16\operatorname{rad}(yz) & \textit{if } z^\ell \equiv 1 \pmod 4. \end{cases}$$

Proof. Once more we apply Tate's algorithm. Let $q \mid y$, so that $Y^2 \equiv X^2(X+2x) \pmod q$ has its singular point at the origin. Then if $q \neq 2$, we see $q \nmid b_2 = 8x$, so that $f_q = 1$. Similarly, if $q \mid z$, we use $x^2 \equiv y^\ell \pmod q$ to write $Y^2 \equiv X(X+x)^2 \pmod q$, so translating the singular point to the origin we obtain $Y^2 = X^2(X-x)$. Now again $q \nmid b_2 = -4x$ and so again $f_q = 1$. Lastly we consider the prime 2. We translate X over x to obtain $Y^2 = (X-x)(X^2 - x^2 + y^\ell) = (X-x)(X^2 - 4z^\ell)$. We see that $2 \mid b_2 = -4x$ and it is easily verified that we can skip steps 3 until 6, so that we end up at step 6. Here we are instructed to make the substitution $y' = y + x + 2$, resulting in

$$Y^2 + 2XY + 4Y = X^3 - (x+1)X^2 - (4z^\ell - 4)X + (4z^\ell x - 4).$$

We then see that

$$P(T) = T^3 - \frac{x+1}{2} + (z^\ell + 1)X + \frac{z^\ell x - 1}{2} \equiv \begin{cases} T^3 \pmod 2 & \text{if } z^\ell \equiv -1 \pmod 4; \\ T^3 + 1 \pmod 2 & \text{if } z^\ell \equiv 1 \pmod 4. \end{cases}$$

In the first case, we skip to step 8, where we find that the polynomial $Y^2 + Y + \frac{z^\ell x - 1}{4}$ will have distinct roots in $\overline{F}_2$ for both possibilities of the constant term. Hence the algorithm tells us that $f_2 = \nu_2(\Delta) - 6 = 2$. Now in the other case, the polynomial $T^3 + 1$ has distinct roots in $\overline{F}_2$ and so we find that $f_2 = \nu_2(\Delta) - 4 = 4$. □

We next treat the first example of the symplectic method. There we considered a solution to $x^\ell + 3y^\ell + 5z^\ell = 0$ such that $xyz \neq 0$. We were allowed to assume that x, $3y$ and $5z$ were coprime. As before, we can also assume that $x^\ell \equiv -1 \pmod 4$. Then we consider the Frey curve

$$E\colon Y^2 = X(X - x^\ell)(X + 3y^\ell).$$

Lemma 2.36. *Let* E *be the elliptic curve as above. Then we have that*

$$\Delta_{\min}(E) = (15)^2(xyz)^{2\ell}/2^8 \quad \textit{and} \quad N_E = \mathrm{rad}(15xyz).$$

Proof. We skip most of the proof, as the reader should find it very straightforward upon comparison to Lemma 2.21. The only primes at which the situation changes are 3 and 5, thus we will restrict our attention to those. At 3, we see that $E\colon Y^2 = X^2(X - x^\ell) \pmod 3$ and $b_2 = 4(3y^\ell - x^\ell)$ is not divisible by 3. Hence the algorithm terminates at step 2 and we obtain $f_3 = 1$ and multiplicative reduction. At 5, we have $x^\ell + 3y^\ell \equiv 0 \pmod 5$ and so we have that $E\colon Y^2 = X(X - x^\ell)^2 \pmod 5$, thus making the obvious change of variables, we obtain $Y^2 = X(X + x^\ell)(X + x^\ell - 3y^\ell)$ which satisfies $b_2 = 4(2x^\ell - 3y^\ell) \equiv 12x^\ell \neq 0 \pmod 5$. Hence we also have $f_5 = 1$ and multiplicative reduction at 5. □

Finally, we consider a primitive, non-trivial solution (x, y, z) to the equation $3x^\ell + 4y^\ell + 5z^\ell = 0$. Then it follows that x and z are odd and we may assume without loss of generality that $x^\ell \equiv -1 \pmod 4$. Consider the elliptic curve

$$E\colon Y^2 = X(X - 3x^\ell)(X + 4y^\ell).$$

Lemma 2.53. *Let* E *be the elliptic curve as above. Then we have that*

$$\Delta_{\min}(E) = 2^8(15)^2(xyz)^{2\ell} \quad \textit{and} \quad N_E = 4\mathrm{rad}(30xyz) \quad \textit{if } y \textit{ is odd,}$$

and

$$\Delta_{\min}(E) = (15)^2(xyz)^{2\ell}/2^4 \quad \textit{and} \quad N_E = \mathrm{rad}(30xyz) \quad \textit{if } y \textit{ is even.}$$

Proof. The situation for the odd primes is precisely the same as in Lemma 2.36, so we restrict our attention to the prime 2. Then we have that $b_2 = 4(4y^\ell - 3x^\ell)$ is indeed even, the vanishing constant term is indeed divisible by 4, $b_8 = -(3x^\ell 4y^\ell)^2$ is indeed divisible by 8 and $b_6 = 0$ is divisible by 8. We must change coordinates to $(x, y) = (x, y + x)$ to obtain

$$Y^2 + 2XY = X^3 + (4y^\ell - 3x^\ell - 1)X^2 - (3x^\ell 4y^\ell)X.$$

Then the algorithm tells us to consider the polynomial

$$T^3 - \frac{4y^\ell - 3x^\ell - 1}{2}T^2 - (3x^\ell y^\ell)T \equiv T^3 - (3x^\ell y^\ell)T \pmod 2.$$

Now we see that we must distinguish two cases. If y is odd, then this polynomial becomes $T^3 + T = T(T + 1)^2 \pmod 2$, which has a double root and a simple root. Then after some dreary calculations in step 7, which we leave to the reader to verify, we find that $f_2 = \nu(\Delta) - 5 = 8 - 5 = 3$. If y is even, we must consider $Y^2 \pmod 2$ and since $16 \mid 3x^\ell 4y^\ell$ and 64 divides zero, we conclude that our Weierstrass equation was not minimal, resulting in

$$Y^2 + XY = X^3 + \frac{4y^\ell - 3x^\ell - 1}{4}X^2 - \frac{3x^\ell y^\ell}{4}X.$$

Now we have that $2 \nmid b_2 = 1 - 3x^\ell y^\ell$ and so it follows that $f_2 = 1$ in this case. This proves the lemma. □

Appendix B: Frobenius traces with Sage

In this appendix we will provide the reader with reference for the code used to compare traces of Frobenius to verify the necessity of the symplectic method for the various examples that we found in Chapter 4. All these computations were done using SageMath and all output lines have been repressed. The theorems are checked in the code below in the order of appearance in the thesis.

Especially when the equation we are trying to solve has coefficients depending on a parameter and in addition an exponent ℓ about which we know very little, locally at a prime p the Frey curve that arises from an equation with signature (ℓ, ℓ, ℓ) can approximately be any curve of the form $E : y^2 = x(x-a)(x-b)$. Curves of this form can usually not attain every value of $a_p(E)$ so assuming good reduction at p, we can compare all these possible values to the value of $a_p(F)$ for the curve of low conductor F that arises from the level lowering theorem. This was done for the equations of signature (ℓ, ℓ, ℓ) that appeared in Chapter 4 and the code can be found below.

```
sage: def ECCards(p):
...       List = []
...       for a in range(1,p+1):
...           for b in range(p,2*p+1):
...               if a != b:
...                   x,y = var('x,y')
...                   E = EllipticCurve(y^2 == x*(x+a)*(x+b))
...                   if E.discriminant() % p != 0:
...                       List.append(E.Np(p))
...       return set(List)
sage: def FrobTrace1(p):
...       F1 = EllipticCurve([0,1,0,-2,0])
...       if F1.Np(p) in ECCards(p):
...           print("No information for %s." %p)
...       else:
...           print("Conductor must be divisible by %s." %p)
sage: def FrobTrace15(p):
...       F2 = EllipticCurve([0,-1,0,-2,0])
...       if F2.Np(p) in ECCards(p):
...           print("No information for %s." %p)
...       else:
...           print("Conductor must be divisible by %s." %p)
sage: def ThmFail1(n):
...       for i in range(n):
...           p = Primes().unrank(i)
...           if p > 3:
...               FrobTrace1(p)
```

```
sage: def ThmFail15(n):
...       for i in range(n):
...           p = Primes().unrank(i)
...           if p > 3:
...               FrobTrace15(p)
sage: ThmFail1(25)
sage: ThmFail15(25)
sage: def FrobTrace2(p):
...       F = EllipticCurve([0,-1,0,-4,4])
...       X = ECCards(p)
...       if F.Np(p) in ECCards(p):
...           print("No information for %s." %p)
...       else:
...           print("Conductor must be divisible by %s." %p)
sage: def ThmFail2(n):
...       for i in range(n):
...           p = Primes().unrank(i)
...           if p > 3:
...               FrobTrace2(p)
sage: ThmFail2(25)
```

Here we change the function that finds all possible values of $a_p(E)$ to work for the Frey curves E attached to an equation of signature $(\ell, \ell, 2)$.

```
sage: def ECCards2(p):
...       List = []
...       for a in range(1,p+1):
...           for b in range(p^2+1,p*(p+1)+1):
...                   x,y = var('x,y')
...                   E = EllipticCurve(y^2 == x*(x^2+a*x+b))
...                   if E.discriminant() % p != 0:
...                       List.append(E.Np(p))
...       return set(List)
sage: def FrobTrace3(p):
...       F = EllipticCurve([0,0,0,-7,-6])
...       X = ECCards2(p)
...       if F.Np(p) in ECCards2(p):
...           print("No information for %s." %p)
...       else:
...           print("Conductor must be divisible by %s." %p)
sage: def ThmFail3(n):
...       for i in range(n):
...           p = Primes().unrank(i)
...           if p != 2 and p!= 5:
...               FrobTrace3(p)
sage: ThmFail3(25)
sage: def FrobTrace4(p):
...       F = EllipticCurve([0,1,0,4,4])
...       X = ECCards2(p)
```

```
...       if F.Np(p) in ECCards2(p):
...           print("No information for %s." %p)
...       else:
...           print("Conductor must be divisible by %s." %p)
sage: def ThmFail4(n):
...       for i in range(n):
...           p = Primes().unrank(i)
...           if p != 2 and p!= 5:
...               FrobTrace4(p)
sage: ThmFail4(25).
sage: def FrobTrace5(p):
...       F = EllipticCurve([0,-1,0,-4,4])
...       X = ECCards2(p)
...       if F.Np(p) in ECCards2(p):
...           print("No information for %s." %p)
...       else:
...           print("Conductor must be divisible by %s." %p)
sage: def ThmFail5(n):
...       for i in range(n):
...           p = Primes().unrank(i)
...           if p > 3:
...               FrobTrace5(p)
sage: ThmFail5(25)
```

Here we change the function that finds all possible values of $a_p(E)$ to work for the Frey curves E attached to an equation of signature $(\ell, \ell, 3)$.

```
sage: def ECCards3(p):
...       List = []
...       for a in range(1,p+1):
...           for b in range(p^2+1,p*(p+1)+1):
...               x,y = var('x,y')
...               E = EllipticCurve(y^2 + a*x*y+b*y == x^3)
...               if E.discriminant() % p != 0:
...                   List.append(E.Np(p))
...       return set(List)
sage: def FrobTrace6(p):
...       F1 = EllipticCurve([1,-1,0,12,8])
...       if F1.Np(p) in ECCards3(p):
...           print("No information for %s." %p)
...       else:
...           print("Conductor must be divisible by %s." %p)
sage: def FrobTrace65(p):
...       F2 = EllipticCurve([1,-1,1,1,-1])
...       if F2.Np(p) in ECCards3(p):
...           print("No information for %s." %p)
...       else:
...           print("Conductor must be divisible by %s." %p)
sage: def ThmFail6(n):
```

```
...       for i in range(n):
...           p = Primes().unrank(i)
...           if p > 3:
...               FrobTrace6(p)
sage: def ThmFail65(n):
...       for i in range(n):
...           p = Primes().unrank(i)
...           if p > 3:
...               FrobTrace65(p)
sage: ThmFail6(25)
sage: ThmFail65(25)
```

Here we specialise the functions that we wrote above to give us more detailed information when the exponent ℓ in the considered equations was equal to 5 or 7.

```
sage: def FiveECCards(p):
...       List = []
...       for a in range(1,p+1):
...           for b in range(p,2*p+1):
...               if a != b:
...                   x,y = var('x,y')
...                   E = EllipticCurve(y^2 == x*(x+a^5)*(x-b^5))
...                   if E.discriminant() % p != 0:
...                       List.append(E.Np(p))
...       return set(List)
sage: FiveECCards(11)
sage: def SevenECCards(p):
...       List = []
...       for a in range(1,p+1):
...           for b in range(p,2*p+1):
...               if a != b:
...                   x,y = var('x,y')
...                   E = EllipticCurve(y^2 == x*(x+a^7)*(x-b^7))
...                   if E.discriminant() % p != 0:
...                       List.append(E.Np(p))
...       return set(List)
sage: def SevenECCards2(p):
...      List = []
...      M = set([n^7 % p for n in range(1, p+1)])
...      for a in range(1,p+1):
...          for b in range(p,2*p+1):
...              if a != b:
...                  x,y = var('x,y')
...                  E = EllipticCurve(y^2 == x^3 + a*x^2 + 2*b^7*x)
...                  if E.discriminant() % p != 0:
...                      if (a^2 - 8*b^7) % p in M:
...                          List.append(E.Np(p))
...      return set(List)
sage: def SevenECCards3(p):
```

```
...       List = []
...       M = set([n^7 % p for n in range(1, p+1)])
...       for a in range(1,p+1):
...           for b in range(p,2*p+1):
...               if a != b:
...                   x,y = var('x,y')
...                   E = EllipticCurve(y^2 + 3*a*x*y + 9*b^7*y == x^3)
...                   if E.discriminant() % p != 0:
...                       if (a^3 - 9*b^7) % p in M:
...                           List.append(E.Np(p))
...       return set(List)
```

Here we specialise to the equation studied in Example 3.21. We tried to find primes that could help us show irreducibility of the mod 3 representation, and to find primes that could help us deal with the one remaining elliptic curve at level 56 by calculating the possible traces of Frobenius of our Frey curve for many primes as precisely as possible.

```
sage: def NineECCards(p):
...       List = []
...       for a in range(1,p+1):
...           for b in range(p,2*p+1):
...               if a != b:
...                   x,y = var('x,y')
...                   E = EllipticCurve(y^2 == x*(x+a^9)*(x-b^9))
...                   if E.discriminant() % p != 0:
...                       List.append(E.Np(p))
...       return set(List)
sage: def NineECCards2(p):
...       M = set([7^5*n^9 % p for n in range(1, p+1)])
...       F = EllipticCurve([0,0,0,1,2])
...       rip = 0
...       for a in range(1,p+1):
...           for b in range(p+1,2*p+1):
...               if rip == 0:
...                   x,y = var('x,y')
...                   E = EllipticCurve(y^2 == x*(x-a^9)*(x+8*b^9))
...                   if E.discriminant() % p != 0:
...                       if (a^9 + 8*b^9) % p in M:
...                           if E.Np(p) == F.Np(p):
...                               rip = 1
...       return rip
sage: def ThmFail9exp(n,m):
...       for i in range(n,m):
...           p = Primes().unrank(i)
...           if p % 9 == 1:
...               if NineECCards2(p) == 1:
...                   print("No information for %s." %p)
...               else:
...                   print("Stonks for %s." %p)
```

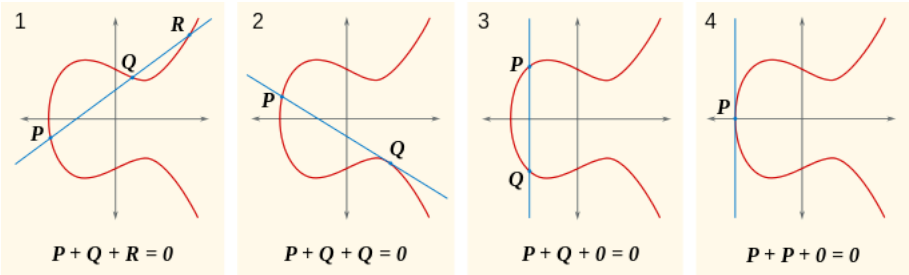
```
sage: def ThmFail9expsmall(n):
...       for i in range(n):
...           p = Primes().unrank(i)
...           if NineECCards2(p) == 1:
...               print("No information for %s." %p)
...           else:
...               print("Stonks for %s." %p)
sage: ThmFail9expsmall(20)
sage: ThmFail9exp(1,100)
sage: def NineECCards3(p):
...       M = set([7^5*n^9 % p for n in range(1, p+1)])
...       L = []
...       for a in range(1,p+1):
...           for b in range(p+1,2*p+1):
...               x,y = var('x,y')
...               E = EllipticCurve(y^2 == x*(x-a^9)*(x+8*b^9))
...               if E.discriminant() % p != 0:
...                   if (a^9 + 8*b^9) % p in M:
...                       L.append(E.Np(p))
...       return set(L)
```

Lastly, we wrote a short program that checks the equation in Example 3.21 for local obstructions. As explained, we need only check until 3136 to have certainty that local obstructions cannot exist.

```
sage: def FindPoint(p):
...       point = 0
...       for x in range(p):
...           if point == 0:
...               for y in range(p):
...                   for z in range(p):
...                       if (x^9 + 8*y^9 + 7^5*z^9) % p == 0:
...                           if x + y + z != 0:
...                               point = 1
...       return point
sage: def LocalOb(n):
...       for p in range(n):
...           if p in Primes():
...               if FindPoint(p) == 0:
...                   print("flip %s." %p)
...               else:
...                   if p % 10 == 1:
...                       print(p)
sage: LocalOb(3136)
```

Populaire samenvatting

De "Laatste Stelling van Fermat" is de bewering dat de vergelijking $a^n + b^n = c^n$ voor $n > 2$ geen niet-triviale gehele oplossingen heeft. Dit bleef een onbewezen vermoeden voor meer dan drie eeuwen tot in 1994 voor het eerst een sluitend bewijs werd geleverd. Men bewees toen een deel van de *modulariteitsstelling*. Het bewijs van de laatste stelling van Fermat maakt gebruik van een *elliptische kromme*: de verzameling van punten (x, y) in het vlak die voldoen aan $y^2 = x^3 + ax + b$ voor zekere getallen a en b, plus een zogeheten *punt op oneindig*. De oplossingen van dit soort vergelijkingen dragen de structuur van een abelse groep met zich mee. Deze optellingsstructuur wordt de *koorde-raaklijn*-optelling genoemd en is hieronder weergegeven. Het eenheidselement is het punt op oneindig; dit bevindt zich oneindig hoog boven de x-as.



Figuur: Optelling in een ellipische kromme

Om de laatste stelling van Fermat te bewijzen, nemen we een mogelijke oplossing van de vergelijking $a^\ell + b^\ell = c^\ell$ met $\ell \geqslant 5$ een priemgetal en $abc \neq 0$. Dan definiëren we een slimme elliptische kromme met vergelijking $y^2 = x(x - a^\ell)(x + b^\ell)$. Daarna wordt het verhaal ietwat technisch: gebruikmakend van de modulariteitsstelling kan men aan deze elliptische kromme een zogeheten *modulaire vorm* toekennen. Dit zijn speciale complexe functies en hebben een *niveau*. In dit geval zou er een modulaire vorm van het lage niveau 2 moeten zijn, maar dit blijkt niet te kunnen; een tegenspraak.

Dit project behandelt een techniek om nog steeds tot een tegenspraak te komen, zelfs wanneer de bovenstaande methode niet voldoende is. Als we alle oplossingen $(x, y) \in \mathbb{C}^2$ toestaan voor de punten van een elliptische kromme E, dan kunnen we bewijzen dat $E[\ell] := \{Q \in E \mid \ell \cdot Q = 0\}$ voor elk priemgetal ℓ isomorf is aan $(\mathbb{Z}/\ell\mathbb{Z})^2$. De hierboven toegelichte strategie geeft ons een tweede elliptische kromme F waarvoor er een bepaald isomorfisme tussen $E[\ell]$ en $F[\ell]$ bestaat. De zogeheten *symplectische methode* bepaalt of de determinant van deze afbeelding $(\mathbb{Z}/\ell\mathbb{Z})^2 \to (\mathbb{Z}/\ell\mathbb{Z})^2$ een kwadraatrest is modulo ℓ of niet. Als men deze vraag langs verschillende wegen beantwoordt, dan kunnen de resultaten elkaar soms tegenspreken. Zo kunnen we aantonen dat bijvoorbeeld de vergelijking $3^n a^\ell + 2^m b^\ell = c^2$ voor bijna alle keuzes van n en m voor minstens de "helft" van de priemgetallen geen niet-triviale oplossingen kan hebben.

Bibliography

[1] Jennifer S Balakrishnan, Netan Dogra, J Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty—Kim for the split Cartan modular curve of level 13. *Annals of Mathematics*, 189(3):885–944, 2019.

[2] Michael A Bennett and Chris M Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canadian Journal of Mathematics*, 56(1):23–54, 2004.

[3] Michael A Bennett, Vinayak Vatsal, and Soroosh Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$. *Compositio Mathematica*, 140(6):1399–1416, 2004.

[4] Laurent Berger, Gebhard Böckle, Lassina Dembélé, Mladen Dimitrov, Tim Dokchitser, and John Voight. *Elliptic curves, Hilbert modular forms and Galois deformations*. Springer Science & Business Media, 2013.

[5] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Annales de l'Institut Fourier*, 63(3):957–984, 2013.

[6] Don Blasius. Elliptic curves, Hilbert modular forms, and the Hodge conjecture. *Contributions to automorphic forms, geometry, and number theory*, pages 83–103, 2004.

[7] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[8] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, 2001.

[9] Jan Hendrik Bruinier. Hilbert modular forms and their applications. In *The 1-2-3 of modular forms*, pages 105–179. Springer, 2008.

[10] Imin Chen and Samir Siksek. Perfect powers expressible as sums of two cubes. *Journal of Algebra*, 322(3):638–656, 2009.

[11] Henri Cohen. *Number theory: Volume II: Analytic and modern tools*, volume 240. Springer Science & Business Media, 2008.

[12] Sander R Dahmen. *Classical and modular methods applied to Diophantine equations*. Utrecht University, 2008.

[13] Sander R Dahmen and Soroosh Yazdani. Level lowering modulo prime powers and twisted Fermat equations. *Canadian Journal of Mathematics*, 64(2):282–300, 2012.

[14] Henri Darmon and Loic Merel. Winding quotients and some variants of Fermat's last theorem. *Journal für die reine und angewandte Mathematik*, 490:81–100, 1997.

[15] Peter Dénes et al. Über die Diophantische Gleichung $x^\ell + y^\ell = cz^\ell$. *Acta Mathematica*, 88:241–251, 1952.

[16] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[17] Luis Dieulefait and Xavier Taixés i Ventosa. Congruences between modular forms and lowering the level mod ℓ^n. *Journal de théorie des nombres de Bordeaux*, 21(1):109–118, 2009.

[18] Nuno Freitas. On the Fermat-type equation $x^3 + y^3 = z^p$. *Commentarii Mathematici Helvetici*, 91:295–304, 01 2016.

[19] Nuno Freitas and Alain Kraus. An application of the symplectic argument to some Fermat-type equations. *Comptes Rendus Mathematique*, 354(8):751–755, 2016.

[20] Nuno Freitas and Alain Kraus. On the symplectic type of isomorphims of the p-torsion of elliptic curves. *arXiv preprint arXiv:1607.01218*, 2016.

[21] Nuno Freitas, Bao V Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular. *Inventiones mathematicae*, 201(1):159–206, 2015.

[22] Nuno Freitas, Bartosz Naskrecki, and Michael Stoll. The generalized Fermat equation with exponents 2, 3, n. *Compositio Mathematica*, 156(1):77–113, 2020.

[23] 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.

[24] Nuno Freitas and Samir Siksek. Criteria for irreducibility of mod p representations of Frey curves. *Journal de théorie des nombres de Bordeaux*, 27(1):67–76, 2015.

[25] Emmanuel Halberstadt and Alain Kraus. Courbes de Fermat: résultats et problemes. *Journal fur die Reine und Angewandte Mathematik*, pages 167–234, 2002.

[26] Haruzo Hida. On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves. *American Journal of Mathematics*, 103(4):727–776, 1981.

[27] Wolfram Research, Inc. Mathematica, Version 12.1. Champaign, IL, 2020.

[28] Alain Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta mathematica*, 69(1):353–385, 1990.

[29] Alain Kraus. Majorations effectives pour l'équation de Fermat généralisée. *Canadian Journal of Mathematics*, 49(6):1139–1161, 1997.

[30] Alain Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experimental Mathematics*, 7(1):1–13, 1998.

[31] Alain Kraus and Joseph Oesterlé. Sur une question de B. Mazur. *Mathematische Annalen*, 293(1):259–275, 1992.

[32] Pedro Lemos. Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies. *Transactions of the American Mathematical Society*, 371(1):137–146, 2019.

[33] Barry Mazur and D Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978.

[34] Kenneth A Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Inventiones mathematicae*, 100(1):431–476, 1990.

[35] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math*, 15:259–331, 1972.

[36] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Mathematical Journal*, 54(1):179–230, 1987.

[37] Jean-Pierre Serre. *A course in arithmetic*, volume 7. Springer Science & Business Media, 2012.

[38] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Annals of Mathematics*, pages 492–517, 1968.

[39] Samir Siksek. On the Diophantine equation $x^2 = y^p + 2^k z^p$. *Journal de théorie des nombres de Bordeaux*, 15(3):839–846, 2003.

[40] Samir Siksek. The modular approach to Diophantine equations. *Panoramas et synthéses*, 36, 2012.

[41] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[42] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[43] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.4)*, 2020. https://www.sagemath.org.

[44] David Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07660*, 2015.