Classical and modular methods applied to Diophantine equations

2000 Mathematics Subject Classification:
Primary 11D41; Secondary 11F11, 11F80, 11G05.

ISBN: 978-90-393-4867-3

Classical and modular methods applied to Diophantine equations

Klassieke en modulaire methoden toegepast op Diophantische vergelijkingen

(met een samenvatting in het Nederlands)

Proefschrift

ter verkrijging van de graad van doctor aan de Universiteit Utrecht op gezag van de rector magnificus, prof. dr. J.C. Stoof, ingevolge het besluit van het college voor promoties in het openbaar te verdedigen op dinsdag 26 augustus 2008 des middags te 12.45 uur

door

Sander Roland Dahmen

geboren op 12 januari 1979 te Amersfoort

Promotor: Prof. dr. F. Beukers

Contents

Introduction

The main theme of this thesis is explicitly solving Diophantine equations. We are especially interested in the generalized Fermat equation and (other) Diophantine equations that can be approached via the modular method.

The modular method

The proof of Fermat's last theorem is based on deep results about Galois representations associated to elliptic curves and modular forms. The method of using such results to tackle Diophantine problems, called the *modular method*, goes back, at least, to [Fre]. Many other (famous) Diophantine problems have been solved, using, amongst other things, the modular method. Certain families of generalized Fermat equations form one example, amongst the earliest contributions are [DM] and [Kra4]. The modular method can often benefit from information obtained by other, classical, methods from number theory, and vice versa. For example, in [BMS1], the modular method is combined with methods from the theory of linear forms in logarithms to show that, amongst other things, the only perfect powers in the Fibonacci sequence are $0, 1, 8$ and 144. See also [BMS2], where a combination of modular and classical methods is used to solve the equation

$$x^2 + D = y^n \quad x, y \in \mathbb{Z} \quad n \in \mathbb{Z}_{\geq 3}$$

for every $D \in \mathbb{Z}$ with $1 \leq D \leq 100$.

Broadly speaking, the *modular method* is as follows. Consider an exponential Diophantine equation with one unknown odd prime exponent l. Associate to a (hypothetical) solution a certain elliptic curve E, or Frey curve, with discriminant an explicitly known constant times an l-th power. Show (using e.g. [Maz2]) that the mod l Galois representation ρ_l^E associated to the l-torsion points of E is irreducible. By modularity ([BCDT]) and level lowering ([Rib1], [Rib2]), we obtain that ρ_l^E is modular of some explicitly known level (weight 2 and trivial character). Finally, the modular forms of this level are used, possibly in a non trivial way, to obtain information about the original Diophantine equation. However, for any particular Diophantine equation a Frey curve need not be available, but even if one makes it to the last step, the information obtained (if any) might not be enough to solve the original problem in general.

The generalized Fermat equation

Let $a, b, c \in \mathbb{Z} - \{0\}$ and $p, q, r \in \mathbb{Z}_{\geq 2}$, then the generalized Fermat equation is given by

$$ax^p + by^q = cz^r \quad x, y, z \in \mathbb{Z}.$$

The exponent triple (p, q, r) is called the *signature* of the equation. A solution to this equation is called *nontrivial* if $xyz \neq 0$ and it is called *proper* if $\gcd(x, y, z) = 1$. If all the exponents are equal, then there exist nontrivial solutions if and only if there exist nontrivial proper solutions, if the exponents are not all equal then this need not be the case. For example if the exponents are pairwise coprime, then by using the Chinese remainder theorem, one easily constructs infinite families of nontrivial non proper solutions. Therefore, most of the time we are interested in nontrivial proper solutions.

As will be explained in chapter 1, it is natural to distinguish between three classes of generalized Fermat equations. The class depends on whether the signature (p, q, r) satisfies $1/p+1/q+1/r > 1$, $1/p+1/q+1/r = 1$ or $1/p+1/q+1/r < 1$.

- If $1/p+1/q+1/r > 1$, then according to [Beu1] there are either 0 or infinitely many nontrivial proper solutions, and if there are solutions they are given by a finite set of parameterizations (just like $(r^2-s^2, 2rs, r^2+s^2)$ parameterizes solutions for the generalized Fermat equation with coefficients $a = b = c = 1$ and signature $(2, 2, 2)$, i.e. Pythagorean triples). The possibilities for the signatures are, up to permutation, given by (with $n \in \mathbb{Z}_{\geq 2}$)

$$(2, 2, n),\ (2, 3, 3),\ (2, 3, 4),\ (2, 3, 5).$$

- If $1/p + 1/q + 1/r = 1$, then finding the nontrivial proper solutions comes down to finding rational points on elliptic curves. For example, a solution to $ay^2 = bx^3 + cz^6$ with $z \neq 0$ gives rise to a rational point on the elliptic curve $aY^2 = bX^3 + c$. The possibilities for the signatures are, up to permutation, given by

$$(2, 3, 6),\ (2, 4, 4),\ (3, 3, 3).$$

- If $1/p + 1/q + 1/r < 1$, then according to [DG] there are only finitely many nontrivial proper solutions.

The case that the coefficients satisfy $a = b = c = 1$ is of special interest.

- If $1/p + 1/q + 1/r > 1$, then there are always infinitely many nontrivial proper solutions. As said before, they are given by finitely many polynomial parameterizations. If $(p, q, r) = (2, 2, n)$ (up to permutation), then they can be found using elementary number theory. The cases (up to permutation)

$$(p, q, r) = (2, 3, 3), (2, 3, 4), (2, 3, 5)$$

  are due to Mordell, Zagier, Edwards respectively.

- If $1/p+1/q+1/r = 1$, then the elliptic curves in question all have rank zero and the only nontrivial proper solution, up to sign and permutation, is given by $1^6 + 2^3 = 3^2$.

- If $1/p + 1/q + 1/r < 1$, then all known nontrivial solutions (up to sign and permutation again) are given by $1^n + 2^3 = 3^2 (n \in \mathbb{Z}_{>6})$ and

$$17^3 + 2^7 = 71^2, \quad 76271^3 + 17^7 = 21063928^2,$$
$$2213459^2 + 1414^3 = 65^7, \quad 15312283^2 + 9262^3 = 113^7;$$
$$1549034^2 + 33^8 = 15613^3, \quad 96222^3 + 43^8 = 30042907^2;$$
$$13^2 + 7^3 = 2^9;$$
$$7^2 + 2^5 = 3^4, \quad 11^4 + 3^5 = 122^2.$$

Note that all known nontrivial proper solutions have p, q or r equal to 2. This has led to a conjectural generalization of Fermat's last theorem.

Conjecture (Beal Prize Conjecture). *Let $p, q, r \in \mathbb{Z}_{\geq 3}$, then the equation*

$$x^p + y^q = z^r \quad x, y, z \in \mathbb{Z} \quad \gcd(x, y, z) = 1 \quad xyz \neq 0 \tag{1}$$

has no solutions.

Apart from computer searches and heuristics, evidence for this conjecture is given by the solution of (1) in a number of cases. The signatures (p, q, r) with $1/p + 1/q + 1/r < 1$ for which (1) has been solved before (mainly by the modular method or Chabauty method) are given in [PSS, Table 1] together with the signatures $(p, q, r) = (2, 2l, 5)$ for primes $l > 17$ with $l \equiv 1 \pmod 4$ due to Imin Chen, and signatures $(p, r, q) = (4, 2n, 3), (2, 4n, 3)$ with $n \geq 2$ due to Mike Bennett and Imin Chen. A couple of new isolated cases solved in this thesis are described in a moment.

Returning to the case of general coefficients, we especially want to mention that for signatures $(p, p, 2), (p, p, 3)$ and (p, p, p) the generalized Fermat equation has been solved for many families of coefficients (and infinitely many primes p), see [BS], [BVY] and [Kra3] respectively.

Thesis outline and results

In chapter 1 we describe how the generalized Fermat equation can be analyzed by coverings of the projective line unramified outside three points. The main results are due to [DG]. We give some examples of so-called geometrically-Galois coverings that can be defined over $\mathbb{Q}$ and describe a partial approach to the generalized Fermat equation $x^3 + y^5 = 15^6 z^7$. This chapter, however, is mainly motivational and with one small exception, the results are not used in the later chapters.

Chapter 2 is an introduction into the modular method for Diophantine equations. The content of this chapter is well known in the literature.

In chapter 3 we produce some new results relevant for the modular method and apply these results (amongst other things) to explicitly solve certain Diophantine equations. We start by constructing some Frey curves, in particular we show how to attach a Frey curve to an equation of the form

$$F(x, y) = z^l \quad x, y, z \in \mathbb{Z} \quad \gcd(x, y) = 1 \quad z \neq 0,$$

where $F(x,y) \in \mathbb{Z}[x,y]$ is a nondegenerate binary cubic form and l denotes an odd prime. Next, we study irreducibility results for the Galois representations associated to the p-torsion points for small primes p (i.e. $p = 5, 7, 13$) of the Frey curves above and another family of Frey curves related to binary quartic forms. We prove irreducibility in some cases and show in some other cases that irreducibility could be proved by finding rational points on genus 2 curves. Finally, we solve certain Diophantine equations. In [Che] it is proven, using the modular method, that the generalized Fermat equation

$$x^2 + y^{2l} = z^3 \quad x, y, z \in \mathbb{Z} \quad \gcd(x,y,z) = 1 \quad xyz \neq 0, \tag{2}$$

has no solutions for primes l with $7 < l < 10^7$, $l \neq 31$. By applying our irreducibility results we show that (2) has no solutions for $l = 5$. By combining the modular method with classical arguments from algebraic number theory we are able to show that (2) also has no solutions for $l = 31$. In [Kra4] the modular method is used to show that the generalized Fermat equation

$$x^3 + y^3 = z^l \quad x, y, z \in \mathbb{Z} \quad \gcd(x,y,z) = 1 \quad xyz \neq 0, \tag{3}$$

has no solutions for primes l with $13 < l < 10000$. The method in *loc. cit.* can easily be extended to show that for $l = 7, 11, 13$ (3) has no solutions. Using our irreducibility results, we show that the modular method can also be used to prove that (3) has no solutions for $l = 5$ (in [Bru] it was already shown, using Chabauty methods, that the equation has no solutions for $l = 4, 5$). We also use our Frey curves and irreducibility results to study equations of the form

$$f(x) = y^l \quad x, y \in \mathbb{Z} \quad y \neq 0,$$

where $f(x) \in \mathbb{Z}[x]$, e.g. $f(x) = x^3 - x - 2$ or $f(x) = x^4 + x^3 - 3x^2 + 11x + 2$.

In chapter 4 we return to purely classical methods in order to find an algorithm to solve the spherical generalized Fermat equation

$$ax^2 + by^3 = cz^5 \quad x, y, z \in \mathbb{Z} \quad \gcd(x,y,z) = 1 \quad xyz \neq 0, \tag{4}$$

for given $a, b, c \in \mathbb{Z} - \{0\}$. In [Edw] already an elegant algorithm (based on classical invariant theory) that solves (4) is obtained, however for increasing $|a|, |b|, |c|$ it becomes quickly infeasible in practice. Our algorithm is quite different and also allows help from the modular method. We implemented it in Magma. As input, however, it needs a certain (finite) list of étale algebras of degree 5 over $\mathbb{Q}$, unramified outside the primes dividing $2 \cdot 3 \cdot 5abc$. This list could in principle be found in finite time, but in practice can take very long. If no prime bigger than 5 divides abc, then luckily such a list is readily available. This enabled us to prove that (4) has no solutions for certain pairwise coprime $a, b, c \in \mathbb{Z} - \{0\}$, thereby solving an open problem due to [DG].

In chapter 5 we use the modular method to study (4). We show that in certain cases the list of étale algebras, needed as input in our algorithm to solve (4), can be obtained from (available) data about elliptic curves and modular forms. In particular, we show how to obtain this list of étale algebras using the modular method in case $a = b = c = 1$. In some sense this completes the work in [Tib], where (4) with $a = b = c = 1$ was already studied using the modular method and some partial results were obtained.

Notation

Most notation is quite standard and will not be repeated here. We want to mention the following.

For $n \in \mathbb{Z} - \{0\}$ we denote by $\mathrm{rad}(n)$ the product of the primes dividing n, if S is some set of primes (of $\mathbb{Z}$), then $\mathrm{rad}_S(n)$ denotes the products of the primes dividing n that are not in S.

For a field K, an element $[u : v] \in \mathbb{P}^1_K$ with $v \neq 0$ will be identified with $u/v \in K$, the element $[1 : 0] \in \mathbb{P}^1_K$ will be denoted by ∞.

A univariate polynomial (over some domain) is called *separable* if its discriminant is nonzero.

For an elliptic curve $E/\mathbb{Q}$, the conductor will be denoted by $N(E)$, the minimal discriminant by $\Delta_{\min}(E)$ and the j-invariant by $j(E)$ or j_E, if E is given by a specific Weierstrass equation, then (by slightly abusing notation), the discriminant of this Weierstrass equation is denoted by $\Delta(E)$. If no confusion should arise, we sometimes simply just use $N, \Delta_{\min}, j$ and Δ. For a prime p, the reduction of E modulo p is denoted by $\tilde{E}(\mathbb{F}_p)$ and we define $a_p(E) := p + 1 - \#\tilde{E}(\mathbb{F}_p)$ (as a consequence $a_p(E) = -1, 1, 0$ if the reduction of E at p is non-split multiplicative, split multiplicative, additive respectively).

By a newform of level N we will mean a newform of weight 2 w.r.t $\Gamma_0(N)$ (so the character is trivial), unless specifically stated otherwise. For a newform f (of some level N) and $n \in \mathbb{Z}_{>0}$, we denote by $a_n(f)$ the n-th Fourier coefficient of the expansion of f at the cusp $i\infty$, K_f denotes the number field $\mathbb{Q}(\{a_n(f)\}_{n=1}^{\infty})$ and $\mathcal{O}_f$ denotes the ring of integers of K_f.

Finally, $G_{\mathbb{Q}}$ will denote the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Chapter 1

Coverings and the generalized Fermat equation

In the study of the generalized Fermat equation coverings of the projective line unramified outside 3 points play an important role. Arithmetic properties of these coverings and their relations to the generalized Fermat equation will be the main theme of this chapter.

1.1 Coverings and the generalized Fermat equation

Recall the generalized Fermat equation

$$ax^p + by^q = cz^r \quad x, y, z \in \mathbb{Z} \quad \gcd(x, y, z) = 1 \quad xyz \neq 0, \tag{1.1}$$

for given $a, b, c \in \mathbb{Z} - \{0\}$ and $p, q, r \in \mathbb{Z}_{\geq 2}$. It is called *spherical* if $1/p+1/q+1/r > 1$, *euclidean* if $1/p+1/q+1/r = 1$, and *hyperbolic* if $1/p+1/q+1/r < 1$. The reason for distinguishing between these cases (and the terminology) will become clear in a moment. The method of analyzing (1.1) described in this section comes from [DG]. Nice surveys can be found in [Beu2] and [Kra5], so we will limit ourselves to the essential points.

Let K be a number field and let C be a complete nonsingular and geometrically irreducible curve over K. Let $\phi : C \to \mathbb{P}^1$ be a covering (i.e. nonconstant morphism) defined over K. This corresponds to a field extension $K(C)/K(\phi)$. The covering is called *Galois* if $K(C)/K(\phi)$ is a Galois extension, we call it *geometrically-Galois* if $\overline{K}(C)/\overline{K}(\phi)$ is a Galois extension.

Suppose from now on that the covering ϕ is geometrically-Galois. The group of covering transformations of the covering associated to $\overline{K}(C)/\overline{K}(\phi)$ is isomorphic to $\mathrm{Gal}(\overline{K}(C)/\overline{K}(\phi))$, these covering transformations are already defined over some finite extension L of K, so that $L(C)/L(\phi)$ is Galois and $\mathrm{Gal}(L(C)/L(\phi)) \simeq \mathrm{Gal}(\overline{K}(C)/\overline{K}(\phi))$. Furthermore, the ramification indices of the points in a fiber

$\phi^{-1}(\alpha)$ ($\alpha \in \mathbb{P}^1$) only depend on α. If $\phi : C \to \mathbb{P}^1$ is unramified outside $\{0, 1, \infty\}$ with ramification indices above $0, 1, \infty$ equal to p, q, r respectively, then we say that ϕ has *signature* (p, q, r) and we define $\chi(p, q, r) := 1/p + 1/q + 1/r - 1$. Let g_C be the genus of C and $\chi_C = 2 - 2g_C$ the Euler characteristics of C. It turns out that χ_C and $\chi(p, q, r)$ have the same sign.

Lemma 1. *Let $\phi : C \to \mathbb{P}^1$ be a geometrically-Galois covering of degree d and signature (p, q, r). Then $\chi_C = d\chi(p, q, r)$. In particular*

- $g_C = 0 \Leftrightarrow \chi(p, q, r) > 0$,
- $g_C = 1 \Leftrightarrow \chi(p, q, r) = 0$,
- $g_C \geq 2 \Leftrightarrow \chi(p, q, r) < 0$.

Proof. Above $0, 1, \infty$ there are $d/p, d/q, d/r$ points respectively, with ramification index p, q, r respectively (and no other ramification points). The Riemann-Hurwitz formula now gives us

$$\begin{aligned} \chi_C &= 2d - \left(\frac{d}{p}(p-1) + \frac{d}{q}(q-1) + \frac{d}{r}(r-1)\right) \\ &= d\chi(p, q, r). \end{aligned}$$

The last statement follows now immediately from $\chi_C = 2 - 2g_C$. □

We also have an existence result for such coverings. A proof is given in section 1.3.

Theorem 2. *Let $(p, q, r) \in \mathbb{Z}^3_{\geq 2}$. Then there exists a curve C and a geometrically-Galois covering $\phi : C \to \mathbb{P}^1$ of signature (p, q, r), defined over a number field K.*

These coverings are used to lift a point $ax^p/(cz^r)$, where x, y, z is a solution to (1.1), to $\phi^{-1}(ax^p/(cz^r))$. In order to bound the ramification of the number field generated by such a lift, the following theorem is of fundamental importance. For $\alpha \in K^*$ and π a finite prime of K we define

$$\nu_\pi^{(0)}(\alpha) := \max(\nu_\pi(\alpha), 0).$$

Theorem 3 (Beckmann). *Let $\phi : C \to \mathbb{P}^1$ be a covering unramified outside $\{0, 1, \infty\}$, defined over a number field K. Then there exists a finite set of primes S_{bad} of K with the following property. Let $\alpha \in K - \{0, 1\} (= \mathbb{P}^1(K) - \{0, 1, \infty\})$ and let $\pi \notin S_{\text{bad}}$. If $\nu_\pi^{(0)}(\alpha), \nu_\pi^{(0)}(\alpha - 1), \nu_\pi^{(0)}(1/\alpha)$ is a multiple of all the ramification indices above $0, 1, \infty$ respectively, then π is unramified in the field $K(\phi^{-1}(\alpha))$.*

Proof. See [Bec, Theorem 5.1] (if the model is not good, finitely many bad primes must be added). □

Solutions to (1.1) can now be described in term of L-rational points on C for some number field L.

Lemma 4. *Let $\phi : C \to \mathbb{P}^1$ be a geometrically-Galois covering of signature (p, q, r), defined over a number field K. Then there exists a finite extension L/K such that for all solutions x, y, z to (1.1) we have $ax^p/(cz^r) \in \phi(C(L))$.*

Proof. Let S_{bad} be the finite set of primes of K associated to ϕ from Theorem 3. Define S'_{bad} to be the union of S_{bad} and the primes of K dividing abc, so S'_{bad} is still finite. Now suppose x, y, z is a solution to (1.1). Let $\alpha := ax^p/(cz^r)$, so $\alpha - 1 = -by^q/(cz^r)$ and $1/\alpha = cz^r/(ax^p)$. Let $L_\alpha := K(\phi^{-1}(\alpha))$, this is a finite extension of K with degree $\leq (\deg \phi)!$.

Since $xyz \neq 0$, we have $\alpha \neq 0, 1, \infty$. Furthermore, since $(x, y, z) = 1$, we have for any prime π of K with $\pi \nmid abc$ that

$$\begin{aligned} \nu_\pi^{(0)}(\alpha) &= \nu_\pi(x^p) = p\nu_\pi(x), \\ \nu_\pi^{(0)}(\alpha - 1) &= \nu_\pi(y^q) = q\nu_\pi(y), \\ \nu_\pi^{(0)}(1/\alpha) &= \nu_\pi(z^r) = r\nu_\pi(z). \end{aligned}$$

So by Theorem 3, L_α is unramified outside S'_{bad}. By Hermite's theorem there are only finitely many field extensions of K with degree $\leq (\deg \phi)!$ and unramified outside S'_{bad}. So there are only finitely many possibilities for L_α. We can take L to be the compositum of those fields, which gives us the finite extension L/K of the theorem. □

Remark 5. From a computational point of view, we want the degrees to be as small as possible (without losing too much information). Instead of a covering $\phi : C \to \mathbb{P}^1$ which is geometrically-Galois, the lemma above already holds for a covering $\phi : C \to \mathbb{P}^1$ unramified outside $\{0, 1, \infty\}$ and such that p, q, r is a multiple of all the ramification indices above $0, 1, \infty$ respectively. Also, instead of considering the Galois extension $L_\alpha = K(\phi^{-1}(\alpha))$, we could consider the K-algebra $K[C]/(\phi - \alpha)$ (of degree $\deg \phi$), where $K[C]$ denotes the integral closure of $K[\phi]$ in $K(C)$. Examples of such approaches to the equations $x^3 + y^5 = 15^6 z^7$ and $ax^2 + by^3 = cz^5$ can be found in section 1.3.2 and chapter 4 respectively.

Reduction of the finiteness of the number of solutions of (1.1) in the hyperbolic case to Faltings' theorem (i.e. Mordell's conjecture) is now easily established. The following theorem first appeared as [DG, Theorem 2].

Theorem 6. *For any $a, b, c \in \mathbb{Z} - \{0\}$ and $p, q, r \in \mathbb{Z}_{>0}$ with $1/p + 1/q + 1/r < 1$, the generalized Fermat equation (1.1) has only finitely many solutions.*

Proof. By Theorem 2, there exists a geometrically-Galois covering $\phi : C \to \mathbb{P}^1$ of signature (p, q, r) defined over a number field K. By Lemma 4, all solutions to (1.1) satisfy $ax^p/(cz^r) \in \phi(C(L))$ for some number field L. Since C has genus ≥ 2 by Lemma 1, Faltings' theorem gives that $C(L)$ is finite and the theorem follows. □

Instead of considering the L-rational points on C for a big number field L (or the L_α-rational points for finitely many number fields L_α) it is possible to consider the K-rational points on finitely many twists of C. By a *twist* of C we mean a curve C' defined over K (which is our groundfield) together with a morphism $\theta : C' \to C$ defined over $\overline{K}$ which is an isomorphism between $C/\overline{K}$ and $C'/\overline{K}$.

Theorem 7. *Let C be a curve and let $\phi : C \to \mathbb{P}^1$ be a geometrically-Galois covering of signature $(p,q,r) \in \mathbb{Z}^3_{\geq 2}$, defined over a number field K. Then there exist finitely many twists $C_1, \ldots C_n$ of C, with morphisms $\theta_i : C_i \to C$ (defined over $\overline{K}$) such that $\phi_i := \phi \circ \theta_i : C_i \to \mathbb{P}^1$ is defined over K for all i and for any solution x, y, z to (1.1) we have $by^p/(cz^q) \in \phi_i(C_i(K))$ for exactly one $i \in \{1, \ldots, n\}$.*

Proof. This follows by a straightforward descent via Galois cohomology. For a detailed and self contained proof, see [Beu2, pp. 11-13]. □

Although currently there is no effective algorithm known to determine all rational points on a curve of genus ≥ 2, in light of the theorem above, it is still interesting to know for which $(p,q,r) \in \mathbb{Z}^3_{>0}$ there exists a geometrically-Galois covering with signature (p,q,r) defined over $\mathbb{Q}$ (and have explicit descriptions of these coverings). Some examples are given in section 1.3.2.

1.2 Ramification and specialization

1.2.1 Index calculation

Consider Theorem 3. For computational purposes, we want to have an explicit set S_{bad} for the covering $\phi : C \to \mathbb{P}^1$. Actually, in [Bec] it is shown that if the covering $\phi : C \to \mathbb{P}^1$ is Galois and the Galois group G has trivial center, then S_{bad} can be taken to be the primes dividing the order of G. We will encounter situations where S_{bad} can actually be taken strictly smaller than this set. We will first introduce classical techniques for ramification computations and then apply this to obtain an S_{bad} in a special case.

The index

Let K be a p-adic field (i.e. K is a finite extension of $\mathbb{Q}_p$) with ring of integers $\mathcal{O}_K$, prime π and residue field $\kappa = \mathcal{O}_K/(\pi)$. Let $f \in \mathcal{O}_K[t]$ be monic and irreducible. We define *the index of* f, denoted $\mathcal{I}(f)$, as follows. Let θ be a root of f and let $A := K(\theta)$, then

$$\nu_\pi\left([\mathcal{O}_A : \mathcal{O}_K[\theta]]\right) = \mathcal{I}(f)[K : \mathbb{Q}_p]$$

for some $\mathcal{I}(f) \in \mathbb{Z}_{\geq 0}$. With this definition we have

$$\nu_\pi(\mathrm{Disc}_t(f(t))) = \nu_\pi(\mathrm{Disc}(\mathcal{O}_A/\mathcal{O}_K)) + 2\mathcal{I}(f). \tag{1.2}$$

From now on suppose that $f \in \mathcal{O}_K[t]$ is monic and separable (and not necessarily irreducible) and let $f = \prod_{i=1}^r g_i$ be the factorization into monic irreducible polynomials $g_i \in \mathcal{O}_K[t]$. Consider the fields $L_i := K[t]/(g_i(t))$ and the K-algebra $A := K[t]/(f(t)) \simeq \prod_{i=1}^r L_i$. We let $\mathcal{O}_A := \prod_{i=1}^r \mathcal{O}_{L_i}$. Since

$$\mathrm{Disc}_t(f(t)) = \prod_{i=1}^r \mathrm{Disc}_t(g_i(t)) \prod_{1 \leq i < j \leq r} \mathrm{Res}_t(g_i(t), g_j(t))^2,$$

we have

$$\begin{aligned}\nu_\pi(\mathrm{Disc}_t(f(t))) &= \sum_{i=1}^{r}(\nu_\pi(\mathrm{Disc}(\mathcal{O}_{L_i}/\mathcal{O}_K)) + 2\mathcal{I}(g_i)) \\ &\quad +2\sum_{1\le i<j\le r}\nu_\pi(\mathrm{Res}_t(g_i(t),g_j(t))) \\ &= \nu_\pi(\mathrm{Disc}(\mathcal{O}_A/\mathcal{O}_K)) + 2\sum_{i=1}^{r}\mathcal{I}(g_i) \\ &\quad +2\sum_{1\le i<j\le r}\nu_\pi(\mathrm{Res}_t(g_i(t),g_j(t))).\end{aligned}$$

This motivates the definition for the index of the (not necessarily irreducible) polynomial f as

$$\mathcal{I}(f) := \sum_{i=1}^{r}\mathcal{I}(g_i) + \sum_{1\le i<j\le n}\nu_\pi(\mathrm{Res}_t(g_i(t),g_j(t))).$$

So in this more general case we also have that (1.2) holds.

Newton polygons

Let $f \in \mathcal{O}_K[t]$ be a monic separable polynomial of degree $n \ge 1$. Denote by $\overline{f}$ the reduction of f modulo π and let $\overline{\phi} \in \kappa[x]$ be a monic irreducible factor of $\overline{f}$ of degree $m \ge 1$. Let $\phi \in \mathcal{O}_K[t]$ denote a monic lift of $\overline{\phi}$. By repeatedly applying the Euclidean algorithm we obtain that

$$f(t) = \sum_{i=0}^{[n/m]} a_i(t)\phi(t)^i$$

for unique polynomials $a_i \in \mathcal{O}_K[t]$ of degree $< m$ (where we use the convention that $\deg(0) < m$). For a nonzero a_i we define $\nu_\pi(a_i)$ to be the highest exponent e such that π^e divides all its coefficients. Define the *ϕ-polygon* of f to be the lower convex hull of the set $\{(i,\nu_\pi(a_i)) \in \mathbb{R}^2 | a_i \neq 0, i = 0,1,\ldots,[n/m]\}$. By $\mathcal{I}_\phi(f)$ we denote $\deg(\phi)$ times the number of points below or belonging to the ϕ-polygon of f with strict positive integer coordinates. Note that both the ϕ-polygon of f and $\mathcal{I}_\phi(f)$ might change if we choose another monic lift ϕ. The following theorem is extremely useful in calculating (an upper bound for) the discriminant of a product of rings of integers explicitly given by a defining polynomial.

Theorem 8. *With notation as above*

$$\mathcal{I}(f) \ge \sum_{\overline{\phi}|\overline{f}}\mathcal{I}_\phi(f).$$

(So $\overline{\phi}$ runs over all monic irreducible factors of $\overline{f}$.)

Proof. See [MN, Theorem of the index, p. 325] (which is essentially obtained from [Ore, Satz 8]). □

Lemma 9. *Let K be a p-adic field and let $f \in \mathcal{O}_K[t]$ be monic and separable. Suppose that*

$$f(t) \equiv \prod_{i=1}^{r} g_i(t)^{e_i} \pmod{\pi^k}, \tag{1.3}$$

for certain $g_i \in \mathcal{O}_K[t]$ and $r, k, e_i \in \mathbb{Z}_{>0}$, that $\prod_{i=1}^r g_i(t)$ has no double roots mod π and that k is a multiple of every e_i. Then

$$\mathcal{I}(f) \geq \frac{k}{2} \sum_{i=1}^{r} (e_i - 1) \deg g_i.$$

Proof. Without loss of generality we can assume that all the g_i are monic and irreducible over K. Since $\overline{g_i}$ has no double roots and g_i is irreducible over K, by Hensel's lemma $\overline{g_i}$ is irreducible (over κ) and since $\prod_{i=1}^r \overline{g_i}$ has no double roots, $\overline{g_i} \neq \overline{g_j}$ for $i \neq j$. Now by Theorem 8

$$\mathcal{I}(f) \geq \sum_{i=1}^{r} \mathcal{I}_{g_i}(f).$$

By (1.3), the line connecting $(0, k)$ and $(e_i, 0)$ lies on or below the g_i-polygon of f (we can assume that $a_0 \neq 0$). Since k is by assumption a multiple of e_i, the line has integral slope and the number of points below or belonging to this line with strict positive integer coordinates is easily seen to be equal to $k(e_i - 1)/2$. So $\mathcal{I}_{g_i}(f) \geq (k/2)(e_i - 1)\deg(g_i)$ and the lemma follows. □

1.2.2 Specialization

In many cases an explicit set S_{bad} for Theorem 3 can be obtained with the techniques above. For simplicity, and because it is the most relevant case for us, we will simply consider coverings, unramified outside $\{0, 1, \infty\}$ given by a polynomial $f \in \mathbb{Q}[t]$. Note that we can find $\gamma, \delta \in \mathbb{Z}$ such that $\gamma f(t/\delta) \in \mathbb{Z}[t]$ is monic (and unramified outside $\{0, \gamma, \infty\}$).

First let us do a simple discriminant computation. Let K be any field and let $\phi \in K[t]$ be of degree $d > 0$ with leading coefficient c and suppose it is unramified outside $\{0, \gamma, \infty\}$ with $\gamma \in K^*$. Say that above 0 we have the different points $P_1, \ldots, P_n \in \overline{K}$ with ramification indices $a_1, \ldots, a_n$ respectively and above $\gamma \in K$ we have the different points $Q_1, \ldots, Q_m \in \overline{K}$ with ramification indices $b_1, \ldots, b_m$. We also suppose that if K has characteristic $p > 0$, then p does not divide any of a_i, b_i or d. Now

$$\phi'(t) = cdt^{d-1} + \ldots = cd \prod_{i=1}^{n} (t - P_i)^{a_i - 1} \prod_{i=1}^{m} (t - Q_i)^{b_i - 1}.$$

We compute

$$\begin{aligned}\mathrm{Res}_t(\phi'(t),\phi(t)-x) &= (cd)^d\prod_{i=1}^{n}(\phi(P_i)-x)^{a_i-1}\prod_{i=1}^{m}(\phi(Q_i)-x)^{b_i-1}\\ &= (cd)^d\prod_{i=1}^{n}(0-x)^{a_i-1}\prod_{i=1}^{m}(\gamma-x)^{b_i-1}\\ &= (-1)^{d-1}(cd)^d x^{s_0}(x-\gamma)^{s_\gamma},\end{aligned}$$

where $s_0 := \sum_{i=1}^{n}(a_i-1)$ and $s_\gamma := \sum_{i=1}^{m}(b_i-1)$ (so $s_0+s_\gamma = d-1$). Furthermore,

$$\mathrm{Res}_t(\phi'(t),\phi(t)-x) = (-1)^{d(d-1)/2}c\mathrm{Disc}_t(\phi(t)-x).$$

We conclude

$$\mathrm{Disc}_t(\phi(t)-x) = (-1)^{d(d+1)/2-1}d^d c^{d-1}x^{s_0}(x-\gamma)^{s_\gamma}. \tag{1.4}$$

We now come to a simple computation of an S_{bad} that works. But first some terminology, an *étale algebra* over a number field K is a finite dimensional commutative K-algebra, without nonzero nilpotent elements, or equivalently, a finite product of number fields over K.

Proposition 10. *Let $\phi \in \mathbb{Z}[t]$ be monic of degree $d > 0$ and suppose that ϕ is unramified outside $\{0,\gamma \in \mathbb{Z}-\{0\},\infty\}$. Let $\alpha \in \mathbb{Q}-\{0,\gamma\}$ and let p be a prime not dividing γ or any of the ramification indices. If $\nu_p^{(0)}(\alpha), \nu_p^{(0)}(\alpha-\gamma), \nu_p^{(0)}(1/\alpha)$ is a multiple of all ramification indices above $0,\gamma,\infty$ respectively, then p is unramified in the étale algebra $A_\alpha := \mathbb{Q}[t]/(\phi(t)-\alpha)$ (or equivalently, unramified in the field $\mathbb{Q}(\phi^{-1}(\alpha))$.*

Proof. Let us first consider the case $\nu_p^{(0)}(1/\alpha) = 0$ (i.e. $\nu_p(\alpha) \geq 0$). We have

$$\mathrm{Disc}_t(\phi(t)-x) = \pm d^d x^{s_0}(x-\gamma)^{s_\gamma}. \tag{1.5}$$

Suppose $\nu_p(\alpha) = 0$ and $k := \nu_p(\alpha-\gamma) \geq 0$, the other case is completely similar ($\nu_p(\alpha), \nu_p(\alpha-\gamma) > 0$ is not possible, because $p \nmid \gamma$). Write

$$\phi(t)-\gamma = \prod_{i=1}^{r} g_i^{e_i}$$

with $g_i \in \mathbb{Z}[t]$ and where $e_i \in \mathbb{Z}_{>0}$ denotes the ramification index for the roots of g_i. From $\nu_p(\alpha-\gamma) = k$ we get (in $\mathbb{Z}_p$)

$$\phi(t)-\alpha \equiv \prod_{i=1}^{r} g_i^{e_i} \pmod{p^k}.$$

Furthermore, by the restrictions on p, no two different ramification points are equal modulo p (consider e.g. the exponent of $x-\gamma$ in (1.4) when working modulo p). So $\prod_{i=1}^{r} g_i$ has no double roots mod p. Lemma 9 now gives us

$$\mathcal{I}(\phi(t)-\alpha) \geq \frac{k}{2}\sum_{i=1}^{r}(e_i-1)\deg g_i = \frac{k}{2}s_\gamma.$$

Form (1.5) we get

$$\nu_p(\mathrm{Disc}_t(\phi(t)-\alpha)) = ks_\gamma.$$

We arrive at

$$\nu_p(\mathrm{Disc}(A_\alpha)) = \nu_p(\mathrm{Disc}_t(\phi(t)-\alpha)) - 2\mathcal{I}(\phi(t)-\alpha) \leq 0,$$

so $\nu_p(\mathrm{Disc}(A_\alpha)) = 0$, i.e. A_α is unramified at p.

Now consider the case $-k := \nu_p(\alpha) < 0$. By assumption we have $d|k$, let

$$z := p^{k/d},\ \beta := p^k\alpha = z^d\alpha.$$

Then $\nu_p(\beta) = 0$. Define

$$f(t) := z^d(\phi(t/z)-\alpha) = z^d\phi(t/z) - \beta.$$

Then $f(t) \in \mathbb{Z}_p[t]$ is monic and for the discriminant we have

$$\mathrm{Disc}_t(f(t)) = \pm d^d\beta^{s_0}(\beta - z^d\gamma)^{s_1}.$$

We see that $\nu_p(\mathrm{Disc}_t(f(t))) = 0$ and we conclude that A_α is unramified at p. □

The main application (analogous to Lemma 4) is when α is related to a solution to the generalized Fermat equation.

Corollary 11. *Let $a,b,c \in \mathbb{Z}-\{0\}$, $p,q,r \in \mathbb{Z}_{\geq 2}$ and suppose that x,y,z is a solution to (1.1). Let $\phi \in \mathbb{Z}[t]$ be monic, unramified outside $\{0,\gamma \in \mathbb{Z}-\{0\},\infty\}$ and suppose that p,q,r is a multiple of all ramification indices above $0,\gamma,\infty$ respectively. Then*

$$\mathbb{Q}[t]/\left(\phi(t) - \gamma\frac{ax^p}{cz^r}\right)$$

is unramified outside the primes dividing $abcpqr\gamma$.

1.3 Existence and examples of Galois coverings

1.3.1 hypergeometric functions

Consider the hypergeometric differential equation

$$t(t-1)\frac{d^2F(t)}{dt^2} + ((a+b+1)t-c)\frac{dF(t)}{dt} + abF(t) = 0, \tag{1.6}$$

with parameters $a,b,c \in \mathbb{C}$. This equation is satisfied by Gauss' hypergeometric function

$$F(a,b,c|t) := \sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(c)_n n!}t^n,$$

where $(x)_n := \prod_{k=1}^{n}(x+k-1)$ is the so called Pochhammer symbol. Here $c \notin \mathbb{Z}_{\leq 0}$, unless $a \in \mathbb{Z}_{\leq 0}$ and $c \leq a$, or $b \in \mathbb{Z}_{\leq 0}$ and $c \leq b$ (for the coefficients we then take

of course the appropriate limit). For the basics, we refer to the very accessible lecture notes [Beu3].

The hypergeometric differential equation (1.6) has regular singularities at $t = 0, 1, \infty$ and is regular at all other $t \in \mathbb{P}^1(\mathbb{C})$. The local exponents $(\rho_{z,1}, \rho_{z,2})$ at $z = 0, 1, \infty$ are given by $(0, 1-c), (0, c-a-b), (a, b)$ respectively. Denote by M_0, M_1, M_∞ the corresponding monodromy matrices (with respect to some basis) such that $M_0 M_1 M_\infty = 1$ and the eigenvalues of M_z are given by $\exp(2\pi i \rho_{z,1})$ and $\exp(2\pi i \rho_{z,2})$. For the local exponent differences $e_z := \rho_{z,2} - \rho_{z,1}$ we thus have

$$\begin{aligned} e_0 &= 1 - c \\ e_1 &= c - a - b \\ e_\infty &= a - b. \end{aligned}$$

Inverting this we get

$$\begin{aligned} a &= \frac{1}{2}(1 - e_0 - e_1 + e_\infty) \\ b &= \frac{1}{2}(1 - e_0 - e_1 - e_\infty) \\ c &= 1 - e_0. \end{aligned}$$

First we will prove an existence theorem about coverings of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$. The proof actually gives a nice geometric construction. See also [DG, Section 3] and [Beu2, Proposition 4.4].

Theorem 12. *Let $p, q, r \in \mathbb{Z}_{\geq 2}$ with $\omega := -\chi(p, q, r) = 1 - (1/p + 1/q + 1/r) > 0$. Then there exists a finite Galois covering of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ which is unramified outside $0, 1, \infty$ and with ramification indices above $0, 1, \infty$ equal to p, q, r respectively.*

Proof. Setting $(e_0, e_1, e_\infty) = (1/p, 1/q, 1/r)$ in (1.7), (1.7), (1.7), we get

$$(a, b, c) = (\omega/2 + 1/r, \omega/2, \omega + 1/q + 1/r).$$

The (full) monodromy group is generated by, say, $A := M_\infty$ and $B := M_0^{-1}$. And the projective monodromy group G (i.e. the monodromy group modulo scalars) is, according to [Beu3, p.38], a so called triangle group, which we shall briefly describe now. Consider a hyperbolic triangle in the upper half plane $\mathfrak{H}$ (with a hyperbolic metric) with angles $\pi/p, \pi/q$ and π/r and call the corresponding vertices P, Q and R. The images m_0, m_1, m_∞ of M_0, M_1, M_∞ in G correspond to rotation around P, Q, R with an angle of $2\pi/p, 2\pi/q, 2\pi/r$ respectively. The triangle group G is generated by m_0, m_1, m_∞ and the only elliptic elements of G are given by the conjugates of the powers of m_0, m_1 and m_∞ other than the identity. Furthermore, G acts discretely on $\mathfrak{H}$, the quotient map gives us an infinite Galois cover $\phi : \mathfrak{H} \to \mathbb{P}^1_{\mathbb{C}}$ unramified outside, say, $0, 1, \infty$ and with ramification indices above $0, 1, \infty$ equal to p, q, r respectively. Suppose we have a normal subgroup H of G without elliptic elements and such that G/H is finite. Then $C := \mathfrak{H}/H$ is an algebraic curve and ϕ factors as $\phi = g \circ f$, where $f : \mathfrak{H} \to C$ is unramified (since H contains no elliptic elements) and $g : C \to \mathbb{P}^1_{\mathbb{C}}$ is a Galois cover (with

Galois group G/H). Since f is unramified, the ramification indices of g above $0, 1, \infty$ equal p, q, r respectively (and g is of course unramified outside $0, 1, \infty$). The branch points of g are defined over $\overline{\mathbb{Q}}$, so by standard descent, g and C can be defined over $\overline{\mathbb{Q}}$ and granted the existence of H, our theorem follows. We are going to explicitly write down the monodromy group, in order to construct H.

Since $A := M_\infty$ and $B := M_0^{-1}$ have disjoint sets of eigenvalues and $AB^{-1} = M_1^{-1}$ has eigenvalue 1, we have (see e.g. [Beu3, lemma 3.13]) that up to common conjugation

$$A = \begin{pmatrix} 0 & -\mathrm{Det}A \\ 1 & \mathrm{Tr}A \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -\mathrm{Det}B \\ 1 & \mathrm{Tr}B \end{pmatrix}.$$

We calculate (w.r.t. the appropriate basis)

$$\begin{aligned} A &= \begin{pmatrix} 0 & -e^{2\pi i\rho_{\infty,1}}e^{2\pi i\rho_{\infty,2}} \\ 1 & e^{2\pi i\rho_{\infty,1}} + e^{2\pi i\rho_{\infty,2}} \end{pmatrix} \\ &= \begin{pmatrix} 0 & -e^{2\pi i(a+b)} \\ 1 & e^{2\pi ia} + e^{2\pi ib} \end{pmatrix} \\ &= \begin{pmatrix} 0 & -e^{2\pi i(\omega+\frac{1}{r})} \\ 1 & e^{\pi i\omega}\left((1+e^{\frac{2\pi i}{r}}\right) \end{pmatrix}, \end{aligned}$$

$$\begin{aligned} B &= \begin{pmatrix} 0 & -e^{-2\pi i\rho_{0,1}}e^{-2\pi i\rho_{0,2}} \\ 1 & e^{-2\pi i\rho_{0,1}} + e^{-2\pi i\rho_{0,2}} \end{pmatrix} \\ &= \begin{pmatrix} 0 & -e^{2\pi i(c-1)} \\ 1 & 1 + e^{2\pi i(c-1)} \end{pmatrix} \\ &= \begin{pmatrix} 0 & -e^{-\frac{2\pi i}{p}} \\ 1 & 1 + e^{-\frac{2\pi i}{p}} \end{pmatrix}. \end{aligned}$$

Dividing by a square root of the determinant, and writing $\zeta_n := e^{\frac{2\pi i}{n}}$, $n \in \mathbb{Z}_{>0}$, we obtain that

$$\begin{aligned} A' &:= e^{-\pi i(\omega+\frac{1}{r})}A \\ &= \begin{pmatrix} 0 & -e^{\pi i(\omega+\frac{1}{r})} \\ e^{-\pi i(\omega+\frac{1}{r})} & e^{\frac{\pi i}{r}} + e^{-\frac{\pi i}{r}} \end{pmatrix} \\ &= \begin{pmatrix} 0 & \zeta_{2p}^{-1}\zeta_{2q}^{-1} \\ -\zeta_{2p}\zeta_{2q} & \zeta_{2r} + \zeta_{2r}^{-1} \end{pmatrix}, \end{aligned}$$

$$\begin{aligned} B' &:= e^{\frac{\pi i}{p}}B \\ &= \begin{pmatrix} 0 & -e^{-\frac{\pi i}{p}} \\ e^{\frac{\pi i}{p}} & e^{\frac{\pi i}{p}} + e^{-\frac{\pi i}{p}} \end{pmatrix} \\ &= \begin{pmatrix} 0 & -\zeta_{2p}^{-1} \\ \zeta_{2p} & \zeta_{2p} + \zeta_{2p}^{-1} \end{pmatrix}. \end{aligned}$$

With $C' := A'B'^{-1}$, we have $A', B', C' \in \mathrm{SL}_2(\mathbb{Z}[\zeta_{2pqr}])$ and A', B', C' modulo $\pm I$ can be identified with $m_\infty, m_0^{-1}, m_1^{-1} \in G \subset \mathrm{PSL}_2(\mathbb{Z}[\zeta_{2pqr}])$ respectively. Now let π be a prime in $\mathbb{Z}[\zeta_{2pqr}]$ not dividing $2pqr$, then $\zeta_{2pqr} \pmod{\pi}$ still has order $2pqr$ and since A, B, C have eigenvalues $(\zeta_{2r}, \zeta_{2r}^{-1}), (\zeta_{2p}, \zeta_{2p}^{-1}), (-\zeta_{2q}, -\zeta_{2q}^{-1})$ respectively, we see that

$$m_\infty \mod \pi,\ m_0 \mod \pi,\ m_1 \mod \pi \in \mathrm{PSL}_2(\mathbb{Z}[\zeta_{2pqr}]/\pi)$$

still have orders r, p, q respectively. This shows that no power other than the identity of m_0, m_1, m_∞ (and hence all their conjugates) lies in the kernel H of the reduction map $G \to G \mod \pi$. This provides us with a suitable normal subgroup H of G and the theorem follows. □

We note (with notation as in the proof) that A', B', C' are actually already defined over $\mathbb{Z}[\zeta_{2p}, \zeta_{2q}, \zeta_{2r} + \zeta_{2r}^{-1}]$ and it is not always necessary to have π not dividing $2pqr$ (especially if one wants to obtain minimal groups G/H). Take $(p, q, r) = (3, 7, 2)$ for example, then $\mathbb{Z}[\zeta_{2p}, \zeta_{2q}, \zeta_{2r} + \zeta_{2r}^{-1}] = \mathbb{Z}[\zeta_{21}]$ and 7 factors as $\pi_1^6\pi_2^6$ in this ring of integers. Taking π equal to one of these primes lying above 7, one easily computes that A', B', C' modulo π still have orders $2, 3, 7$ respectively and in fact generate the Hurwitz group $\mathrm{PSL}_2(\mathbb{F}_7)$.

In the case $\chi \geq 0$, coverings can be constructed analogously, or directly written down explicitly.

1.3.2 Examples over $\mathbb{Q}$

Consider a short exact sequence of groups

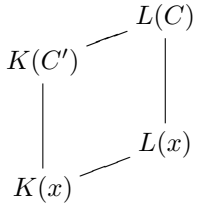
$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

We call a homomorphism $s : C \to B$ such that $g \circ s : C \to C$ is the identity a *right-splitting*.

Now let L/K be an extension of number fields, C a curve and $x : C \to \mathbb{P}^1$ a covering, both defined over L and suppose that the field extensions L/K and $L(C)/K(x)$ are both Galois. This induces the short exact sequence

$$0 \to \mathrm{Gal}(L(C)/L(x)) \xrightarrow{f} \mathrm{Gal}(L(C)/K(x)) \xrightarrow{g} \mathrm{Gal}(L/K) \to 0. \tag{1.7}$$

Suppose that it has a right-splitting s. Then the subfield of $L(C)$ fixed by $s(\mathrm{Gal}(L/K)) \subset \mathrm{Gal}(L(C)/K(x)$ is the function field $K(C')$ of a curve C' defined over K, see the figure below. Of course, $K(C')/K(x)$ need not be Galois, if however the image of s is normal, then $K(C')/K(x)$ is Galois and we have $\mathrm{Gal}(K(C')/K(x)) \simeq \mathrm{Gal}(L(C)/L(x))$. Further, $L(C')/L(x)$ is isomorphic to $L(C)/L(x)$ (and we could say that $x : C \to \mathbb{P}^1$ can be defined over K).



Example 13 (Signature $(3,2,p)$ coverings). Let p be a prime which is $\pm 1 \pmod 4$, and let $L := \mathbb{Q}(\zeta_p)$. As is well known, the j map from the modular curve $X(p)$ to $X(1)$, provides us with a Galois covering $\phi : C \to \mathbb{P}^1$ defined over L with signature $(3,2,p)$. Let $K := \mathbb{Q}$, then (1.7) is given by

$$0 \to \mathrm{SL}_2(\mathbb{F}_p)/\pm I \to \mathrm{GL}_2(\mathbb{F}_p)/\pm I \to \mathbb{F}_p^* \to 0.$$

It has a right-splitting, so we see that ϕ can actually be defined over $\mathbb{Q}$. Now let $K := \mathbb{Q}(\sqrt{\pm p})$ be the unique quadratic subfield of L. Then (1.7) is given by

$$0 \to \mathrm{SL}_2(\mathbb{F}_p)/\pm I \to \{M \in \mathrm{GL}_2(\mathbb{F}_p) \mid \det M \in (\mathbb{F}_p^*)^2\}/\pm I \to (\mathbb{F}_p^*)^2 \to 0.$$

It has a right-splitting with normal image, so ϕ becomes already Galois over $\mathbb{Q}(\sqrt{\pm p})$.

The strategy of the following two examples is as follows (where we have $K = \mathbb{Q}$). Construct a rational map $x \in K(t)$, say of degree n, unramified outside $0, 1, \infty$ and such that there is at least one ramification index above $0, 1, \infty$ of order p, q, r respectively and all other ramification indices are equal to 1. Let F denote the Galois closure of $K(t)/K(x)$ and let $L := \overline{\mathbb{Q}} \cap F$ denote the field of constants of F. Then L/K is Galois and F is the function field of a curve C defined over L and the covering corresponding to $L(C)/L(x)$ is a Galois covering of signature (p,q,r). We regard $\mathrm{Gal}(L(C)/K(x))$ embedded in S_n. Now suppose that $\mathrm{Gal}(L(C))/L(x))$ contains the alternating group A_n. Then obviously (1.7) has a right-splitting and the covering corresponding to $K(C')/K(x)$ (with C' defined as before) is a geometrically-Galois covering of signature (p,q,r) defined over K. If $L = K$, then trivially this covering is already Galois over K. If $L \neq K$, then $\mathrm{Gal}(L(C))/L(x)) = A_n$, and writing $x = u/v$ with $u, v \in K[t]$ relatively prime, we have $\mathrm{Disc}_t(u(t) - v(t)a) = da^{e_0}(a-1)^{e_1}$ for certain even $e_0, e_1 \in \mathbb{Z}_{>0}$ and $d \in K^* - (K^*)^2$. We have $L = K(\sqrt{d})$ and an explicit birational model for C' (corresponding to the choice that the section s maps the nontrivial element to the transposition $(1,2)$) is given as follows.

Write $u(t) - av(t) = \sum_{i=0}^{n} c_{n-i}(a)t^i$, where the $c_k(a) \in K[a]$ (of degree ≤ 1) and assume for simplicity that $u(t) - av(t)$ is monic in t, i.e. $c_0(a) = 1$. Let $\sigma_k(t_1, \ldots, t_n)$ denote the standard elementary symmetric polynomial of degree k in the n variables $t_1, \ldots, t_n$. Now consider the following n equations in the $n+1$ variables $t_1, \ldots, t_n, a$

$$\sigma_k(t_1, \ldots, t_n) = (-1)^k c_k(a), \quad k = 1, \ldots, n. \tag{1.8}$$

These equations define a curve which is irreducible over K, but over L it has two components, each birational (over L) to C. We also have

$$D(t_1, \ldots, t_n) := \prod_{1 \leq i < j \leq n} (t_i - t_j) = \pm\sqrt{d}a^{e_0/2}(a-1)^{e_1/2} \tag{1.9}$$

and the choice of a sign determines one of the two components. Now introduce two variables T_1, T_2 and eliminate t_1, t_2 by the variable substitution

$$t_1 := T_1 + \sqrt{d}T_2, \; t_2 := T_1 - \sqrt{d}T_2.$$

Since

$$\sigma_k(T_1+\sqrt{d}T_2, T_1-\sqrt{d}T_2, t_3, \ldots, t_n)$$

is invariant under the action of $\mathrm{Gal}(L/K)$ it has still coefficients in K. The same holds for

$$D(T_1+\sqrt{d}T_2, T_1-\sqrt{d}T_2, t_3, \ldots, t_n)/\sqrt{d}.$$

So the equations

$$\begin{aligned}\sigma_k(T_1+\sqrt{d}T_2, T_1-\sqrt{d}T_2, t_3, \ldots, t_n) &= (-1)^k c_k(a),\ k=1,\ldots,n\\ D(T_1+\sqrt{d}T_2, T_1-\sqrt{d}T_2, t_3, \ldots, t_n)/\sqrt{d} &= \pm a^{e_0/2}(a-1)^{e_1/2}\end{aligned}$$

actually have their coefficients in K and together with a choice of the sign they give a birational model for C'.

Coverings from hypergeometric polynomials

Let $p, q, r \in \mathbb{Z}_{\geq 1}$, say with $p \leq q \leq r$. We impose two extra conditions, namely

$$p+q+r \equiv 1 \pmod 2, \quad r \leq p+q-1.$$

For the local exponent differences we take $(e_0, e_1, e_\infty) = (p, q, r)$. The values of a, b, c are given by $(1.7, 1.7, 1.7)$. Let $d := (p+q+r-1)/2 \in Z_{>0}$. We are going to consider hypergeometric polynomials, basic calculations can be found in [BT, pp. 197-198] (with substitutions $k := q, m := d-r, n := d-q, l$ so $k-m-1 = d-p$). Solutions to the hypergeometric differential equation (1.6) are given by

$$\begin{aligned}t^{1-c}F(a-c+1, b-c+1, 2-c|t) &= t^p F(p+r-d, p-d, 1+p|t)\\ (1-t)^{c-a-b}F(c-b, c-a, c|t) &= (1-t)^q F(q+r-d, q-d, 1-p|t)\\ F(a, b, c|t) &= F(r-d, -d, 1-p|t).\end{aligned}$$

Recall that a necessary condition for $F(a', b', c'|t)$ to be a (well defined) polynomial is, that $a' \in Z_{\leq 0}$ or $b' \in \mathbb{Z}_{\leq 0}$. If $c' \notin \mathbb{Z}_{\leq 0}$ this is also sufficient. Otherwise we also need $a' \in \mathbb{Z}_{\leq 0}$ and $c' \leq a'$, or $b' \in \mathbb{Z}_{\leq 0}$ and $c' \leq b'$. So the conditions imposed on p, q, r give that these solutions are actually polynomials. Up to a constant they are given by

$$\begin{aligned}A(t) &:= (-1)^{d-r}t^p \int_0^1 (1-x)^{d-r}x^{d-q}(1-tx)^{d-p}dx\\ B(t) &:= (1-t)^q \int_0^1 (1-x)^{d-r}x^{d-p}(1-x+tx)^{d-q}dx\\ C(t) &:= \int_0^1 (1-x)^{d-q}x^{d-p}(1-x-t)^{d-r}dx.\end{aligned}$$

Since $A(t), B(t), C(t)$ all satisfy the (second order) hypergeometric differential equation

$$t(t-1)\frac{d^2F(t)}{dt^2} + ((2-p-q)t+p-1)\frac{dF(t)}{dt} + (d-r)dF(t) = 0,$$

they are linearly dependent and in fact satisfy

$$A(t) + B(t) = C(t).$$

In particular, the map $\phi(t) := A(t)/C(t)$ is unramified outside $\{0, 1, \infty\}$, of degree d and the ramification data is as follows. Above $0, 1, \infty$ there lies one ramified point with ramification p, q, r respectively, all other points are unramified. To compute the Galois group of the covering, we are going to use dessins d'enfant for which we refer to [LZ, Chapter 2]. It is easy to see that there is only one dessin d'enfant (on the Riemann sphere) with this ramification, so the dessin d'enfant of $\phi(t)$ is given in Figure 1.1, where $i := d - q, j := d - r + 1$ and $k := d - p$.

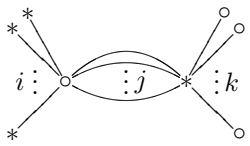


Figure 1.1: dessin d'enfant associated to $\phi(t) = A(t)/C(t)$

From this we calculate the Galois group $G_{p,q,r} := \mathrm{Gal}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}(\phi(t))) \subset S_d$.

Proposition 14. *Suppose $p, q, r \geq 2$. If p, q, r are all odd, then $G_{p,q,r} = A_d$, otherwise $G_{p,q,r} = S_d$.*

Proof. The permutation pairs associated with the ramification above $0, 1$ are respectively $\sigma := (1, 2, \ldots i+j), \tau := (i+1, i+2, \ldots, i+j+k)$. So $G_{p,q,r}$ is the group generated by σ, τ and we are left with an elementary, though tedious exercise in permutation group theory. We will show that $G_{p,q,r}$ contains a 3-cycle. By conjugating this 3-cycle with $\sigma, \tau, \sigma^{-1}, \tau^{-1}$ and the 3-cycles found along the way, one can show that $G_{p,q,r}$ in fact contains every 3-cycle and hence contains A_d, from which the proposition follows. For simplicity we will assume that $c > b > 0$ and $a > 1$, other cases are similar or can be reduced to this one. We will now show that $G_{p,q,r}$ contains a 3-cycle. We compute

$$\begin{aligned} X &:= \tau^{-1}\sigma\tau\sigma^{-1} \\ &= (i+1, i+j+k)(1, i+j). \end{aligned}$$

If $j = 1$ then $X = (1, i+1+k, i+1)$ (by assumption $1 < i+1 < i+1+k$) and we are done in this case, so assume $j > 1$. Conjugating $j+1$ times with τ gives

$$\tau^{j+1} X \tau^{-j-1} = (i+j+2, i+j+1)(1, i+2j+1).$$

Note that $i + 2j + 1 \leq i + j + k$, since by assumption $j < k$. Conjugating with σ gives

$$\sigma(i+j+2, i+j+1)(1, i+2j+1)\sigma^{-1} = (i+j+2, i+j+1)(2, i+2j+1).$$

Conjugating $j+1$ times with τ^{-1} gives

$$\begin{aligned} Y &:= \tau^{-j-1}(i+j+2, i+j+1)(2, i+2j+1)\tau^{j+1} \\ &= (i+1, i+j+k)(2, i+j) \\ &= (2, i+j)(i+1, i+j+k). \end{aligned}$$

Finally

$$YX = (2, i+j)(1, i+j) = (1, 2, i+j).$$

□

We conclude that by taking Galois closure, ϕ induces a geometrically-Galois covering $\phi' : C' \to \mathbb{P}^1$ of signature (p, q, r) defined over $\mathbb{Q}$. To see over which field the covering ϕ' is Galois, we will now do some explicit calculations. These are also useful for applying the method of proof of Proposition 10 to obtain S_{bad} explicitly.

Suppose $p + q \neq r + 1$. Write

$$A = A(t) = \alpha t^d + \ldots, \; C = C(t) = \gamma t^{d-r} + \ldots$$

and denote by $'$ differentiation with respect to t. Then

$$A'C - AC' = r\alpha\gamma t^{p-1}(t-1)^{q-1}.$$

We compute

$$\begin{aligned} (r\alpha\gamma)^{d-r} C(0)^{p-1} C(1)^{q-1} &= \mathrm{Res}_t(r\alpha\gamma t^{p-1}(t-1)^{q-1}, C) \\ &= \mathrm{Res}_t(A'C - AC', C) \\ &= \mathrm{Res}_t(-AC', C) \\ &= (-1)^{d-r}\mathrm{Res}_t(A, C)\mathrm{Res}_t(C', C) \\ &= (-1)^{(d-r)(d-r+1)/2}\gamma \mathrm{Res}_t(A, C)\mathrm{Disc}_t(C), \end{aligned}$$

where in the third equality we used that $p + q \neq r + 1$ (which implies that $C(t)$ is not constant, so that $A'C - AC'$ and AC' have the same degree). Let $f = f_x(t) := A(t) - C(t)x$ (where x does not depend on t), then $f'C - fC' = A'C - AC'$ and

$$\begin{aligned} \mathrm{Res}_t(A'C - AC', f) &= \mathrm{Res}_t(r\alpha\gamma x^{p-1}(x-1)^{q-1}, f) \\ &= (r\alpha\gamma)^d (A(0) - C(0)x)^{p-1}(A(1) - C(1)x)^{q-1} \\ &= (r\alpha\gamma)^d C(0)^{p-1} C(1)^{q-1}(0-x)^{p-1}(1-x)^{q-1} \\ &= (r\alpha\gamma)^r (-1)^{s'} \gamma \mathrm{Res}_t(A, C)\mathrm{Disc}_t(C) x^{p-1}(x-1)^{q-1}, \end{aligned}$$

where $s' := (d-r)(d-r+1)/2 + p + q$. Further,

$$\begin{aligned} \mathrm{Res}_t(f, A'C - AC') &= \mathrm{Res}_t(f, f'C - fC') \\ &= \mathrm{Res}_t(f, f'C) \\ &= \mathrm{Res}_t(f, f')\mathrm{Res}_t(A - Cx, C) \\ &= (-1)^{d(d-1)/2}\alpha \mathrm{Disc}_t(f)\mathrm{Res}_t(A, C). \end{aligned}$$

We conclude

$$\mathrm{Disc}_t(f_x(t)) = (-1)^s(r\alpha\gamma)^r\frac{\gamma}{\alpha}\mathrm{Disc}_t(C(t))x^{p-1}(x-1)^{q-1},$$

where $s := s' + d(d-1)/2 + d(p+q)$. If p, q, r are all odd, we have

$$\mathrm{Disc}_t(f_x(t)) \equiv (-1)^s r\mathrm{Disc}_t(C(t)) \pmod{(\mathbb{Q}(t)^*)^2},$$

so in that case ϕ' is Galois over $\mathbb{Q}(\sqrt{(-1)^s r\mathrm{Disc}_t(C(t))})$ (which might be equal to $\mathbb{Q}$). It would of course be nice to have a simple expression of $\mathrm{Disc}_t(C(t))$ in terms of p, q, r, but we will leave it at this.

Note that in the case that r is maximal, i.e. $r = p+q-1$, the map $A(x)/C(x)$ simply becomes a polynomial. Without using hypergeometric polynomials it is immediately obvious that a formula for the dessin d'enfant in Figure 1.1 with $j = 1$ is given by

$$\phi_{p,q}(t) := \frac{\int_0^t x^{p-1}(x-1)^{q-1}dx}{\int_0^1 x^{p-1}(x-1)^{q-1}dx}.$$

According to (1.4) we have

$$\mathrm{Disc}_t(\phi_{p,q}(t) - x) = (-1)^{r(r+1)/2-1}r^r\sigma^{r-1}x^{p-1}(x-1)^{q-1},$$

where now

$$\sigma = \frac{1}{(p+q-1)\int_0^1 x^{p-1}(x-1)^{q-1}dx} = (-1)^{q-1}\binom{p+q-2}{p-1}.$$

In the most interesting case that p, q, r are all odd, we see that the geometrically-Galois covering ϕ' of signature $(p, q, p+q-1)$ is Galois over $\mathbb{Q}(\sqrt{\pm(p+q-1)})$. Furthermore, we actually have $\phi_{p,q} \in \mathbb{Z}[t]$ (so $\sigma^{p+q-2}\phi_{p,q}(t/\sigma) \in \mathbb{Z}[t]$ is monic and unramified outside $\{0, \sigma^{p+q-2}, \infty\}$) using Corollary 11 we get that for a solution x, y, z to (1.1) with $r = p+q-1$ we have $\mathbb{Q}(\phi_{p,q}^{-1}(ax^p/(cz^r)))$ is unramified outside the primes dividing $pq(p+q-1)\binom{p+q-2}{p-1}abc$.

The equation $x^5 + y^3 = 15^6z^7$

As an example, we will now study the equation

$$x^5 + y^3 = 15^6z^7 \quad x, y, z \in \mathbb{Z} \quad \gcd(x, y, 15z) = 1 \quad xyz \neq 0. \tag{1.10}$$

Note that the gcd-condition means that x, y, z are pairwise coprime. Consider the covering $\mathbb{P}^1 \to \mathbb{P}^1$, given by

$$\begin{aligned}\phi_{5,3}(t) &= t^5(15t^2 - 35t + 21)\\ &= (t-1)^3(15t^4 + 10t^3 + 6t^2 + 3t + 1) + 1.\end{aligned}$$

To a hypothetical solution x, y, z of (1.10) we can associate the (Frey) polynomial $\phi_{5,3}(t) - x^5/(15^6z^7)$, or better, scale a bit and define

$$\begin{aligned}F_{x,y,z}(t) &:= z^7 15^6\phi_{5,3}(t/(15z)) - x^5\\ &= t^5(t^2 - 35zt + 315z^2) - x^5\\ &= (t-15z)^3(t^4 + 10zt^3 + 90z^2t^2 + 675z^3t + 3375z^4) + y^3.\end{aligned}$$

We have

$$\mathrm{Disc}_t(F_{x,y,z}(t)) = -7^7 x^{20}(15^6 z^7 - x^5)^2 = -7^7 x^{20} \cdot y^6$$

Let $A := \mathbb{Q}[t]/(F_{x,y,z}(t))$. By Corollary 11 we get that A is unramified outside $\{3, 5, 7\}$. From (1.10) we get directly $3, 5 \nmid xy$, so by the discriminant computation we get that A is unramified at 3 and 5. We conclude that the étale algebra A is unramified outside 7. Furthermore, if $7 \nmid xy$, then of course $\nu_7(\mathrm{Disc}(\mathcal{O}_A)) \leq \nu_7(\mathrm{Disc}_t(F_{x,y,z}(t))) = 7$. If $7|xy$, say $7|x$ (the other case is again completely similar), then $7 \nmid y$ and $\nu_7(\mathrm{Disc}_t(F_{x,y,z}(t))) = 7 + 20\nu_7(x)$. The t-polygon of $F_{x,y,z}(t)$ contains the line connecting $(0, 5\nu_7(x))$ and $(5, 1)$, so (working in $\mathbb{Z}_7$) $\mathcal{I}_t(F_{x,y,z}(t)) = 10\nu_7(x) + 1$. We conclude by Theorem 8 that $\nu_7(\mathrm{Disc}(\mathcal{O}_A)) \leq \nu_p(\mathrm{Disc}_t(F_{x,y,z}(t))) - 2\mathcal{I}_t(F_{x,y,z}(t)) = 5$.

We summarize what we obtained so far. If x, y, z is a solution to (1.10), then $F_{x,y,z}$ defines a product of rings of integers $\mathcal{O}_A$, unramified outside 7, with $\nu_7(\mathrm{Disc}(\mathcal{O}_A)) \leq 7$.

It is known (see e.g. [JR]) that if K is a number field unramified outside 7 and with $[K : \mathbb{Q}] \leq 7$, then K equals one of the 4 subfields of the cyclotomic field $\mathbb{Q}(\zeta_7)$, or $[K : \mathbb{Q}] = 7$ and $\nu_7(\mathrm{Disc}(\mathcal{O}_K)) > 7$. So we only have to deal with the subfields of $\mathbb{Q}(\zeta_7)$. Since $5 \nmid x$, we obtain that

$$F_{x,y,z}(t) \equiv t^7 - x^5 \pmod 5$$

has an irreducible factor of degree 6. So $\mathbb{Q}(\zeta_7)$ must occur as a factor of A, and the only case left to deal with is $A = \mathbb{Q}[t]/(F_{x,y,z}(t)) \simeq \mathbb{Q}[t]/(t^7 - 1)$. Unfortunately we are at this time unable to eliminate this case, but we can reduce it to finding certain cubic points on a hyperelliptic curve as follows.

First of all, $15^6\phi_{5,3}(t/15) - x^5/z^7$ must have a rational root s. So

$$x^5/z^7 = 15^6\phi_{5,3}(s/15)$$

and we get

$$\begin{aligned} G(t,s) &:= 15^6 \frac{\phi_{5,3}(t/15) - \phi_{5,3}(s/15)}{t-s} \\ &= 315t^4 - 35t^5 + t^6 + 315t^3 s - 35t^4 s + t^5 s \\ &\quad +315t^2 s^2 - 35t^3 s^2 + t^4 s^2 + 315ts^3 - 35t^2 s^3 + t^3 s^3 \\ &\quad +315s^4 - 35ts^4 + t^2 s^4 - 35s^5 + ts^5 + s^6 \\ &= 0 \end{aligned}$$

for certain $t \in \mathbb{Q}(\zeta_7)$ and $s \in \mathbb{Q}$ (in fact t must generate $\mathbb{Q}(\zeta_7)$). To make this a little more symmetric, write $t = a + b\sqrt{-7}$, with $a, b \in \mathbb{Q}(\zeta_7 + 1/\zeta_7)$, then we have

$$G(a + b\sqrt{-7}, y) = F_1(a, b, y) + bF_2(a, b, y)\sqrt{-7}$$

with $F_1(a, b, y), F_2(a, b, y) \in \mathbb{Q}[a, b, y]$. Since $b = 0$ is already ruled out, we get the equation $Res_y(F_1(a, b, y), F_2(a, b, y)) = 0$, which is equivalent to

$$225a^4 - 30a^5 + a^6 - 3150a^2b^2 + 700a^3b^2 - 35a^4b^2 + 2205b^4 - 1470ab^4 + 147a^2b^4 - 49b^6$$

equals 0. One can check, e.g. with Magma, that the curve defined by this equation is isomorphic over $\mathbb{Q}$ to the hyperelliptic of genus 3, given by

$$\begin{aligned} y^2 + (x^4 + x^2 + 1)y &= 131x^8 - 525x^7 + 857x^6 - 735x^5 + 918x^4 \\ &\quad -1225x^3 + 1102x^2 - 525x + 201. \end{aligned}$$

And so we have reduced solving (1.10) to finding the cubic points in $\mathbb{Q}(\zeta_7 + 1/\zeta_7)$ of the hyperelliptic curve of genus 3 above.

(Of course, we could have written t out with respect to a $\mathbb{Q}$-basis, getting 6 equations in 7 unknowns, defining a curve. So that we really had to find the points over $\mathbb{Q}$, but the equations are more messy.)

Signature $(p, 3, 2p + 1)$ coverings

There are many other easy to compute coverings, we briefly describe one more example. Let $p \in \mathbb{Z}_{\geq 2}$. Consider the covering ramified above ∞ with index $2p+1$, above 1 with index 3 and $2(p-1)$ times index 1, and ramified above 0 with twice index p and one time 1. We claim that the following polynomial gives such a map,

$$\phi_p(t) := \left(\frac{p+1}{2}t^2 + t + 1\right)^p (1 - pt).$$

This follows almost immediately from

$$\frac{d\phi_p(t)}{dt} = -p(2p+1)\frac{p+1}{2}\left(\frac{p+1}{2}t^2 + t + 1\right)^{p-1} t^2.$$

Again, it is easy to see that there is only one dessin d'enfant (on the Riemann sphere) with the desired ramification data, it is given in Figure 1.2.

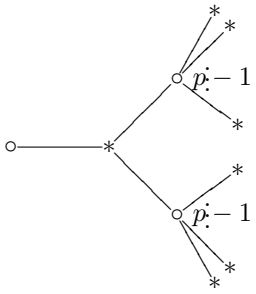


Figure 1.2: dessin d'enfant associated to $\phi_p(t)$

The Galois group G_p of the dessin d'enfant already contains a three cycle, and by suitably conjugating, we again obtain that G_p contains all three cycles of S_{2p+1}, hence G_p contains A_{2p+1}. We conclude that the geometrically-Galois covering of signature $(3, p, 2p + 1)$ can be defined over $\mathbb{Q}$.

Chapter 2

Modular methods for Diophantine equations

We turn to Galois representations attached to elliptic curves and modular forms to study Diophantine equations.

2.1 Galois representations

In this section we shall describe basic definitions and theorems about 2-dimensional Galois representations associated to elliptic curves and modular forms that will be needed for our applications to Diophantine equations. We will only be concerned with mod l representations. For the modular forms to be considered, we will limit ourselves to cuspforms of weight 2 w.r.t. $\Gamma_0(N)$ (so the character is trivial).

2.1.1 Elliptic curves, modular forms and Galois representations

We start with the definition of one of our basic objects.

Definition 15. Let $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group (endowed with the Krull topology), let $\mathbb{F}$ be a finite field of characteristic l (endowed with the discrete topology) and let $d \in \mathbb{Z}_{>0}$. A *Galois representation* is a continuous group homomorphism

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(\mathbb{F}),$$

where d is called the *dimension* of ρ. If ρ' is another d-dimensional Galois representation, then ρ and ρ' are considered isomorphic if there exists an $M \in \mathrm{GL}_d(\bar{\mathbb{F}})$ such that $\rho'(\sigma) = M\rho(\sigma)M^{-1}$ for all $\sigma \in G_{\mathbb{Q}}$.

These Galois representations are sometimes called *mod l Galois representations*, but since we will not consider other (e.g. l-adic) Galois representations, we will not

use this terminology. Most of the time we will be concerned with 2-dimensional Galois representations, and occasionally we will encounter 1-dimensional ones (characters). We say that a Galois representation ρ is unramified at a prime p if I_p is contained in the kernel of ρ for some inertia group $I_p \subset G_{\mathbb{Q}}$ of p. By the continuity of ρ, the kernel of ρ is an open subgroup of $G_{\mathbb{Q}}$, so it corresponds to a finite Galois extension K of $\mathbb{Q}$. So ρ factors through $\mathrm{Gal}(K/\mathbb{Q})$ and ρ is ramified at a prime p if and only if p is ramified in K. The following lemma gives us a useful criterium to determine when 2-dimensional Galois representations are isomorphic.

Lemma 16. *Let $\mathbb{F}$ be a finite field and let*

$$\rho_1, \rho_2 : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$$

be two semisimple Galois representations. If for all but finitely many primes p, where ρ_1, ρ_2 are unramified, we have $\mathrm{Trace}(\rho_1(\mathrm{Frob}_p)) = \mathrm{Trace}(\rho_2(\mathrm{Frob}_p))$ and $\mathrm{Det}(\rho_1(\mathrm{Frob}_p)) = \mathrm{Det}(\rho_2(\mathrm{Frob}_p))$, then ρ_1 and ρ_2 are isomorphic.

Proof. Since ρ_1, ρ_2 are continuous it suffices to prove the statement of the lemma with $G_{\mathbb{Q}}$ replaced by $G := \mathrm{Gal}(K/\mathbb{Q})$ where K is some finite Galois extension of $\mathbb{Q}$ (which can be taken equal to the compositum of two finite Galois extensions where ρ_1 and ρ_2 factor through). Let $\sigma \in G$. By the Chebotarev density theorem we get $\sigma = \mathrm{Frob}_p$ (modulo conjugation) for infinitely many primes p, so in particular for a prime p with $\mathrm{Trace}(\rho_1(\mathrm{Frob}_p)) = \mathrm{Trace}(\rho_2(\mathrm{Frob}_p))$ and $\mathrm{Det}(\rho_1(\mathrm{Frob}_p)) = \mathrm{Det}(\rho_2(\mathrm{Frob}_p))$. So $\rho_1(\sigma)$ and $\rho_2(\sigma)$ have the same characteristic equation. Now by the Brauer-Nesbitt theorem [CR, Theorem 30.16], ρ_1 and ρ_2 are isomorphic. □

For the lemma above, note, that if the characteristic of $\mathbb{F}$ is not 2, then the equality between the determinants is already implied by the equality between the traces.

Galois representations attached to elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve and $n \in \mathbb{Z}_{>0}$. The absolute Galois group $G_{\mathbb{Q}}$ acts in a natural way on $E[n]$ (the $\mathbb{Z}/n\mathbb{Z}$ module consisting of the n-torsion points of E), inducing a homomorphism $G_{\mathbb{Q}} \to \mathrm{Aut}(E[n])$. By choosing a basis for $E[n]$, we can identify $\mathrm{Aut}(E[n])$ with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. In this way we get a Galois representation

$$\rho_n^E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

which is unique up to conjugation (i.e. depends on the chosen basis above). Let $K := \mathbb{Q}(E[n])$, then ρ_n^E factors through $\mathrm{Gal}(K/\mathbb{Q})$ and ρ_n^E is ramified at a prime p if and only if p is ramified in K. The case $n = l$ a prime is of most interest to us. The following theorem gives us very useful arithmetic information about ρ_l^E.

Theorem 17. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and let l, p be primes. If $p \nmid lN$, then the Galois representation $\rho_l^E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_l)$ is unramified at p and*

$$\mathrm{Trace}(\rho_l^E(\mathrm{Frob}_p)) \equiv a_p(E) \pmod{l}, \tag{2.1}$$

$$\mathrm{Det}(\rho_l^E(\mathrm{Frob}_p)) \equiv p \pmod{l}. \tag{2.2}$$

Furthermore, if $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_l)$ is another Galois representation satisfying (2.1) and (2.2), then the semisimplifications of ρ' and ρ_l^E are isomorphic.

Proof. The last statement follows immediately from Lemma 16. For the rest, see the proof of [DS, Theorem 9.4.1] (where we only need to consider $E[l^n]$ for $n = 1$). □

If $p|N$, then it may still happen that ρ_l^E is unramified at p. We will give some criteria for this to happen and give the trace (and determinant) of Frobenius in that case. Before we go into this, we need to say a bit more about $\mathrm{Det}(\rho_l^E)$. For this we consider the cyclotomic character of order l, $\chi_l : G_{\mathbb{Q}} \to \mathbb{F}_l^*$, determined by $\sigma(\zeta_l) = \zeta_l^{\chi_l(\sigma)}$, $\sigma \in G_{\mathbb{Q}}$ and where ζ_l denotes a primitive l-th root of unity.

Lemma 18. *Let $E/\mathbb{Q}$ be an elliptic curve and let l, p be primes. If $p \neq l$, then χ_l is unramified at p and*

$$\chi_l(\mathrm{Frob}_p) \equiv p \pmod{l}. \tag{2.3}$$

Furthermore,

$$\mathrm{Det} \circ \rho_l^E = \chi_l. \tag{2.4}$$

Proof. Note that χ_l factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$. Since $p \neq l$, the Galois extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ is unramified at p, hence χ_l is unramified at p. Also, $\zeta_l \pmod{\mathfrak{P}}$ remains a primitive l-th root of unity in $\mathbb{Z}[\zeta_l]/\mathfrak{P}$ for a prime $\mathfrak{P} \subset \mathbb{Z}[\zeta_l]$ lying above p. So from $\mathrm{Frob}_p(\zeta_l) \equiv \zeta_l^p \pmod{\mathfrak{P}}$, we get $\chi_l(\mathrm{Frob}_p) \equiv p \pmod{l}$.

Together with (2.2) we see that (at least) for all primes $p \nmid lN$ (with N the conductor of E), the one dimensional Galois representations $\mathrm{Det} \circ \rho_l^E$ and χ_l take the same values at Frob_p. It follows, as in the proof of Lemma 16, that $\mathrm{Det} \circ \rho_l^E = \chi_l$. (Alternatively, one can first use basic properties of the Weil pairing to show that $\mathrm{Det} \circ \rho_l^E = \chi_l$ and then deduce (2.3) from this and (2.2).) □

Proposition 19. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and minimal discriminant Δ and let l, p be primes. Suppose that $p \neq l$ and $p||N$. Then ρ_l^E is unramified at p if and only if $\nu_p(\Delta) \equiv 0 \pmod{l}$. Moreover, if ρ_l^E is unramified at p, then*

$$\begin{aligned} \mathrm{Trace}(\rho_l^E(\mathrm{Frob}_p)) &\equiv a_p(E)(1+p) \equiv \pm(1+p) \pmod{l}, \\ \mathrm{Det}(\rho_l^E(\mathrm{Frob}_p)) &\equiv p \pmod{l}. \end{aligned}$$

Proof. That ρ_l^E is unramified at p if and only if $\nu_p(\Delta) \equiv 0 \pmod{l}$ follows from the theory of Tate curves (see [Sil2, Chapter V]). That $\mathrm{Det}(\rho_l^E(\mathrm{Frob}_p)) \equiv p \pmod{l}$ follows immediately form Lemma 18. From [KO, Lemme 1] we have that a_p is a characteristic root of $\rho_l^E(\mathrm{Frob}_p)$. Since $p||N$ we have $a_p = \pm 1$ and together with the value of $\mathrm{Det}(\rho_l^E(\mathrm{Frob}_p))$ we get $\mathrm{Trace}(\rho_l^E(\mathrm{Frob}_p)) \equiv a_p(E)(1+p) \pmod{l}$. □

Galois representations attached to modular forms

Attaching Galois representations to modular forms instead of elliptic curves is somewhat more involved and we will not give the construction here. The existence, uniqueness and useful arithmetic properties are given in the following theorem.

Theorem 20. *Let f be a newform of level N, let l be a prime, $\mathfrak{L} \subset \mathcal{O}_f$ a prime lying above l and denote by $\mathbb{F}$ the finite residue field $\mathcal{O}_f/\mathfrak{L}$. Then there exists a semisimple Galois representation*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$$

such that for all primes p with $p \nmid Nl$ the Galois representation ρ is unramified at p and

$$\mathrm{Trace}(\rho(\mathrm{Frob}_p)) \equiv a_p(f) \pmod{\mathfrak{L}}, \tag{2.5}$$

$$\mathrm{Det}(\rho(\mathrm{Frob}_p)) \equiv p \pmod{\mathfrak{L}}. \tag{2.6}$$

Furthermore, if $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ is another semisimple Galois representation satisfying (2.5) and(2.6), then ρ' is isomorphic to ρ.

Proof. In paragraph 9.5 of [DS] it is shown how to construct a so called l-adic Galois representation $\hat{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\mathfrak{L}})$, where $K_{f,\mathfrak{L}}$ denotes the local field obtained by completing K_f at $\mathfrak{L}$. By Proposition 9.3.5 of *loc. cit.* we may assume that the image of $\hat{\rho}$ lands in $\mathrm{GL}_2(\mathcal{O}_{f,\mathfrak{L}})$, where $\mathcal{O}_{f,\mathfrak{L}}$ denotes the local ring obtained by completing $\mathcal{O}_f$ at $\mathfrak{L}$. The reduction $\mathcal{O}_{f,\mathfrak{L}} \to \mathcal{O}_{f,\mathfrak{L}}/\mathfrak{L} \simeq \mathcal{O}_f/\mathfrak{L} = \mathbb{F}$ induces a Galois representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ and the semisimplification of this Galois representation gives us the ρ from the theorem. The desired properties of ρ follow immediately from the properties of $\hat{\rho}$ given in Theorem 9.5.4 and the construction of ρ from it. The last statement follows immediately from Lemma 16. □

The Galois representation ρ from the theorem above will from now on be denoted by $\rho^f_{\mathfrak{L}}$. Note that if $E/\mathbb{Q}$ is an elliptic curve such that ρ^E_l is not semisimple for a certain prime l and f is a newform such that $a_p(E) = a_p(f)$ for all primes p, then ρ^f_l is not isomorphic to ρ^E_l (since by construction ρ^f_l is semisimple), but ρ^f_l is isomorphic to the semisimplification of ρ^E_l.

Remark 21. The newform in the theorem above has (by convention) weight 2 and trivial character. If f is a newforms w.r.t. $\Gamma_1(N)$, say with character χ, and weight $k \in \mathbb{Z}_{\geq 2}$, the theorem still holds with (2.6) replaced by

$$\mathrm{Det}(\rho(\mathrm{Frob}_p)) \equiv \chi(p)p^{k-1} \pmod{\mathfrak{L}}.$$

For weight $k = 2$, this also follows from [DS, paragraph 9.5]. For weight $k > 2$ see [Del], again, an l-adic representation is constructed and the mod l representation is obtained by reduction (due to Deligne and Serre there is also a construction of certain Galois representations attached to weight one forms).

2.1.2 Irreducibility

In theorems about so called level lowering of modular Galois representations ρ, one of the conditions that must be satisfied is that ρ is irreducible. The following theorems give some sufficient conditions for Galois representations attached to elliptic curves to be irreducible.

Theorem 22. *Let $E/\mathbb{Q}$ be an elliptic curve with j-invariant j and let l be a prime. Then the Galois representation ρ_l^E is irreducible if (at least) one of the following conditions holds*

i. $l = 11$ *or* $l \geq 17$ *(i.e. the genus of $X_0(l)$ is nonzero) and the pair (l, j) has no corresponding entry in Table 2.1,*

ii. E has a rational 2-torsion point, $l \geq 7$ and

$$(l, j) \neq (7, -3^3 \cdot 5^3), (7, 3^3 \cdot 5^3 \cdot 17^3),$$

iii. $l \geq 5$*, E is semistable and all 2-torsion points are rational,*

iv. $l \geq 11$ *and E is semistable.*

Proof. i. If ρ_l^E is reducible, this would give rise to a noncuspidal rational point on $X_0(l)$. If $l = 11$ or $l \geq 17$, then according to [Maz2, Theorem 7.1] there are no noncuspidal rational points on $X_0(l)$, except when $l = 11, 17, 19, 37, 43, 67, 163$ respectively in which case there are $3, 2, 1, 2, 1, 1, 1$ such points respectively. Using [BK, pp. 79,80] and [Cre2] a representing elliptic curve corresponding to these points is easily found. In the notation of *loc. cit.* we can take for example the elliptic curves 121b1, 121c1, 121c2, 14450bk1, 14450bk2, 361a1, 1225h1, 1225h2, 1849a1, 4489a1 and 26569a1. The j-invariants of these elliptic curves are given in Table 2.1 (note that in [BK] the j-invariant of a curve with a rational 19-isogeny is not given correctly).

ii. One checks that if $l = 11$ or $l \geq 17$, then the elliptic curves with a rational l-isogeny mentioned above, have no rational 2-isogeny. So if ρ_l^E is reducible for $l \geq 7$ and E has a rational 2-torsion point, this would give rise to a noncuspidal rational point on $X_0(2l)$ for $l = 7, 13$. Now [MV] tells us that there are no such point on $X_0(26)$. According to [Lig, Chapter 5] $X_0(14)$ has 6 rational points, 4 of these are cusps. As before, 2 elliptic curves corresponding to the 2 noncuspidal rational points on $X_0(14)$ are easily found. We can take the elliptic curves 49a1 and 49a2 respectively, which have j-invariant $-3^3 \cdot 5^3$ and $3^3 \cdot 5^3 \cdot 17^3$ respectively.

iii. This is essentially [Ser2, Proposition 6], but for the convenience of the reader we give a proof here. Suppose that ρ_l^E is reducible for $l \geq 5$, then E has a rational l-isogeny, say with kernel X. Since E is semistable [Ser1, p. 307] tells us that E or E/X has a rational l-torsion point. But E and E/X also have full rational 2-torsion. So the rational torsion group of E or E/X contains

a group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times Z/2l\mathbb{Z}$. But by the classification of torsion groups of elliptic curves over $\mathbb{Q}$, [Maz1, Theorem 8] or [Maz2, Theorem 2], this is impossible for $l \geq 5$.

iv. This is essentially the same argument as before, but now we use that the rational torsion group of an elliptic curve over $\mathbb{Q}$ cannot contain a cyclic subgroup of prime order ≥ 11.

□

l	j
11	$-2^{15}, -11^2, -11 \cdot 131^3$
17	$-17 \cdot 373^3/2^{17}, -17^2 \cdot 101^3/2$
19	$-2^{15} \cdot 3^3$
37	$-7 \cdot 11^3, -7 \cdot 137^3 \cdot 2083^3$
43	$-2^{18} \cdot 3^3 \cdot 5^3$
67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

Table 2.1: Pairs (l, j) corresponding to rational isogenies

The theorem above was mainly obtained from knowledge of rational points on modular curves. The following theorem follows from representation theoretic considerations. We note that for $p = 2$ it was already stated as [Sik, Theorem 5].

Theorem 23. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and let $p = 2, 3$. If $\nu_p(N) \geq 3$ and odd, then ρ_l^E is irreducible for all primes $l \neq p$.*

Proof. Since $\nu_p(N) \geq 3$ and odd, the wild conductor exponent at p is odd. By the proof of [DK, Lemma 3] it follows that for $l \neq p$ the restriction of ρ_l^E to an inertia subgroup I_p of p is irreducible and hence ρ_l^E itself is irreducible. □

In section 3.2 we describe some more situations in which ρ_l^E is irreducible. Finally, we want to say something about the absolute irreducibility of ρ_l^E.

Lemma 24. *Let $E/\mathbb{Q}$ be an elliptic curve and let l be an odd prime. Then ρ_l^E is absolutely irreducible if and only if ρ_l^E is irreducible.*

Proof. If ρ_l^E is absolutely irreducible, then ρ_l^E is of course irreducible. So suppose that ρ_l^E is not absolutely irreducible. Let $c \in G_{\mathbb{Q}}$ denote complex conjugation. From the definition of the cyclotomic character it follows immediately that $\chi_l(c) = -1$, together with (2.4) we obtain that $\mathrm{Det}(\rho_l^E(c)) = -1$ (i.e. ρ_l^E is odd). Since c has order 2 we now obtain that $\rho_l^E(c)$ has eigenvalues $+1, -1$. Furthermore, $-1 \neq 1$ (since l is odd), so we get that $\rho_l^E(c)$ has two 1-dimensional eigenspaces, generated by, say, $v_+, v_- \in \mathbb{F}_l^2$. From the absolute reducibility of ρ_l^E we get that ρ_l^E leaves invariant a one dimensional subspace of $\overline{\mathbb{F}_l}^2$, generated by, say, $w \in \overline{\mathbb{F}_l}^2$. In particular w is an eigenvector of $\rho_l^E(c)$, hence v_+ or v_- is a scalar multiple of w and we obtain a 1-dimensional subspace of $\mathbb{F}_l^2$ left invariant by ρ_l^E, i.e. ρ_l^E is not irreducible. □

We want to mention that there exist elliptic curves $E/\mathbb{Q}$ such that $\rho_2^E : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_2)$ is irreducible, but over $\mathbb{F}_4$ it becomes reducible. In fact, E has this property, exactly when the image of ρ_2^E is $\mathrm{GL}_2(\mathbb{F}_2)$ has order 3. In that case, the image is generated by $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, which is diagonalizable over $\mathbb{F}_4$. An explicit example is given by $E : y^2 = x^3 - x^2 - 2x + 1$.

2.1.3 Modularity

Definition 25. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Then E is said to be *modular* if there exists a newform f of level N such that $a_p(E) = a_p(f)$ for all primes p.

Theorem 26. *Every elliptic curve over $\mathbb{Q}$ is modular.*

Proof. See [BCDT]. □

Remark 27. For semistable elliptic curves the theorem was of course proved in the celebrated papers [Wil] and [TW]. Furthermore, there are various equivalent ways to define the notion of modular (for an elliptic curve over $\mathbb{Q}$), see for example [DI, Theorem 13.0.5].

The modularity of elliptic curves over $\mathbb{Q}$ can be seen as a converse to a theorem due to Eichler and Shimura.

Theorem 28 (Eichler-Shimura). *Let f be a newform of level N. If f is rational, then there exists an elliptic curve $E/\mathbb{Q}$ of conductor N, such that $a_p(E) = a_p(f)$ for all primes p.*

Proof. See [DS, Chapter 8]. □

(In general, the Eichler-Shimura correspondence associates to a newform f a certain abelian variety over $\mathbb{Q}$ of dimension $[K_f : \mathbb{Q}]$.) The elliptic curve in the theorem is determined uniquely up to isogeny over $\mathbb{Q}$. In this way we get for all $N \in \mathbb{Z}_{>0}$ an injective function from the set of rational newforms of level N to the set of isogeny classes of elliptic curves over $\mathbb{Q}$ of conductor N. From Theorem 26 we obtain that this function is actually bijective. Given a newform f, any elliptic curve $E/\mathbb{Q}$ such that $a_p(E) = a_p(f)$ for all primes p will simply be called an elliptic curve *associated* to f.

Definition 29. Let $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F})$ be an absolutely irreducible Galois representation, where $\mathbb{F}$ is a finite field of characteristic l and let $N \in \mathbb{Z}_{>0}$. Then ρ is called *modular of level N*, if there exists a newform f of level N and a prime $\mathfrak{L} \subset \mathcal{O}_f$ lying above l such that $\rho \simeq \rho_\mathfrak{L}^f$.

Following e.g. [Rib1] and [DS], we have chosen to consider really a newform (of weight 2 and trivial character, by convention) instead of just an eigenform in the definition above.

Corollary 30. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N, let l be a prime and suppose that ρ_l^E is absolutely irreducible. Then ρ_l^E is modular of level N.*

Proof. By Theorem 26 there exists a newform f of level N with $a_p(E) = a_p(f)$ for all primes p, in particular $\mathcal{O}_f = \mathbb{Z}$. So according to Theorems 17 and 20, we get semisimple (because ρ_l^E is irreducible) Galois representations $\rho_l^E, \rho_l^f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_l)$, satisfying $\mathrm{Trace}(\rho_l^E(\mathrm{Frob}_p)) = \mathrm{Trace}(\rho_l^f(\mathrm{Frob}_p))$ and $\mathrm{Det}(\rho_l^E(\mathrm{Frob}_p)) = \mathrm{Det}(\rho_l^E(\mathrm{Frob}_p))$ for all primes $p \nmid Nl$. Now Lemma 16 gives us that $\rho_l^E \simeq \rho_l^f$, hence ρ_l^E is modular. □

2.1.4 Level lowering

Let ρ be a 2-dimensional Galois representation and let p be a prime. There exists a notion of ρ being *finite* at p. For a Galois theoretic description of finiteness, see pages 185,186 of [Ser2] (where it is called *peu ramifiée*). A characterization in terms of group schemes is given in *loc. cit.* on page 189. See also [Edi, Propostion 8.2] for some equivalent characterizations and proofs of these. We will only need finiteness in one particular situation, which is described in the following proposition.

Proposition 31. *Let $E/\mathbb{Q}$ be an elliptic curve with minimal discriminant $\Delta_{\min}$. Suppose E has multiplicative reduction at a prime p. If for a prime l we have $l|\nu_p(\Delta_{\min})$, then ρ_l^E is finite at p.*

Proof. This follows from the theory of Tate curves, see [Ser2, Propositions 4,5]. □

The main theorem we need on level lowering of modular Galois representations is the following.

Theorem 32 (Ribet). *Let $\mathbb{F}$ be a finite field of characteristic $l \geq 3$ and let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ be an irreducible Galois representation. Suppose that ρ is modular of level N. If p is a prime with $p||N$ and such that ρ is finite at p, then ρ is modular of level N/p.*

Proof. In [Rib1, Thm. 1.1] the theorem is proved in case that $p \not\equiv 1 \pmod{l}$ (or $l \not| N$), so in particular it holds for $p = l$. In [Rib2, Thm. 1.5] the theorem is proved for $p \neq l$. □

Remark 33. The case $p \not\equiv 1 \pmod{l}$ is actually due to Barry Mazur. Furthermore, for most of our applications we have that ρ_l^f is finite at l and then [Rib1, Thm. 1.1] suffices for our application. For some generalizations, see e.g. [Dia].

Definition 34. Let $E/\mathbb{Q}$ be an elliptic curve and l an odd prime. Define

$$N_0(E, l) := N / \prod_{\substack{p \| N \\ l | \nu_p(\Delta_{\min})}} p, \tag{2.7}$$

where N and $\Delta_{\min}$ denote the conductor and minimal discriminant respectively of E. Furthermore, for a newform f we write

$$E \sim_l f, \tag{2.8}$$

if there exists a prime $\mathfrak{L} \subset \mathcal{O}_f$ lying above l such that $\rho_l^E \simeq \rho_{\mathfrak{L}}^f$. For an elliptic curve $E'/\mathbb{Q}$ we write

$$E \sim_l E'$$

if $\rho_l^E \simeq \rho_l^{E'}$.

By combining modularity and level lowering in the case of elliptic curves, we obtain the following very useful theorem.

Theorem 35. *Let $E/\mathbb{Q}$ be an elliptic curve and let l be an odd prime. Suppose that ρ_l^E is irreducible. Then there exists a newform f of level $N_0(E,l)$ such that $E \sim_l f$.*

Proof. From Lemma 24 we obtain that ρ_l^E is absolutely irreducible. By Corollary 30 we get that ρ_l^E is modular of level N (with N the conductor of E). For all primes p with $p||N$ and $l|\nu_p(\Delta_{\min})$, where $\Delta_{\min}$ denotes the minimal discriminant of E, Proposition 31 tells us that ρ_l^E is finite at p. By repeatedly using Theorem 32, we get that ρ_l^E is modular of level $N_0(E,l)$. □

If $E \sim_l f$ as in the theorem above, then we obtain valuable congruence relations between $a_p(E)$ and $a_p(f)$ as follows.

Theorem 36. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N, let l be an odd prime and write $N_0 := N_0(E,l)$. Suppose that $\rho_l^E \simeq \rho_{\mathfrak{L}}^f$ for a newform f of level N_0 and a prime $\mathfrak{L} \subset \mathcal{O}_f$ lying above l. Then*

- *for all primes p with $p \nmid Nl$*

$$a_p(f) \equiv a_p(E) \pmod{\mathfrak{L}},$$

- *for all primes p with $p \nmid N_0 l$ and $p|N$*

$$a_p(f) \equiv a_p(E)(1+p) \equiv \pm(1+p) \pmod{\mathfrak{L}}.$$

If furthermore $\mathcal{O}_f = \mathbb{Z}$, then

- *for all primes p with $p \nmid N$*

$$a_p(f) \equiv a_p(E) \pmod{l},$$

- *for all primes p with $p \nmid N_0$ and $p|N$*

$$a_p(f) \equiv a_p(E)(1+p) \equiv \pm(1+p) \pmod{l}.$$

Proof. The first part of the theorem (for general $\mathcal{O}_f$) follows by comparing traces of Frobenius using Theorems 17 and 20 and Proposition 19. If $\mathcal{O}_f = \mathbb{Z}$, then $\rho_{\mathfrak{L}}^f \simeq \rho_l^{E'}$ for some elliptic curve E' of conductor N_0 and the theorem follows from [KO, Proposition 3]. □

For computational purposes we want to rephrase the theorem above slightly and also note some inequalities. Let p be a prime and denote by $F_p(x)$ the characteristic polynomial of $a_p(f)$ w.r.t. the extension $K_f/\mathbb{Q}$. So if we denote by $\sigma_1, \ldots, \sigma_d$ the embeddings of K_f in $\mathbb{R}$, then $F_p(x) = \prod_{i=1}^{d}(x - \sigma_i(a_p(f)))$. If $\mathcal{O}_f = \mathbb{Z}$, then of course simply $F_p(x) = x - a_p(f)$.

Theorem 37. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N, let l be an odd prime and write $N_0 := N_0(E, l)$. Suppose $E \sim_l f$ for a newform of level N_0. Let $p \nmid N_0$ be a prime and also suppose $p \neq l$ if f is not rational. Denote by $F_p(x)$ the characteristic polynomial of $a_p(f)$ w.r.t. the extension $K_f/\mathbb{Q}$.*

- *If $p \nmid N$, then $l | F_p(a_p(E))$.*
- *If $p | N$, then $l | F_p(\pm(1+p))$.*

Furthermore, if $p|N$ or $a_p(E) \neq a_p(f)$, then

$$l < (1 + \sqrt{p})^{2[K_f:\mathbb{Q}]}.$$

Proof. Note that if $a \equiv a_p(f) \pmod{\mathfrak{L}}$ for some $a \in \mathbb{Z}$, then

$$\begin{aligned} l \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(a - a_p(f)) &= \prod_{i=1}^{d} \sigma_i(a - a_p(f)) \\ &= \prod_{i=1}^{d} (a - \sigma_i(a_p(f))) \\ &= F_p(a). \end{aligned}$$

Consider the case $p \nmid N$. Theorem 36 gives us that $a_p(E) \equiv a_p(f) \pmod{\mathfrak{L}}$, so we get $l | F_p(a_p(E))$. If $a_p(E) \neq a_p(f)$ we have $F_p(a_p(E)) = \mathrm{Norm}(a_p(E) - a_p(F)) \neq 0$. Also $|a_p(E)|, |\sigma_i(a_p(f))| < 2\sqrt{p}$, so

$$\begin{aligned} l &\leq |F_p(a_p(E))| = \prod_{i=1}^{d} |a_p(E) - \sigma_i(a_p(f))| \\ &< (4\sqrt{p})^d \\ &< (1 + p + 2\sqrt{p})^d = (1 + \sqrt{p})^{2d}. \end{aligned}$$

Now consider the case $p|N$. Theorem 36 gives us that $a_p(E) \equiv \pm(1+p) \pmod{\mathfrak{L}}$, so we get $l | F_p(\pm(1+p))$. For all primes p we have $|a_p(f)| < 2\sqrt{p} < 1 + p$, so $a_p(f) \neq \pm(1+p)$ and hence $F_p(\pm(1+p)) = \mathrm{Norm}(\pm(1+p) - a_p(f)) \neq 0$. So

$$\begin{aligned} l &\leq |F_p(\pm(1+p))| = \prod_{i=1}^{d} |\pm(1+p) - \sigma_i(a_p(f))| \\ &< (1 + p + 2\sqrt{p})^d = (1 + \sqrt{p})^{2d}. \end{aligned}$$

□

2.2 Applying the modular method

Let $f \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$, let l denote an odd prime and define

$$P_l(x_1, \ldots, x_n, y_1, \ldots, y_m) := f(x_1, \ldots, x_n, y_1^l, \ldots, y_m^l).$$

We are interested in solving

$$P_l(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \quad x_i, y_i \in \mathbb{Z} \tag{2.9}$$

for infinitely many l (an exponential Diophantine equation) or sometimes in solving it for one particular l. Possibly some extra conditions (like $y_i \neq 0$ or gcd-conditions) are imposed. A typical example is

$$f(x, y) = cz^l \quad x, y, z \in \mathbb{Z} \quad \gcd(x, y, z) = 1, z \neq 0, \tag{2.10}$$

where $f \in \mathbb{Z}[x, y]$ is homogeneous and $c \in \mathbb{Z} - \{0\}$. However, only very specific equations from the example above can be handled by the modular (or any other) method.

The starting point of using the machinery of elliptic curves and modular forms to study (2.9) is the construction of an elliptic curve associated to a hypothetical solution satisfying certain properties (to be described in a moment). Such elliptic curves are often called Hellegouarch-Frey curves (or Frey-Hellegouarch curves) or simply Frey curves. For brevity we shall use the latter terminology. One can consider a Frey curve as an elliptic curve $E_{x_1,\ldots,x_n,y_1,\ldots,y_m}$, or simply $E_{\{x_i,y_i\}}$, given by an equation $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ where the coefficients $a_i = a_i(x_1, \ldots, x_n, y_1, \ldots, y_m)$ are functions of the x_i, y_i from $\mathbb{Z}^{n+m}$ to $\mathbb{Z}$ (in practice the a_i are given by finitely many polynomials in x_i, y_i^l over $\mathbb{Q}$). Furthermore, there must exist a finite set S of primes, not depending on the x_i, y_i, and not depending on l if we consider an exponential Diophantine equation, such that when we now specialize to a hypothetical solution $x_1, \ldots, x_n, y_1, \ldots, y_m \in \mathbb{Z}$, we have that $E := E_{x_1,\ldots,x_n,y_1,\ldots,y_m}$ is nonsingular and if it has bad reduction at a prime $p \notin S$, then the reduction at p is multiplicative and $l | \nu_p(\Delta_{\min})$, where $\Delta_{\min}$ denotes the minimal discriminant of E. In this situation, the conductor N of E is of the form $N_0 \prod_{i=1}^m p_i$ where the primes dividing N_0 are elements of S and the p_i are primes for which $p_i \notin S$ and $l | \nu_{p_i}(\Delta_{\min})$. Suppose we can prove that ρ_l^E is irreducible, then by Theorem 35 we now see that $E \sim_l f$ for some newform f of level N_0. There are only finitely many possibilities for N_0 and only finitely many newforms per level, this gives us only finitely many possibilities for our newforms f. Thus in order to prove that (2.9) (possibly with some extra conditions) has no solutions, it suffices to show that for these finitely many f we cannot have $E \sim_l f$. Instead of proving directly that there are no solutions, this method might also provide valuable information about possible solutions. Many concrete examples will appear in the rest of this chapter and the next chapter.

We will restrict our attention to Frey curves defined over $\mathbb{Q}$. For the first application of Frey curves with only the isogeny class defined over $\mathbb{Q}$ (so called $\mathbb{Q}$-curves) to solve generalized Fermat equations we refer to [Ell]. For ideas about Frey hyperelliptic curves (and much more) we refer to [Dar].

2.2.1 No newforms

If after level lowering one ends up at a level at which there are no newforms, then a contradiction is immediately obtained. These levels are known explicitly as follows.

Proposition 38. *Let $N \in \mathbb{Z}_{>0}$. Then there are no newforms of level N if and only if $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60\}$.*

Proof. The dimension of $S_2^{\text{new}}(\Gamma_0(N))$ is given by an explicit recursive formula from which the result follows in a straightforward matter. See e.g. [Mar]. □

Example 39 (Fermat's last theorem). This is the 'canonical example', so let us quickly describe it here. Suppose there exist $x, y, z, n \in \mathbb{Z}$ with $xyz \neq 0$, $n \geq 4$ and $x^n + y^n = z^n$. We can assume that $(x, y, z) = 1$ and that $l := n \geq 5$ is prime (for $n = 3, 4$ the equation already is known to have no solutions). We can also assume that y is even and $x \equiv -1 \pmod 4$. To our hypothetical solution we associate the Frey curve

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

The discriminant of E equals $2^4(xyz)^{2l}$, which is nonzero, so E is indeed an elliptic curve. As shown in appendix A, the model is minimal at all primes, except at 2 and for the minimal discriminant of E and the conductor we have

$$\Delta_{\min} = \frac{(xyz)^{2l}}{2^8}, \qquad N = \operatorname{rad}(xyz). \tag{2.11}$$

We see that E is semistable and that all 2-torsion points are rational, so ρ_l^E is irreducible by Theorem 22. From (2.11) we obtain that $N_0(E, l) = 2$. So Theorem 35 tells us that ρ_l^E is modular of level 2. But according to Proposition 38 there are no newforms of level 2, a contradiction which proves Fermat's last theorem.

2.2.2 Different a_p's

Suppose we are in the situation of Theorem 37 with $E = E_{\{x_i, y_i\}}$ some Frey curve associated to a hypothetical solution (2.9) (possibly with some extra conditions). A first approach to restrict the possibilities of l is as follows. For simplicity we shall assume that for a prime $p \nmid N_0$ the reduction of $E_{\{x_i, y_i\}}$ modulo p only depends on the x_i, y_i modulo p. In this case $a_p(E_{\{x_i, y_i\}})$ also only depends on the x_i, y_i modulo p. We shall also assume that for the x_i, y_i under consideration $E_{\{x_i, y_i\}}$ is indeed an elliptic curve (i.e. it is nonsingular), possible x_i, y_i which do not meet this criterion have to be considered separately (if possible). Now for the finitely many x_i, y_i modulo p under consideration such that $E_{\{x_i, y_i\}}$ has good reduction at p, we calculate the possible $a_p(E_{\{x_i, y_i\}})$. If all these values differ from $a_p(f)$, we are left by Theorem 37 with only finitely many possibilities for l for which $E \sim_l f$. We can of course try different primes p and combine the information. In general there might a priori be multiple possibilities for the newform f and the level N_0. For all these possibilities the above approach can of course be repeated.

We remark that if $\mathcal{O}_f \neq \mathbb{Z}$, then $a_p(E) \neq a_p(f)$ for infinitely many p, since then $a_p(f) \notin \mathbb{Z}$ for infinitely many p (and $a_p(E) \in \mathbb{Z}$ for all p). In fact, a bound on the smallest prime $p \nmid N_0$ such that $a_p(f) \notin \mathbb{Z}$ for a nonrational f is easily obtained by considering $f - \bar{f}$ for some conjugate $\bar{f}$ of f (see [Kra3, Lemme 1]), we have

$$p \leq \frac{N_0}{6} \prod_{\text{primes } q|N_0} \left(1 + \frac{1}{q}\right).$$

We also note that $[K_f : \mathbb{Q}]$ can be bounded above in terms of N_0, namely

$$[K_f : \mathbb{Q}] \leq \dim S^{\text{new}}(N_0) \leq \frac{N_0 + 1}{12},$$

where the last inequality comes from [Mar, Theorem 2]. Together with the bound on l from Theorem 37 we get a bound on l in terms of only N_0. Knowing the actual q-expansion of f may lead in practice to a much better bound.

Example 40 (The equation $x^2 - 11 = y^l$). Consider the equation

$$x^2 - 11 = y^l \quad x, y \in \mathbb{Z}$$

where l denotes an odd prime. For a hypothetical solution (x, y) we consider the Frey curve

$$E_x : Y^2 = X^3 - 4xX^2 + 4(x^2 - 11)X \tag{2.12}$$

(it is a twist over $\mathbb{Q}(\sqrt{2})$ of the Frey curve (3.24)). According to appendix A we get for the minimal discriminant and conductor of E_x that

$$\begin{aligned} \Delta_{\min}(E_x) &= 2^{12} \cdot 11(x^2 - 11)^2 = 2^{12} \cdot 11 y^{2l}, \\ N(E_x) &= 2^5 \cdot 11 \operatorname{rad}_{\{2,11\}}(x^2 - 11) = 2^5 \cdot 11 \operatorname{rad}_{\{2,11\}}(y). \end{aligned}$$

So $N_0(E_x, l) = 2^5 \cdot 11$. Now assume $l \geq 7$. Using Theorem 22, we easily obtain that $\rho_l^{E_x}$ is irreducible. So we have $E \sim_l f$ for some newform f of level 352. At level 352 there are 6 rational newforms and 2 conjugacy classes of nonrational ones. For a rational newform f we get $a_3(f) \in \{\pm 1, \pm 3\}$. For a nonrational newform f, the characteristic equation for $a = a_3(f)$ reads $a^2 \pm a - 4 = 0$. Since 11 is not a square mod 3, E_x must have good reduction modulo 3 and by plugging in the values $x' = 0, 1, 2$ into $E_{x'}$, we obtain $a_3(E_x) \in \{-2, 0, 2\}$. Theorem 37 and an elementary computation now gives us that $l < 7$. We have proved the following.

Proposition 41. *The equation $x^2 - 11 = y^l$ has no solutions for $x, y \in \mathbb{Z}$ and $l \geq 7$ prime.*

Note that we do have a solution with $l = 5$, namely $56^2 - 11 = 5^5$.

A typical problem that may arise in this method, is that for certain x_i', y_i' (not necessarily related to some solution of (2.9)) we have that $E' := E_{\{x_i', y_i'\}}$ has conductor equal to some a priori possible level N_0. In that case the method can not eliminate the possibility that $E_{\{x_i, y_i\}} \sim_l E'$ for any l.

If f is not rational (i.e. $\mathcal{O}_f \neq \mathbb{Z}$), then as remarked above, we are guaranteed to find infinitely many primes $p \nmid N_0$ such that $a_p(E_{\{x_i,y_i\}}) \neq a_p(f)$. If f is rational, with associated elliptic curve E', then in general there is no a priori reason why we should find any such prime p. However, if the torsion structure of the isogeny classes of $E_{\{x_i,y_i\}}$ and E' are sufficiently different, then we are guaranteed to find infinitely many primes $p \nmid N_0$ such that $a_p(E_{\{x_i,y_i\}}) \neq a_p(E') = a_p(f)$. To make this more precise we have the following.

Proposition 42. *Let $E/\mathbb{Q}$ be an elliptic curve and let $m \in \mathbb{Z}_{>0}$. Then the following statements are equivalent.*

i. For all primes p where E has good reduction we have $m|p+1-a_p(E)$.

ii. For a set of primes p with (Dirichlet) density 1 we have $m|p+1-a_p(E)$.

iii. There exists an elliptic curve $F/\mathbb{Q}$ isogenous over $\mathbb{Q}$ to E with $m|\#F(\mathbb{Q})_{\text{tors}}$.

Proof. See Theorem 2 and the appendix of [Kat]. (In fact, an appropriate generalization to number fields is proven there.) □

If now $m|\#E(\mathbb{Q})_{\text{tors}}$ for some $m \in \mathbb{Z}_{\geq 2}$, but $m \nmid \#E''(\mathbb{Q})_{\text{tors}}$ for all elliptic curves $E''/\mathbb{Q}$ isogenous to E', then according to the theorem above we have $a_p(E) \equiv p+1 \pmod{m}$ for all but finitely many primes p and $a_p(E') \not\equiv p+1 \pmod{m}$ for infinitely many primes p. So $a_p(E) \neq a_p(E')$ for infinitely many primes p. In case E is a Frey curve and E' a curve at level N_0 (so E' and N_0 are known explicitly), arbitrarily many primes $p \nmid N_0$ with $a_p(E') \not\equiv p+1 \pmod{m}$ can be found explicitly, giving explicit restrictions on l for which $E \sim_l E'$. In fact, an upper bound for the smallest prime $p \nmid N_0$ such that $a_p(E') \not\equiv p+1 \pmod{m}$ can easily be given in terms of N_0. In the situation where the roles of E and E' are reversed, much less is known explicitly, since the conductor of a Frey curve depends on some hypothetical solution.

Example 43. Recall the previous example. The Frey curve E_x from (2.12) obviously has a rational 2-torsion point. But the 6 elliptic curves of conductor 352 associated to the 6 rational newforms of level 352 all have no rational 2-torsion. So a priori we are guaranteed to find for every elliptic curve E' of conductor 352 a prime $p \neq 2, 11$ such that $a_p(E') \neq a_p(E_{x'})$ for all $x' \in \mathbb{Z}$ with $p \nmid x'^2 - 11$. In practice, we see that $a_3(E')$ is odd for all the 6 elliptic curves E' and without plugging in values of x' into $E_{x'}$ we can conclude by the rational 2-torsion of E_x that $a_3(E_x)$ is even, and the Weil bounds then give $a_3(E_x) \in \{-2, 0, 2\}$.

For an interesting example where the Frey curve has a rational 3-torsion point, but the non CM elliptic curves at the levels N_0 do not, we refer to [BVY] (we will deal with CM curves in a moment). In this paper, certain infinite families of generalized Fermat equations (1.1) with $p = q$ and $r = 3$ are solved.

We also mention that if more than one Frey curve is available, the information given by these Frey curves can be combined. In [BMS3] this (amongst other things) was used to solve certain infinite families of binary Thue equations.

The method of Kraus

To illustrate the method of Kraus, we will first restrict to an equation of the form

$$f(x) = cy^l \quad x, y \in \mathbb{Z} \quad y \neq 0, \tag{2.13}$$

where $f \in \mathbb{Z}[x]$, $c \in \mathbb{Z} - \{0\}$ and l denotes an odd prime. For simplicity we will assume that we have a Frey curve E_x for this equation with coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}[x]$, $\Delta(E_x) = Cf(x)^e$, for certain $C \in \mathbb{Z} - \{0\}, e \in \mathbb{Z}_{>0}$ and $R := \mathrm{Res}_x(f(x), c_4(E_x)) \neq 0$. For a given l, suppose that (x, y) is a hypothetical solution to (2.13) and suppose that $\rho_l^{E_x}$ is irreducible. Then $E_x \sim_l f$ for a certain newform f of level $N_0 := N_0(E_x, l)$. The (finitely many) possibilities of N_0 are known explicitly, they depend on the explicitly known Frey curve. Take a newform f at an appropriate level N_0 and assume for simplicity that it is rational with an associates elliptic curve E' (the nonrational case is not harder to handle). We want to show that it is impossible that $E_x \sim_l E'$. Instead of simply plugging in all possible x modulo p for a certain prime p and compute the possible $a_p(E_x)$, a natural thing to do is use local information to restrict the possibilities of x modulo p by reducing (2.13) modulo p.

Suppose that $p \nmid c$ (which is the case most interesting to us). Recall that $\mathbb{F}_p^*$ is cyclic of order $p-1$. So if $l \nmid p-1$, then $\{a^l \mid a \in \mathbb{F}_p\} = \mathbb{F}_p$ and we get no restriction at all for $x \pmod p$ from $f(x) \equiv cy^l \pmod p$. If however $l | p-1$, say $p = nl+1, n \in \mathbb{Z}$, then $\{a^l \mid a \in \mathbb{F}_p\} = \{b \in \mathbb{F}_p \mid b^n = 1\} \cup \{0\}$ and we may get a lot of information on $x \pmod p$ from $f(x) \equiv cy^l \pmod p$. So suppose that $p = nl+1$ and $p \nmid N_0$. If $p | y$, then $p | N(E_x)$, so $a_p(E') \equiv \pm(1+p) \equiv \pm 2 \pmod l$ and otherwise, $a_p(E') \equiv a_p(E_x) \pmod l$.

We conclude that in order to rule out the option that $E_x \sim_l E'$ it suffices to find a prime $p \nmid N_0$ such that

- $p = nl+1,\ n \in \mathbb{Z}$,
- $a_p(E')^2 \not\equiv 4 \pmod l$,
- $a_p(E') \not\equiv a_p(E_{x'}) \pmod l$ for all $x' \in \mathbb{F}_p$ such that

$$f(x') \in c\{b \in \mathbb{F}_p \mid b^n = 1\}.$$

Note that if $f(x)$ has no roots modulo p, then we do not need $a_p(E')^2 \not\equiv 4 \pmod l$. If $f(x)$ has a root modulo p and at all the roots $x \pmod p$ the reduction of E_x at p is split resp. non-split multiplicative, then we only need $a_p(E') \not\equiv 2 \pmod l$ resp. $a_p(E') \not\equiv -2 \pmod l$ instead of $a_p(E')^2 \not\equiv 4 \pmod l$.

A typical situation where this method fails, is when there exists an $x \in \mathbb{Q}$ such that $f(x) = \pm c$ and E_x has conductor equal to some a priori possible level N_0. If this is not the case there is still no a priori guarantee that the method will work, but heuristically speaking for a fixed prime l, the existence of "small" n (compared to l) such that $nl+1$ is prime increases the chance of the method to work. For $l = 19, 31$ the smallest n such that $nl+1$ is prime is $n = 10$ and in practice we see that the method fails frequently for $l = 19, 31$.

Example 44. For some straightforward examples with $c = 1$ and $f(x) = x^3 - x - 2$ or $f(x) = x^4 + x^3 - 3x^2 + 11x + 2$ we refer to section 3.3.3, except for the irreducibility of $\rho_l^{E_x}$ for some small primes l everything necessary to understand these examples has been treated so far.

Let us treat the special case $x^3 - x - 2 = y^l$ with $l = 13$ here. To a hypothetical solution x, y the Frey curve

$$E_x : Y^2 = X^3 + X^2 - x(6 + x)X - (2x^3 + x^2 + 4x + 4)$$

is associated. The minimal discriminant $\Delta_{\min}$ and conductor N are, according to appendix A, given by

$$\begin{aligned} \Delta_{\min} &= -\frac{13}{2^5}(x^3 - x - 2)^2 = -\frac{13}{2^5}y^{2l}, \\ N &= 2 \cdot 13 \operatorname{rad}_{\{2,13\}}(x^3 - x - 2) = 2 \cdot 13 \operatorname{rad}_{\{2,13\}}(y). \end{aligned}$$

So we have $N_0 := N_0(E_x, l) = 2 \cdot 13 = 26$. As shown in section 3.3.3 we can assume that for $l = 13$ the representation $\rho_l^{E_x}$ is irreducible and furthermore that $E_x \sim_l E26a$, where $E26a$ denotes an elliptic curve from the isogeny class $26a$ in the notation from [Cre2]. We note that for $x' = -2, 6, 38/25$ the elliptic curve $E_{x'}$ is isogenous to $E26a$. Now let $n := 4$ and $p := nl + 1 = 4 \cdot 13 + 1 = 53$ (so p is prime). First of all $a_p(E26a) = 0$, so $a_p(E26a) \not\equiv \pm 2 \equiv \pm(p + 1) \pmod{l}$, hence $p \nmid N$. This tells us that $y \not\equiv 0 \pmod{l}$. We compute $y^l \equiv \pm 1, \pm 23 \pmod{p}$, together with $x^3 - x - 2 \equiv y^l \pmod{p}$ we get $x \equiv 19, 37, 38 \pmod{p}$. We note that none of these values are congruent to $-2, 6, 38/25 (\equiv 10 \pmod{p})$ modulo p. We also compute $a_p(E_{19}) = 2, a_p(E_{37}) = -2, a_p(E_{38}) = -12$. Finally note that $2, -2, -12 \not\equiv a_p(E26a) \pmod{l}$, so we conclude that $x^3 - x - 2 = y^{13}$ has no solutions with $x, y \in \mathbb{Z}$.

Instead of (2.13) consider a Diophantine equation of the form (2.10) (with $f \in \mathbb{Z}[x, y]$ homogeneous and $c \in \mathbb{Z} - \{0\}$). In practice, reducing this equation modulo some prime of the form $p = nl + 1, n \in \mathbb{Z}$ leaves one with too many possibilities for x, y modulo p by the homogeneity of f. If however $f(x, y)$ factors over $\mathbb{Z}$ as $f(x, y) = g(x, y)h(x, y)$ with $\operatorname{Res}(g(x, y), h(x, y)) \neq 0$, then up to primes dividing this resultant, the factors $g(x, y)$ and $h(x, y)$ must both be l-th powers. This information can of course be used in restricting the possibilities of x, y modulo p. The first example of this approach is given in [Kra4] to study $x^3 + y^3 = z^l$. In [Che] the study of $x^2 + y^{2l} = z^3$ is reduced to the study of $v(3u^2 - v^2) = y^l$ and solved (for primes l with $7 < l < 10^7, l \neq 31$) using a similar approach. This last example is recalled in section 3.3.1 and (again) except for irreducibility results for small primes, uses only methods developed so far.

We actually also solve the equation above for $l = 31$; this was done by using extra local information coming from classical algebraic number theory. In general, instead of just factoring $f(x, y)$ over $\mathbb{Z}$, we can factor the equation further over a number field (assuming $f(x)$ does not already factor as a product of linear factors over $\mathbb{Z}$). The factors will be l-th powers, up to finitely many primes and up to units. These units can cause problems, but if we choose our prime $p = nl + 1$ in such a way that all units become n-th roots of unity modulo p, these problems

disappear and we have more local information at our disposal. For a concrete example we refer to section 3.3.1.

A related approach, where the units are required to be not n-th roots of unity modulo p to obtain (partial) information about solutions of Diophantine equations, is given in [Sik, section 9].

Different residue fields

If $\rho_l^E \simeq \rho_{\mathfrak{L}}^f$, then under some mild conditions we must have that $\mathcal{O}_f/\mathfrak{L} = \mathbb{F}_l$. We have the following elementary result from algebraic number theory.

Lemma 45. *Let $K = \mathbb{Q}(\alpha)$ for some algebraic integer α and let $\mathfrak{L} \subset \mathcal{O}_K$ be a prime lying above $l \in \mathbb{Z}$. If $\alpha \equiv n \pmod{\mathfrak{L}}$ for some $n \in \mathbb{Z}$ and $l \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, then $\mathfrak{L}$ has inertia degree 1.*

Proof. The image of the natural homomorphism $\phi : \mathbb{Z}[\alpha] \to \mathcal{O}_K/\mathfrak{L}$ is isomorphic to $\mathbb{F}_l$ because $\alpha \equiv n \pmod{\mathfrak{L}}$. Since $l \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, ϕ is surjective (see e.g. the proof the Kummer-Dedekind theorem in [Coh1, pp. 197-198]) and the lemma follows. □

We obtain the following computationally convenient criterion for eliminating newforms.

Proposition 46. *Let f be a newform of level N_0 and let l be a prime. Suppose that for some prime $p \nmid N_0 l$ the characteristic polynomial of $a_p(f)$ w.r.t. $K_f/\mathbb{Q}$, denoted $F_p(x)$, is irreducible, that $l \nmid [\mathcal{O}_f : \mathbb{Z}[a_p(f)]]$ and that $F_p(x)$ does not have a root modulo l. Then it is impossible that $E \sim_l f$ for any elliptic curve $E/\mathbb{Q}$.*

Proof. Suppose we do have $E \sim_l f$ for some elliptic curve $E/\mathbb{Q}$. Then $a_p(f) \equiv n \pmod{\mathfrak{L}}$ for some $n \in \mathbb{Z}$ and some prime $\mathfrak{L} \subset \mathcal{O}_f$ lying above l. Since $F_p(x)$ is irreducible we have $K_f = \mathbb{Q}(a_p(f))$. The preceding lemma gives us that $\mathfrak{L}$ has inertia degree 1. Since $l \nmid [\mathcal{O}_f : \mathbb{Z}[a_p(f)]]$ the Kummer-Dedekind theorem now gives us that $F_p(x)$ has a root modulo l. A contradiction which proves the proposition. □

Example 47. Consider the generalized Fermat equation

$$x^2 + y^3 = z^l \quad x, y, z \in \mathbb{Z} \quad xyz \neq 0, \gcd(x, y, z) = 1,$$

for an odd prime $l \geq 5$. To a hypothetical solution we associate the Frey curve

$$E_{x,y} : Y^2 = X^3 + 3yX + 2x.$$

It has (not necessarily minimal) discriminant $-2^6 \cdot 3^3(x^2 + y^3) = -2^6 \cdot 3^3 z^l$, and from [Pap] one easily obtains that $N_0 := N_0(E_{x,y}, l)|2^6 \cdot 3^3$. Suppose that $\rho_l^{E_{x,y}}$ is irreducible, then $E_{x,y} \sim_l f$ for some newform f of level N_0. Up to quadratic twist there is only one nonrational newform of level dividing $2^6 \cdot 3^3$ and $a_5(f), a_7(f)$ both satisfy $x^2 - 13 = 0$. By quadratic reciprocity we have that $x^2 - 13$ is irreducible modulo a prime l if and only if $l \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$. The proposition above now tells us that for these prime exponents l we only have to consider $E_{x,y} \sim_l E'$ for elliptic curves E' with conductor dividing $2^6 \cdot 3^3$.

2.2.3 Complex multiplication

Let $F/\mathbb{Q}$ be an elliptic curve with complex multiplication. Then for an odd prime l the possibilities for $\mathrm{Gal}(\mathbb{Q}(F[l])/\mathbb{Q})$ are quite restrictive, in particular it is strictly smaller than $\mathrm{GL}_2(\mathbb{F}_l)$. If now $\rho_l^E \simeq \rho_l^F$, then of course the same holds for $\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q})$. By studying certain modular curves we can get, sometimes under additional assumptions on E, much information about where E has potentially good reduction, thereby restricting the possibilities of the primes in the denominator of j_E. This provides valuable information, since in applications of the modular method there is a strong relation between the primes where the Frey curve associated to a solution $x_i, y_i \in \mathbb{Z}$ of (2.9) has multiplicative reduction and the primes dividing y_i.

Definition 48. A *Cartan subgroup* of $\mathrm{GL}_2(\mathbb{F}_l)$ is a subgroup G of $\mathrm{GL}_2(\mathbb{F}_l)$ such that $G \simeq R^*$ for a subring R of $\mathrm{Mat}(2 \times 2, \mathbb{F}_l)$ with $R \simeq \mathbb{F}_l \times \mathbb{F}_l$ or $R \simeq \mathbb{F}_{l^2}$. If $R \simeq F_l \times F_l$, then G is called *split*, otherwise G is called *nonsplit*.

Proposition 49. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic number field K. Let l be a prime which does not divide the discriminant of $\mathcal{O}$. Then* $\mathrm{Im}\ \rho_l^E$ *is contained in the normalizer of a split (resp. nonsplit) Cartan subgroup of* $\mathrm{GL}_2(\mathbb{F}_l)$ *if l splits (resp. stays inert) in K.*

Proof. Consider the natural restriction homomorphism

$$f : \mathcal{O} \cong \mathrm{End}(E) \to \mathrm{End}(E[l])$$

and denote the image under f by R. The kernel is generated by l, so $R \cong \mathcal{O}/(l) \cong \mathcal{O}_K/(l)$ (since $l \nmid \Delta(\mathcal{O})$), which is isomorphic to $\mathbb{F}_l \times \mathbb{F}_l$ or $\mathbb{F}_{l^2}$ respectively depending on whether l splits or stays inert respectively in K. So R^* is a split resp. nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_l)$. Let $\sigma \in G_{\mathbb{Q}}$, and denote by σ' the image of σ under ρ_l^E. The natural action of $G_{\mathbb{Q}}$ on $\mathrm{End}(E)$ induces an action of $G_{\mathbb{Q}}$ on R and on R^*. One easily checks that for $\phi \in R^*$ we have $\sigma'\phi = \phi^\sigma\sigma'$ (where ϕ^σ denotes the action of σ on ϕ). In other words, $\sigma'\phi\sigma'^{-1} = \phi^\sigma \in R^*$ and so $\mathrm{Im}\ \rho_l^E$ is contained in the normalizer of R^*. □

Let $X_{\mathrm{split}}(l)$ resp. $X_{\mathrm{nonsplit}}(l)$ denote the (complete) modular curve corresponding to the congruence subgroup $\{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \bmod l \in H\}$, where $H \subset \mathrm{GL}_2(\mathbb{F}_l)$ is the normalizer of a split resp. nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_l)$. The modular curves $X_{\mathrm{split}}(l)$ resp. $X_{\mathrm{nonsplit}}(l)$ admit a natural structure over $\mathbb{Q}$, where the noncuspidal rational points correspond to elliptic curves $E/\mathbb{Q}$ (up to twist) with $\mathrm{Im}\ \rho_l^E$ contained in the normalizer of a split resp. nonsplit Cartan subgroup; see e.g. [Maz1, Introduction].

Much is known about the rational points of $X_{\mathrm{split}}(l)$. Already in [Maz1, III, Theorem 6.1] it is proved that if $l \geq 11, l \neq 13$, then $X_{\mathrm{split}}(l)(\mathbb{Q})$ is finite. In fact, since the genus of $X_{\mathrm{split}}(l)$ is at least 2 if and only if $l \geq 11$, we now know by Faltings' theorem that if $l \geq 11$, then $X_{\mathrm{split}}(l)(\mathbb{Q})$ is finite. In [Par, Theorem 1.1] it is proved that the set of primes l, such that $X_{\mathrm{split}}(l)$ contains a noncuspidal rational point not corresponding to an elliptic curve with complex multiplication,

is contained in a set of density at most $7/2^9$, in [Reb, Théorème 0.2] the upper bound for this density was improved to $9/2^{10}$. Also, in *loc. cit.* it is shown that the only noncuspidal rational points of $X_{\text{split}}(l)$ for $11 \leq l \leq 1871,\ l \neq 13$ correspond to elliptic curves with complex multiplication. The most useful property for the modular method, however, is the following.

Theorem 50. *Let $E/\mathbb{Q}$ be an elliptic curve, let $l \geq 11, l \neq 13$ be prime and suppose that* $\operatorname{Im} \rho_l^E$ *is contained in the normalizer of a split Cartan subgroup of* $\mathrm{GL}_2(\mathbb{F}_l)$. *Then*

i. $j_E \in \mathbb{Z}$,

ii. If $F/\mathbb{Q}$ is an elliptic curve with $\rho_l^F \simeq \rho_l^E$, then the conductors of E and F are equal.

Proof. Part one follows form [Mer2, Theorem 5]. For the second part see [HK, Théorème 1]. □

Remark 51. From [Mom, Proposition 3.1] it follows that part one of the above theorem with $j_E \in \mathbb{Z}$ replaced by $j_E \in \mathbb{Z}[1/2]$ holds. This already suffices for most applications.

About the rational points on the modular curves $X_{\text{nonsplit}}(l)$ much less is known. We have that the genus of $X_{\text{nonsplit}}(l)$ is at least 2 (in fact at least 3) if and only if $l \geq 13$. And we really need Faltings' theorem to conclude that if $l \geq 13$, then $X_{\text{nonsplit}}(l)(\mathbb{Q})$ is finite. So for elliptic curves E with $\operatorname{Im} \rho_l^E$ contained in the normalizer of a nonsplit Cartan subgroup much less is known. If however E also has a nontrivial $\mathbb{Q}$-rational torsion point (or even just a $\mathbb{Q}$ rational isogeny of the right order), then more is known, also in the split case when $l = 5, 7, 13$.

Theorem 52. *Let $E/\mathbb{Q}$ be an elliptic curve and $l \geq 5$ prime. Suppose that E has a $\mathbb{Q}$-rational p-isogeny where $p = 2, 3, 5, 7$ or 13 and $p \neq l$.*

- *If* $\operatorname{Im} \rho_l^E$ *is contained in the normalizer of a split Cartan subgroup, then $j(E) \in \mathbb{Z}[\frac{1}{2l}]$.*
- *If* $\operatorname{Im} \rho_l^E$ *is contained in the normalizer of a nonsplit Cartan subgroup, then $j(E) \in \mathbb{Z}[\frac{1}{l}]$.*

Proof. See [Mer1, Theorem 2.15] and the remarks after this (and also note that 'isomorphic to' can be replaced by 'contained in'). (See also [DM, Theorem 8.1].) □

Example 53. In [Kra4] the generalized Fermat equation

$$x^3 + y^3 = z^l \quad x, y, z \in \mathbb{Z} \quad xyz \neq 0, \gcd(x, y, z) = 1,$$

for an odd prime l is analyzed. To a hypothetical solution the Frey curve

$$E_{x,y} : Y^2 = X^3 + 3xyX + y^3 - x^3$$

is associated, with (not necessarily minimal) discriminant $-2^4 \cdot 3^3(x^3+y^3)^2 = -2^4 \cdot 3^3 z^{2l}$. Suppose that $l \geq 5$ and that $\rho_l^{E_{x,y}}$ is irreducible. A priori we could have that $N_0(E_{x,y}, l) = 36$. But we have the elliptic curve $E_{0,1}$ of conductor 36, and the relation $0^3 + 1^3 = 1^l$ shows that there is no way the methods from section 2.2.2 can be used to eliminate the possibility of $E_{x,y} \sim_l E_{0,1}$ for any l. The elliptic curve $E_{0,1}$ has however complex multiplication by $\mathbb{Z}[\zeta_3]$ and we use the theorem above (following the arguments from *loc. cit.* closely) to eliminate $E_{x,y} \sim_l E_{0,1}$.

So suppose $N_0(E_{x,y}, l) = 36$ and $E_{x,y} \sim_l E_{0,1}$. Proposition 49 gives us that $\operatorname{Im} \rho_l^{E_{0,1}}$ and hence $\operatorname{Im} \rho_l^{E_{x,y}}$ is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_l)$. Note that $E_{x,y}$ has a rational 2-torsion point, so from Theorem 52 we obtain $j_{E_{x,y}} \in \mathbb{Z}[1/(2l)]$. We compute

$$j_{E_{x,y}} = \frac{2^8 \cdot 3^3 x^3 y^3}{(x^3+y^3)^2} = \frac{2^8 \cdot 3^3 x^3 y^3}{z^{2l}},$$

hence $z = \pm 2^a l^b$ for $a, b \in \mathbb{Z}_{\geq 0}$. If $l | z$, then in fact $l | N(E)$ and Theorem 36 give us that

$$a_l(E_{0,1}) \equiv \pm(1+l) \equiv \pm 1 \pmod{l}.$$

Together with the Weil bounds we obtain $a_l(E_{0,1}) = \pm 1$, but $E_{0,1}$ has a rational 2-torsion point and good reduction at l (since $l \geq 5$), so $a_l(E_{0,1})$ is even. A contradiction which proves that $l \nmid N(E)$. We are left with $z = \pm 2^a$ for some $a \in \mathbb{Z}_{\geq 0}$. The equation

$$(x+y)(x^2 - xy + y^2) = \pm 2^{al} \quad x, y \in \mathbb{Z} \quad \gcd(x, y, 2) = 1$$

leads to $x^2 - xy + y^2 = \pm 1$, with solutions $(x, y) = (\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)$. None of these solutions give rise to solutions of our original equation and the possibility $E_{x,y} \sim_l E_{0,1}$ is ruled out.

2.2.4 Different images of inertia

Let $E, E'/\mathbb{Q}$ be elliptic curves and let l be a prime. If $\rho_l^E \simeq \rho_l^{E'}$, then of course $\rho_l^E(G) \simeq \rho_l^{E'}(G)$ for all subgroups $G \subset G_{\mathbb{Q}}$. Taking $G = I_p$ for some inertia subgroup $I_p \subset G_{\mathbb{Q}}$ of a prime $p \neq l$, we will use this to show that, under some mild conditions, if $\rho_l^E \simeq \rho_l^{E'}$, then it is impossible that the reduction at p of E is potentially good when that of E' is not. In the proofs of [Kra4, Théorème 6.1.c] and [BS, Proposition 4.4] this was used to show that $\rho_l^E \not\simeq \rho_l^{E'}$ (for appropriate l), where E is a certain Frey curve with potentially good reduction at some prime p and E' is some elliptic curve obtained by level lowering (à la Theorem 35) where the reduction at p is not potentially good. The purpose of [Kra4] is to obtain information about $j(E)$ and the purpose of [BS] is to eliminate E'. Recall that E has potentially good reduction at p if and only if $\nu_p(j_E) \geq 0$; see [Sil1, Chapter VII, Proposition 5.5].

Now suppose that $l \geq 3$ and that E has potentially good reduction at $p \neq l$. Consider $E/\mathbb{Q}_p^{\mathrm{nr}}$, where $\mathbb{Q}_p^{\mathrm{nr}}$ denotes the maximal unramified extension of $\mathbb{Q}_p$. There exists a minimal extension $K/\mathbb{Q}_p^{\mathrm{nr}}$ such that E has good reduction over K,

in fact we have $K = \mathbb{Q}_p^{\mathrm{nr}}(E[n])$ for any integer $n \geq 3$ with $p \nmid n$; see [ST, 2. Corollary 3 (p. 498)]. Define $\Phi_p := \mathrm{Gal}(K/\mathbb{Q}_p^{\mathrm{nr}})$ as in [Ser1, 5.6 pp. 311-312]. Since we can write $K = \mathbb{Q}_p^{\mathrm{nr}}(E[l])$, we see that $\rho_l^E(I_p) \simeq \Phi_p$. In *loc. cit.* all the possibilities for the group structure of Φ_p are given. In particular we have that $\#\Phi_p$ is not divisible by primes ≥ 5. An explicit characterization of Φ_p is terms of basic quantities of E is given in [Kra1]. From our discussion we obtain the following.

Proposition 54. *Let $E/\mathbb{Q}$ be an elliptic curve and let $l \geq 5$ be a prime. Suppose that E has potentially good reduction at some prime $p \neq l$. Then $l \nmid \#\rho_l^E(I_p)$.*

We also have some useful information about $\rho_l^E(I_p)$ in the case that E does not have potentially good reduction at p.

Proposition 55. *Let $E/\mathbb{Q}$ be an elliptic curve and let $l \geq 3$ be a prime. Suppose that the reduction of E at some prime p is not potentially good and that $l \nmid \nu_p(j_E)$. Then $l|\#\rho_l^E(I_p)$.*

Proof. See [Sil2, Chapter V, Proposition 6.1] (it follows from the theory of Tate curves). □

By combining the 2 propositions (and the characterization of potentially good reduction) above, we immediately obtain the following consequence, which will be useful in practice.

Corollary 56. *Let $E, E'/\mathbb{Q}$ be elliptic curves and let $l \geq 5$ be a prime. Suppose that for some prime $p \neq l$ we have $\nu_p(j_E) \geq 0$, $\nu_p(j_{E'}) < 0$ and $l \nmid \nu_p(j_{E'})$. Then ρ_l^E and $\rho_l^{E'}$ are* not *isomorphic.*

In practice, the conclusion of the corollary above can sometimes also been shown to hold for $l = 3$ by examining $\rho_l^E(I_p)$ (for $l = 3$) a little bit more, see for example [BS, Proposition 4.4].

Example 57. Consider the equation

$$x^3 + 17y^3 = z^l \quad x, y, z \in \mathbb{Z} \quad xyz \neq 0,\ \gcd(x, y, z) = 1,$$

where l denotes an odd prime. To a hypothetical solution we associate the Frey curve

$$E_{x,y} : Y^2 = X^3 + 3^3 \cdot 17xyX + 3^3 \cdot 17(x^3 - 17y^3).$$

Suppose that $l \geq 5$ and that $\rho_l^{E_{x,y}}$ is irreducible. It turns out that $N_0(E_{x,y}, l) = 2^a \cdot 3^b \cdot 17^2$, where $a \in \{1, 2, 3\}$ and $b = 2$ if $3 \nmid z$ and $b = 1$ if $3|z$. The elliptic curve

$$E' : Y^2 = X^3 - 102X + 425$$

has conductor $2^3 \cdot 3^2 \cdot 17^2$ and a priori we may have $E_{x,y} \sim_l E'$. We will use the corollary above to discard this possibility. So suppose that $E_{x,y} \sim_l E'$. In this case we must have for our hypothetical solution that $3 \nmid z$. We compute

$$j_{E_{x,y}} = \frac{2^8 \cdot 3^3 \cdot 17x^3y^3}{(x^3 + 17y^3)^2} = \frac{2^8 \cdot 3^3 \cdot 17x^3y^3}{z^{2l}},$$

hence $\nu_3(j_{E_{x,y}}) \geq 3$. However, $\nu_3(j_{E'}) = -1$ and by the corollary above we conclude that $E_{x,y} \sim_l E'$ is impossible.

Chapter 3

Frey curves, irreducibility and applications

In this chapter we will first construct some Frey curves for certain Diophantine equations. Next we will prove for some of these Frey curves irreducibility results for ρ_p^E when p is small. Finally we will apply some of the Frey curve constructions and irreducibility results to solve some Diophantine equations. We will also solve for the first time the generalized Fermat equation $x^2+y^{2l} = z^3$ for $l = 31$ by combining modular methods with arguments from classical algebraic number theory.

3.1 Some Frey curves

In this section we want to give some constructions of Frey curves associated to equations of the form

$$f(x_1, \ldots, x_n) = Cy^l \quad x_1, \ldots, x_n, y \in \mathbb{Z} \text{ and } l \text{ an odd prime}, \tag{3.1}$$

where $f \in \mathbb{Z}[x_1, \ldots, x_n]$ (for some $n \in \mathbb{Z}_{>0}$) and $C \in \mathbb{Z} - \{0\}$. Let $f_1, \ldots, f_m$ be the irreducible factors over $\mathbb{Q}$ of f. Suppose we can solve $g^2 + h^3 = \prod_{i=1}^m f_i^{a_i}$ for $g, h \in \mathbb{Z}[x_1, \ldots, x_n]$ with no common factors of positive degree and $a_i \in \mathbb{Z}_{\geq 0}$ not all zero. Then

$$E : Y^2 = X^3 + 3hX + 2g \tag{3.2}$$

is a Frey curve with basic quantities

$$\begin{aligned} \Delta &= -2^6 \cdot 3^3(g^2 + h^3) \\ &= -2^6 \cdot 3^3 \prod_{i=1}^m f_i^{a_i} \\ c_4 &= -2^4 \cdot 3^2 h \\ c_6 &= -2^6 \cdot 3^3 g. \end{aligned}$$

We will concentrate on some special cases. Amongst other things, we will obtain Frey curves for the generalized Fermat equation (1.1) with signature (p, q, r) of the form $(3, 3, l), (5, 5, l)$ and $(7, 7, l)$. These were all known before (see [Kra5]) but the Frey curves for the last two signatures are obtained via a new route. For some other signatures there are also Frey curves. We especially want to mention that a detailed description of the Frey curves for quite general coefficients for signature $(l, l, 2), (l, l, 3), (l, l, l)$ is given in [BS], [BVY], [Kra3] respectively.

Binary cubic forms

Consider the binary cubic form

$$F(x, y) := ax^3 + bx^2y + cxy^2 + dy^3 \in \mathbb{Z}[x, y]. \tag{3.3}$$

Frey curves for $F(x, y) = Cz^l$ are given in the literature for some special cases of F, we construct a Frey curve for every nondegenerate F. Define the corresponding invariant and covariants as follows

$$\begin{aligned} \Delta_F &:= \text{Discriminant}(F) && (3.4)\\ H(x, y) &:= -\frac{1}{4}\begin{vmatrix} F_{xx} & F_{xy} \\ F_{xy} & F_{yy} \end{vmatrix} && (3.5)\\ G(x, y) &:= \begin{vmatrix} F_x & F_y \\ H_x & H_y \end{vmatrix}. && (3.6) \end{aligned}$$

Then one has the classical syzygy

$$4H(x, y)^3 = G(x, y)^2 + 27\Delta_F F(x, y)^2. \tag{3.7}$$

Now consider the Frey curve given by

$$E : Y^2 = X^3 - 3H(x, y)X + G(x, y). \tag{3.8}$$

The fundamental quantities associated to E are

$$\begin{aligned} \Delta &= 2^4 \cdot 3^6 \Delta_F F(x, y)^2 && (3.9)\\ c_4 &= 2^4 \cdot 3^2 H(x, y) && (3.10)\\ c_6 &= -2^5 \cdot 3^3 G(x, y) && (3.11)\\ j &= \frac{2^8 H(x, y)^3}{\Delta_F F(x, y)^2} && (3.12)\\ &= \frac{2^6 G(x, y)^2}{\Delta_F F(x, y)^2} + 1728. && (3.13) \end{aligned}$$

One easily checks that if F has a linear factor over $\mathbb{Q}$, then E has a rational 2-torsion point.

Binary quartic forms

Consider the binary quartic form

$$F(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \in \mathbb{Z}[x,y]. \tag{3.14}$$

If $12ae - 3bd + c^2 = 0$ and F is nondegenerate, we can construct a Frey curve for $F(x,y) = Cz^l$. Following [Cre1], define the invariants and covariants as follows

$$\begin{aligned}
I &:= 12ae - 3bd + c^2 && (3.15)\\
J &:= 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3 \\
g_4(x,y) &:= (3b^2 - 8ac)x^4 + 4(bc - 6ad)x^3y + 2(2c^2 - 24ae - 3bd)x^2y^2 \\
&\quad +4(cd - 6be)xy^3 + (3d^2 - 8ce)y^4 \\
g_6(x,y) &:= (b^3 + 8a^2d - 4abc)x^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)x^5y \\
&\quad +5(8abe + b^2d - 4acd)x^4y^2 + 20(b^2e - ad^2)x^3y^3 \\
&\quad -5(ade + bd^2 - 4bce)x^2y^4 - 2(16ae^2 + 2bde - 4c^2e + cd^2)xy^5 \\
&\quad -(d^3 + 8be^2 - 4cde)y^6.
\end{aligned}$$

Then one has the classical syzygy

$$g_4^3 - 48IF^2g_4 - 64JF^3 = 27g_6^2. \tag{3.16}$$

If now $I = 0$, then this reduces to

$$g_4^3 - 27g_6^2 = 64JF^3, \tag{3.17}$$

where $J^2 = -27\Delta_F$. Now consider the Frey curve given by

$$E : Y^2 = X^3 - g_4X + 2g_6. \tag{3.18}$$

The fundamental quantities associated to E are

$$\begin{aligned}
\Delta &= 2^{12}JF^3 && (3.19)\\
c_4 &= 2^4 \cdot 3g_4 && (3.20)\\
c_6 &= -2^6 \cdot 3^3 g_6 && (3.21)\\
j &= \frac{3^3 g_4^3}{JF^3} && (3.22)\\
&= \frac{3^6 g_6^2}{JF^3} + 1728. && (3.23)
\end{aligned}$$

One easily checks that if F has a linear factor over $\mathbb{Q}$, then E has a rational 3-isogeny.

Klein forms

Let $F \in \overline{\mathbb{Q}}[x,y]$ be a binary form and $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{Q}})$, then by letting

$$(F \circ M)(x,y) = F(ax + by, cx + dy),$$

we obtain a right action of $\mathrm{GL}_2(\overline{\mathbb{Q}})$ on the set of nondegenerate binary forms over $\overline{\mathbb{Q}}$ of given degree k. Define binary forms F_r for $r = 2, 3, 4, 5$ as follows,

$$\begin{aligned} F_2(x,y) &= xy(x+y) \\ F_3(x,y) &= y(x^3+y^3) \\ F_4(x,y) &= xy(x^4+y^4) \\ F_5(x,y) &= xy(x^{10}-11x^5y^5-y^{10}). \end{aligned}$$

Let $r \in \{2,3,4,5\}$ and let $M \in \mathrm{GL}_2(\overline{\mathbb{Q}})$ such that $F := F_r \circ M \in \mathbb{Q}[x,y]$, then in fact there exist binary forms $g_r(x,y), h_r(x,y) \in \mathbb{Q}[x,y]$ with no common factors of positive degree and a $d \in \mathbb{Q}^*$, such that

$$g^2 + h^3 = dF^r.$$

So (3.2) gives us a Frey curve for the equation $F(x,y) = Cz^l$. Call any binary form F such that $F = F_r \circ M$ a *Klein form*. If F is a nondegenerate binary form of degree 3, then it turns out that it is always a Klein form and the associated Frey curve is simply the one given by (3.8). If F is nondegenerate and of degree 4, then it turns out that F is a Klein form if and only if $I = 0$ (with notation as in (3.14), (3.15)) and the associated Frey curve is given by (3.18). For nondegenerate binary forms of degree 6 and 12 the Klein forms are given by 5 and 10 (dependent) conditions on the coefficients respectively (it amounts to the vanishing of the so-called 4-th transvectant of F). For more details, especially for explicit formulas for g, h, d and the vanishing conditions, we refer to [Edw].

It turns out that the Frey curves associated to the Klein forms actually describe families of elliptic curves with constant $2, 3, 4$, and 5 torsion, see [RS1], [RS2], [Sil]. An example of how constant 2-torsion of Frey curves attached to certain binary cubic forms can be used in the modular method is described in [BD], where amongst other things the following result is obtained.

Theorem 58. *Let D be a cube free integer $\neq \pm 1$ with $\gcd(D,6) = 1$. Suppose that the equation*

$$x^3 + Dy^3 = 2^a 3^b \prod_{p|D} p^{c_p} \quad x,y \in \mathbb{Z}, xy \neq 0, \gcd(x,y) = 1 \quad a,b,c_p \in \mathbb{Z}_{\geq 0} \ (\forall p|D)$$

has no solutions. Then the equation

$$x^3 + Dy^3 = z^l \quad x,y,z \in \mathbb{Z}, xyz \neq 0, \gcd(x,y,z) = 1$$

has no solutions for primes $l \equiv 1 \pmod 3$ with

$$l > \left(2^3 \cdot 3^3 \prod_{p|D} p(p+1) \right)^{2 \cdot 3^3 \prod_{p|D} p^2}.$$

The problems for odd primes $l \equiv -1 \pmod 3$ are caused by the fact that for the Frey curve $E_{x,y}$ attached to $F = x^3 + Dy^3$ given by (3.8) we have that Im $\rho_l^{E_{x,y}}$

is contained in the normalizer of a nonsplit Cartan subgroup when $(x, y) = (1, 0)$ or $(x, y) = (0, 1)$. If the cubic form F also does not represent ± 1, the methods in *loc. cit.* can be used to prove similar results but without the restriction that $l \equiv 1 \pmod 3$.

Theorem 59. *Let $F \in \mathbb{Z}[x, y]$ be a binary cubic form and assume that F is irreducible over $\mathbb{Q}$. Denote by $\Delta \in \mathbb{Z} - \{0\}$ the discriminant of F. Suppose that the equation*

$$F(x, y) = \prod_{p|2\Delta} p^{a_p} \quad x, y, a_p \in \mathbb{Z} \ (\forall p|2\Delta) \quad \gcd(x, y) = 1$$

has no solutions. Then the equation

$$F(x, y) = z^l \quad x, y, z \in \mathbb{Z}, xyz \neq 0, \gcd(x, y, z) = 1$$

has no solutions for primes l with

$$l > \left(2^8 \cdot 3^4 \prod_{p|\Delta, p\neq 2,3} p(p+1) \right)^{2^6 \cdot 3^4 \prod_{p|\Delta, p\neq 2,3} p^2}.$$

Univariate polynomials of degree 2

If we take the coefficient of x^3 in (3.3) equal to 0 and dehomogenize, we obtain a Frey curve for the equation $f(x) = ax^2 + bx + c = Cy^l$. This Frey curve has a rational 2-torsion point (the right hand side of (3.8) contains a factor $X + 2ax + b$). After a translation of X and a twist over $\mathbb{Q}(\sqrt{3})$, we obtain the following Frey curve

$$E : Y^2 = X^3 - (2ax + b)X^2 + a(ax^2 + bx + c)X \tag{3.24}$$

Basic quantities are given by

$$\begin{aligned} \Delta(E) &= 2^4 a^2 \Delta_f f(x)^2, && (3.25)\\ c_4 &= 2^4(b^2 - 3ac + abx + a^2x^2), && (3.26)\\ c_6 &= 2^5(b + 2ax)(2b^2 - 9ac - abx - a^2x^2). && (3.27) \end{aligned}$$

Other Frey curves can be obtained by solving $g^2 + h^3 = C(ax^2 + bx + c)$ for some $g, h \in \mathbb{Z}[x]$ and $C \in \mathbb{Z}$. Taking $\deg(g) = 3$ and $\deg(h) = 2$ we obtain the identity

$$\begin{aligned} &((b + 2ax)(-b^2 + 36ac + 32abx + 32a^2x^2))^2 \\ &+(-b^2 - 12ac - 16abx - 16a^2x^2)^3 = -108a(b^2 - 4ac)^2(c + bx + ax^2). \end{aligned}$$

The Frey curve obtained from this has a rational 2-torsion point. By a linear transformation and a twist over $\mathbb{Q}(\sqrt{3})$ we end up with the Frey curve

$$E : Y^2 = X^3 + 2(2ax + b)X^2 + (b^2 - 4ac)X.$$

This Frey curve, however, is simply 2-isogenous to (3.24).

Taking $\deg(g) = \deg(h) = 1$, we obtain the identity

$$((-b^2+4ac)(b+2ax))^2 + (-b^2+4ac)^3 = 4a(b^2-4ac)^2(ax^2+bx+c).$$

The Frey curve obtained from this is

$$E : Y^2 = X^3 - 3(b^2-4ac)X - 2(b^2-4ac)(2ax+b)$$

with discriminant

$$\Delta = -2^8 \cdot 3^3 a(b^2-4ac)^2(ax^2+bx+c).$$

Univariate polynomials of degree 3

First of all we can of course take the dehomogenized version of (3.8).

Next, if we take the coefficient of x^4 in (3.14) equal to zero and dehomogenize, we obtain a Frey curve for the equation $f(x) = ax^3+bx^2+cx+d = Cy^l$ if $b^2 = 3ac$. Recall that the Frey curve has a rational 3-isogeny. We must have $a \neq 0$ (in order to have nonzero discriminant), if $b = 0$, then we need $c = 0$ and we arrive at the following Frey curve

$$E : Y^2 = X^3 - 3ax(ax^3-8d)X + 2a(a^2x^6 + 20adx^3 - 8d^2)$$

with discriminant

$$\Delta = -2^{12} \cdot 3^3 a^2 d(ax^3+d)^3.$$

It turns out that up to quadratic twist, this Frey curve is 3-isogenous to a certain specialization of the Frey curve in [BVY, Section 2].

Other Frey curves are obtained by solving $\deg(g^2+h^3) = 3$ for some $g, h \in \mathbb{Z}[x]$. Taking $\deg(g) = 3$ and $\deg(h) = 2$, leads to the Frey curve

$$E : Y^2 = X^3 - 3(x^2+2c_1x+2c_2-c_1^2)X + 2(x^3+3c_1x^2+3c_2x+c_3).$$

For the discriminant we have

$$\begin{aligned} -\frac{\Delta}{1728} &= c_1^6 - 6c_1^4c_2 + 12c_1^2c_2^2 - 8c_2^3 + c_3^2 - 6(c_1^5 - 4c - 1^3c_2 + 4c_1c_2^2 - c_2c_3)x \\ &\quad +3(3c_1^4 - 4c_1^2c_2 - c_2^2 + 2c_1c_3)x^2 + 2(2c_1^3 - 3c_1c_2c_3)x^3. \end{aligned}$$

As a special case we want to mention the following. Take $c_1 = c_2 = 0$ and $c_3 = 2d/a$ and twist over $\mathbb{Q}(\sqrt{a})$ to obtain

$$E : Y^2 = X^3 - 3a^2x^2X + 2a^2(2d+ax^3)$$

with

$$\Delta = -2^8 \cdot 3^3 a^4 d(ax^3+d).$$

Taking $\deg(g) = \deg(h) = 1$ leads to the Frey curve

$$E : Y^2 = X^3 + (b_1x+b_2)X + a_2x + a_3$$

with

$$\Delta = 2^4(-27a_3^2 - 4b_2^3 - 6(9a_2a_3 + 2b_1b_2^2)x - 3(9a_2^2 + 4b_1^2b_2)x^2 - 4b_1^3x^3).$$

Taking $a_2 = b_2 = 0$, $b_1 = 3ad$ and $a_3 = 2ad^2$ we obtain

$$E : Y^2 = X^3 + 3adxX + 2ad^2$$

with

$$\Delta = -2^6 \cdot 3^3a^2d^3(ax^3 + d).$$

Along these lines we can of course also obtain Frey curves for some families of higher degree equations.

Coverings

Via coverings one can obtain new Frey curves from old ones. We want to mention one special case. Let $F(a, b)$ be a *symmetric* binary form of degree 6. Then $F(a, b) = f(a^2 + b^2, ab)$ for a binary cubic form $f(a, b)$. In [Kra5] Frey curves for the equations $a^5 + b^5 = c^l$ and $a^7 + b^7 = c^l$ were obtained via factorization over appropriate number fields. Here we want to obtain Frey curves via coverings.

First consider $a^5 + b^5 = c^l$. Then $F(a, b) := (a + b)(a^5 + b^5)$ is a symmetric binary form of degree 6 and one easily finds that $F(a, b) = f(a^2 + b^2, ab)$ when $f(x, y) = (x + 2y)(x^2 - xy - y^2)$. Using (3.8), we obtain the Frey curve

$$\begin{aligned} E : Y^2 &= X^3 - 15(2a^4 + 3a^3b + 7a^2b^2 + 3ab^3 + 2b^4)X \\ &\quad -25(a^2 + b^2)(a^4 + 9a^3b + 11a^2b^2 + 9ab^3 + b^4) \end{aligned}$$

with discriminant

$$\Delta = 2^4 \cdot 3^6 \cdot 5^3(a + b)^2(a^5 + b^5)^2.$$

Since $f(x, y)$ has a linear factor, E has a rational 2-torsion point and in fact after a linear change of variable and a twist over $\mathbb{Q}(\sqrt{-3})$ we obtain the Frey curve

$$Y^2 = X^3 + 5(a^2 + b^2)X^2 + 5\left(\frac{a^5 + b^5}{a + b}\right)X$$

with discriminant

$$\Delta = 2^4 \cdot 5^3(a + b)^2(a^5 + b^5)^2.$$

Now consider $a^7 + b^7 = c^l$. Then $F(a, b) := (a^7 + b^7)/(a + b)$ is a symmetric binary form of degree 6 and one easily finds that $F(a, b) = f(a^2 + b^2, ab)$ when $f(x, y) = x^3 - x^2y - 2xy^2 + y^3$. Using (3.8), we obtain the Frey curve

$$\begin{aligned} E : Y^2 &= X^3 - 21(a^4 - a^3b + 3a^2b^2 - ab^3 + b^4)X \\ &\quad +7(a^6 - 15a^5b + 15a^4b^2 - 29a^3b^3 + 15a^2b^4 - 15ab^5 + b^6) \end{aligned}$$

with discriminant

$$\Delta = 2^4 \cdot 3^6 \cdot 7^2\left(\frac{a^7 + b^7}{a + b}\right)^2.$$

3.2 Irreducibility in some special cases

Let p be a prime for which the modular curve $X_0(p)$ has genus 0, i.e. $p = 2, 3, 5, 7, 13$. Proving irreducibility for ρ_p^E, where E is some Frey curve, might be problematic in this case. In this section we study for $p = 5, 7, 13$ the irreducibility of ρ_p^E in the case that E is a Frey curve associated to a binary cubic or binary quartic form, i.e. the Frey curves given by (3.8), (3.18). This is done by finding nice quotients of certain fiber products. In the next section we shall apply some of the results to solve certain Diophantine equations.

Denote by j_p the j map $X_0(p) \to X(1)$. For $p = 5, 7, 13$ the maps j_p are explicitly given by

$$\begin{aligned} j_5(t) &= \frac{(t^2+10t+5)^3}{t} && (3.28)\\ &= \frac{(t^2+4t-1)^2(t^2+22t+125)}{t} + 1728 && (3.29)\\ j_7(t) &= \frac{(t^2+5t+1)^3(t^2+13t+49)}{t} && (3.30)\\ &= \frac{(t^4+14t^3+63t^2+70t-7)^2}{t} + 1728 && (3.31)\\ j_{13}(t) &= \frac{(t^4+7t^3+20t^2+19t+1)^3(t^2+5t+13)}{t} && (3.32)\\ &= \frac{f_6(t)^2(t^2+6t+13)}{t} + 1728 && (3.33)\\ \text{where } f_6(t) &:= t^6+10t^5+46t^4+108t^3+122t^2+38t-1. && (3.34) \end{aligned}$$

Binary cubic forms

Let $j(x, y)$ denote the j-invariant given by (3.12), (3.13) of the Frey curve (3.8) associated to a binary cubic form. If this Frey curve has a rational p-isogeny, this would give rise to a rational point on the curve X_p determined by

$$\{([x : y], t) \in \mathbb{P}^1 \times X_0(p) \mid j(x, y) = j_p(t)\}.$$

Up to twisting, the map $j(x, y)$ is the j-map $X(2) \to X(1)$. Furthermore, for $A := \begin{pmatrix} 2^{\frac{1}{2}} & 0 \\ 0 & 2^{-\frac{1}{2}} \end{pmatrix}$ we have $A\Gamma(2)A^{-1} = \Gamma_0(4)$. We obtain that for $p \neq 2$, X_p is birational (over $\overline{\mathbb{Q}}$) to $X_0(4p)$.

For $p = 5$, X_p has genus 1 and is explicitly given by

$$\frac{2^6 G(x, y)^2}{\Delta_F F(x, y)^2} = \frac{(t^2+4t-1)^2(t^2+22t+125)}{t}. \tag{3.35}$$

(The notation is not very canonical, x, y are homogeneous coordinates and t is not, but for our explicit computations the notation is convenient.) From this equation we see that X_5 maps (over $\mathbb{Q}$) to the elliptic curve given by

$$\Delta_F s^2 = t(t^2 + 22t + 125).$$

We note that for $\Delta_F = 1$ this elliptic curve is isogenous to $X_0(20)$.

For $p = 7$, X_p has genus 2.

For $p = 13$, X_p has genus 5 and is explicitly given by

$$\frac{2^6 G(x,y)^2}{\Delta_F F(x,y)^2} = \frac{(t^6 + 10t^5 + 46t^4 + 108t^3 + 122t^2 + 38t - 1)^2(t^2 + 6t + 13)}{t}. \tag{3.36}$$

We see that X_{13} maps (over $\mathbb{Q}$) to the elliptic curve given by

$$\Delta_F s^2 = t(t^2 + 6t + 13).$$

We note that for $\Delta_F = 1$ this elliptic curve has conductor 52.

Theorem 60. *Let F be a binary cubic form with discriminant $\Delta_F \neq 0$ and let E be the Frey curve (3.8) associated to it. Write $\Delta_F = dx^2$, with $d, x \in \mathbb{Z}$ and d square free. Let*

$$E_{d,5} : dy^2 = x(x^2 + 22x + 125).$$

If $d \neq -3$ and $E_{d,5}$ has rank 0, then ρ_5^E is irreducible. If $d = -3$ and $j_E \neq 2^{12} \cdot 5/3^5, -2^{12} \cdot 5^2/3$, then ρ_5^E is irreducible. Let

$$E_{d,13} : dy^2 = x(x^2 + 6x + 13).$$

If $E_{d,13}$ has rank 0, then ρ_{13}^E is irreducible.

Proof. The 2 rational 2-torsion points on $E_{d,p}$ for $p = 5$ and $p = 13$ respectively correspond to $t = 0, \infty$ (and infinite j-invariant) in (3.35) and (3.36) respectively. If $E_{d,p}$ has no further rational points, then X_p has no rational points corresponding to finite j-invariant and hence E has no rational p-isogeny. $E_{d,13}$ has no rational isogenies other then a 2-isogeny. So if $\mathrm{Rank}(E_{d,13}) = 0$, then $\#E_{d,13}(\mathbb{Q}) = 2$. The only rational isogenies (of prime power degree) of $E_{d,5}$ are a 2- and 3-isogeny. One easily checks that $E_{d,5}$ has a rational 3-torsion point if and only of $d = -3$. So if $\mathrm{Rank}(E_{d,5}) = 0$ and $d \neq -3$, then $\#E_{d,5}(\mathbb{Q}) = 2$. If $\mathrm{Rank}(E_{d,5}) = 0$ and $d = -3$, then $\#E_{d,5}(\mathbb{Q}) = 6$ and the 4 extra rational points correspond (2 to 1) to the values of j_E as stated in the theorem. □

Binary quartic forms

We proceed analogously as in the case of binary cubic forms. Let $j(x, y)$ denote the j-invariant given by (3.22), (3.23) of the Frey curve (3.18) associated to a binary quartic form. If this Frey curve has a rational p-isogeny, this would give rise to a rational point on the curve Y_p determined by

$$\{([x : y], t) \in \mathbb{P}^1 \times X_0(p) \mid j(x, y) = j_p(t)\}.$$

Up to twisting, the map $j(x, y)$ is the j-map $X(3) \to X(1)$. Furthermore, for $A := \begin{pmatrix} 3^{\frac{1}{2}} & 0 \\ 0 & 3^{-\frac{1}{2}} \end{pmatrix}$ we have that modulo $\pm I$, $A\Gamma(3)A^{-1} = \Gamma_0(9)$. We obtain that for $p \neq 3$, Y_p is birational (over $\overline{\mathbb{Q}}$) to $X_0(9p)$.

d	Rank$(E_{d,5})$	Rank$(E_{-d,5})$	Rank$(E_{d,13})$	Rank$(E_{-d,13})$
1	0	0	0	0
2	0	1	0	1
3	0	0	1	1
5	0	0	1	1
6	1	0	0	1
7	1	0	0	0
10	1	0	1	2
11	1	1	0	0
13	1	1	0	0
14	1	0	1	0
15	1	1	0	0
17	1	1	0	0
19	1	1	0	0
21	0	0	1	1
22	0	1	1	0
23	0	0	1	1

Table 3.1: Ranks of elliptic curves

For $p = 5$, Y_p has genus 3.

For $p = 7$, Y_p has genus 5 and is explicitly given by

$$\frac{3^3 g_4^3}{JF^3} = \frac{(t^2+5t+1)^3(t^2+13t+49)}{t}. \tag{3.37}$$

We see that Y_7 maps (over $\mathbb{Q}$) to the curve

$$C_7' : s^3 = Jt^2(t^2+13t+49).$$

One easily check that C_7' has genus 2 and that the map given by

$$(s,t) \mapsto (x,y) := \left(\frac{s}{t}, J\left(t - \frac{49}{t}\right)\right)$$

defines a birational morphism from C_7' to

$$C_7 : y^2 = (x^3 - 13J)^2 - (14J)^2$$

with inverse

$$(x,y) \mapsto (s,t) = \left(\frac{x(x^3+y-13J)}{2J}, \frac{x^3+y-13J}{2J}\right).$$

We note that for $J = 1$ the jacobian of C_7 is isogenous to the abelian variety associated to the pair of conjugate newforms of level 63.

For $p = 13$, Y_p has genus 11 and is explicitly given by

$$\frac{3^3 g_4^3}{JF^3} = \frac{(t^4+7t^3+20t^2+19t+1)^3(t^2+5t+13)}{t}. \tag{3.38}$$

We see that Y_{13} maps (over $\mathbb{Q}$) to the curve

$$C'_{13} : s^3 = Jt^2(t^2 + 5t + 13).$$

One easily checks that C'_{13} has genus 2 and that the map given by

$$(s,t) \mapsto (x,y) := \left(\frac{s}{t}, J\left(t - \frac{13}{t}\right)\right)$$

defines a birational morphism from C'_{13} to

$$C_{13} : y^2 = (x^3 - 5J)^2 - 13(2J)^2$$

with inverse

$$(x,y) \mapsto (s,t) = \left(\frac{x(x^3 + y - 5J)}{2J}, \frac{x^3 + y - 5J}{2J}\right).$$

We note that for $J = 1$ the jacobian of C_{13} is isogenous to the abelian variety associated to a certain pair of conjugate newforms of level 117.

We conclude that for $p = 7, 13$, proving irreducibility of the Galois representation associated to the p-torsion of the Frey curve (3.18) is reduced to finding rational points on a genus 2 curve.

3.3 Applications to some Diophantine equations

The Frey curve constructions and irreducibility results we have obtained will be applied to some Diophantine equations. We will also solve the generalized Fermat equation $x^2 + y^{2l} = z^3$ for $l = 31$ by combining modular and classical methods.

3.3.1 The equation $x^2 + y^{2l} = z^3$

In [Che], the equation

$$x^2 + y^{2l} = z^3 \quad x, y, z \in \mathbb{Z} \quad (x, y, z) = 1 \quad xyz \neq 0 \tag{3.39}$$

with l a prime is studied. In particular an explicit criterion is given to check that for a given prime $l > 7$ (3.39) has no solution. This criterion is verified for all primes $7 < l < 10^7$ except $l = 31$. We will describe how extra local information obtained from classical algebraic number theory solves the equation for $l = 31$. We will also apply our irreducibility results to solve the equation for $l = 5$. Note that the case $l = 7$ follows from [PSS] (there are no solutions). Before we solve (3.39) for $l = 5, 31$, we briefly describe the method of [Che].

It is easily shown that a solution to $a^2 + b^2 = c^3$ where $a, b, c \in \mathbb{Z}$, $(a, b, c) = 1$ and $abc \neq 0$ satisfies $(a, b, c) = (u(u^2 - 3v^2), v(3u^2 - v^2), u^2 + v^2)$ for some $u, v \in \mathbb{Z}$ with $(u, v) = 1$ and $uv \neq 0$. So a solution x, y, z to (3.39) would give rise to a solution of

$$v(3u^2 - v^2) = y^l \quad u, v, y \in \mathbb{Z} \quad (u, v) = 1 \quad uvy \neq 0. \tag{3.40}$$

Now suppose that u, v, y is a solution to this equation. Then up to primes dividing $(v, 3u^2 - v^2)$, both v and $3u^2 - v^2$ must be l-th powers. It is easily checked that $(v, 3u^2 - v^2)$ equals either 1 or 3. These two cases are going to be considered separately.

First suppose $(v, 3u^2 - v^2) = 1$. Then $v = r^l$ and $3u^2 - v^2 = s^l$ for some $r, s \in \mathbb{Z}$. Furthermore $(r, s, u) = 1$, $rsu \neq 0$ and $(r^2)^l + s^l = 3u^2$. However, [BS, Theorem 1.1] tells us that $x^l + y^l = 3z^2$ has no nontrivial proper solutions for $l \geq 5$.

Now suppose $(v, 3u^2 - v^2) = 3$. Then $3|v$ and of course $3 \nmid u$, so $3||3u^2 - v^2$. We get that $3v = r^l$ and $3u^2 - v^2 = 3s^l$ for some $r, s \in \mathbb{Z}$. Furthermore, $3 \nmid s$ and r, s, u are nonzero pairwise coprime. To a solution, we associate the Frey curve

$$E_{u,v} : Y^2 = \begin{cases} X^3 + 2uX^2 + \frac{v^2}{3}X & \text{if } u \text{ is even;} \\ X^3 \pm uX^2 + \frac{v^2}{12}X, \ \pm u \equiv 1 \pmod 4 & \text{if } u \text{ is odd.} \end{cases} \tag{3.41}$$

Note that if u is even, then v is odd (since $(u, v) = 1$). Also, if u is odd, then v is even. This is because if both u, v are odd, then $v(3u^2 - v^2) \equiv 2 \pmod 4$, but this contradicts that $v(3u^2 - v^2)$ is an l-th power (with $l > 1$). It can readily be shown (using irreducibility, modularity and level lowering theorems) that if u is odd for $l > 7$ $E_{u,v}$ would give rise to a newform of level 6. This is impossible by Proposition 38, so from now on we assume that u is even. Since $E = E_{u,v}$ has a rational 2-torsion point, Theorem 22 tells us that ρ_l^E is irreducible for primes $l > 7$. For the (not necessary minimal) discriminant Δ of E we have $\Delta = 64/27(3u^2 - v^2)v^4 = 64s^l r^{4l}$ and for primes $p \geq 5$ it is minimal. The conductor N of E is given by $N = 96 \operatorname{rad}_{\{2,3\}}(rs)$. Now from (2.7) we compute $N_0(N, l) = 96$ and from Theorem 35 we get that $E \sim_l f$ for some newform f of level 96. In fact there are two such newforms, both rational and quadratic twists of each other (to each of them we can associate a corresponding elliptic curve from the isogeny class, say number 96a1 and 96b1 from [Cre2], they are given by the equation $Y^2 = X^3 \pm X^2 - 2X$). Let E_0 denote an elliptic curve such that $E \sim_l E_0$. Note that since E_0 is uniquely determined up to isogeny and quadratic twist, we have that $a_q(E_0)^2$ is uniquely determined for all primes q. For an odd prime l, let $n \in \mathbb{Z}_{>0}$ such that $q := nl+1$ is prime. Now if v or $3u^2 - v^2$ is divisible by q, then E has multiplicative reduction at q and so $a_q(E_0)^2 \equiv (q+1)^2 \equiv 4 \pmod l$. Suppose that q is such that $a_q(E_0)^2 \not\equiv 4 \pmod l$, then E has good reduction at q and in particular $q \nmid v$. Define $U := u/(3v)$ and consider the elliptic curve

$$E_U : Y^2 = X^3 + 2UX^2 + \frac{1}{27}X,$$

which is a quadratic twist of $E_{u,v}$. From $3v = r^l$ and $3u^2 - v^2 = 3s^l$, we get $U^2 = 1/(27) + (s/r^2)^l$. Since $q \nmid sr$, we have that $U^2 \equiv 1/27 + \zeta \pmod q$, for some $\zeta \in \mu_n := \{x \in \mathbb{F}_q \mid x^n = 1\}$. If for all such U, $a_q(E_U)^2 \not\equiv a_q(E_0)^2 \pmod l$, then $\rho_l^E \not\simeq \rho_l^{E_0}$ and hence (3.39) has no solutions for this l. According to [Che], it can be checked with this method that (3.39) has no solutions for all primes $l \neq 31$ with $7 < l < 10^7$.

Now we are going to use more local information, to solve (3.39) for $l = 31$. Consider the ring of integers $R := \mathbb{Z}[\sqrt{3}]$, it has class number one and in it we

have the factorization $3u^2-v^2 = (\sqrt{3}u-v)(\sqrt{3}u+v)$. From the restrictions on u, v we see that $(\sqrt{3}u-v, \sqrt{3}u+v) = \sqrt{3}$ and $\sqrt{3}||\sqrt{3}u-v, \sqrt{3}u+v$. From $3u^2-v^2 = 3s^l$, we now obtain $\sqrt{3}u - v = \sqrt{3}x_1^l\epsilon_1, \sqrt{3}u + v = \sqrt{3}x_2^l\epsilon_2$, for certain $x_1, x_2 \in R$ and $\epsilon_1, \epsilon_2 \in R^*$. By Dirichlet's unit theorem $R^* = \langle -1, \epsilon_f \rangle$ for some fundamental unit $\epsilon_f \in R$ (we can take for example $\epsilon_f = 2 + \sqrt{3}$). Let $l := 31, n := 718$ and $q := nl + 1 = 22259$. Then q is prime and it splits in R. Denote by $\mathfrak{q}$ any of the 2 primes of R lying above q and for $x \in R$ denote by $\overline{x}$ the canonical image of x in $R/\mathfrak{q} \simeq \mathbb{F}_q$. One can check that $\overline{\epsilon_f}^n = 1$, and hence that for any unit $\epsilon \in R^*$ we have $\overline{\epsilon} \in \mu_n$. We calculate $a_q(E_0) = \pm 140$, so $a_q(E_0)^2 \equiv 8 \not\equiv 4 \pmod{l}$. So $q \nmid v, 3u^2 - v^2$ and E has good reduction at q. Set $r_3 := \overline{\sqrt{3}}$. We have $3\overline{v} = \zeta_0, r_3\overline{u} - \overline{v} = r_3\zeta_1, r_3\overline{u} + \overline{v} = r_3\zeta_2$ for $\zeta_0, \zeta_1, \zeta_2 \in \mu_n$. Let $U = u/(3v)$ as before, set $\zeta_1' := \zeta_1/\zeta_0, \zeta_2' := \zeta_2/\zeta_0$ and divide by $3r_3\overline{v} = r_3\zeta_0$ to obtain

$$\overline{U} - \frac{1}{3r_3} = \zeta_1', \quad \overline{U} + \frac{1}{3r_3} = \zeta_2'.$$

We conclude that $\overline{U} \in (\mu_n + 1/(3r_3)) \cap (\mu_n - 1/(3r_3))$. This set is easily determined explicitly, the possible values of U are given in the first column of Table 3.2.

$\pm U \pmod q$	$a_q(E_U)$	$a_q(E_U)^2 \pmod l$
127	$\pm$ 20	28
1852	$\mp$ 40	19
2818	$\mp$ 156	1
3146	$\mp$ 172	10
3615	$\pm$ 152	9
3764	$\mp$ 120	16
4419	$\pm$ 148	18
5889	$\pm$ 88	25
7994	$\mp$ 12	20
8058	$\mp$ 248	0
8330	$\mp$ 84	19
10171	$\mp$ 100	18
10561	$\mp$ 180	5

Table 3.2: values of U, a_q and a_q^2

Recall that $a_q(E_0)^2 \equiv 8 \pmod{l}$. From the last column of Table 3.2 we see that $a_q(E_U)^2 \not\equiv a_q(E_0)^2 \pmod{l}$ for all possible U. We conclude that $x^2 + y^{62} = z^3$ has no nontrivial primitive solutions.

Now let $l = 5$. If for the Frey curve $E_{u,v}$ given by (3.41) we would know that $\rho_l^{E_{u,v}}$ is irreducible, then it would readily follow that $x^2+y^{10} = z^3$ has no nontrivial proper solutions. Namely, if u is odd, then we would get a newform of level 6 as before, which is impossible. If u is even, then we apply the method of Kraus. Let $n := 2$ and $q := nl + 1 = 11$. Now $a_q(E_0) = \pm 4$, so $a_q(E_0)^2 \not\equiv 4 \pmod 5$ hence $q \nmid v$. So we only have to consider E_U with $\overline{U}^2 \equiv 1/27 \pm 1 \pmod{11}$. But one easily checks that $1/27 \pm 1$ are not squares in $\mathbb{F}_{11}$. So we are left with the question

of irreducibility. Since $\nu_2(N) = 5$ if u is even, Theorem 23 shows irreducibility in that case. For u odd, we can not apply this theorem. But in any case, we can use Theorem 60 as follows. The Frey curve (3.41) is a quadratic twist of the curve given by

$$Y^2 = X^3 + 3uX^2 + \frac{3v^2}{4}X.$$

This curve is 2-isogenous to the curve given by

$$Y^2 = X^3 - 6uX^2 + 3(3u^2 - v^2)X.$$

And this is a homogenized version of the Frey curve given by (3.24), which is a twist over $\mathbb{Q}(\sqrt{3})$ of the Frey curve (3.8) associated to the binary cubic form $v(3u^2 - v^2)$, call this last curve F. So $\rho_l^{E_{u,v}}$ is irreducible if and only if ρ_l^F is irreducible. Since the binary quadratic form has discriminant $2^2 \cdot 3^3$, Theorem 60 and Table 3.1 show that ρ_5^F is irreducible. So $\rho_5^{E_{u,v}}$ is also irreducible. We conclude that $x^2 + y^{10} = z^3$ has no nontrivial proper solutions.

3.3.2 The equation $x^3 + y^3 = z^l$

In [Kra4, Théorème 3.1] an explicit criterion for primes $l \geq 17$ is given, such that if this criterion holds for a certain l, then the equation $x^3 + y^3 = z^l$ has no nontrivial proper solutions. According to *loc. cit.* this criterion holds for all l with $17 \leq l \leq 10000$. To a hypothetical solution (x, y, z) the Frey curve

$$E_{x,y} : Y^2 = X^3 + 3xyX + y^3 - x^3 \tag{3.42}$$

is associated. If for $l = 5, 7, 11, 13$ the Galois representation $\rho_l^{E_{x,y}}$ is irreducible, then we would also have this criterium for these l. Since $E_{x,y}$ has a rational 2-torsion point, the irreducibility for $l = 7, 11, 13$ follows from Theorem 22 (the fact that $j_{E_{x,y}} \neq -3^3 \cdot 5^3, 3^3 \cdot 5^3 \cdot 17^3$ is easily verified). For $l = 5$ we can use Theorem 60. Indeed, the binary cubic form $x^3 + y^3$ has discriminant $-27 = -3 \cdot 3^2$ and the associated Frey curve (3.8) is given by $Y^2 = X^3 + 27xyX + 27(x^3 - y^3)$, which is a twist over $\mathbb{Q}(\sqrt{-3})$ of $E_{x,y}$. One easily verifies that $j_{E_{x,y}} \neq 2^{12} \cdot 5/3^5, -2^{12} \cdot 5^2/3$, so Theorem 60 tells us that $\rho_5^{E_{x,y}}$ is irreducible.

We checked that the criterion in *loc. cit.* holds for $l = 5, 7, 11, 13$ and conclude that $x^3 + y^3 = z^l$ has no nontrivial proper solutions for $l = 5, 7, 11, 13$. In fact, the values in Table 3.3 could be added to Tableau 1 of *loc. cit.* (where p is used instead of l).

p	n
5	2
7	10
11	2
13	10

Table 3.3: Pairs (p, n) satisfying the conditions of [Kra4, Théorème 3.1]

Remark 61. In [Bru], it is shown that the nontrivial proper solutions to $x^3 + y^3 = z^l$ for $l = 4, 5, 7, 11, 13$ can be found by finding rational points on certain hyperelliptic curves. Chabauty methods are used to show that for $l = 4, 5$ there are no nontrivial proper solutions. It is also remarked that the method in [Kra4] might be extended to $l = 5, 7, 11, 13$ if one knows the irreducibility of $\rho_l^{E_{x,y}}$ (with $E_{x,y}$ as above) and arguments for the irreducibility in the cases $l = 7, 11, 13$ are mentioned.

3.3.3 The equation $f(x) = y^l$

In this section we study some equations of the form

$$f(x) = y^l \quad x, y \in \mathbb{Z} \quad y \neq 0, \tag{3.43}$$

where $f(x) \in \mathbb{Q}[x]$ and $l \in \mathbb{Z}_{\geq 2}$ (we will focus on the case that l is an odd prime as usual). Due to [SchTij] we know that if $f(x)$ has at least two different roots, then there exists an effectively computable constant $C \in \mathbb{Z}_{>0}$ (depending on f) such that (3.43) has no solutions for $l > C(f)$. If $f(x)$ is separable and of degree 3, then we have at least one Frey curve for (3.43) (namely the dehomogenized version of (3.8)), and if $f(x) \pm 1$ has no rational roots, we suspect (based on heuristics) that for every prime l, up to finitely many exceptions, the method of Kraus can be used to prove that (3.43) has no solutions.

The equation $x^3 - x - 2 = y^l$

We start with an example where $f(x)$ has degree 3. Furthermore, this example illustrates how the methods from section 3.2 can be used to obtain irreducibility results, even if Theorem 60 does not apply. Consider the equation $x^3 - x - 2 = y^l$. To a hypothetical solution $x, y, l \in \mathbb{Z}$ with $l \geq 3$, we can associate the dehomogenized version of the Frey curve given by (3.8). After a twist over $\mathbb{Q}(\sqrt{3})$ and a linear change of the X variable we arrive at the Frey curve

$$E_x : Y^2 = X^3 + X^2 - x(6 + x)X - (2x^3 + x^2 + 4x + 4). \tag{3.44}$$

The minimal discriminant $\Delta_{\min}$ and conductor N are, according to appendix A, given by

$$\begin{aligned} \Delta_{\min} &= -\frac{13}{2^5}(x^3 - x - 2)^2 = -\frac{13}{2^5}y^{2l}, \\ N &= 2 \cdot 13 \operatorname{rad}_{\{2,13\}}(x^3 - x - 2) = 2 \cdot 13 \operatorname{rad}_{\{2,13\}}(y). \end{aligned}$$

So we have $N_0 := N_0(E_x, l) = 2 \cdot 13 = 26$. There are 2 newforms at level 26, both rational. Let $E26a, E26b$ be elliptic curves associated to these newforms from the isogeny classes $26a, 26b$ respectively, with notation from [Cre2]. Suppose for now that $\rho_l^{E_x}$ is irreducible. Then by Theorem 35 we have $E_x \sim_l E26a$ or $E_x \sim_l E26b$. Now suppose that $E_x \sim_l E26b$. Since E_x has good reduction at 3, Theorem 36 tells us that $a_3(E_x) \equiv a_3(E26b) \pmod{l}$. We have $a_3(E26b) = -3$ and by plugging in the values $x' = 0, 1, 2$ in $E_{x'}$, we see that in any case $a_3(E_x) = 1$. So $l|4$,

a contradiction. So $E_x \sim_l E26a$. Since for $x' = -2, 6, 38/25$ we have that $E_{x'}$ is isogenous to $E26a$ we can not obtain a contradiction by the previous method. The other methods to obtain a contradiction for infinitely many l do also not apply. So we will use the method of Kraus to eliminate possibilities $E_x \sim_l E26a$ for finitely many l. For this we have to find for a given prime l an $n \in \mathbb{Z}_{>0}$ such that $q := nl + 1$ is prime, $a_q(E26a) \not\equiv \pm 2 \pmod{l}$ and for all $x' \in \mathbb{F}_q$ with $x'^3 - x' - 2 \in Z_n := \{z \in \mathbb{F}_q \mid z^n = 1\}$ we have $a_q(E_{x'}) \not\equiv a_q(E26a) \pmod{l}$. A straightforward check with the help of a computer gives that for $l = 5$ or primes l with $13 \leq l \leq 10^7$ there exists such n (and presumably there also exists such n for all primes $l > 10^7$). It follows that for such l we can not have $E_x \sim_l E26a$. It remains to check the irreducibility of ρ_l^E for these l. Using Theorem 22 we easily check that we have irreducibility for all primes $l \geq 17$ (and for $l = 11$ but we cannot rule out $E_x \sim_{11} E26a$). Theorem 60 gives us irreducibility for $l = 13$, since $\mathrm{Rank}(E_{-26,13}) = 0$ according to Table 3.1. According to this Table we have $\mathrm{Rank}(E_{-26,5}) = 2$, so for $l = 5$ we cannot use Theorem 60. But in fact we do have irreducibility for $l = 5$. Accepting this last claim for the moment, we arrive at the following conclusion.

Proposition 62. *Let l be a prime with $l = 5$ or $13 \leq l < 10^7$. Then the equation $x^3 - x - 2 = y^l$ has no solutions with $x, y \in \mathbb{Z}$.*

Let us now show that $\rho_5^{E_x}$ is irreducible by performing an explicit descent. Let $F(x), H(x), G(x)$ denote the dehomogenized versions of (3.3), (3.5), (3.6) respectively (so $F(x) = x^3 - x - 2$). Suppose $\rho_5^{E_x}$ is not irreducible. Then (by considering $j - 1728$) we have,

$$\frac{\left(\frac{G(x)}{2}\right)^2}{-2 \cdot 13 \left(\frac{F(x)}{2^3}\right)^2} = \frac{(t^2 + 4ts - s^2)^2((t + 11s)^2 + (2s)^2)}{ts^5}$$

for $x, s, t \in \mathbb{Z}$ with s, t nonzero and coprime. Since $F(x) \equiv 0 \pmod 2$, we have $F(x) \equiv 0 \pmod{2^3}$ and consequently $x \equiv 6 \pmod{2^3}$. So $G(x)/2 = 27x^3 + 9x^2 + 27x + 53 \equiv 1 \pmod 2$ and $F(x)/2^3 \in \mathbb{Z}$. Also, $\mathrm{Res}_x(F(x)/2^3, G(x)/2) = 13^3$, but $13 \nmid G(x)$ (if $G(x) \equiv 0 \pmod{13}$, then $x \equiv 10 \pmod{13}$, but then $F(x) \equiv 0 \pmod{13}$, so $F(x) \equiv 0 \pmod{13^2}$, but then $x \equiv 162 \pmod{13^2}$, so $x \equiv 6 \pmod{13}$, contradiction). So $(G(x)/2)^2$ and $-2 \cdot 13(F(x)/2^3)^2$ are coprime. From

$$\frac{(t^2 + 10ts + 5s^2)^3}{ts^5} = \frac{2^8 H(x)^2}{-2 \cdot 13 F(x)^2}$$

and the fact that always $H(x), F(x) \not\equiv 0 \pmod 5$, we obtain that $5 \nmid t$ or $5^3 || t$. First suppose that $5 \nmid t$. In this case $(t^2 + 4ts - s^2)^2((t^2 + 11s)^2 + (2s)^2)$ and ts^5 are coprime. So

$$\left(\frac{G(x)}{2}\right)^2 = (t^2 + 4ts - s^2)^2((t + 11s)^2 + (2s)^2) \tag{3.45}$$

(left- and right hand side are both positive, so the sign is right). Now $t + 11s$ and $2s$ are coprime and $(t + 11s)^2 + (2s)^2$ must be a square, hence $t + 11s = u^2 - v^2$

and $2s = 2uv$ for some coprime $u, v \in \mathbb{Z}$. This gives us $s = uv, t = u^2 - 11uv - v^2$. Substituting these values in (3.45), we can factor and obtain

$$27x^3 + 9x^2 + 27x + 53 = \pm(u^4 - 18u^3v + 74u^2v^2 + 18uv^3 + v^4)(u^2 + v^2). \quad (3.46)$$

Now these equations have no solutions with $x \equiv 6 \pmod 8$, contradiction. Now suppose that $5^3 || t$. In this case $((t^2 + 4ts - s^2)^2((t^2 + 11s)^2 + (2s)^2), ts^5) = 5^3$. Write $t = 5^3T$, then we obtain

$$\left(\frac{G(x)}{2}\right)^2 = (5^6T^2 + 4 \cdot 5^3Ts - s^2)^2((s + 11T)^2 + (2T)^2). \quad (3.47)$$

Along the same lines as before we conclude that $x \not\equiv 6 \pmod 8$ (in fact, after performing the transformation $(T, s) \mapsto (s, t)$ in (3.47) we obtain mod 8 the same equation as in (3.45)). We conclude that $\rho_5^{E_x}$ is irreducible.

As remarked earlier, one can easily obtain similar results as Proposition 62 with $x^3 - x - 2$ replaced by another separable cubic $f(x) \in \mathbb{Z}[x]$ such that $f(x) \pm 1$ is irreducible. Examples where the levels N_0 are relatively low are given e.g. by $f(x) = x^3 - 6x - 2, f(x) = x^3 + x^2 - x - 3$.

The equation $x^3 + 13 = y^l$

Consider the equation $x^3 + 13 = y^l$ for $x, y \in \mathbb{Z}$ and l prime. Although it is nice to see the modular method in action for small primes, we will assume $l > 19$ here. To a hypothetical solution we associate the Frey curve

$$E_x : Y^2 = X^3 - 3x^2X \pm 2(x^3 + 26),$$

where the $+$ sign is chosen if x is even and the $-$ sign otherwise. According to appendix A the minimal discriminant and conductor are given by

$$\begin{aligned} \Delta_{\min} &= -2^8 \cdot 3^3 \cdot 13(x^3 + 13)/2^c = -2^{8-c} \cdot 3^3 \cdot 13y^l, \\ N &= 2^a 3^b 13 \operatorname{rad}_{\{2,3,13\}}(x^3 + 13) = 2^a 3^b 13 \operatorname{rad}_{\{2,3,13\}}(y), \end{aligned}$$

where $a = 1$, $c = 12$ if x is odd and $a \in \{2, 3\}$, $c = 0$ otherwise, in both cases $b \in \{2, 3\}$. So $N_0 := N_0(E_x, l) = 2^a \cdot 3^b \cdot 13$. At these level there are a total of 76 newforms of which 53 are rational. Let f be such a newform, it turns out that comparing $a_p(E_x)$ to $a_p(f)$ for $p = 5, 7, 31$ leads to our desired result. Irreducibility of $\rho_l^{E_x}$ follows again from Theorem 22. Let $p = 7$, then E_x has bad reduction at p if and only if $x \equiv 1, 2, 4 \pmod 7$. Plugging in the other values of x modulo 7, we get that if $7 \nmid y$, then $a_7(E_x) = \{-5, 3\}$ if x is even and $a_7(E_x) = \{5, -3\}$ if x is odd. If x is odd, it turns out that no newform at level N_0 has $a_7(f) \in \{-3, 5\}$. If x is even, then the only *rational* newforms at level N_0 with $a_7(f) \in \{-5, 3\}$ correspond (with notation from [Cre2]) to the elliptic curves $E2808e$ and $E2808n$. But we can take $p = 31$. We first of all note that $31 \nmid x^3 + 13$, plugging the 31 possible values modulo 31 into E_x we get that $a_{31}(E_x) \neq 9$, but $a_{31}(E2808e) = a_{31}(E2808n) = 9$. At this point we know that the modular method implies that there exists an $L \in \mathbb{Z}_{>0}$ such that for all primes $l > L$ we have that

$x^3 + 13 = y^l$ has no solutions in $x, y \in \mathbb{Z}$. We can even get an a priori estimate for L without considering the newforms at level N_0 anymore, but since they are available we can get without too much trouble the nice bound $L = 19$ as follows. Fix a newform f at some level N_0 not corresponding to $E2808e$ or $E2808n$ and, with notation as in Theorem 37, calculate the primes dividing $F_5(a_5(E_x))$ for all possible $a_5(E_x)$ when E_x has good reduction modulo 5 (for x even and x odd we both have $a_5(E_x) \in \{0, -1, 1, 4\}$) and calculate the primes dividing $F_5(\pm 6)$, call this set of primes P_5. For $p = 7$ we similarly calculate the set P_7. Now it turns out that the intersection of P_5 and P_7 contains no primes bigger than 19, so by Theorem 37 it follows that we cannot have $E_x \sim_l f$ for $l > 19$. Furthermore, no primes greater than 19 divide $a_{31}(E_x) - a_{31}(E2808e)$ or $a_{31}(E_x) - a_{31}(E2808n)$ (for the 31 different values of x modulo 31) and we arrive at the following result.

Proposition 63. *Let $l > 19$ be prime. Then the equation $x^3 + 13 = y^l$ has no solutions with $x, y \in \mathbb{Z}$.*

After writing this down we realized that the preceding result is actually a special case of [BVY, Theorem 1.6], but we think it still provides an instructive example.

The equation $x^4 + x^3 - 3x^2 + 11x + 2 = y^l$

Let us also consider an example of (3.43) where $f(x)$ has degree 4. Consider the equation $f(x) := x^4 + x^3 - 3x^2 + 11x + 2 = y^l$ for $x, y \in \mathbb{Z}$ and $l > 19$ prime. To a hypothetical solution we can associate the dehomogenized version of the Frey curve given by (3.18). After a twist over $\mathbb{Q}(\sqrt{-1})$ we arrive at the Frey curve

$$E_x : Y^2 = X^3 - 3a(x)X - 2b(x),$$

where

$$\begin{aligned} a(x) &:= 9x^4 - 92x^3 - 42x^2 - 60x + 137 \\ b(x) &:= 101x^6 + 30x^5 + 795x^4 - 2380x^3 - 1605x^2 + 654x - 1627. \end{aligned}$$

From appendix A we have

$$\begin{aligned} \Delta_{\min} &= -2^2 \cdot 3^3 \cdot 37 f(x)^3 = -2^2 \cdot 3^3 \cdot 37 y^{3l}, \\ N &= 2 \cdot 3^2 \cdot 37 \operatorname{rad}_{\{2,3,37\}}(f(x)) = 2 \cdot 3^2 \cdot 37 \operatorname{rad}_{\{2,3,37\}}(y). \end{aligned}$$

So we have $N_0 := N_0(E_x, l) = 2 \cdot 3^2 \cdot 37 = 666$. At this level there are 11 newforms of which 7 are rational. Irreducibility of $\rho_l^{E_x}$ follows again from Theorem 22. We note that for $p = 5, 7$ we have $p \nmid f(x)$ and the possible values for $a_p(E_x)$ are given by $a_5(E_x) \in \{-2, 1, 4\}, a_7(E_x) \in \{-3, 0, 3\}$. By using a_7 we can eliminate the nonrational newforms and by using a_5 we can eliminate 4 of the 7 rational newforms. Elliptic curves associated to the 3 newforms we are left with are given by (with notation from [Cre2]) $E666d1, E666f1, E666g1$ (which are isomorphic to E_x for $x = 0, 2, -22/7$ respectively). A straightforward application of Kraus's method eliminates these curves for primes l with $19 < l < 10^7$.

Proposition 64. *The equation $x^4 + x^3 - 3x^2 + 11x + 2 = y^l$ has no solutions with $x, y \in \mathbb{Z}$ and l prime with $19 < l < 10^7$.*

Chapter 4

The quintic and $ax^2 + by^3 = cz^5$

In this chapter we will depart form the modular method and use classical methods to find all parameterized solutions to the Diophantine equation

$$ax^2 + by^3 = cz^5 \quad x, y, z \in \mathbb{Z} \quad \gcd(x, y, z) = 1 \quad xyz \neq 0, \tag{4.1}$$

where $a, b, c \in \mathbb{Z}$ are given nonzero integers. Our approach is inspired by 19-th century mathematics about quintic (univariate) polynomials as can be found e.g. in [Kie], [Kle], or the modern text [Kin]. As a starting point we need however a certain (finite) list of quintic polynomials $f \in \mathbb{Q}[t]$ such that the algebra $\mathbb{Q}[t]/(f(t))$ is unramified outside $\{2, 3, 5\}$ and the primes dividing abc. This list can in principle be found in finite time, but in practice takes very long and it is the computational bottle neck of our algorithm to obtain the solutions to (4.1). In the case that all primes dividing abc are contained in $\{2, 3, 5\}$, such a list is available, see [JR]. In the next chapter we will show how in some cases the modular method can be used to obtain this list. In [Edw] an algorithm to obtain parameterized solutions for (4.1) was given for the first time, and the solutions with $a = b = c = 1$ were obtained. For slightly larger values of the coefficients it becomes in practice infeasible to obtain solutions with this algorithm. By using our algorithm we obtained for the first time an example of the violation of the so called local-to-global principle for (4.1).

4.1 Strategy and preliminaries

Consider the covering $\mathbb{P}^1 \to \mathbb{P}^1$ given by the polynomial

$$\phi(t) := t^3(t^2 + 5t + 40) = (t^2 + 4t + 24)^2(t - 3) + 1728, \tag{4.2}$$

it is unramified outside $0, 1728, \infty$ with ramification indices multiples of $3, 2, 5$ respectively. The dessin d'enfant of $\phi(t)/1728$ is given in Figure 4.1.

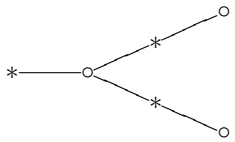


Figure 4.1: dessin d'enfant associated to $\phi(t)/1728$

Let

$$f_j(t) := \phi(t) - j,$$

it has discriminant

$$\mathrm{Disc}_t(f_j(t)) = 5^5 j^2 (j - 1728)^2. \tag{4.3}$$

Let $a, b, c \in \mathbb{Z} - \{0\}$, to a solution $x, y, z \in \mathbb{Z}$ of (4.1), we associate the polynomial $f_{j(x,y,z)}(t)$, where

$$j(x, y, z) := 1728 \frac{by^3}{cz^5}. \tag{4.4}$$

Note that $xyz \neq 0$ implies that $j(x, y, z) \in \mathbb{Q} - \{0, 1728\}$. Let S_{abc} denote the set of primes dividing $2 \cdot 3 \cdot 5abc$.

Proposition 65. *Let $a, b, c \in \mathbb{Z} - \{0\}$ and let x, y, z be a solution to (4.1). Then $A := \mathbb{Q}[t]/(f_{j(x,y,z)}(t))$ is an étale algebra over $\mathbb{Q}$ of degree 5, unramified outside S_{abc}, with $\mathrm{Disc}(A) \equiv 5 \pmod{(\mathbb{Q}^*)^2}$. Furthermore, $f_j(x, y, z)$ has exactly one real root.*

Proof. As remarked before, we have $j(x, y, z) \neq 0, 1728$ and by (4.3) we get that $\mathrm{Disc}_t(f_j(t)) \neq 0$ and in fact

$$\mathrm{Disc}_t(f_j(t)) \equiv 5 \pmod{(\mathbb{Q}^*)^2}.$$

So A is an étale algebra over $\mathbb{Q}$ of degree 5, with

$$\mathrm{Disc}(A) \equiv \mathrm{Disc}_t(f_j(t)) \equiv 5 \pmod{(\mathbb{Q}^*)^2}.$$

For every $t \in \mathbb{R}$ we have

$$\frac{d}{dt}\phi(t) = 5t^2((t + 2)^2 + 20) \geq 0,$$

and since $\phi(t)$ has odd degree, it is bijective considered as a function from $\mathbb{R}$ to $\mathbb{R}$. This shows that for every $j \in \mathbb{R}$ f_j has exactly one real root (if we take multiplicities into account we must exclude $j = 0$, but $j(x, y, z) \neq 0$ anyway).

That A is unramified outside S_{abc} follows directly from the ramification properties of ϕ and Corollary 11 (or alternatively, from [Bec, Theorem 1.2] since the icosahedral covering factors through ϕ). □

The algebras A of the proposition are of course of the following form (i.e. isomorphic to)

- $\mathbb{Q} \times \mathbb{Q}(\sqrt{d'}) \times \mathbb{Q}(\sqrt{5d'})$
- $\mathbb{Q}(\sqrt{d}) \times K_3$
- $\mathbb{Q} \times K_4$
- K_5,

where d, d' are of the form $d' = -\prod_{p \in S_{abc}-\{5\}} p^{\epsilon_p}$, $d = -\prod_{p \in S_{abc}} p^{\epsilon_p}$ and $\epsilon_p \in \{0,1\}$ not all zero, K_n is a number field of degree n, unramified outside S_{abc}, with the maximum number of complex embeddings, K_4, K_5 have their discriminants in $5(\mathbb{Q}^*)^2$ and K_3 has its discriminant in $5d(\mathbb{Q}^*)^2$ (the sum of the real embeddings must be one, since f_j has exactly one real root).

The key to obtain the parameterized solutions to (4.1) is as follows. By Hermite's theorem there are only finitely many algebras as above (for fixed a, b, c). Suppose that we have a list $A_1, \ldots, A_n$ of them given by polynomials $F_1, \ldots F_n \in \mathbb{Q}[t]$, in the sense that $A_i \simeq \mathbb{Q}[t]/(F_i(t))$. The first step in solving (4.1) is to find necessary and sufficient conditions to determine if $\mathbb{Q}[t]/(F_i(t)) \simeq \mathbb{Q}[t]/(f_j(t))$ for some $j \in \mathbb{Q} - \{0, 1728\}$. Next, if F_i is of this form, we want to describe all such $j \in \mathbb{Q} - \{0, 1728\}$ such that $\mathbb{Q}[t]/(F_i(t)) \simeq \mathbb{Q}[t]/(f_j(t))$. This leads to a description of all quotients $x^3/z^5 \in \mathbb{Q}$, and finally we need to determine all solutions $x, y, z \in \mathbb{Z}$ from these quotients. This program will be carried out in the next two sections. But first we will discuss Tschirnhausen transformations, quintic resolvents and quadratic forms.

4.1.1 Tschirnhausen transformations

Let K be a field and let $F \in K[t]$ be monic, separable and of degree n. Any element $s \in K[t]/(F(t))$ is of the form $s = \sum_{k=0}^{n-1} c_k t^k$, $c_k \in K$ (where we identify t with its image in $K[t]/(F(t))$) and s satisfies $G(s) = 0$, where

$$G(s) := \mathrm{Res}_t \left(F(t), s - \sum_{k=0}^{n-1} c_k t^k \right). \tag{4.5}$$

If $F, G \in K[t]$ are monic, separable and $K[t]/(F(t)) \simeq K[t]/(G(t))$, then we call F and G *equivalent*, denoted $F \sim G$. We obviously have the following.

Lemma 66. *Let $F, G \in K[t]$ be monic, separable and of degree n. Then $F(t) \sim G(t)$ if and only if $G(s) = \mathrm{Res}_t(F(t), s - \sum_{k=0}^{n-1} c_k t^k)$ for certain $c_0, \ldots, c_{n-1} \in K$.*

Again, let $F(t) \in K[t]$ be monic separable and of degree n, and consider $c_0, \ldots, c_{n-1}$ now as variables. Let $G(s) \in K[s, c_0, \ldots, c_{n-1}]$ be given by (4.5). We claim that

$$\mathrm{Disc}_s(G(s)) = \mathrm{Disc}_t(F(t)) I(c_0, \ldots, c_{n-1})^2, \tag{4.6}$$

where $I(c_0, \ldots, c_{n-1}) \in K[c_0, \ldots, c_{n-1}] - \{0\}$. To prove this, let $t_i, i = 1, \ldots, n$ denote the roots of $F(t)$ (in some algebraic closure of K), then the roots s_i of $G(s)$ are give by $s_i = \sum_{k=0}^{n-1} c_k t_i^k$. We obtain (dropping the index of the roots for a moment)

$$s^j = \sum_{i=0}^{n-1} p_{i,j} t^i,$$

for certain $p_{i,j} \in K[c_0, \ldots, c_{n-1}]$. So, if we define the n by n matrices, S, T, P as $S := (s_i^{j-1})_{i,j=1}^n, T := (t_i^{j-1})_{i,j=1}^n, P := (p_{i-1,j-1})_{i,j=1}^n$, then $S = TP$ and by evaluating Vandermonde determinants we obtain

$$\mathrm{Disc}_s(G(s)) = \mathrm{Det}(S)^2 = \mathrm{Det}(T)^2 \mathrm{Det}(P)^2 = \mathrm{Disc}_t(F(t)) \mathrm{Det}(P)^2,$$

where $\mathrm{Det}(P) \in K[c_0, \ldots, c_{n-1}]$, and we see that $\mathrm{Det}(P) \neq 0$ by evaluating at $(c_0, c_1, c_2, \ldots, c_{n-1}) = (0, 1, 0 \ldots, 0)$. This proves our claim.

4.1.2 Quintic resolvents

In this section, let K be a field of characteristic 0. The explicit calculations we are going to perform with quintics in section 4.2 are related to the geometry and invariant theory of the icosahedron, for which we refer to [Kle] or [Kin] (especially pp. 103-106). We actually only need very little of this and most of the facts we use are readily checked.

We have the following icosahedral invariants

$$\begin{aligned} f &:= uv(u^{10} + 11u^5v^5 - v^{10}), && (4.7)\\ H &:= -u^{20} + 228u^{15}v^5 - 494u^{10}v^{10} - 228u^5v^{15} - v^{20}, && (4.8)\\ T &:= u^{30} + 522u^{25}v^5 - 10005u^{20}v^{10} && (4.9)\\ &\quad -10005u^{10}v^{20} - 522u^5v^{25} + v^{30}, \end{aligned}$$

satisfying $T^2 + H^3 = 1728f^5$. And the octahedral invariants

$$\begin{aligned} \tau &:= uv(u^4 - v^4)\\ W &:= u^8 + 14u^4v^4 + 8v^8\\ \chi &:= u^{12} - 33u^8v^4 - 33u^4v^8 + v^{12}, \end{aligned}$$

satisfying $-\chi^2 + W^3 = 108\tau^4$. Let $\zeta = \zeta_5$ be a primitive 5-th root of unity, for $k = 0, \ldots, 4$ we consider rotated octahedral invariants

$$\begin{aligned} t_k &:= \zeta^{3k}u^6 + 2\zeta^{2k}u^5v - 5\zeta^k u^4v^2 - 5\zeta^{4k}u^2v^4 - 2\zeta^{3k}uv^5 + \zeta^{2k}v^6\\ W_k &:= -\zeta^{4k}u^8 + \zeta^{3k}u^7v - 7\zeta^{2k}u^6v^2 - 7\zeta^k u^5v^3 +\\ &= 7\zeta^{4k}u^3v^5 - 7\zeta^{3k}u^2v^6 - \zeta^{2k}uv^7 - \zeta^k v^8. \end{aligned}$$

A straightforward calculation gives

$$\prod_{k=0}^{4}(t - t_k) = t^5 - 10ft^3 + 45f^2t - T$$

called the Brioschi quintic. Rescaling the roots by a factor $r := T/f^2$ leads to a principal quintic only depending on one parameter j (or $Z(j)$)

$$h_j(t) := \prod_{k=0}^{4}(t - t_k/r) = t^5 - 10Z(j)t^3 + 45Z(j)^2t - Z(j)^2, \tag{4.10}$$

where $Z(j) := 1/(1728 - j) = f^5/T^2$. This quintic has its coefficient of t^4 equal to zero, a quintic with this property is by definition called *depressed*, if a quintic $\in K[t]$ also has its coefficient of t^3 equal to zero, it is called *principal*. Much more interesting than the Brioschi quintic for our purposes is a whole family of principal quintics. For $\lambda, \mu \in K$ we let

$$s_k := \lambda T W_k + f^2 \mu t_k W_k.$$

Then

$$\prod_{k=0}^{4}(t - s_k) = t^5 + 5a't^2 + 5b't + c',$$

with

$$\begin{aligned} a' &= f^2T(8\lambda^3T^2 + \lambda^2\mu T^2 + 72\lambda\mu^2f^5 + \mu^3f^5) \\ b' &= fH(-\lambda^4T^4 + 18\lambda^2\mu^2f^5T^2 + \lambda\mu^3f^5T^2 + 27\mu^4f^{10}) \\ c' &= H^2T(\lambda^5T^4 - 10\lambda^3\mu^2f^5T^2 + 45\lambda\mu^4f^{10} + \mu^5f^{10}). \end{aligned}$$

Rescaling the roots by a factor $r := HT/f$ leads to a principal quintic only depending on one parameter j (for fixed λ, μ)

$$g_{\lambda,\mu,j}(t) := \prod_{k=0}^{4}(t - s_k/r) = t^5 + 5at^2 + 5bt + c,$$

with

$$a = \left(8\lambda^3 + \lambda^2\mu + 72\lambda\mu^2Z(j) + \mu^3Z(j)\right)/j \tag{4.11}$$

$$b = \left(-\lambda^4 + 18\lambda^2\mu^2Z(j) + \lambda\mu^3Z(j) + 27\mu^4Z(j)^2\right)/j \tag{4.12}$$

$$c = \left(\lambda^5 - 10\lambda^3\mu^2Z(j) + 45\lambda\mu^4Z(j)^2 + \mu^5Z(j)^2\right)/j \tag{4.13}$$

and $Z(j) = 1/(1728 - j)$ as before. Furthermore, we define

$$g_j(t) := g_{1,0,j}(t) = t^5 + \frac{40}{j}t^2 - \frac{5}{j}t + \frac{1}{j}.$$

For $z := u/v$ we consider

$$J(z) := \frac{H^3}{f^5} = \frac{(-z^{20} + 228z^{15} - 494z^{10} - 228z^5 - 1)^3}{z^5(z^{10} + 11z^5 - 1)^5}. \tag{4.14}$$

Let $L := K(\zeta_5)$ and write $j = J(z)$. The extension $L(z)/L(j)$ is Galois with Galois group $A_5 \simeq \mathrm{SL}_2(\mathbb{F}_5)/\{\pm I\}$. In fact, $L(z)/K(j)$ is Galois, and if $[L : K] =$

$4, [L : K] = 2$, then the Galois group of $L(z)/K(j)$ is $\mathrm{GL}_2(\mathbb{F}_5)/\{\pm I\}, \{M \in \mathrm{GL}_2(\mathbb{F}_5) \mid \mathrm{Det}M = \pm 1\}/\{\pm I\}$ respectively. From the construction of $h_j, g_{\lambda,\mu,j}$ we obtain that the fields

$$K_h := K(j)[t]/(h_j(t))$$

and (for $\lambda, \mu \in K$ not both zero)

$$K_g := K(j)[t]/(g_{\lambda,\mu,j})$$

are subextensions of degree 5 over $K(j)$. Furthermore let

$$\begin{aligned} \tau(z) \quad := \quad & z^{-1}(z^{10} + 11z^5 - 1)^{-1}(-z^{12} - z^{11} + 6z^{10} + 20z^9 - 15z^8 \\ & +24z^7 - 11z^6 - 24z^5 - 15z^4 - 20z^3 + 6z^2 + z - 1) \end{aligned} \tag{4.15}$$

and as before

$$\phi(t) := t^3(t^2 + 5t + 40),$$

then

$$J(z) = \phi(\tau(z)).$$

So, with $f_j(t) := \phi(t) - j$ we also have that

$$K_j := K(j)[t]/(f_j(t))$$

is a subextension of degree 5 over $K(j)$. Moreover, since in all three cases of $[L : K]$, the Galois group of $L(z)/K(j)$ has up to conjugation only one subgroup of index 5, we have $K_f \simeq K_g \simeq K_h$. In other words, $f_j(t) \sim g_{\lambda,\mu,j}(t) \sim h_j(t)$ (over $K(j)$).

For $j \in K - \{0, 1728\}$, we can specialize the polynomials $f_j(t), g_{\lambda,\mu,j}(t), h_j(t)$, obtaining (monic) polynomials in $K[t]$. If the discriminant is nonzero we obtain equivalent polynomials over K. For the discriminants we have

$$\begin{aligned} \mathrm{Disc}_t(f_j(t)) &= 5^5 j^2 (j - 1728)^2, \\ \mathrm{Disc}_t(g_j(t)) &= 5^5 \frac{(j - 1728)^2}{j^6}, \\ \mathrm{Disc}_t(h_j(t)) &= 5^5 \frac{j^2}{(j - 1728)^{10}}. \end{aligned}$$

We obtain the following useful fact.

Proposition 67. *Let $j \in K - \{0, 1728\}$. Then $f_j(t) \sim g_j(t) \sim h_j(t)$ (over K). If furthermore $\lambda, \mu \in K$ are such that $\mathrm{Disc}_t(g_{\lambda,\mu,j}) \neq 0$, then $g_{\lambda,\mu,j}$ is also equivalent to $f_j(t), g_j(t), h_j(t)$.*

The relation between $f_j(t)$ and $g_j(t)$ is actually very direct, we simply have

$$jt^5 g_j(-1/t) = f_j(t). \tag{4.16}$$

4.1.3 Quadratic forms

For the convenience of the reader we will recall some basic definitions and properties of quadratic forms (over fields). We will also state and prove some specific lemmas needed later. For (most) proofs of the basic results, we refer to the very nice and accessible [Cas], where most of the time $\mathbb{Q}$, or a completion of it, is taken as a ground field. Almost everything can be generalized to (at least) arbitrary number fields, for this we refer to [O'M]. In this section p will always denote a finite prime of $\mathbb{Q}$ or the archimedean prime (denoted, $p = \infty$).

Quadratic forms over general fields

Let K be a field of characteristic $\neq 2$. A quadratic form over K of *dimension* n is a homogeneous polynomial over K in n variables of degree 2. Call the variables $x_1, \ldots, x_n$. Since by assumption 2 is invertible, we can write

$$f = \sum_{i=1}^{n} c_{i,i} x_i^2 + \sum_{1 \leq i < j \leq n} 2c_{i,j} x_i x_j$$

for certain $c_{i,j} \in K$, $1 \leq i \leq j \leq n$. With $c_{i,j} := c_{j,i}$ for $n \geq i > j \geq 1$ this becomes

$$f = \sum_{1 \leq i,j \leq n} c_{i,j} x_i x_j.$$

To the quadratic form f we can associate the symmetric matrix

$$M := (c_{i,j})_{1 \leq i,j \leq n}.$$

With $x = (x_1, \ldots, x_n)^t$ the column vector of the variables, we have

$$f = x^t M x.$$

The *determinant* of f, denoted $\mathrm{Det}(f)$, is by definition $\mathrm{Det}(M)$. If $\mathrm{Det}(f) = 0$, then we call f *singular*, otherwise we call f *regular*. Let $T \in \mathrm{GL}_n(K)$ and consider the linear change of variables $x = Ty$. With the matrix coefficients $d_{i,j}$ defined by

$$(d_{i,j})_{1 \leq i,j \leq n} = T^t M T,$$

we can write

$$f = \sum_{1 \leq i,j \leq n} d_{i,j} y_i y_j = y^t (T^t M T) y.$$

Linear change of variables obviously defines an equivalence relation on quadratic forms and any two quadratic forms in the same equivalence class are simply called *equivalent* (over K, if the base field is not obvious). Since $\mathrm{Det}(T^t M T) = \mathrm{Det}(M)\mathrm{Det}(T)^2$, we see that up to multiplication with an element in $(K^*)^2$ two equivalent quadratic forms have the same determinant. For a regular quadratic form f, $\mathrm{Det}(f) \mod (K^*)^2$ is an element in the group $K^*/(K^*)^2$ and it obviously is an invariant under the given equivalence relation. By abuse of notation

this element is sometimes simply denoted by $\mathrm{Det}(f)$, no confusion should arise. A regular quadratic form f is called *isotropic* if it represents 0 nontrivially, i.e. $f(x_1, \ldots, x_n) = 0$ for some $x_1, \ldots, x_n \in K$ not all zero. Obviously, being isotropic is preserved under the equivalence relation. Finally we note that, by essentially repeatedly completing the square, any quadratic form is equivalent to a diagonal form, i.e. of the shape $\sum_{i=1}^{n} c_i x_i^2$.

Remark 68. The different (base free) language of quadratic spaces is sometimes more convenient. A *quadratic space* over K of *dimension* $n \in \mathbb{Z}_{\geq 0}$ is an n-dimensional vector space V over K together with a symmetric bilinear form $\phi : V \times V \to K$. For any basis $(v_1, \ldots, v_n)$ of V we define

$$f(x_1, \ldots, x_n) := \phi\left(\sum_{i=1}^{n} x_i v_i, \sum_{i=1}^{n} x_i v_i\right).$$

From the bilinearity we get

$$f(x_1, \ldots, x_n) = \sum_{1 \leq i,j \leq n} c_{i,j} x_i x_j, \; c_{i,j} := \phi(v_i, v_j).$$

So f is a quadratic form over K of dimension n. Furthermore, any quadratic form arises this way and notions from quadratic forms (such as regularity and isotropy) can be translated in a natural and straightforward way to notions for quadratic spaces and vice versa. For example, two quadratic forms are equivalent if and only if they arise from isomorphic (straightforwardly defined) quadratic spaces. For more details (and precise statements) we refer to [Cas].

Lemma 69. *Let f be a regular quadratic form of dimension n. If f is isotropic, then f is equivalent to a quadratic form of the shape $x_1 x_2 + g(x_3, \ldots, x_n)$, where g is a regular quadratic form of dimension $n - 2$.*

Proof. See [Cas, Chapter 2, Lemma 2.1 and Corollary 1]. □

Remark 70. A quadratic form $f(x_1, \ldots, x_n)$ is called *universal* if for all $k \in K$ there exist $x_1, \ldots, x_n \in K$ such that $f(x_1, \ldots, x_n) = k$. From the preceding lemma it is obvious that an isotropic quadratic form is universal. The converse is not true in general, for example the quadratic form $x^2 + y^2$ over $\mathbb{F}_3$ is universal but not isotropic.

We now come to two particular statements needed later.

Lemma 71. *Let f be a regular quadratic form of dimension 4 with $\mathrm{Det}(f) \in (K^*)^2$. Then f is isotropic if and only if f is equivalent to the quadratic form $XY - ZW$.*

Proof. Obviously $XY - ZW$ is isotropic, hence a form equivalent to it is isotropic. Conversely, suppose that f is isotropic. By Lemma 69 and diagonalization, we see that f is equivalent to $g := xy + az^2 + bw^2$. Since $\mathrm{Det}(g) = -ab/4 \in (K^*)^2$, we see that $b = -ak^2$ for a certain $k \in K^*$, so $g = xy + a(z^2 - (kw)^2) = xy - a(kw + z)(kw - z)$ and the regular change of variables, $X := x, Y := y, Z := a(kw + z), W := kw - z$ leads to the equivalent form $XY - ZW$. □

Lemma 72. *Let $a, b, c, d \in K$ such that the quadratic form $f := ax^2 + by^2 + cz^2 + dw^2$ is equivalent to $XY - ZW$. Then $g := ax^2 + by^2 + cz^2$ is isotropic.*

Proof. On the 2-dimensional subspace of the vector space K^4 given by all the (X, Y, Z, W) such that $X = Z = 0$, the quadratic form $XY - ZW$ vanishes. The intersection of a 3-dimensional and a 2-dimensional subspace of K^4 is at least 1-dimensional. This shows that g must be isotropic. □

Quadratic forms over $\mathbb{Q}_p$

For every $a, b \in \mathbb{Q}_p^*$ we define the *Hilbert norm residue symbol*

$$(a, b)_p := \begin{cases} 1 & \text{if } ax^2 + by^2 - z^2 \text{ is isotropic over } \mathbb{Q}_p; \\ -1 & \text{otherwise.} \end{cases}$$

Obviously, $(a, b)_p$ only depends on $a, b \mod (\mathbb{Q}_p^*)^2$.

Lemma 73. *For $a, b \in \mathbb{Q}_p^*$ we have*

i. $(a, b)_p = (b, a)_p$

ii. $(a_1 a_2, b)_p = (a_1, b)_p (a_2, b)_p$

iii. if $p \neq 2, \infty$ and $|a|_p = |b|_p = 1$, then $(a, b)_p = 1$.

Proof. See [Cas, Chapter 3, Lemma 2.1] (i. follows of course directly from the definition). □

The Hilbert norm residue symbol can easily be calculated effectively. In fact $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ is finite and there are essentially 4 tables (distinguishing between $p = 2, p \equiv 1 \pmod 4, p \equiv -1 \pmod 4$ and $p = \infty$) giving the values of the symbol, see [Cas, pp. 43-44]. For fixed $a, b \in \mathbb{Q}_p^*$ and varying p we have a product formula (or quadratic reciprocity statement).

Lemma 74. *Let $a, b \in \mathbb{Q}_p^*$. Then $(a, b)_p = 1$ for all but possibly finitely many p and $\prod_p (a, b)_p = 1$.*

Proof. See [Cas, Chapter 3, Lemma 3.4]. □

Let f be a regular quadratic form of dimension n over $\mathbb{Q}_p$, then f is equivalent to a form of the shape $\sum_{i=1}^n a_i x_i^2$, $a_i \in \mathbb{Q}_p^*$. Define

$$\mathrm{c}_p(f) := \prod_{i<j} (a_i, a_j)_p.$$

If f is also equivalent to $\sum_{i=1}^n b_i x_i^2, b_i \in \mathbb{Q}_p^*$, then, according to [Cas, Chapter 4, Lemma 2.2], $\prod_{i<j}(a_i, a_j)_p = \prod_{i<j}(b_i, b_j)_p$. So $\mathrm{c}_p(f)$ indeed only depends on f, this invariant is called the *Hasse-Minkowski invariant*. For quadratic forms over $\mathbb{R} = \mathbb{Q}_\infty$ we mention a stronger invariant, namely the number of negative coefficients in a diagonal form equivalent to f, denoted $s(f)$. One easily computes that $\mathrm{c}_\infty(f) = (-1)^{s(f)(s(f)-1)/2}$. We now have enough invariants to determine when two quadratic forms are equivalent.

Theorem 75. *Let f, g be regular quadratic forms of dimension $n \geq 1$ over $\mathbb{Q}_p$. If $p \neq \infty$, then f and g are equivalent if and only if $\mathrm{Det}(f) = \mathrm{Det}(g)$ (in $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$) and $\mathrm{c}_p(f) = \mathrm{c}_p(g)$. If $p = \infty$, then f and g are equivalent if and only if $s(f) = s(g)$.*

Proof. See [Cas, Chapter 4, Theorems 1.1-1.2]. □

Quadratic forms of dimension 4 will be of fundamental importance to us.

Lemma 76. *Let f be a regular quadratic form over $\mathbb{Q}_p$ of dimension 4 with $\mathrm{Det}(f) \in (\mathbb{Q}_p^*)^2$. Then the following are equivalent*

i. f is isotropic

ii. f is equivalent to the quadratic form $XY - ZW$

iii. $\mathrm{c}_p(f) = (-1, -1)_p$.

Proof. i $\Leftrightarrow$ ii: This follows immediately from Lemma 71.

ii $\Rightarrow$ iii: Since $XY - ZW$ is equivalent to $x_1^2 - x_2^2 + x_3^2 - x_4^2$ we see that $\mathrm{c}_p(XY - ZW) = (-1, -1)_p$.

iii $\Rightarrow$ ii: We have $\mathrm{Det}(XY - ZW) \in (\mathbb{Q}_p^*)^2$ and (again) $\mathrm{c}_p(XY - ZW) = (-1, -1)_p$, so by Theorem 75 we have for $p \neq \infty$ that f is equivalent to $XY - ZW$. For $p = \infty$, $\mathrm{c}_p(f) = (-1, -1)_p$ implies $s(f) = 2$ or $s(f) = 3$, together with $\mathrm{Det}(f) \in (\mathbb{Q}_\infty^*)^2 = \mathbb{R}_{>0}$ we see that $s(f) = 2 = s(XY - ZW)$. By Theorem 75 the result follows. □

Remark 77. Every regular quadratic form f over $\mathbb{Q}_p$ with $\mathrm{Det}(f) \notin (\mathbb{Q}_p^*)^2$ is isotropic, see [Cas, Chapter 4, Lemma 2.6].

Either by a direct calculation, or using Lemma 73.iii, Lemma 74 and the obvious $(-1, -1)_\infty = -1$, we get

$$(-1, -1)_p = \begin{cases} -1 & \text{if } p = 2, \infty; \\ 1 & \text{otherwise.} \end{cases} \tag{4.17}$$

The Hasse principle

Given a quadratic form over $\mathbb{Q}$, we can of course consider it as a quadratic form over $\mathbb{Q}_p$ for all p. We have the important local-to-global principle or Hasse principle.

Theorem 78 (Weak Hasse Principle). *Let f, g be two regular quadratic forms over $\mathbb{Q}$. Then f is equivalent to g over $\mathbb{Q}$ if and only if f is equivalent to g over $\mathbb{Q}_p$ for all p.*

Proof. See [Cas, Chapter 6, Theorem 1.2]. □

Theorem 79 (Strong Hasse Principle). *Let f be a regular quadratic form over $\mathbb{Q}$, then f is isotropic over $\mathbb{Q}$ if and only if f is isotropic over $\mathbb{Q}_p$ for all p.*

Proof. See [Cas, Chapter 6, Theorem 1.1]. □

One of these principles can be used to obtain a global variant of Lemma 76.

Lemma 80. *Let f be a regular quadratic form over $\mathbb{Q}$ of dimension 4 with $\mathrm{Det}(f) \in (\mathbb{Q}^*)^2$. Then the following are equivalent*

i. f is isotropic (over $\mathbb{Q}$)

ii. f is equivalent (over $\mathbb{Q}$) to the quadratic form $XY - ZW$

iii. $\mathrm{c}_2(f) = \mathrm{c}_\infty(f) = -1$ and $\mathrm{c}_p(f) = 1$ for all odd p.

Proof. The equivalence between i and ii follows immediately from Lemma 71. By (4.17) iii is equivalent to $\mathrm{c}_p(f) = (-1,-1)_p$ for all p. Lemma 76 together with the weak Hasse principle now shows the equivalence between ii and iii (or use the strong instead of the weak Hasse principle to show the equivalence between i and iii). □

Note that by the product formula (Lemma 74) item iii (and hence all items) of the lemma above is equivalent to $\mathrm{c}_p(f) = (-1,-1)_p$ for all but possibly one prime p (e.g. $p = 2$ or $p = \infty$).

Trace forms

Let K be a field of characteristic $\neq 2$ again and let $F \in K[t]$ be monic, separable and of degree n. Let $L := K[t]/(F(t)) \simeq \prod_{i=1}^{r} L_i$, where the L_i are finite separable field extensions of K. We can consider L as a vector space over K and the map $L \times L \to K$ given by $(x,y) \mapsto \mathrm{Trace}_{L/K}(xy)$ is a bilinear map (making L into a quadratic space). For any basis $(v_1,\dots,v_n)$ of L we get a quadratic form

$$f(x_1,\dots,x_n) := \mathrm{Trace}_{L/K}\left(\left(\sum_{i=1}^{n} x_i v_i\right)^2\right) = \sum_{i,j=1}^{n} \mathrm{Trace}_{L/K}(v_i v_j) x_i x_j.$$

Such a quadratic form is called a *trace form* on L (w.r.t. the basis $(v_1,\dots,v_n)$). Changing the basis will of course yield an equivalent quadratic form.

Lemma 81. *Let $F \in K[t]$ be monic, separable and of degree n and Let $L := K[t]/(F(t))$. If f is a trace form on L, then $\mathrm{Det}(f) = \mathrm{Disc}_t(F(t)) \mod (K^*)^2$. In particular, f is regular.*

Proof. Since by assumption $\mathrm{Disc}_t(F(t)) \neq 0$, the last statement follows from the first. Let $t_1,\dots,t_n$ be the n (different) roots of F in $\overline{K}$. We will calculate the trace form $f(x_1,\dots,x_n)$ w.r.t. the power basis $(1,t,\dots,t^{n-1})$. Define $(s_1,\dots,s_n)^t := T(x_1,\dots,x_n)^t$, where

$$T := \begin{pmatrix} 1 & t_1 & t_1^2 & t_1^3 & t_1^4 \\ 1 & t_2 & t_2^2 & t_2^3 & t_2^4 \\ 1 & t_3 & t_3^2 & t_3^3 & t_3^4 \\ 1 & t_4 & t_4^2 & t_4^3 & t_4^4 \\ 1 & t_5 & t_5^2 & t_5^3 & t_5^4 \end{pmatrix}.$$

Then

$$f(x_1, \dots, x_n) = \sum_{i=1}^{n} s_i^2 = (x_1, \dots, x_n) T^t T (x_1, \dots, x_n)^t.$$

So

$$\mathrm{Det}(f) = \mathrm{Det}(T)^2 = \prod_{1 \le i < j \le n} (t_i - t_j)^2 = \mathrm{Disc}(F(t)),$$

where we used the well known formula for the Vandermonde determinant. □

For a nice survey of trace forms when K is a number field, see [CP]. We will only need the following.

Lemma 82. *Let $F \in \mathbb{Q}[t]$ be monic, separable of degree n and let*

$$L := \mathbb{Q}[t]/(F(t)) \simeq \prod_{i=1}^{r} L_i,$$

where the L_i are number fields. Let f be a trace form on L and let p be a finite prime. If p is odd and unramified in all the L_i, then $\mathrm{c}_p(f) = 1$. Furthermore, $s(f)$ equals the number of conjugate pairs of nonreal roots of F.

Proof. Choose an integral basis for each of the L_i, by taking direct products they form a basis $(v_1, \dots, v_n)$ of L. The trace form

$$f(x_1, \dots, x_n) := \mathrm{Trace}_{L/\mathbb{Q}} \left(\left(\sum_{i=1}^{n} x_i v_i \right)^2 \right)$$

has

$$\mathrm{Det}(f) = \mathrm{Det}(\mathrm{Trace}_{L/\mathbb{Q}}(v_i v_j))_{1 \le i,j \le n} = \prod_{i=1}^{r} \mathrm{Disc}(\mathcal{O}_{L_i}/\mathbb{Z}).$$

So $p \nmid \mathrm{Det}(f) \in \mathbb{Z}$. Reducing f modulo p, gives us a regular quadratic form over $\mathbb{F}_p$ ($p \neq 2$). This form can of course be diagonalized, showing that the original form is equivalent to a form of the shape $\sum_{1 \le i,j \le q} c_{i,j} x_i x_j$, where all $c_{i,j} \in \mathbb{Z}$, $p \nmid c_{i,i}$ and $p | c_{i,j} = c_{j,i}$ for $i \neq j$. From this form one easily arrives inductively at an equivalent diagonal form with all coefficients integral and not divisible by p. Lemma 73.iii now gives us $\mathrm{c}_p(f) = 1$. For the last statement, note that

$$g(x_1, x_2) := \mathrm{Trace}_{\mathbb{C}/\mathbb{R}} \left((x_1 + x_2 i)^2 \right) = \mathrm{Trace}_{\mathbb{C}/\mathbb{R}}(x_1^2 - x_2^2 + 2 x_1 x_2 i) = 2x_1^2 - 2x_2^2$$

has $s(g) = 1$ and that $L \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{r'} \times \mathbb{C}^s$ (as $\mathbb{R}$-algebras), where r' denotes the number of real roots of F and s the number of conjugate pairs of nonreal roots of F (the last statement actually was the main theme of [Tau] and this paper was one of the first calling for an investigation of trace forms). □

4.2 Parameterized solutions for y^3/z^5

Throughout this section 4.2 we let K be a field of characteristic zero.

4.2.1 Parameterizing principal quintics

Let $F = \sum_{k=0}^{5} a_k t^k \in K[t]$ be monic, separable and of degree 5. We are interested in Tschirnhausen transformations that turn F into a principal quintic. For the variables $c_0, \ldots, c_4$ (which shall be specialized later to some K-algebra like $K, \overline{K}$ or $K[u_1, v_1, u_2, v_2]$), define

$$G_{c_0,\ldots,c_4}(s) := \mathrm{Res}_t\left(F(t), s - \sum_{k=0}^{4} c_k t^k\right).$$

In our notation we will frequently drop the index. We have

$$G(s) = \sum_{k=0}^{5} (-1)^{5-k} \sigma_{5-k} s^k,$$

where $\sigma_k \in K[c_0, c_1, \ldots, c_4]$ is homogeneous of degree k (in particular $\sigma_0 = 1$). If $t_1, \ldots, t_n$ denote the roots of F, then the roots $s_1, \ldots, s_5$ of $G(s)$ are given by

$$\begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \end{pmatrix} = \begin{pmatrix} 1 & t_1 & t_1^2 & t_1^3 & t_1^4 \\ 1 & t_2 & t_2^2 & t_2^3 & t_2^4 \\ 1 & t_3 & t_3^2 & t_3^3 & t_3^4 \\ 1 & t_4 & t_4^2 & t_4^3 & t_4^4 \\ 1 & t_5 & t_5^2 & t_5^3 & t_5^4 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix}.$$

Consider the quadratic form

$$Q_5(c_0, \ldots, c_4) := \sigma_1^2 - 2\sigma_2.$$

Writing Trace for $\mathrm{Trace}_{L/K}$ from now on, we see that Q_5 is simply the trace form $s \mapsto \mathrm{Trace}(s^2)$ on $L := K[t]/(F(t))$ w.r.t. the power basis $(1, t, t^2, t^3, t^4)$. The matrix associated to the quadratic form $Q_5(c_0, \ldots, c_4)$ is given by

$$(\mathrm{Trace}(t^{i+j}))_{0 \le i,j \le 4}.$$

We have

$$\sigma_1 = \mathrm{Trace}(s) = \sum_{n=0}^{4} \mathrm{Trace}(t^n) c_n.$$

Since $\mathrm{Trace}(x^0) = 5$ we can always eliminate c_0 as

$$\begin{aligned} c_0 &= \frac{1}{5}\left(\sigma_1 - \sum_{n=1}^{4} \mathrm{Trace}(t^n) c_n\right) \qquad (4.18) \\ &= \frac{1}{5}\left(\sigma_1 + a_4 c_1 + (2a_3 - a_4^2) c_2 + (3a_2 - 3a_3 a_4 + a_4^3) c_3 + \right. \\ &\quad \left. (4a_1 - 2a_3^2 - 4a_2 a_4 + 4a_3 a_4^2 - a_4^4) c_4\right). \end{aligned}$$

For the terms of Q_5 involving c_0 we have

$$\begin{aligned} Q_5(c_0,\ldots,c_4) &- Q_5(0,c_1,\ldots,c_4) \\ &= c_0\left(\sum_{n=0}^{4}\mathrm{Trace}(t^n)c_n + \sum_{n=1}^{4}\mathrm{Trace}(t^n)c_n\right) \\ &= \frac{1}{5}\left(\sigma_1 - \sum_{n=1}^{4}\mathrm{Trace}(t^n)c_n\right)\left(\sigma_1 + \sum_{n=1}^{4}\mathrm{Trace}(t^n)c_n\right) \\ &= \frac{1}{5}\left(\sigma_1^2 - \left(\sum_{n=1}^{4}\mathrm{Trace}(t^n)c_n\right)^2\right). \end{aligned}$$

So we see that

$$Q_5 = \sigma_1^2/5 + Q_4 \tag{4.19}$$

for the quadratic form

$$Q_4 = \frac{4}{5}\sigma_1^2 - 2\sigma_2 = Q_5(0,c_1,\ldots,c_4) - \frac{1}{5}\left(\sum_{n=1}^{4}\mathrm{Trace}(t^n)c_n\right)^2$$

which only depends on $c_1,\ldots,c_4$. To denote the dependency of the quadratic form Q_4 on the quintic F we shall sometimes write it as $Q_4(F)$.

Lemma 83. *Let $F \in K[t]$ be monic, separable and of degree 5. Then*

$$\mathrm{Det}(Q_4(F)) \equiv 5\mathrm{Disc}_t(F(t)) \mod (K^*)^2.$$

In particular, $\mathrm{Disc}(Q_4(F)) \in (K^*)^2$ *if and only if* $\mathrm{Disc}_t(F(t)) \in 5(K^*)^2$.

Proof. By (4.19) we get $\mathrm{Det}(Q_4) = 5\mathrm{Det}(Q_5)$. By Lemma 81, the trace form Q_5 satisfies $\mathrm{Det}(Q_5) = \mathrm{Disc}_t(F(t)) \mod (K^*)^2$ (actually, $\mathrm{Det}(Q_5) = \mathrm{Disc}_t(F(t))$, so even $\mathrm{Det}(Q_4(F)) = 5\mathrm{Disc}_t(F(t))$ holds). The last statement now follows immediately. □

Let $F_1, F_2 \in K[t]$ be monic polynomials of degree $n \in \mathbb{Z}_{\geq 1}$, we call F_1 and F_2 *scaling equivalent* if $F_1(t) = F_2(\alpha t)/\alpha^n$ for some $\alpha \in K$. Clearly this defines an equivalence relation and the notions of depressed and principal are preserved under this relation. Define

$$\begin{aligned} \Gamma &:= \{G_{c_0,\ldots,c_4}(s) \in K[s] \mid (c_0,\ldots c_4) \in K^5 - \{0,\ldots,0\}\} \\ &= \{G_{c_0,\ldots,c_4}(s) \in K[s] \mid (c_0,\ldots c_4) \in K^5\} - \{s^5\}. \end{aligned}$$

Consider $[c_0 : \ldots : c_4] \in \mathbb{P}^4(K)$, then $G_{c_0,\ldots,c_4}(s) \in K[s]$ is defined up to scaling equivalence. In this way $\mathbb{P}^4(K)$ naturally parameterizes Γ modulo scaling equivalence. The K-rational points on the hyperplane in $\mathbb{P}^4$ given by $\sigma_1(c_0,\ldots,c_4) = 0$ parameterizes all depressed quintics in Γ modulo scaling equivalence. The K-rational points on the surface S in $\mathbb{P}^4$ given by $\sigma_1 = \sigma_2 = 0$ parameterizes all principal quintics in Γ modulo scaling equivalence. Eliminating c_0 using (4.18)

with $\sigma_1 = 0$, we see that S is (isomorphic over K to) the quadratic surface in $\mathbb{P}^3$ given by $Q_4(F) = 0$.

Any nondegenerate quadratic form over $\overline{K}$ in 4 variables is equivalent (over $\overline{K}$) to the quadratic form $XY - ZW$. The quadratic surface given by $XY = ZW$ is doubly ruled in the sense that it is isomorphic (over K) to $\mathbb{P}^1 \times \mathbb{P}^1$. An isomorphism is given by mapping $([u_1 : v_1], [u_2 : v_2]) \in \mathbb{P}^1 \times \mathbb{P}^1$ to

$$[X : Y : Z : W] = [u_1u_2 : v_1v_2 : v_1u_2 : u_1v_2]. \tag{4.20}$$

So S is isomorphic (over $\overline{K}$) to $\mathbb{P}^1 \times \mathbb{P}^1$. For the quintics F we are interested in, it turns out that we have the very nice property that the quadratic form $Q_4(F)$ is already isomorphic over K to $XY - ZW$ and hence our surface S is isomorphic over K to $\mathbb{P}^1 \times \mathbb{P}^1$.

Lemma 84. *Let $F \in K[t]$ be monic, separable, of degree 5 and suppose that $\mathrm{Disc}_t(F(t)) \in 5(K^*)^2$. If $F \sim G_0$ for a certain monic separable and* principal *$G_0 \in K[s]$, then $Q_4(F)$ is isomorphic (over K) to the quadratic form $XY - ZW$.*

Proof. From Lemma 83 we obtain that $\mathrm{Det}(Q_4(F)) \in (K^*)^2$, and the existence of the G_0 implies that $Q_4(F)$ is isotropic. By Lemma 71 we obtain the desired result. □

Actually the converse also holds. But note that for certain $G(s) \in \Gamma$ we might have $\mathrm{Disc}_s(G(s)) = 0$. This equation actually defines a curve in S and the points on S away from this discriminant locus correspond to principal and separable quintics (modulo scaling equivalence).

Conditions for Q_4 if $K = \mathbb{Q}$

Suppose for the moment that $K = \mathbb{Q}$, this is the case we are eventually interested in. Let $F \in \mathbb{Q}[t]$ be monic, separable, of degree 5 and suppose that $\mathrm{Disc}_t(F(t)) \in 5(\mathbb{Q}^*)^2$. Considering the previous lemma, it would be nice to have a good algorithm for testing whether $Q_4(F)$ is equivalent (over $\mathbb{Q}$) to $XY - ZW$ or not. By Lemma 83 we have $\mathrm{Det}(Q_4(F)) \in (\mathbb{Q}^*)^2$, so by Lemma 80 we have that Q_4 is equivalent to $XY - ZW$ if and only if $\mathrm{c}_2(Q_4) = \mathrm{c}_\infty(Q_4) = -1$ and $\mathrm{c}_p(Q_4) = 1$ for all odd primes p. To decide whether or not this last statement holds we need to obtain an explicit finite set P of odd primes p such that for all odd primes p not in P we have $\mathrm{c}_p(Q_4) = 1$ (such a finite set exists by Lemma 74).

A straightforward method to obtain P is as follows. Diagonalize $Q_4(F)$ to, say, $ax^2 + by^2 + cz^2 + dw^2,\ a, b, c, d \in \mathbb{Q}^*$. Let P be the set of odd primes p that do not satisfy $|a|_p = |b|_p = |c|_p = |d|_p = 1$. By Lemma 73.iii we have $\mathrm{c}(Q_4(F))_p = 1$ for all odd $p \notin P$ and P is finite since $abcd \neq 0$. This set P can of course be found by factoring a, b, c and d. However, there is no a priori bound on the size of this set P and we can do better.

By Proposition 65 we only need to consider polynomials F such that the étale algebra $\mathbb{Q}[t]/(F(t))$ is unramified outside an a priori fixed set of primes. We can in fact bound P in terms of these primes.

Lemma 85. *Let $F \in \mathbb{Q}[t]$ be monic, separable, of degree 5 and suppose that $\mathrm{Disc}_t(F(t)) \in 5(\mathbb{Q}^*)^2$. Let $L := \mathbb{Q}[t]/(F(t)) \simeq \prod_{i=1}^r L_i$, where the L_i are number fields. Let P be the set of odd primes that ramify in some L_i. Then $Q_4(F)$ is equivalent to $XY - ZW$ if and only if $\mathrm{c}_2(Q_4(F)) = -1$ and $\mathrm{c}_p(Q_4(F)) = 1$ for all $p \in P$.*

Proof. By Lemma 83 we have $\mathrm{Det}(Q_4(F)) \in (\mathbb{Q}^*)^2$. Suppose $\mathrm{c}_2(Q_4(F)) = -1$ and $c_p(Q_4(F)) = 1$ for all $p \in P$. By Lemma 80 and the product formula (Lemma 74) it suffices to prove that $\mathrm{c}_p(Q_4(F)) = 1$ for all odd $p \notin P$ to conclude that $Q_4(F)$ is equivalent to $XY - ZW$. By diagonalizing Q_4 in (4.19) it follows for all p that $\mathrm{c}_p(Q_5) = (5, \mathrm{Det}(Q_4))_p \mathrm{c}_p(Q_4)$. Since $\mathrm{Det}(Q_4(F)) \in (\mathbb{Q}^*)^2$, we obtain $\mathrm{c}_p(Q_5(F)) = \mathrm{c}_p(Q_4(F))$. Lemma 82 now gives us that $\mathrm{c}_p(Q_4(F)) = 1$ for all odd $p \notin P$. The other implication is immediate from 80. □

The implementation in Magma of an algorithm to decide whether $Q_4(F)$ is equivalent (over $\mathbb{Q}$) to $XY - ZW$ or not, based on the lemma above, is given by `function integritycheck` in appendix B.

Remark 86. Note that by (4.19) and Lemma 80 we have that $s(Q_4) = s(Q_5) = s_F$, where s_F denotes the number of conjugate pairs of nonreal roots of F. If we add to the conditions of the above lemma that furthermore F has only one real root, then we obtain the slightly nicer statement that $Q_4(F)$ is equivalent to $XY - ZW$ if and only if $c_p(Q_4(F)) = 1$ for all $p \in P$.

4.2.2 From principal quintics to j values

By definition (and since 5 is invertible), any monic principal quintic over K is of the form

$$P_{a,b,c}(t) := t^5 + 5at^2 + 5bt + c,$$

for certain $a, b, c \in K$. We want to find $\mu, \nu, j \in K$, $j \neq 0, 1728$ (if any) such that $P_{a,b,c}(t) = g_{\lambda,\mu,j}(t)$, i.e. (4.11),(4.12),(4.13) hold. Define the quadratic polynomial

$$L_{a,b,c}(\lambda) := (a^4+abc-b^3)\lambda^2-(11a^3b-ac^2+2b^2c)\lambda+(64a^2b^2-27a^3c-bc^2). \quad (4.21)$$

We have the important discriminant relation

$$\mathrm{Disc}_\lambda(L_{a,b,c}(\lambda)) = a^2\mathrm{Disc}_t(P_{a,b,c}(t))/5^5. \quad (4.22)$$

In particular we shall consider $P_{a,b,c}$ such that $\mathrm{Disc}_t(P_{a,b,c}(t)) \in 5(K^*)^2$ with $a \neq 0$, $a, b, c \in K$, in which case the polynomial $L_{a,b,c}$ has a root in K (and exactly two different roots in K if $a^4 + abc - b^3 \neq 0$). If $a, b, c, \lambda, \mu, j \in K$ ($j \neq 0, 1728$) are such that (4.11),(4.12),(4.13) hold, then the following hold

$$\begin{aligned} L_{a,b,c}(\lambda) &= 0, \\ a^2((ac-b^2)\lambda - bc)j &= (a\lambda^2 - 3b\lambda - 3c)^3, \\ ((ac-b^2)\lambda - bc)\mu &= a^2\lambda^4 - 10ab\lambda^3 - 9(2ac-5b^2)\lambda^2 + 18bc\lambda - 27c^2. \end{aligned}$$

Conversely, for any $a, b, c \in K$ such that $\lambda \in K$ satisfies $L_{a,b,c}(\lambda) = 0$ and

$$\begin{aligned} a^2((ac-b^2)\lambda - bc) &\neq 0, \\ a\lambda^2 - 3b\lambda - 3c &\neq 0, \\ (a\lambda^2 - 3b\lambda - 3c)^3 - 1728a^2((ac-b^2)\lambda - bc) &\neq 0, \end{aligned}$$

we can set

$$\mu := \frac{a^2\lambda^4 - 10ab\lambda^3 - 9(2ac-5b^2)\lambda^2 + 18bc\lambda - 27c^2}{(ac-b^2)\lambda - bc} \in K, \tag{4.23}$$

$$j := \frac{(a\lambda^2 - 3b\lambda - 3c)^3}{a^2((ac-b^2)\lambda - bc)} \in K - \{0, 1728\}, \tag{4.24}$$

and now λ, μ, j satisfy (4.11),(4.12),(4.13). For all this, see [Kin, pp. 106-107](or use computer algebra). The nonvanishing conditions for some $\lambda \in K$ satisfying $L_{a,b,c}(\lambda) = 0$ are of course implied by

$$\begin{aligned} \mathrm{Res}_\lambda(L_{a,b,c}(\lambda), a^2((ac-b^2)\lambda - bc)) &\neq 0, \quad (4.25) \\ \mathrm{Res}_\lambda(L_{a,b,c}(\lambda), a\lambda^2 - 3b\lambda - 3c) &\neq 0, \quad (4.26) \\ \mathrm{Res}_\lambda(L_{a,b,c}(\lambda), (a\lambda^2 - 3b\lambda - 3c)^3 - 1728a^2((ac-b^2)\lambda - bc)) &\neq 0, \quad (4.27) \end{aligned}$$

and one can check that the left hand sides are nonzero polynomials in $K[a, b, c]$.

Remark 87. If $\lambda \in K$ satisfies $L_{a,b,c}(\lambda) = 0$, but

$$a^2((ac-b^2)\lambda - bc) = a\lambda^2 - 3b\lambda - 3c = 0, \tag{4.28}$$

it might still be possible to find $j \in K - \{0, 1728\}, \mu \in K$ such that λ, μ, j satisfy (4.11),(4.12),(4.13). For example, suppose that $a = 0, bc \neq 0$. Then $L_{a,b,c}(\lambda) = 0$ reduces to $-b(b\lambda + c)^2 = 0$, so $\lambda = -c/b$ and (4.28) holds. Now μ, j are given by

$$\begin{aligned} b^7\mu^2 - bc(144b^5 + c^4)\mu + 8c^2(648b^5 + c^4) &= 0, \\ j &= \frac{(-216b^5c + c^5 + 3b^6\mu)^3}{b^5c^6(-72b^5c - c^5 + b^6\mu)}, \end{aligned}$$

and certainly $j \neq 0, 1728$ if $(144b^5 - c^4)(648b^5 + c^4) \neq 0$.

Lemma 88. *Let $F \in K[t]$ be monic, separable, of degree 5 and suppose that $Q_4(F)$ is isomorphic to $XY - ZW$. Then $F \sim f_j$ for some $j \in K - \{0, 1728\}$.*

Proof. By Proposition 67 it suffices to prove that $F \sim g_{\lambda,\mu,j}$ for some $\lambda, \mu, j \in K$ with $j \neq 0, 1728$ and $\mathrm{Disc}_t(g_{\lambda,\mu,j}(t)) \neq 0$. By using (4.20) we have that with

$$G_{c_0,\ldots,c_4}(s) := \mathrm{Res}_t\left(F(t), s - \sum_{k=0}^{4} c_k t^k\right) = \sum_{k=0}^{4} (-1)^{5-k}\sigma_{5-k}s^k$$

the equations $\sigma_1(c_0, \ldots, c_4) = \sigma_2(c_0, \ldots, c_4) = 0$ define a surface S in $\mathbb{P}^4$, isomorphic over K to $\mathbb{P}^1 \times \mathbb{P}^1$. Let $a := -\sigma_3/5, b := \sigma_4/5$ and $c := -\sigma_5$, so $G(s) =$

$s^5+5as^2+5bs+c$. None of $\mathrm{Disc}_s(G(s))$ or the left hand sides of (4.25), (4.26), (4.27) vanish identically on $S(\overline{K})$ since as polynomials in $\overline{K}[a,b,c]$ they are nonzero. Now since K is infinite, there are in fact infinitely many points in $S(K)$ were these 4 polynomials in the c_i are all nonzero. Take such a point $[c_0 : \ldots : c_4] \in \mathbb{P}^4(K)$, they determine $a, b, c \in K$. First of all $G(s) = G_{c_0,\ldots,c_4}(s) = s^5 + 5as^2 + 5bs + c$ has by construction (from F and Lemma 83) $\mathrm{Disc}_s(G(s)) \in 5(K^*)^2$, so by (4.22) (and $a \neq 0$) we get $\mathrm{Disc}_\lambda(L_{a,b,c}) \in (K^*)^2$. Now (4.21), (4.23), (4.24) provide us with $\lambda, \mu, j \in K,\ j \neq 0, 1728$, such that $G_{c_0,\ldots,c_4} = g_{\lambda,\mu,j}$. By construction, $\mathrm{Disc}_s(g_{\lambda,\mu,j}(s)) \neq 0$, so Lemma 66 finally gives us $F \sim g_{\lambda,\mu,j}$ as desired. □

We are now in a position to give nice characterizations for when a polynomial is equivalent to f_j ($j \in K - \{0, 1728\}$).

Proposition 89. *Let $F \in K[t]$ be monic, separable and of degree 5. Then the following are equivalent*

i. $F \sim f_j$ for a certain $j \in K - \{0, 1728\}$,

ii. $Disc_t(F(t)) \in 5(K^*)^2$ and $F \sim G_0$ for a certain monic separable and principal *$G_0 \in K[s]$,*

iii. The quadratic form $Q_4(F)$ is isomorphic (over K) to the quadratic form $XY - ZW$.

Proof. Follows from the lemma above, Lemma 84 and (4.16),(4.3). □

In the case that $K = \mathbb{Q}$, Lemma 85 supplies us with a very useful algorithm to decide whether or not $F \sim f_j$ for a certain $j \in K - \{0, 1728\}$.

Now if $F \sim f_j$ for some $j \in K - \{0, 1728\}$, then the strategy to obtain all $J \in K - \{0, 1728\}$ such that $F \sim f_J$ is as follows. In the following computations we will consider j transcendental over K, but at every stage j can also be specialized to some element of $K - \{0, 1728\}$. We start from the polynomial

$$g_j = t^5 + \frac{40}{j}t^2 - \frac{5}{j}t + \frac{1}{j} \sim f_j.$$

Let $G_{c_0,\ldots,c_4}(s) = \sum_{k=0}^{5}(-1)^{5-k}\sigma_{5-k}s^k$ be as usual. Express c_0 in terms of $c_1, \ldots, c_4$, so that $\sigma_1(c_1, \ldots, c_4) = 0$, in this case

$$c_0 = (24/j)c_3 - (4/j)c_4.$$

The quadratic form σ_2 in the variables of the column vector $c = (c_1, c_2, c_3, c_4)^t$ is given by $c^t M c$, where

$$M := \begin{pmatrix} 0 & 60/j & -10/j & (5/2)/j \\ 60/j & -10/j & (5/2)/j & -2400/j^2 \\ -10/j & (5/2)/j & -960/j^2 & 460/j^2 \\ (5/2)/j & -2400/j^2 & 460/j^2 & -170/j^2 \end{pmatrix}. \tag{4.29}$$

A priori we know that this quadratic form is equivalent over $K(j)$ to $XY - ZW$. We claim that this is obtained by the change of variables

$$(c_1, c_2, c_3, c_4)^t = T(X, Y, Z, W)^t, \tag{4.30}$$

where

$$T := \begin{pmatrix} 1/2 & j/720 & (j^3/4800 - 8j^2/5)/(j-1728) & 10/(3j) - 12800/j^2 \\ 6 & 0 & (j^3/400)/(j-1728) & 0 \\ 0 & 0 & (j^3/200)/(j-1728) & -80/j \\ 0 & 0 & -(j^3/25)/(j-1728) & -320/j \end{pmatrix}.$$

A straightforward calculation gives

$$T^t M T = \begin{pmatrix} 0 & 1/2 & 0 & 0 \\ 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1/2 \\ 0 & 0 & -1/2 & 0 \end{pmatrix}.$$

So indeed T transforms σ_2 into $XY - ZW$. Now we parameterize the surface $XY - ZW = 0$ via (4.20) and by using (4.30), we get $c_1, \ldots, c_4$ as functions of u_1, v_1, u_2, v_2. Explicitly

$$\begin{aligned} c_1 &= (1/2)u_1u_2 + (((10/3)j - 12800/j^2)u_1v_2 + \\ &\quad (((1/4800)j^3 - (8/5)j^2)/(j-1728))v_1u_2 + (1/720)jv_1v_2 \\ c_2 &= 6u_1u_2 + ((1/400)j^3/(j-1728))v_1u_2 \\ c_3 &= (-80/j)u_1v_2 + ((1/200)j^3/(j-1728))v_1u_2 \\ c_4 &= (-320/j)u_1v_2 - ((1/25)j^3/(j-1728))v_1u_2. \end{aligned}$$

This way the σ_k become homogeneous in u_i, v_i of degree k for each $i = 1, 2$ and of course $\sigma_1 = \sigma_2 = 0$. Let $a := -\sigma_3/5, b := \sigma_4/5$ and $c := -\sigma_5$, so $G(s) = s^5 + 5as^2 + 5bs + c$. The discriminant of $L_{a,b,c}(\lambda)$ is a nonzero square in $K(j)[u_1, v_1, u_2, v_2]$ (without a brute force computation, this follows from $\mathrm{Disc}_t(g_j(t)) \in 5(K(j)^*)^2$, (4.6) and (4.22)). So the two roots λ_1, λ_2 can be considered as elements of $K(j, u_1, v_1, u_2, v_2)$. Finally μ_i, j_i, (where the index $i = 1, 2$ refers to the corresponding root λ_i,) are obtained from (4.23), (4.24). The quantities $a, b, c, \lambda_i, \mu_i, j_i$ can quickly be calculated explicitly using a computer algebra package, e.g. Magma, but we do not write them down here because of their size. A priori (for fixed j) we have that j_1 and j_2 both depend on u_1, v_1, u_2, v_2, but something fantastic has happened, we have (by possibly swapping λ_1 and λ_2) that $j_i \in K(u_i, v_i)$!

For every $j \in K - \{0, 1728\}$ these j_1, j_2 define rational maps (over K)

$$J_1, J_2 : \mathbb{P}^1 \to \mathbb{P}^1$$

and they are of the form

$$\begin{aligned} J_i &= \frac{b(u,v)^3}{c(u,v)^5} \\ &= -\frac{a(u,v)^2}{c(u,v)^5} + 1728, \end{aligned}$$

for nondegenerate relatively prime binary forms $a(u,v), b(u,v), c(u,v) \in K[u,v]$ of degree $30, 20, 12$ respectively.

Let J_1, J_2 be the two maps induced by a certain $j \in K - \{0, 1728\}$. We claim that for all $j_0 \in K - \{0, 1728\}$ such that $f_j \sim f_{j_0}$ we have $j_0 = J_i(P)$ for some $i = 1, 2$ and $P \in \mathbb{P}^1(K)$. By construction of J_1, J_2, for every $j_0 \in K - \{0, 1728\}$ such that $g_{\lambda,\mu,j_0} \sim g_j$ for certain $\lambda, \mu \in K$, we have that $j_0 = J_i(P)$ for some $i = 1, 2$ and $P \in \mathbb{P}^1(K)$. Now note that if $f_j \sim f_{j_0}$, then $g_j \sim g_{j_0} = g_{1,0,j_0}$.

Let $a, b, c \in \mathbb{Z} - \{0\}$ and let us go back to the original equation (4.1) (so we consider $K = \mathbb{Q}$). First some terminology, any rational map $\mathbb{P}^1 \to \mathbb{P}^1$ over $\mathbb{Q}$ of the form

$$\frac{b(u,v)^3}{c(u,v)^5} = -\frac{a(u,v)^2}{c(u,v)^5} + 1728$$

for nondegenerate relatively prime binary forms $a(u,v), b(u,v), c(u,v) \in \mathbb{Q}[u,v]$ of degree $30, 20, 12$ respectively is called a *quotient parameterization*. We know that there exist finitely many $F_1, \dots F_n \in \mathbb{Q}[t]$ of monic separable quintics equivalent to some f_j, $j \in \mathbb{Q} - \{0, 1728\}$, such that for every solution x, y, z to (4.1) we have $f_{j(x,y,z)} \sim F_k$ for a unique $k \in \{1, \dots, n\}$ (with $j(x,y,z)$ as in (4.4)). The algorithm described above gives us for every F_k two quotient parameterizations $J_{1,k}, J_{2,k}$ and we obtain that for any solution x, y, z to (4.1) we have

$$\frac{y^3}{z^5} = \frac{c}{1728b} J_{i,k}(P),$$

for certain $i \in \{1, 2\}$, $k \in \{1, \dots, n\}$ and $P \in \mathbb{P}^1(\mathbb{Q})$. Certainly k is unique, but it might happen that $i = 1, 2$ both are possible. We will show that if i is not unique, then in fact $J_{1,k}(\mathbb{P}^1(\mathbb{Q})) = J_{2,k}(\mathbb{P}^1(\mathbb{Q}))$.

Lemma 90. *Let J_1, J_2 be two quotient parameterizations. If $J_1(P_1) = J_2(P_2) \in \mathbb{P}^1(\mathbb{Q}) - \{0, 1728, \infty\}$ for certain $P_1, P_2 \in \mathbb{P}^1(\mathbb{Q})$, then $J_1 = J_2 \circ \theta$ for a $\theta \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{P}^1)$.*

Proof. Any quotient parameterization is unramified outside $\{0, 1728, \infty\}$ and the ramification indices above $0, 1728, \infty$ are $3, 2, 5$ respectively. It is well known (e.g. by considering dessins d'enfant) that any rational map of degree 60 with such ramification is a twist of the icosahedral map (4.14). Since J_1, J_2 are both twists of the icosahedral map, we have $J_1 = J_2 \circ \theta$ for some $\theta \in \mathrm{Aut}_{\overline{\mathbb{Q}}}(\mathbb{P}^1)$. In particular $J_2(P_2) = J_1(P_1) = J_2(\theta(P_1))$, so by composing θ with a covering transformation of $J_2 : \mathbb{P}^1 \to \mathbb{P}^1$ we can assume that

$$P_2 = \theta(P_1).$$

Denote the group of covering transformations over $\overline{\mathbb{Q}}$ of $J_1 : \mathbb{P}^1 \to \mathbb{P}^1$ by G (it is isomorphic to A_5). Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We have

$$\begin{aligned} J_1 &= J_2 \circ \theta, \\ J_1 &= J_2 \circ \theta^\sigma, \end{aligned}$$

where the first equality was already known and the second follows from the first since J_1, J_2 are defined over $\mathbb{Q}$. Let

$$g_\sigma := \theta^{-1} \circ \theta^\sigma.$$

Then $J_1 \in G$ since

$$J_1 \circ g_\sigma = (J_1 \circ \theta^{-1}) \circ \theta^\sigma = J_2 \circ \theta^\sigma = J_1.$$

Furthermore, note that $P_1^\sigma = P_1, P_2^\sigma = P_2$, so

$$g_\sigma(P_1) = \theta^{-1}(\theta^\sigma(P_1^\sigma)) = \theta^{-1}((\theta(P_1))^\sigma) = \theta^{-1}(P_2) = P_1.$$

Because P_1 is not a ramification point and $g_\sigma \in G$ we obtain from this that g_σ is the identity. In other words, $\theta^\sigma = \theta$ for all $\theta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and we conclude that θ is defined over $\mathbb{Q}$. □

Given some appropriate $F \in K[t]$, then instead of first finding one $j \in K - \{0, 1728\}$ such that $F \sim f_j$ and then using the above method to obtain two quotient parameterizations, more elegantly, one can of course combine these two steps and follow the procedure above starting from F. The only difference is that one needs to find another transformation T, since the matrix associated to the quadratic form $Q_4(F)$ need not be of the form (4.29). So let us quickly describe how one can obtain the necessary transformation. First of all diagonalize $Q_4(F) = cMc^t$, i.e. find a matrix $T_1 \in \mathrm{GL}_4(K)$ such that $T_1^t M T_1$ is diagonal (this is straightforward). Say that the diagonal form is given by $ax^2 + by^2 + cz^2 + dw^2$. By Lemma 72, the quadratic form in 3 variables $ax^2 + by^2 + cz^2$ is isotropic, let $[x_0 : y_0 : z_0] \in \mathbb{P}^2(K)$ be a point on the conic $ax^2 + by^2 + cz^2 = 0$. Suppose $x_0 \neq 0$ (otherwise, change the role of x and y or find another point). Let $k \in K$ be a square root of $d/(abc)$. Consider the matrix

$$T_2 := \begin{pmatrix} x_0/2 & y_0/2 & z_0/2 & 0 \\ 1/(2ax_0) & -y_0/(2ax_0^2) & -z_0/(2ax_0^2) & 0 \\ 0 & -z_0/(4abx_0) & y_0/(4acx_0) & -1/(4abck) \\ 0 & -cz_0/x_0 & by_0/x_0 & 1/k \end{pmatrix}^t.$$

Then one calculates with $T := T_1 T_2$ and $\theta := (ax_0^2 + by_0^2 + cz_0^2)/(4ax_0^2) = 0$ that

$$\begin{aligned} T^t M T &= T_2^t \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{pmatrix} T_2 \\ &= \begin{pmatrix} ax_0^2\theta & 1/2 - \theta & 0 & 0 \\ 1/2 - \theta & \theta/(ax_0^2) & 0 & 0 \\ 0 & 0 & \theta/(4abc) & \theta - 1/2 \\ 0 & 0 & \theta - 1/2 & 4abc\theta \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1/2 & 0 & 0 \\ 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1/2 \\ 0 & 0 & -1/2 & 0 \end{pmatrix}. \end{aligned}$$

So T gives us the desired transformation. The implementation in Magma of an algorithm to obtain the two quotient parameterizations from an appropriate $F \in \mathbb{Q}[t]$ based on this method is given by `function param` in appendix B, testing for twists over $\mathbb{Q}$ using Lemma 90 is implemented as `function Twists`.

Remark 91. We want to conclude this section by pointing out that there is a degree 7 map that maps points in $J_1(\mathbb{P}^1(K))$ to $J_2(\mathbb{P}^1(K))$ and vice versa, which leads to a funny recursive relation. Consider again the principal quintic $g_j(t) = t^5 + (40/j)t^2 - (5/j)t + (1/j)$. We want to find λ, μ, J such that $g_j = g_{\lambda,\mu,J}$ (or actually we are only interested in J). One solution is of course $(\lambda, \mu, J) = (1, 0, j)$, we want to find the other solution. For this we substitute

$$a = 8/j, b = -1/j, c = 1/j$$

into (4.21), this leads to the solutions

$$\lambda = 1, \lambda = \frac{-j + 9728}{7j - 4096}.$$

Substituting the second value of λ in (4.24) leads to

$$\begin{aligned} J &= \frac{j(j^2 - 1456j - 3670016)^3}{(-7j + 4096)^5} \\ &= -\frac{(-j + 1728)(j^3 - 1320j^2 + 9043968j + 1073741824)^2}{(-7j + 4096)^5} + 1728. \end{aligned}$$

Now define

$$\begin{aligned} X(x, y, z) &:= x(y^9 - 1320y^6z^5 + 9043968y^3z^{10} + 1073741824z^{15}), \\ Y(x, y, z) &:= y(y^6 - 1456y^3z^5 - 3670016z^{10}), \\ Z(x, y, z) &:= z^2(-7y^3 + 4096z^5). \end{aligned}$$

Then

$$X(x, y, z)^2 + Y(x, y, z)^3 = 1728Z(x, y, z)^5 + E(x, y, z),$$

where

$$E(x, y, z) = (x^2 + y^3 - 1728z^5)(y^9 - 1320y^6z^5 + 9043968y^3z^{10} + 1073741824z^{15}).$$

In particular, if $x, y, z \in \mathbb{Z}$ are such that $x^2 + y^3 = 1728z^5$, then $E(x, y, z) = 0$, so with $X = X(x, y, z), Y = Y(x, y, z), Z = Z(x, y, z)$ we get $X^2 + Y^3 = 1728Z^5$. If $\gcd(x, y, z) = 1$, then we may have $\gcd(X, Y, Z) > 1$, but we do have that the primes dividing $\gcd(X, Y, Z)$ are contained in $\{2, 5\}$.

We can of course rescale a bit to obtain recursions for $ax^2 + by^3 = cz^5$ for every $a, b, c \in \mathbb{Z} - \{0\}$. For example, for $a = b = c = 1$ we have the following recursion.

Define

$$\begin{aligned} X'(x,y,z) &:= X(2^3\cdot 3^9 x, 2^2\cdot 3^6 y, 3^3 z)/(2^{18}\cdot 3^{54}) \\ &= x(157464y^9 - 120285y^6z^5 + 476928y^3z^{10} + 32768z^{15}), \\ Y'(x,y,z) &:= Y(2^3\cdot 3^9 x, 2^2\cdot 3^6 y, 3^3 z)/(2^{12}\cdot 3^{36}) \\ &= y(2916y^6 - 2457y^3z^5 - 3584z^{10}), \\ Z'(x,y,z) &:= Z(2^3\cdot 3^9 x, 2^2\cdot 3^6 y, 3^3 z)/(2^6\cdot 3^{21}) \\ &= z^2(-189y^3 + 64z^5). \end{aligned}$$

Then

$$X'(x,y,z)^2 + Y'(x,y,z)^3 = Z'(x,y,z)^5 + E'(x,y,z),$$

where

$$E'(x,y,z) = (x^2 + y^3 - z^5)(157464y^9 - 120285y^6z^5 + 476928y^3z^{10} + 32768z^{15})^2.$$

4.3 Parameterized solutions for x, y, z

By an *integral parameterization* to (4.1) (for given $a, b, c \in \mathbb{Z} - \{0\}$) we mean a triple (X, Y, Z) of homogeneous polynomials $X, Y, Z \in \mathbb{Z}[u, v]$ of degree $30, 20, 12$ respectively and with no common factor of positive degree such that

$$aX^2 + bY^3 = cZ^5.$$

Given a quotient parameterization $J : \mathbb{P}^1 \to \mathbb{P}^1$, the objective of this section is to find finitely many integral parameterizations (X_i, Y_i, Z_i), $i = 1, \ldots, n$ (some $n \in \mathbb{Z}_{\geq 0}$) such that for any solution (x, y, z) to (4.1) with $1728by^3/(cz^5) = J(P)$ for some $P \in \mathbb{P}^1(\mathbb{Q})$ we have

$$(\pm x, y, z) = (X_i(u,v), Y_i(u,v), Z_i(u,v))$$

for some $i \in \{1, \ldots, n\}$ and $u, v \in \mathbb{Z}$. The methods for obtaining this are elementary but quite tedious.

4.3.1 Integral parameterizations needing rational specializations

First of all, since 2,3,5 are pairwise coprime, we can write any quotient parameterization J as

$$\frac{J}{1728} = \frac{bY^3}{cZ^5} = 1 - \frac{aX^2}{cZ^5}$$

with $X, Y, Z \in \mathbb{Z}[u, v]$ homogeneous of degree $30, 20, 12$ respectively and with no common factor of positive degree, so (X, Y, Z) gives us an integral parameterization to (4.1). This is explicitly accomplished by the functions in section B.1.3 (the appendix).

Now let (X, Y, Z) be such an integral parameterization obtained from a quotient parameterization J and suppose that (x, y, z) is a solution to (4.1) such that $by^3/cz^5 = J(P)/1728$ for some $P \in \mathbb{P}^1(\mathbb{Q})$, then for certain $u, v \in \mathbb{Q}$

$$\begin{aligned} x^2 &= \mu X^2(u, v), \\ y^3 &= \mu Y^3(u, v), \\ z^5 &= \mu Z^5(u, v), \end{aligned}$$

for some $\mu \in \mathbb{Q}$. We see that $\mu = \lambda^{30}$ for some $\lambda \in \mathbb{Q}$. By rescaling u, v we can assume that $\lambda \in \mathbb{Z}$ and that λ is square free. This leads to

$$\begin{aligned} \pm x &= \lambda^{15} X(u, v), \\ y &= \lambda^{10} Y(u, v), \\ z &= \lambda^6 Z(u, v). \end{aligned}$$

Note that $(\lambda^{15}X, \lambda^{10}Y, \lambda^6 Z)$ is also an integral parameterization. Furthermore, we claim that if $p|\lambda$, then $p|\mathrm{Res}(Y, Z)$ (say), so we only have to take finitely many λ into consideration. Suppose $p|\lambda$. Write

$$\tilde{X} := (\lambda/p)^{15} X, \ \tilde{Y} := (\lambda/p)^{10} Y, \ \tilde{Z} := (\lambda/p)^6 Z.$$

This gives us

$$(\pm x, y, z) = (p^{15}\tilde{X}(u, v), p^{10}\tilde{Y}(u, v), p^6 \tilde{Z}(u, v)).$$

with $u, v \in \mathbb{Q}$. Let

$$m := -\min(\nu_p(u), \nu_p(v)).$$

By the integrality of $\tilde{X}, \tilde{Y}, \tilde{Z}$ and since $\gcd(x, y, z) = 1$ we must have $m \geq 1$. Let

$$(u_0, v_0) := (p^m u, p^m v),$$

then $u_0, v_0 \in \mathbb{Z}_{(p)}$ and u_0, v_0 are relatively prime (in $\mathbb{Z}_{(p)}$); here $\mathbb{Z}_{(p)}$ denotes of course the localizations of $\mathbb{Z}$ at the prime ideal (p), i.e. the ring of all $q \in \mathbb{Q}$ with $\nu_p(q) \geq 0$. Furthermore,

$$(p^{30m-15}x, p^{20m-10}y, p^{12m-6}z) = (\tilde{X}(u_0, v_0), \tilde{Y}(u_0, v_0), \tilde{Z}(u_0, v_0))$$

This shows that $p|\mathrm{Res}(\tilde{Y}, \tilde{Z})$, hence $p|\mathrm{Res}(Y, Z)$, which proves our claim.

We have shown how one quotient parameterization J leads to finitely many integral parameterizations (X_i, Y_i, Z_i) such that for any solution x, y, z such that $j(x, y, z) = J(P)$ for some $P \in \mathbb{P}^1(\mathbb{Q})$ we have

$$(\pm x, y, z) = (X_i(u, v), Y_i(u, v), Z_i(u, v))$$

for some i and $u, v \in \mathbb{Q}$. So we possibly have to specialize at nonintegral values to obtain our solutions.

4.3.2 Integral parameterizations needing integer specializations

We will now show how to obtain integral parameterizations that only need integer specializations. First some terminology. Any $M \in \mathrm{GL}_2(\mathbb{Q})$ defines a map from $\mathbb{Q}^2$ to $\mathbb{Q}^2$, given by $(u,v)^t \mapsto M(u,v)^t$, in this way we get a right-action of $\mathrm{GL}_2(\mathbb{Q})$ on binary forms over $\mathbb{Q}$, simply by composing $F \in \mathbb{Q}[u,v]$ with $M \in \mathrm{GL}_2(\mathbb{Q})$ on the right. The arguments of a form $F \in \mathbb{Q}[u,v]$ will not be written as column vectors, so we have

$$(f \circ M)(u,v) := f(u',v'),\ (u',v')^t = M(u,v)^t.$$

Similarly we let $\mathrm{GL}_2(\mathbb{Q})$ act on n-tuples componentwise, explicitly

$$(X,Y,Z) \circ M := (X \circ M, Y \circ M, Z \circ M).$$

Specialization is also defined componentwise

$$(X,Y,Z)(u,v) := (X(u,v), Y(u,v), Z(u,v)).$$

We will focus on a special type of matrices, for every $[a:b] \in \mathbb{P}^1(\mathbb{F}_p)$ we define a matrix in $\mathrm{GL}_2(\mathbb{Q})$ as follows,

$$M_{[a:b]} := \begin{cases} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} & \text{if } [a:b] = [0:1]; \\ \begin{pmatrix} 1 & 0 \\ k & p \end{pmatrix} & \text{if } [a:b] = [1 : k \bmod p] \text{ with } k \in \mathbb{Z} \text{ and } 0 \le k < p. \end{cases}$$

With this definition we have for relatively prime $u, v \in \mathbb{Z}_{(p)}$

$$(u,v)^t = M_{[\overline{u}:\overline{v}]}(u',v')^t$$

where $u', v' \in \mathbb{Z}_{(p)}$ and u', v' are relatively prime (as elements of $\mathbb{Z}_{(p)}$), and the bar above u, v denotes reduction modulo p. We make some other simple but very useful observations.

Lemma 92. *Let $F(u,v)$ be a binary form over $\mathbb{Z}$, p a prime and suppose that $p | F(u,v)$ for certain relatively prime $u, v \in \mathbb{Z}_{(p)}$. Then $p | \mathrm{content}(F \circ M_{[\overline{u}:\overline{v}]})$.*

Proof. Since u, v are relatively prime, by changing basis, we can without loss of generality assume that $(u,v) = (1,0)$. Now $(F \circ M_{[1:0]})(u,v) = F(u,pv)$, so $p | \mathrm{content}(F \circ M_{[\overline{u}:\overline{v}]})$ if and only if p divides the coefficient of $u^{\deg F}$ in F. But this coefficient equals $F(1,0)$ which, by assumption, is divisible by p. □

For an integral parameterization (X,Y,Z) we define

$$C_p(X,Y,Z) := \min(2\nu_p(\mathrm{content}(X)), 3\nu_p(\mathrm{content}(Y)), 5\nu_p(\mathrm{content}(Z))).$$

Corollary 93. *Let (X,Y,Z) be an integral parameterization, p a prime and suppose that*

$$\min(2\nu_p(X(u,v)), 3\nu_p(Y(u,v)), 5\nu_p(Z(u,v))) > C_p(X,Y,Z)$$

for certain relatively prime $u, v \in \mathbb{Z}_{(p)}$. Then

$$C_p((X,Y,Z) \circ M_{[\overline{u}:\overline{v}]}) > C_p(X,Y,Z).$$

Proof. Divide the binary (degree 60) forms X^2, Y^3, Z^5 by $p^{C_p(X,Y,Z)}$ and apply the previous lemma. □

Obtaining an integral parameterization from a solution

Let (X, Y, Z) be an integral parameterization and suppose that specialization to $u, v \in \mathbb{Q}$ leads to a solution

$$(x, y, z) := (X, Y, Z)(u, v)$$

of (4.1). We focus on one prime p. Let

$$m := -\min(\nu_p(u), \nu_p(v)).$$

By the integrality of X, Y, Z and since $\gcd((X, Y, Z)(u, v)) = 1$ we have $m \geq 0$. Write

$$(u_0, v_0) := p^m(u, v).$$

Then $u_0, v_0 \in \mathbb{Z}_{(p)}$ and they are relatively prime. We are going to find an integral parameterization $(X', Y', Z)'$ such that $(X, Y, Z)(u, v)$ is obtained by specialization of (X', Y', Z') to some $u', v' \in \mathbb{Z}_{(p)}$ and furthermore, $(X', Y', Z') = (X, Y, Z) \circ M$ for some $M \in \mathrm{GL}_2(\mathbb{Q})$ such that $p^k M^{-1}$ is integral for some $k \in \mathbb{Z}_{\geq 0}$.

For this we define inductively two sequences, one of integral parameterizations (X_i, Y_i, Z_i) and one of relatively prime tuples $(u_i, v_i) \in \mathbb{Z}^2_{(p)}$. Furthermore, write

$$M_i := M_{[\overline{u_i}, \overline{v_i}]}.$$

Let $(X_0, Y_0, Z_0) := (X, Y, Z)$ and $(u_0, v_0) := p^m(u, v)$ as above. Define for $i \geq 0$

$$\begin{aligned} (u_{i+1}, v_{i+1})^t &:= M_i^{-1}(u_i, v_i)^t \\ (X_{i+1}, Y_{i+1}, Z_{i+1}) &:= (X_i, Y_i, Z_i) \circ M_i. \end{aligned}$$

It follows immediately that (for $i \in \mathbb{Z}_{\geq 0}$) we have

$$(X_i, Y_i, Z_i) = (X, Y, Z) \circ \prod_{k=0}^{i-1} M_k$$

and

$$(u_i, v_i)^t = \left(\prod_{k=0}^{i-1} M_k \right)^{-1} p^m (u, v)^t$$

(the order of matrix multiplication is of course $M_0 \dots M_{i-1}$). Note in particular that

$$(X_i, Y_i, Z_i)(u_i, v_i) = (X, Y, Z)(p^m u, p^m v) = (p^{30m} x, p^{20m} y, p^{12m} z). \tag{4.31}$$

So if $C_p(X_i, Y_i, Z_i) < 60m$, then by Corollary 93

$$C_p(X_{i+1}, Y_{i+1}, Z_{i+1}) > C_p(X_i, Y_i, Z_i).$$

Furthermore, from (4.31) and the fact that $\gcd(x, y, z) = 1$, we get

$$C_p(X_i, Y_i, Z_i) \leq 60m + \min(\nu_p(x^2), \nu_p(y^3), \nu_p(z^5)) = 60m.$$

For later reference we note that from (4.31) we get $60m \leq \nu_p(\mathrm{Res}(Y^3, Z^5))$, so together with the inequality above we get

$$C_p(X_i, Y_i, Z_i) \leq \nu_p(\mathrm{Res}(Y^3, Z^5)). \tag{4.32}$$

Now we conclude that for some $n \leq 60m$, we have $C_p(X_n, Y_n, Z_n) = 60m$, so with

$$(u', v') := (u_n, v_n), \quad (X', Y', Z') := (X_n/p^{30m}, Y_n/p^{20m}, Z_n/p^{12m})$$

we have that (X', Y', Z') is an integral parameterization, $u', v' \in \mathbb{Z}_{(p)}$ and

$$(X', Y', Z')(u', v') = (X, Y, Z)(u, v) = (x, y, z).$$

In fact

$$(X', Y', Z') = (X, Y, Z) \circ M,$$

where

$$M := p^{-m} \prod_{i=0}^{n-1} M_i.$$

First of all note that

$$\prod_{i=1}^{n-1} M_i \not\equiv 0 \pmod{p}.$$

Next, note that M has only powers of p as denominators in its coefficients and a power of p as its determinant. This means that M^{-1} has integral coefficients away from p (i.e. has only powers of p as denominators in its coefficients) and since $(u', v')^t = M^{-1}(u, v)^t$ we see that if u, v are integral at some prime p', then u', v' are integral at p'. So, by repeating the process above for all primes in the denominators of u, v we obtain an integral parameterization such that specialization to *integer* $\tilde{u}, \tilde{v}$ gives rise to the solution x, y, z.

Obtaining integral parameterizations in general

We now come to the heart of the matter. Starting with some parameterized solution (X, Y, Z) we now want to obtain finitely many parameterized solutions such that every solution to (4.1) obtained from specializing (X, Y, Z) at some rational values can be obtained by specialization of one of the mentioned finitely many parameterized solutions at some integer values. The construction is per prime p (dividing $\mathrm{Res}(Y, Z)$) as follows. We define inductively sets S_i, $i \in \mathbb{Z}_{\geq 0}$ consisting of pairs $((X_i, Y_i, Z_i), M_i)$, where (X_i, Y_i, Z_i) is an integral parameterization and $M_i \in \mathrm{GL}_2(\mathbb{Q})$ with integer entries and determinant a power of p. From these sets S_i, we construct a set P of integral parameterizations. We take

$$S_0 := \{((X_0, Y_0, Z_0), I)\}.$$

Given S_i, we define S_{i+1} as follows. For all $((X_i, Y_i, Z_i), M_i) \in S_i$ and $[a : b] \in \mathbb{P}^1(\mathbb{F}_p)$, we define

$$(X_{i+1}, Y_{i+1}, Z_{i+1}) := (X_i, Y_i, Z_i) \circ M_{[a:b]}, \quad M_{i+1} := M_i \circ M_{[a:b]}.$$

Now we let the pair $((X_{i+1}, Y_{i+1}, Z_{i+1}), M_{i+1})$ belong to S_{i+1} if and only if

$$C_p(X_{i+1}, Y_{i+1}, Z_{i+1}) > C_p(X_i, Y_i, Z_i)$$

and

$$M_{i+1} \not\equiv 0 \pmod{p}.$$

Note that (X_i, Y_i, Z_i) play the same role as in the previous discussion, but M_i is defined differently. We claim that for some $n > 0$ we have that S_n is empty and consequently by construction, S_i is empty for all $i \geq n$. Suppose $i \geq 0$ is such that S_i is not empty and let $((X_i, Y_i, Z_i), M_i) \in S_i$. By construction and from (4.32) we get

$$i \leq C_p(X_i, Y_i, Z_i) \leq \nu_p(\mathrm{Res}(Y^3, Z^5)),$$

which proves our claim (the bound is not very sharp). Note in particular that if $p \nmid \mathrm{Res}(Y, Z)$, then $S_i = \emptyset$ for all $i > 0$.

Now for the set P. Let $((X_i, Y_i, Z_i), M_i) \in S_i$ for some i. If

$$60 | C_p(X_i, Y_i, Z_i) =: e,$$

then we let

$$(X_i/p^{e/2}, Y_i/p^{e/3}, Z_i/p^{e/5})$$

belong to P, unless

$$60 | C_p(X_{i+1}, Y_{i+1}, Z_{i+1}),$$

where $((X_{i+1}, Y_{i+1}, Z_{i+1}), M_{i+1}) \in S_{i+1}$ with $M_{i+1} = M_i \circ M_{[a:b]}$ for a certain $[a : b] \in \mathbb{P}^1(\mathbb{F}_p)$.

The discussion on obtaining an integral parameterization from a solution, shows that for every $u, v \in \mathbb{Q}$ such that $(x, y, z) := (X, Y, Z)(u, v)$ is a solution to (4.1) one of the parameterizations $(X_i/p^{e/2}, Y_i/p^{e/3}, Z_i/p^{e/5})$ in some S_i with $60 | C_p(X_i, Y_i, Z_i) = e$ gives rise to the solution (x, y, z) when specialized to some $u', v' \in \mathbb{Z}_{(p)}$. Now if $((X_i, Y_i, Z_i), M_i) \in S_i$ and $((X_{i+1}, Y_{i+1}, Z_{i+1}), M_{i+1}) \in S_{i+1}$ both satisfy $60 | C_p(X_i, Y_i, Z_i) =: e_i$ and $60 | C_p(X_{i+1}, Y_{i+1}, Z_{i+1}) =: e_{i+1}$, with $M_{i+1} = M_i \circ M_{[a:b]}$ for a certain $[a : b] \in \mathbb{P}^1(\mathbb{F}_p)$, then $e_{i+1} = e_i + 60$ (using $e_i < e_{i+1} \leq e_i + 60$). With

$$(X_1', Y_1', Z_1') := (X_i/p^{e_i/2}, Y_i/p^{e_i/3}, Z_i/p^{e_i/5})$$

and

$$(X_2', Y_2', Z_2') := (X_{i+1}/p^{e_{i+1}/2}, Y_{i+1}/p^{e_{i+1}/3}, Z_{i+1}/p^{e_{i+1}/5})$$

we obtain

$$(X_2', Y_2', Z_2') = (X_1', Y_1', Z_1') \circ (M_{[a:b]}/p).$$

Now $N := (M_{[a:b]}/p)^{-1}$ has integer entries and together with

$$(X_1', Y_1', Z_1') = (X_2', Y_2', Z_2') \circ N$$

we see that solutions obtained by specializing (X_1', Y_1', Z_1') at values integral at p are already obtained by specializing (X_2', Y_2', Z_2') at values integral at p (of course, (X_2', Y_2', Z_2') need not belong to P, but then there is some appropriate (X_3', Y_3', Z_3'), and so on). We conclude that for every solution (x, y, z) to (4.1) that can be written as

$$(\pm x, y, z) = (X, Y, Z)(u, v)$$

for some $u, v \in \mathbb{Q}$, there exists an integral parameterization $(X', Y', Z') \in P$ such that

$$(\pm x, y, z) = (X', Y', Z')(u', v')$$

for some (necessarily coprime) $u', v' \in \mathbb{Z}_{(p)}$.

As discussed before, if u, v are integral at some prime p', then so are u', v'. This proves that the following construction finally gives all integral parameterizations such that specialization at integer values covers all solutions obtained from specializing (X, Y, Z) at rational values. Let $p_1, \ldots, p_n$ denote the primes dividing $\mathrm{Res}(Y, Z)$. Let P_1 be the set of integral parameterizations obtained from (X, Y, Z) by applying the method above with $p = p_1$ and (for $1 < i \leq n$), let P_i denote the set of integral parameterizations obtained from all integral parameterizations in P_{i-1} by applying the above method with $p = p_i$, then P_n gives us the desired set of integral parameterizations obtained from (X, Y, Z). Of course an integral parameterization in P_n need not give rise to any solutions to (4.1) when specialized at integer values, this is simply decided by calculation modulo p for $p = p_1, \ldots, p_n$. In practice it is best to throw away any integral parameterization as soon as it is obvious that it will not give rise to solutions. In our algorithm we check for integral parameterizations in P_i if there are specializations with p_i not dividing the gcd. The implementation in Magma of the algorithm described above, combined with the algorithm from section 4.3.1, to obtain all the relevant integral parameterizations from one integral parameterization coming from one quotient parameterization, is given in section B.1.4 (the appendix).

4.4 Some results for $S_{abc} = \{2, 3, 5\}$

In this section we describe some results obtained by using our algorithms for solving (4.1) in some cases. We are in fact able to solve (4.1) if abc is only composed of primes in $\{2, 3, 5\}$, i.e. if $S_{abc} = \{2, 3, 5\}$. For this, we need a finite list of polynomials covering all relevant algebras $\mathbb{Q}[t]/(f_j(t))$ as explained earlier. It would suffice to have a list of all number fields up to degree 5 unramified outside $\{2, 3, 5\}$. Such a list can in principle be obtained in finite time, see e.g. [Coh2, Chapter 9], but in practice can be infeasible. Up to degree 4 is in fact feasible via (relative) Hunter's theorem from *loc. cit.* (degree 2 is of course trivial and degree 3 can also be dealt with easily). But finding all relevant degree 5 number fields within a reasonable time is not so easy. Lucky for us J. Jones and D.

Roberts have already obtained (amongst other things) a list of all number fields up to degree 5, unramified outside $\{2, 3, 5\}$ by using clever variations of Hunter's theorem. Lists of these (and other) number fields are available on-line, see [JR]. To obtain our list of polynomials we multiplied polynomials defining the number fields to obtain degree 5 polynomials and then checked, using Lemma 85 (and Proposition 89) if the polynomials are equivalent to some f_j. In practice, we used `function integritycheck` from Appendix B. Of course, we used the facts that the discriminant of the resulting degree 5 polynomial is 5 times a square (in $\mathbb{Q}^*$) and that the polynomial has exactly one real root. For example, in the case that our algebra is the direct product of two quadratic number fields and $\mathbb{Q}$, we only need to consider the 4 polynomials

$$t(t^2+5)(t^2+1),\ t(t^2+10)(t^2+2),\ t(t^2+15)(t^2+3),\ t(t^2+30)(t^2+6).$$

In fact, only $t(t^2+10)(t^2+2)$ and $t(t^2+15)(t^2+3) \sim (t^2+15)(t^3-1)$ pass the test. The number of algebras being a direct product of number fields of degree 3 and 2, degree 4 and 1, degree 5 we found is given by 19, 12, 300 respectively. In total, we have $2 + 19 + 12 + 300 = 333$ algebras of the form $\mathbb{Q}[t]/(f_j(t)),\ j \in \mathbb{Q} - \{0, 1728\}$ unramified outside $\{2, 3, 5\}$. The algorithms described in the previous sections, or in practice, `function poltosols` from Appendix B can now be used to find all parameterized solutions to (4.1) whenever $S_{abc} = \{2, 3, 5\}$.

4.4.1 Primitive solutions to $x^2 + y^3 = z^5$

In [Edw] a complete solution to (4.1) with $a = b = c = 1$ was given for the first time. There were 27 parameterizations found such that all solutions can be obtained by specializing the variables of one of these parameterized solutions to integer values. Applying our algorithm to the 333 relevant polynomials to find parameterized solutions induced by these polynomials, we also found 27 parameterizations, which are, up to $\mathrm{GL}_2(\mathbb{Z})$ equivalence, the same as the 27 parameterizations from [Edw]. In fact, Table 4.1 gives all the polynomials $F(t)$ that give rise to some parameterized solution, together with the numbers from *loc. cit.* of these parameterizations.

We want to mention that, using Newton polygon techniques, it is possible to bound the discriminant d of an algebra $\mathbb{Q}[t]/(f_j(t))$ corresponding to a solution in our $a = b = c = 1$ case, to $d_0 := 2^6 \cdot 3^4 \cdot 5^5$, in the sense that $d | d_0$. We do not need the full list of 333 polynomials (with discriminant for the corresponding algebra going up to $2^8 \cdot 3^6 \cdot 5^9$), and the computation time of a list with the extra discriminant condition would probably be significantly less than the time for computing all 333 polynomials. But since a complete list for $S_{abc} = \{2, 3, 5\}$ is available anyhow, we leave it at this.

4.4.2 No local-to-global principle

Let $a, b, c \in \mathbb{Z} - \{0\}$, $r \in \{2, 3, 4, 5\}$ and consider the spherical generalized Fermat equation

$$ax^2 + by^3 = cz^r \tag{4.33}$$

$F(t)$	parameterization number
$(t^2 + 15)(t^3 - 5)$	2,10,26
$t(t^4 + 180)$	3,4,12,17,18,27
$t^5 - 12$	1
$t^5 - 18$	20
$t^5 - 3$	25
$t^5 - 10t^2 - 15t - 6$	5,9,13
$t^5 - 30t^2 + 45t - 18$	8,14,16
$t^5 - 20t^2 + 30t - 60$	15,21,24
$t^5 - 10t^2 + 15t + 48$	7
$t^5 - 10t^2 + 15t + 18$	19
$t^5 - 30t - 60$	6,23
$t^5 + 15t - 6$	11
$t^5 - 20t^2 + 30t - 6$	22

Table 4.1: polynomials with corresponding parameterizations to $x^2 + y^3 = z^5$

By a *global solution* to this equation we mean, as always, a solution $x, y, z \in \mathbb{Z}$ satisfying $\gcd(x, y, z) = 1$ and $xyz \neq 0$. A *local solution* to this equation, is simply, a solution $x, y, z \in \mathbb{Z}_p$, satisfying $\gcd(x, y, z) = 1$ and $xyz \neq 0$. One can consider a local-to-global principle for the equation. That is, if for all (finite) primes p there exist a local solution (in $\mathbb{Z}_p$), then does this imply that there exists a global solution? For $r = 2, 3, 4$ the fact that the exponents in (4.33) are not pairwise relatively prime, makes that it is possible to find (pairwise relatively prime) $a, b, c \in \mathbb{Z} - \{0\}$ such that (4.33) has everywhere local solutions but no global solutions, see [DG, Section 8]. For $r = 5$ it has been an open problem since the publication of *loc. cit.* whether or not a local-to-global principle holds for $r = 5$. By applying our algorithm we finally obtain examples showing that the local-to-global principal does also not hold in the case $r = 5$.

Theorem 94. *Let $(a, b, c) = (16, 9, 1)$ or $(a, b, c) = (16, 3, 1)$. Then (4.33) with $r = 5$ has local solutions for every prime p, but no global solutions.*

Proof. For $(a, b, c) = (16, 9, 1)$ we have $(x, y, z) = (5^9, 5^6, 5^4)$ as local solution for all $p \neq 5$ and $(x, y, z) = (2^7, -2^5, -2^3)$ as local solution for all $p \neq 2$. For $(a, b, c) = (16, 3, 1)$ we have $(x, y, z) = (19^{12}, 19^8, 19^5)$ as local solution for all $p \neq 19$ and $(x, y, z) = (13^{12}, -13^8, 13^5)$ as local solution for all $p \neq 13$. Note that for both choices of (a, b, c) we have $S_{abc} = \{2, 3, 5\}$. We applied our algorithm to obtain all parameterized solutions from the 333 relevant polynomials. As output we got zero parameterized solutions in both cases, showing that there are no global solutions. □

We expect to find more examples upon further investigation, also ones with S_{abc} strictly larger than $\{2, 3, 5\}$ using the modular method.

Using the fact that $2, 3, 5$ are pairwise coprime, it is not so difficult (though tedious) to show in general that there are in fact always everywhere local solutions

to (4.33) for $r = 5$ if a, b, c are pairwise coprime. Furthermore, one can consider (local and global) solutions such that x, y, z are pairwise coprime, instead of just coprime. Taking $(a, b, c) = (16, 5, 9)$ it is easy to find everywhere local pairwise coprime solutions (e.g. $(x, y, z) = (2^{14}, 2^{10}, 2^6)$ or $(x, y, z) = (3, -3, 1)$), and our algorithm gives 24 parameterized solutions for the coprime case. But a straightforward check showed that none of these 24 parameterized solutions specialize to global pairwise coprime solutions, showing that there are no global pairwise coprime solutions in this case. We want to mention that the three triples (a, b, c) above where kindly supplied by Nils Bruin as candidates for counterexamples to the local-to-global principle (in the pairwise coprime case).

Chapter 5

A modular approach to $ax^2 + by^3 = cz^5$

We describe how the list of étale algebras, necessary to perform the algorithms described in the previous chapter, can be obtained in some cases using the modular method.

5.1 Icosahedron

The icosahedral covering of $\mathbb{P}^1$ and the corresponding invariants from the previous chapter are intimately related to 5-torsion on elliptic curves. We describe here quickly the basics of this relation and the consequences we need. For an extensive treatment we refer to [Kle].

Let f, H, T be the icosahedral invariants from (4.7), (4.8), (4.9). Consider the elliptic curve

$$E_{u,v} : Y^2 = X^3 + 3H(u,v)X + 2T(u,v).$$

The discriminant and the j-invariant are given by

$$\begin{aligned} \Delta(E_{u,v}) &= -1728(T^2 + H^3) \\ &= -2^{12}3^6 f^5 \\ j_{E_{u,v}} &= \frac{1728H^3}{T^2 + H^3} \\ &= \frac{H^3}{f^5}. \end{aligned}$$

In particular, the (dehomogenized) j-invariant is exactly the icosahedral covering $J(z)$ from (4.14). One can check that

$$\begin{aligned} X_0(u,v) := \; & u^{10} + 12u^8v^2 - 12u^7v^3 + 24u^6v^4 + 30u^5v^5 \\ & +60u^4v^6 + 36u^3v^7 + 24u^2v^8 + 12uv^9 + v^{10} \end{aligned}$$

is the X-coordinate of a point of order 5 on $E_{u,v}$ (after twisting over $\mathbb{Q}(\sqrt{3})$ the corresponding Y-coordinates are also homogeneous elements in $\mathbb{Q}[u, v]$), $X_0(\zeta_5 u, v)$ is the X-coordinate of an independent point of order 5 and for the field generated over $\mathbb{Q}$ by the X-coordinates of all points of order 5, we have $\mathbb{Q}(E_{u,v}[5]_x) = \mathbb{Q}(X_0(u, v), X_0(\zeta_5 u, v))$. Switching to dehomogeneous notation from now on (that is, let $z = u/v$), we have in fact

$$\mathbb{Q}(E_{z,1}[5]_x) = \mathbb{Q}(\zeta_5, z),$$

so the icosahedral extension $\mathbb{Q}(\zeta_5, z)/\mathbb{Q}(\zeta_5, J(z))$ is given by

$$\mathbb{Q}(E_{z,1}[5]_x)/\mathbb{Q}(\zeta_5, j_{E_{z,1}}).$$

Now consider an elliptic curve $E/\mathbb{Q}$. Let $l_0, \ldots, l_5$ denote the 6 lines in $E[5]$, then the field $K := \mathbb{Q}(\{\sum_{P \in l_i - \{0\}} x_P\}_{i=0}^5)$ is a Galois extension of $\mathbb{Q}$ and is completely determines by $L := \mathbb{Q}(E[5]_x)$ (if $\zeta_5 \notin K$, then $[L : K] = 2$, otherwise $L = K$). We see that K is the splitting field of the polynomial

$$I_5^E(x) := \prod_{i=0}^{5} \left(x - \sum_{P \in l_i - \{0\}} x_P/2 \right) \in \mathbb{Q}[x].$$

If the elliptic curve is given by

$$E : Y^2 = X^3 + aX + b,$$

then we compute that

$$I_5^E(x) = x^6 + 20ax^4 + 160bx^3 - 80a^2x^2 - 128abx - 80b^2. \tag{5.1}$$

If E has j-invariant $j \neq 0, 1728$, then the roots of the Brioschi quintic $h_j(t)$ from (4.10) can be expressed in terms of the roots of $I_5(x)$ and vice versa in such a way that we obtain that the splitting fields of $h_j(t)$ and $I_5(x)$ are the same (historically, this was first done through the Jacobi sextic, which in one parameter form reads, $t^6 - 10jt^3 + j^2t + 5j^2$).

Now consider the representations induced from the 5-torsion points of elliptic curves $E_1, E_2/\mathbb{Q}$,

$$\rho_5^{E_i} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_5), \ i = 1, 2$$

and write $\rho_i := \rho_5^{E_i}$. Suppose that $\rho_1 \simeq \rho_2$. Then with $H_i := \rho_i^{-1}(\pm I) \subset G_{\mathbb{Q}}$, we have $H_1 = H_2$. The fixed field of H_i is $\mathbb{Q}(E_i[5]_x)$, so $\mathbb{Q}(E_1[5]_x) = \mathbb{Q}(E_2[5]_x)$. Consequently the splitting fields of $I_5^{E_1}$ and $I_5^{E_2}$ are equal (with no restriction on the j values of E_1, E_2).

Proposition 95. *Let E_1, E_2 be elliptic curves over $\mathbb{Q}$ with j-invariants j_1, j_2 respectively. Suppose that $\rho_5^{E_1} \simeq \rho_5^{E_2}$ and $j_i \neq 0, 1728$. Then $f_{j_1} \sim f_{j_2}$.*

Proof. We obtain from the discussion above (using $j \neq 0, 1728$) that the splitting fields of h_{j_1} and h_{j_2} are equal. By Proposition 67 we obtain that the splitting fields of f_{j_1} and f_{j_2} are equal. In fact, for $j \neq 0, 1728$, the splitting field of f_j determines $\mathbb{Q}[t]/(f_j(t))$ uniquely and the result follows. □

The case that one j-invariant equals 0 or 1728 can be dealt with separably.

Proposition 96. *Let E_1, E_2 be elliptic curves over $\mathbb{Q}$. Suppose that $\rho_5^{E_1} \simeq \rho_5^{E_2}$ and $j_1 \neq 0, 1728$.*

i. If E_2 is isomorphic to $Y^2 = X^3 + b$, then $f_{j_1} \sim (t^2 + 15)(t^3 + 100b)$.

ii. If E_2 is isomorphic to $Y^2 = X^3 + aX$, then $f_{j_1} \sim t(t^4 + 20a^2)$.

Proof. We use again the results of the discussion above.

i: Plugging $a = 0$ into (5.1) gives $I_5^{E_2} = x^6 + 160bx^3 - 80b^2$. The splitting field of this polynomial equals the splitting field of $F(t) := (t^2+15)(t^3+100b)$ (this can be established by writing down radical expressions for the roots of these polynomials). The criteria from section 4.2 show that $F(t) \sim f_j$ for some $j \in \mathbb{Q} - \{0, 1728\}$ and the splitting field of such an f_j determines $\mathbb{Q}[t]/(f_j(t))$.

ii: This case is similar. Plugging $b = 0$ into (5.1) gives $I_5^{E_2} = x^2(x^4 + 20ax^2 - 80a^2)$. The splitting field of this polynomial equals the splitting field of $t(t^4 + 20a^2) \sim f_j$ for some $j \in \mathbb{Q} - \{0, 1728\}$. □

5.2 Irreducible 5-torsion

To a solution x, y, z of (4.1) we associate the Frey curve

$$E : Y^2 = X^3 + 3abyX + 2a^2bx. \tag{5.2}$$

Basic quantities associated to E are given by

$$\begin{aligned} \Delta &= -1728a^3b^2(ax^2 + by^3) \\ &= -1728a^3b^2cz^5, \\ c_4 &= -144aby, \\ c_6 &= -1728a^2bx. \end{aligned}$$

Note in particular that

$$j_E = 1728\frac{by^3}{cz^5}$$

which equals $j(x, y, z)$ from(4.4). Let p be a prime such that $p \nmid 2 \cdot 3abc$. Then we see that E has good or multiplicative reduction at p and $\nu_p(\Delta_{\min}(E)) = \nu_p(\Delta) = 5\nu_p(z)$. So if ρ_5^E is irreducible, then we can use level lowering and by Theorem 35 we get that $E \sim_5 f$ for some newform f of level $N_0(E)$, where the primes dividing $N_0(E)$ form a subset of the primes dividing $2 \cdot 3abc$.

If f is a rational newform, then $\rho_5^E \simeq \rho_5^F$ for some elliptic curve $F/\mathbb{Q}$ and Propositions 95 and 96 give us the desired algebra $\mathbb{Q}[t]/(f_j(t))$.

If f is not rational, then possibly we can eliminate it using Proposition 46. If this does not work, we can try to raise to a level where ρ_5^f comes from an elliptic curve, i.e. find an elliptic curve $F/\mathbb{Q}$ such that $\rho_5^F \simeq \rho_5^f$ (for proving that a candidate F does the job, one can e.g. use the well known Sturm bound). But

in general there is no a priori reason that either of these methods will work for a nonrational newform f.

As our main example, we will now obtain all relevant polynomials f_j in the case that $a = b = c = 1$. Our Frey curve is given by

$$E : Y^2 = X^3 + 3yX + 2x,$$

with basic quantities

$$\begin{aligned} \Delta &= -2^6 \cdot 3^3 z^5, \\ c_4 &= -2^4 \cdot 3^2 y, \\ c_6 &= -2^6 \cdot 3^3 x. \end{aligned}$$

From the tables in [Pap] we obtain immediately that $N(E) = 2^\alpha \cdot 3^\beta \operatorname{rad}_{\{2,3\}}(z)$ with $\alpha \leq 6, \beta \leq 3$ (in fact, there is always a quadratic twist E' of E with $\nu_2(N(E')) \leq 5$, but the tables in [Pap] do not suffice for showing this and we really have to work through Tate's algorithm). Furthermore, for all primes $p \neq 2, 3$ dividing z we have $\nu_p(\Delta_{\min}(E)) = \nu_p(\Delta) = 5\nu_p(z)$. So under the assumption that ρ_5^E is irreducible, we obtain that $E \sim_5 f$ for some newform of level $N_0(E) = 2^\alpha \cdot 3^\beta$ with $\alpha \leq 6, \beta \leq 3$. All newforms at these levels can be calculated quickly (or looked up at several places). The nonrational newforms at these levels (they are in fact quadratic twists of each other) all have $a_p(f)^2 - 13 = 0$ for $p = 7$, so Proposition 46 gives us that it is impossible to have $E \sim_5 f$ for nonrational f. Consequently $\rho_5^E \simeq \rho_5^F$ for some elliptic curve F of conductor $N_0(E)$ (this is actually a special case of Example 47). All possible elliptic curves up to isogeny and quadratic twist with irreducible 5-torsion and conductor dividing $2^6 \cdot 3^3$ are found in a straightforward manner using [Cre2]. In fact, they can already be found in Table 4 of [BK] (which has been extracted from the Ph.D. thesis of Francis B. Coghlan). Anyway, they are given as follows. The CM-curves (up to isogeny and quadratic twist) are given by

$$\begin{aligned} Y^2 &= X^3 + 1, \\ Y^2 &= X^3 + 2, \\ Y^2 &= X^3 + 4, \\ Y^2 &= X^3 + X, \\ Y^2 &= X^3 + 3X. \end{aligned}$$

For the non CM-curves we get the j-invariants (we choose one from each isogeny class)

$$-6, -216, 1536, -3072, -13824, 2048/3, 9261/8, 21952/9.$$

Propositions 95 and 96 now give us explicitly a total of 13 polynomials $p(t)$, which determine 13 algebras $A = \mathbb{Q}[t]/(p(t))$ for the solutions related to irreducible 5-torsion. Spelled out, if x, y, z is a solution to (4.1) with $a = b = c = 1$ and the Frey curve E given by (5.2) has ρ_5^E irreducible, then $\mathbb{Q}[t]/(f_{j(x,y,z)}(t)) \simeq A$, with A one of the 13 algebras.

5.3 Reducible 5-torsion

Consider the two coverings $\mathbb{P}^1 \to \mathbb{P}^1$ given by

$$J_0(r) := \frac{(r^2 + 10r + 5)^3}{r} \tag{5.3}$$

and

$$\rho(s) := \frac{-125s}{s^2 + 11s - 1}.$$

Then the icosahedral map $J(z)$ given by (4.14) factors as

$$J(z) = J_0(\rho(z^5)).$$

Note that J_0 is the j-map from the modular curve $X_0(5)$ to $X(1)$ and $J_0 \circ \rho$ is the j-map from the modular curve $X_1(5)$ to $X(1)$. The dessin d'enfant of $J_0(r)/1728$ is given in Figure 5.1. Now suppose the Frey curve E from (5.2) has reducible

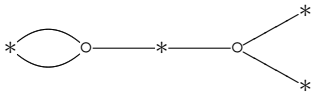


Figure 5.1: dessin d'enfant associated to $J_0(r)/1728$

5 torsion, i.e. ρ_5^E is reducible. This is equivalent to saying that $j_E = J_0(r)$ for some $r \in \mathbb{Q}$, note that in particular we have $j_E \neq 0, 1728$. Let $G(z) := \rho(z^5)$, then $G(z)$ defines in fact a D_5 cover of $\mathbb{P}^1$. Let $S := G^{-1}(r)$, then the 10 points in S are mapped 2 to 1 by τ (from (4.15)) onto the 5 roots of $f_{J_0(r)}$. If $r' \in \mathbb{Q}$ is such that $\mathbb{Q}(G^{-1}(r)) = \mathbb{Q}(G^{-1}(r'))$, then $f_{J_0(r)} \sim f_{J_0(r')}$. Furthermore, $\mathbb{Q}(G^{-1}(r))$ is unramified outside S_{abc}. So in order to find all relevant algebras, defined by $f_{J_0(r)}$ for some $r \in \mathbb{Q}$, we must find finitely many $r \in \mathbb{Q}$ covering all fields of the form $\mathbb{Q}(G^{-1}(r))$ unramified outside S_{abc}. The solvable nature of the covering G allows that this can be done very explicitly.

Let $r = \rho(s)$ and define $R := -(11 + 125/r)/2$, then s satisfies,

$$s^2 - 2Rs - 1 = 0,$$

with roots given by

$$s = R \pm \sqrt{1 + R^2}. \tag{5.4}$$

We distinguish two cases, namely that $s \in \mathbb{Q}$ and $s \notin \mathbb{Q}$. We start with the simplest, namely $s \in \mathbb{Q}$ (this corresponds to the case that E, or a quadratic twist, has a rational point of order 5). The possible fields $\mathbb{Q}(G^{-1}(r))$ are simply the splitting fields of $z^5 - s$. In order to get all fields of this form, unramified outside S_{abc}, we simply let s run through all elements of the form

$$\prod_{p \in S_{abc}} p^{e_p},$$

where $e_p \in \{0, \ldots, 4\}$. The defining polynomials for the algebras are then given by f_j, with $j = J_0(\rho(s))$ and in fact, we simply have $f_j \sim t^5 - s$. Note that if s_1, s_2 are of the shape above and $s_1 = s_2^k, k \in \mathbb{Z}_{>0}$, then the corresponding polynomials f_j are equivalent.

Now suppose we are in the case that $s \notin \mathbb{Q}$. Then from (5.4) we obtain that $s \in \mathbb{Q}(\sqrt{d})$ for some squarefree $d \in \mathbb{Z}_{\geq 2}$ with no prime which is $-1 \mod 4$ dividing d, furthermore, s must have norm -1. The ramification conditions imply that d is only divisible by primes in S_{abc}. Now fix such an appropriate d. If $\mathrm{Norm}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(s) = -1$, then the fractional ideal (s) of $\mathbb{Q}(\sqrt{d})$ is of the form

$$\prod_{i=1}^{n} \left(\frac{\mathfrak{P}_i}{\mathfrak{P}_i'} \right)^{e_i}, \tag{5.5}$$

$n, e_i \in \mathbb{Z}_{\geq 0}$ and where $\mathfrak{P}_i, \mathfrak{P}_i'$ denote two prime ideals lying above a prime $p \in \mathbb{Z}$ that splits in $\mathbb{Q}(\sqrt{d})$. Since in all the cases we are actually going to compute here, we will have that the class number of $\mathbb{Q}(\sqrt{d})$ is 1 or 2, we will assume this from now on, making things a bit easier to describe. Now every fractional ideal of the form (5.5) is in fact principal and generated by an element $s' \in \mathbb{Q}(\sqrt{d})$ of norm 1. Let ϵ_d denote a fundamental unit of $\mathbb{Q}(\sqrt{d})$ (so ϵ has norm -1). Then $s := s'\epsilon^k$ has norm -1 for odd $k \in \mathbb{Z}$. Since $z^5 - s$ and $z^5 - s\alpha^5$, for any $\alpha \in \mathbb{Q}(\sqrt{d})^*$ determine the same field, we can restrict to $k \in \{1, 3, 5, 7, 9\}$. Together with the ramification conditions we arrive at a description of all relevant fields $\mathbb{Q}(G^{-1}(r))$ containing $\mathbb{Q}(\sqrt{d})$ (where $\mathbb{Q}(\sqrt{d})$ has class number 1 or 2). They are given by the splitting fields of $z^5 - s$ over $\mathbb{Q}(\sqrt{d})$, with $s = s'\epsilon^k$, $k \in \{1, 3, 5, 7, 9\}$ and where s' is any element of norm 1 such that the fractional ideal $(s') = (s)$ is of the form

$$\prod_{\substack{p \in S_{abc} \\ p \text{ splits}}} \left(\frac{\mathfrak{P}_p}{\mathfrak{P}_p'} \right)^{e_p},$$

with $e_p \in \{0, 1, 2, 3, 4\}$ and $\mathfrak{P}_p, \mathfrak{P}_p'$ are the primes lying above p (in any order). So letting k and e_p run through all finitely many possibilities, we obtain all s, hence all r, hence all f_j (up to equivalence), with $j = J_0(r) = J_0(\rho(s))$ (and again we overcounted by allowing powers of s). In case the class number of $\mathbb{Q}(\sqrt{d})$ is greater than 2, the calculations will be a bit more involved (especially when 5 divides the class number), but in the same spirit as above, [Coh2, Chapter 5] might be helpful.

As our main example, we will now obtain all relevant polynomials f_j in the case that $S_{abc} = \{2, 3, 5\}$. We will be careful in naming every polynomial (modulo equivalence) only once. First of all, for $s \in \mathbb{Q}$, we get the polynomials $t^5 - s$, with s of the form

$$\begin{aligned} s &= 2 \cdot 3^j \cdot 5^k, \ 0 \leq i, j \leq 4 \\ s &= 3 \cdot 5^k, \ 0 \leq k \leq 4 \\ s &= 5 \\ s &= 1. \end{aligned}$$

If $s \notin \mathbb{Q}$, then $d \in \{2, 5, 10\}$. We note that $\mathbb{Q}(\sqrt{d})$ has class number 1 if $d = 2, 5$ and class number 2 if $d = 10$. If $d = 2, 5$ no prime in S_{abc} splits in $\mathbb{Q}(\sqrt{d})$, so

$d = 2$ and $d = 5$ each give rise to one polynomial f_j with $j = J_0(\rho(s))$, s a fundamental unit. For $d = 2$ we can take $s = 1 + \sqrt{2}$, leading to $r = -125/13$ and $j = -2^6 \cdot 11^3/13^5$. For $d = 5$ we can take $s = (1 + \sqrt{5})/2$, leading to $r = -125/12$ and $j = -269^3/(2^{10} \cdot 3^5)$. For $d = 10$, the only prime in S_{abc} that splits in $\mathbb{Q}(\sqrt{d})$ is 3. We have (by choosing the right notation) that the fractional ideal $\mathfrak{P}_3/\mathfrak{P}_3'$ is generated by the element $s' := 7/3 - (2/3)\sqrt{10}$ of norm 1. A fundamental unit is given by $\epsilon := 3 + \sqrt{10}$. The case $s = \epsilon$ leads to $r = -125/17$ and $j = 2^6 \cdot 11^3 \cdot 19^3/17^5$. All other relevant s are given by $s = s'\epsilon^k$, $k \in \{1, 3, 5, -3, -1\}$. These values of s (or actually $3s$) with corresponding values for r are given in Table 5.1, the values $j = J_0(r)$ can be calculated directly from this data. We conclude that all polynomials f_j (modulo equivalence) related to

k	$3s = 3s'\epsilon^k$	r
1	$1 + \sqrt{10}$	$-75/7$
3	$79 + 25\sqrt{10}$	$-375/191$
5	$3001 + 949\sqrt{10}$	$-75/1207$
-3	$-1559 + 493\sqrt{10}$	$75/617$
-5	$-41 + 13\sqrt{10}$	$375/49$

Table 5.1: values of s and r

reducible 5-torsion if $S_{abc} = \{2, 3, 5\}$ are given by the 40 polynomials above.

We note that parts of the discussion above might be expressed more elegantly in terms of Galois representations. But the actual computations still have to be done one way or the other.

5.4 Solving $x^2 + y^3 = z^5$ the modular way

In order to find all parameterized solutions to (4.1) with $a = b = c = 1$ we have to find all relevant algebras $\mathbb{Q}[t]/(f_j(t))$. After that, we can use the algorithms in sections 4.2 and 4.3. In the previous sections of this chapter we obviously have already done all the work and found 53 polynomials f_j that cover all algebras. After running our algorithms with these polynomials we found again (up to $\mathrm{GL}_2(\mathbb{Z})$ equivalence) the same 27 parameterizations as before.

Remark 97. Let $E/\mathbb{Q}$ be an elliptic curve. From [RS1] we can obtain an explicit formula for the j-map from $X_{E[5]}$ to $X(1)$, where $X_{E[5]}$ denotes the projective closure of the affine curve over $\mathbb{Q}$ whose points classify elliptic curves E' together with an isomorphism between the $G_\mathbb{Q}$ modules $E[5]$ and $E'[5]$ that takes the Weil pairing on $E[5]$ to that on $E'[5]$. This j-map provides us with one of the two quotient parameterizations related to f_{j_E}. The other parameterization can actually be identified with the j-map from $X_{E[5]'}$ to $X(1)$, where now the noncuspidal rational points on $X_{E[5]'}$ classify elliptic curves E' together with an isomorphism of $G_\mathbb{Q}$ modules $\phi : E[5] \to E'[5]$ such that, identifying $\bigwedge^2 E[5]$ and $\bigwedge^2 E'[5]$ with the $G_\mathbb{Q}$ module of 5-th roots of unity μ_5 via the Weil pairing, the induced map

$\bigwedge^2 \phi : \bigwedge^2 E[5] \to \bigwedge^2 E'[5]$ is the a-th power map $\mu_5 \to \mu_5$ for a fixed nonsquare $a \in \mathbb{F}_5$ ($a = 2$ or $a = 3$), see [PSS, section 4]. Probably the methods in [RS1] could be used to find this other j-map explicitly. But since we already have a perfectly fine algorithm to obtain the two j-maps, we will leave it at this.

Appendix A

Minimal discriminants and conductors

In principle Tate's algorithm [Tat] can always be used. In practice [Pap] is very handy to use. We note however that *loc. cit.* is not complete in the sense that if $\nu_2(c_4) = 6, \nu_2(c_6) \geq 9$ and $\nu_2(\Delta) = 12$, no criteria are given whether $\nu_2(N) = 6$ or $\nu_2(N) = 5$ and we must use Tate's algorithm. There is also a small mistake in Tableau IV, the '12' in the first column under 'Equation non minimale' should be replaced by '≥ 12'.

FLT

We consider the Frey curve

$$E_{a,b} : Y^2 = X(X-a)(X+b)$$

where $a, b \in \mathbb{Z}$ with $a \equiv -1 \pmod 4, b \equiv 0 \pmod{2^5}, ab(a+b) \neq 0$ and $\gcd(a,b) = 1$. Basic invariants are

$$\begin{aligned} c_4 &= 2^4(a^2+ab+b^2), \\ c_6 &= 2^5(a-b)(2a+b)(a+2b), \\ \Delta &= 2^4a^2b^2(a+b)^2. \end{aligned}$$

We have $\nu_2(c_4) = 4, \nu_2(c_6) = 6, \nu_2(\Delta) \geq 14$. Using [Pap, Proposition 4] we obtain that the model E above is not minimal at 2. So for a minimal model we get $\nu_2(c_4) = 0, \nu_2(c_6) = 0, \nu_2(\Delta) \geq 2$ and consequently $\nu_2(N) = 1$. Furthermore, $\mathrm{Res}(\Delta, c_4) = 2^{24}$, so for an odd prime p the model E above is minimal at p and $\nu_p(N) = 1$ if $p|\Delta$ and $\nu_p(N) = 0$ otherwise. We conclude

$$\begin{aligned} \Delta_{\min} &= \frac{\Delta}{2^{12}}, \\ N &= \mathrm{rad}(ab(a+b)). \end{aligned}$$

Alternatively, we can write down explicitly a minimal model as follows

$$Y^2 + XY = X^3 + \frac{b-a-1}{4}X^2 - \frac{ab}{4}X.$$

The equation $x^2 - 11 = y^l$

Consider the Frey curve

$$E : Y^2 = X^3 - 4xX^2 + 4(x^2 - 11)X$$

and assume that $x^2 - 11 = y^n$ for $x, y, n \in \mathbb{Z}$ and $n \geq 3$. Basic invariants are

$$\begin{aligned} c_4 &= 2^6(x^2 + 33), \\ c_6 &= -2^9 x(x^2 - 99), \\ \Delta &= 2^{12} \cdot 11(x^2 - 11)^2. \end{aligned}$$

If x is odd, then $x^2 - 11 \equiv 2 \pmod 4$, so x is even. We obtain $\nu_2(c_4) = 6, \nu_2(c_6) \geq 10$ and $\nu_2(\Delta) = 12$. According to [Pap] the equation is minimal at 2, but to obtain $\nu_2(N)$ we must use Tate's algorithm. Applying this in a straightforward way, we get $\nu_2(N) = 5$. Furthermore $\mathrm{Res}_x(c_4, \Delta) = 2^{56} \cdot 11^6$. Obviously $11 \nmid x$, so $11 \nmid c_4$.

We conclude that

$$\begin{aligned} \Delta_{\min} &= 2^{12} \cdot 11(x^2 - 11)^2, \\ N &= 2^5 \cdot 11 \,\mathrm{rad}_{\{2,11\}}(x^2 - 11). \end{aligned}$$

The equation $x^3 - x - 2 = y^l$

Consider the Frey curve

$$E : Y^2 = X^3 + X^2 - x(6 + x)X - (2x^3 + x^2 + 4x + 4)$$

and assume that $x^3 - x - 2 = y^n$ for $x, y, n \in \mathbb{Z}$ and $n \geq 3$. Basic invariants are

$$\begin{aligned} c_4 &= 2^4(3x^2 + 18x + 1), \\ c_6 &= 2^6(27x^3 + 9x^2 + 27x + 53), \\ \Delta &= -2^7 \cdot 13(x^3 - x - 2)^2. \end{aligned}$$

We have $x^3 - x - 2 \equiv 1 \pmod 3$. So $3 \nmid \Delta$, hence $3 \nmid N$. Since $x \equiv 0 \pmod 2$ we have $3x^2 + 18x + 1, 27x^3 + 9x^2 + 27x + 53 \equiv 1 \pmod 2$. So $\nu_2(c_4) = 4, \nu_2(c_6) = 6, \nu_2(\Delta) \geq 13$. By [Pap, Proposition 4] we have that the model above is not minimal at 2. So for a minimal model we have $\nu_2(c_4) = 0, \nu_2(c_6) = 0, \nu_2(\Delta) \geq 1$, hence $\nu_2(N) = 1$ and $\nu_2(\Delta_{\min}) = \nu_2(\Delta/2^{12})$. Furthermore $\mathrm{Res}_x(c_4, \Delta) = 2^{50} \cdot 13^6$. But $13 \nmid c_4$, namely if $c_4 \equiv 0 \pmod{13}$, then $x \equiv 10 \pmod{13}$, but then $x^3 - x - 2 \equiv 0 \pmod{13}$, so $x^3 - x - 2 \equiv 0 \pmod{13^2}$, but then $x \equiv 162 \pmod{13^2}$, so $x \equiv 6 \pmod{13}$, contradiction.

We conclude that

$$\begin{aligned} \Delta_{\min} &= -\frac{13}{2^5}(x^3 - x - 2), \\ N &= 2 \cdot 13 \,\mathrm{rad}_{\{2,13\}}(x^3 - x - 2). \end{aligned}$$

The equation $x^3 + 13 = y^l$

Consider the Frey curve

$$E : Y^2 = \begin{cases} X^3 - 3x^2X + 2(x^3 + 26) & \text{if } x \text{ is even;} \\ X^3 - 3x^2X - 2(x^3 + 26) & \text{if } x \text{ is odd,} \end{cases}$$

and assume that $x^3 + 13 = y^n$ for $x, y, n \in \mathbb{Z}$ and $n \geq 5$. Basic invariants are

$$\begin{aligned} c_4 &= 2^4 \cdot 3^2 x^2, \\ c_6 &= \mp 2^6 \cdot 3^3 (x^3 - 26), \\ \Delta &= -2^8 \cdot 3^3 \cdot 13 (x^3 + 13), \end{aligned}$$

where the sign in c_6 is taken to be $-$ if x is even and $+$ if x is odd. First consider the case that x is even. Then $\nu_2(c_4) \geq 6, \nu_2(c_6) = 7, \nu_2(\Delta) = 8$. Applying [Pap, Proposition 3] we get that 'Cas de Tate ≥ 7' and hence $\nu_2(N) \in \{2, 3\}$. Now suppose x is odd. Then $\nu_2(c_4) = 4, \nu_2(c_6) = 6, \nu_2(\Delta) \geq 13$. By [Pap, Proposition 4] we have that our model of E is not minimal at 2. So for a minimal model we have $\nu_2(c_4) = 0, \nu_2(c_6) = 0, \nu_2(\Delta) \geq 1$, hence $\nu_2(N) = 1$ and $\nu_2(\Delta_{\min}) = \nu_2(\Delta/2^{12})$.

Next we calculate $\nu_3(N)$. If $3|x^3 + 13$, then we get $x^3 + 13 \equiv 3 \pmod 9$, which is impossible. So $\nu_3(\Delta) = 3$ and the model is minimal at 3. Together with $3|\nu_3(c_4)$ we get $1 < \nu_3(N) \leq \nu_3(\Delta)$, i.e. $\nu_3(N) \in \{2, 3\}$ (and both possibilities actually occur, depending on x modulo 3).

Furthermore, the primes dividing $\mathrm{Res}_x(c_4, \Delta)$ are $2, 3, 13$. Certainly $13 \nmid x$ and we conclude

$$\Delta_{\min} = \begin{cases} \Delta & \text{if } x \text{ is even;} \\ 2^{-12}\Delta & \text{if } x \text{ is odd,} \end{cases}$$

$$N = \begin{cases} 2^a 3^b 13 \operatorname{rad}_{\{2,3,13\}}(x^3 + 13) & \text{if } x \text{ is even;} \\ 2 \cdot 3^b 13 \operatorname{rad}_{\{2,3,13\}}(x^3 + 13) & \text{if } x \text{ is odd,} \end{cases}$$

where $a, b \in \{2, 3\}$.

The equation $x^4 + x^3 - 3x^2 + 11x + 2 = y^l$

Consider the Frey curve

$$E : Y^2 = X^3 - 3a(x)X - 2b(x),$$

where

$$\begin{aligned} a(x) &:= 9x^4 - 92x^3 - 42x^2 - 60x + 137 \\ b(x) &:= 101x^6 + 30x^5 + 795x^4 - 2380x^3 - 1605x^2 + 654x - 1627 \end{aligned}$$

and assume that $f(x) := x^4 + x^3 - 3x^2 + 11x + 2 = y^n$ for $x, y, n \in \mathbb{Z}$ and $n \geq 5$. Basic invariants are

$$\begin{aligned} c_4 &= 2^4 \cdot 3^2 a(x), \\ c_6 &= 2^6 \cdot 3^3 b(x), \\ \Delta &= -2^{14} \cdot 3^3 \cdot 37 f(x)^3. \end{aligned}$$

For any $x \in \mathbb{Z}$ we have $2|f(x)$, so $8|f(x)$, which gives us $x \equiv 6 \pmod 8$. Furthermore, $2|a(x) \Leftrightarrow 2|b(x) \Leftrightarrow x \equiv 1 \pmod 2$, so in fact $a(x)$ and $b(x)$ are both odd. We get $\nu_2(c_4) = 4, \nu_2(c_6) = 6, \nu_2(\Delta) \geq 13$. Using [Pap, Proposition 4] we get that our model of E is not minimal at 2. So for a minimal model we have $\nu_2(c_4) = 0, \nu_2(c_6) = 0, \nu_2(\Delta) \geq 1$, hence $\nu_2(N) = 1$ and $\nu_2(\Delta_{\min}) = \nu_2(\Delta/2^{12})$.

We have $3|a(x) \Leftrightarrow 3|b(x) \Leftrightarrow x \equiv 1 \pmod 3$, but if $x \equiv 1 \pmod 3$, then $f(x) \equiv 3 \pmod 9$, which is impossible. We arrive at $\nu_3(c_4) = 2, \nu_3(c_6) = 3$. If $3|f(x)$, then $\nu_3(\Delta) \geq 7$ and we immediately get $\nu_3(N) = 2$. If $3 \nmid f(x)$, then $\nu_3(\Delta) = 3$ and together with 'condition P_2' from [Pap, p. 123], we also get $\nu_3(N) = 2$.

Furthermore, the only primes dividing $\mathrm{Res}_x(c_4, \Delta)$ are $2, 3, 37$ and we conclude

$$\begin{aligned} \Delta_{\min} &= 2^{-12}\Delta, \\ N &= 2 \cdot 3^2 \cdot 37 \,\mathrm{rad}_{\{2,3,37\}}(f(x)). \end{aligned}$$

Appendix B

Magma programs

In this appendix we give the implementations in Magma of our algorithm to solve (4.1). Only `function integritycheck` and `function poltosols` need to be called by the user, all other functions (and procedure) are only needed because they are called (possibly indirectly) by the 2 user functions. Sometimes the symbols used in the programs are different than those used in the main text. We especially mention that instead of writing $ax^2 + by^3 = cz^5$ (in the programs and their descriptions) we will use the notation $Aa^2 + Bb^3 = Cc^5$. For the rest we will use in the descriptions mainly the notation from the main text without introducing the notation again.

B.1 The algorithms

We have the following global objects, needed by several functions.

```
QQ:=RationalField(); R1<c1,c2,c3,c4>:=PolynomialRing(QQ,4);
R2<x,y>:=PolynomialRing(R1,2); P2<X,Y,Z>:=ProjectiveSpace(QQ,2);
Z2<s,t>:=PolynomialRing(Integers(),2);
Z1<z>:=PolynomialRing(Integers()); M0:=MatrixRing(Integers(),2)!1;
```

B.1.1 Checking for relevant polynomials

The following function calculates $\mathrm{c_p}(\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d})$.

```
function HasseMinkowski(a,b,c,d,p)
  return HilbertSymbol(a,b,p)*HilbertSymbol(a,c,p)*
         HilbertSymbol(a,d,p)*HilbertSymbol(b,c,p)*
         HilbertSymbol(b,d,p)*HilbertSymbol(c,d,p);
end function;
```

The following function outputs `true` if $F(t) := t^5+\mathtt{a4}\cdot t^4+\mathtt{a3}\cdot t^3+\mathtt{a2}\cdot t^2+\mathtt{a1}\cdot t+\mathtt{a0}$ is equivalent to f_j for some $j \in \mathbb{Q} - \{0, 1728\}$ and otherwise outputs `false`. `SbadOdd` must consist of the odd primes ramifying in the splitting field of $F(t)$ (no integrity checking on `SbadOdd` is done).

```
function integritycheck(a0,a1,a2,a3,a4,SbadOdd);
  integrity:=true;
  PrimeIndex:=1;
  di:=Discriminant(z^5+a4*z^4+a3*z^3+a2*z^2+a1*z+a0);
  if di eq 0 or not IsSquare(5*di) then
    integrity:=false;
  end if;
  c0:=1/5*(a4*c1+2*a3*c2-a4^2*c2+3*a2*c3-3*a3*a4*c3+a4^3*c3+
           4*a1*c4-2*a3^2*c4-4*a2*a4*c4+4*a3*a4^2*c4-a4^4*c4);
  Res:=UnivariatePolynomial(
         -Resultant(x^5+a4*x^4+a3*x^3+a2*x^2+a1*x+a0,
                    c0+c1*x+c2*x^2+c3*x^3+c4*x^4-y,x));
  QF:=Coefficient(Res,3);
  g,T:=DiagonalForm(QF);
  a:=QQ!Coefficient(g,c1,2);
  b:=QQ!Coefficient(g,c2,2);
  c:=QQ!Coefficient(g,c3,2);
  d:=QQ!Coefficient(g,c4,2);
  if HasseMinkowski(a,b,c,d,2) ne -1 then
    integrity:=false;
  end if;
  while integrity and PrimeIndex le #SbadOdd do
    if HasseMinkowski(a,b,c,d,SbadOdd[PrimeIndex]) ne 1 then
      integrity:=false;
    end if;
    PrimeIndex:=PrimeIndex+1;
  end while;
  return integrity;
end function;
```

B.1.2 From a polynomial to 2 quotient parameterizations

The following function outputs two quotient parameterizations `J1`, `J2` induced by the polynomial $t^5 + \mathtt{a4} \cdot t^4 + \mathtt{a3} \cdot t^3 + \mathtt{a2} \cdot t^2 + \mathtt{a1} \cdot t + \mathtt{a0}$.

```
function param(a0,a1,a2,a3,a4)
  c0:=1/5*(a4*c1+2*a3*c2-a4^2*c2+3*a2*c3-3*a3*a4*c3+a4^3*c3+
           4*a1*c4-2*a3^2*c4-4*a2*a4*c4+4*a3*a4^2*c4-a4^4*c4);
  Res:=UnivariatePolynomial(
         -Resultant(x^5+a4*x^4+a3*x^3+a2*x^2+a1*x+a0,
                    c0+c1*x+c2*x^2+c3*x^3+c4*x^4-y,x));
  QF:=Coefficient(Res,3);
  g,T:=DiagonalForm(QF);
  a:=QQ!Coefficient(g,c1,2);
  b:=QQ!Coefficient(g,c2,2);
  c:=QQ!Coefficient(g,c3,2);
  d:=QQ!Coefficient(g,c4,2);
```

```
  iss,k:=IsSquare(d/(a*b*c));
  C:=Conic(P2,a*X^2+b*Y^2+c*Z^2);
  Pt:=RationalPoint(C);
  X0:=Pt[1];
  Y0:=Pt[2];
  Z0:=Pt[3];
  if X0 ne 0 then
    S:=Matrix(QQ,4,4,
         [X0/2,Y0/2,Z0/2,0,
          1/(2*a*X0),-Y0/(2*a*X0^2),-Z0/(2*a*X0^2),0,
          0,-Z0/(4*a*b*X0),Y0/(4*a*c*X0),-1/(4*a*b*c*k),
          0,-c*Z0/X0,b*Y0/X0,1/k]);
  else
    S:=Matrix(QQ,4,4,
         [X0/2,Y0/2,Z0/2,0,
          -X0/(2*b*Y0^2),1/(2*b*Y0),-Z0/(2*b*Y0^2),0,
          -Z0/(4*a*b*Y0),0,X0/(4*b*c*Y0),-1/(4*a*b*c*k),
          -c*Z0/Y0,0,a*X0/Y0,1/k]);
  end if;
/* The role of c1,c2,c3,c4 in the definition of v below will be
different than before. Instead of coefficients in a Tschirnhausen
transformation they represent parameters on P^1 X P^1. */
  v:=Vector(4,[c1*c3,c2*c4,c2*c3,c1*c4])*(MatrixRing(R1,4)!(S*T));
  a:=Evaluate(Coefficient(Res,2),[v[1],v[2],v[3],v[4]])/5;
  b:=Evaluate(Coefficient(Res,1),[v[1],v[2],v[3],v[4]])/5;
  c:=Evaluate(Coefficient(Res,0),[v[1],v[2],v[3],v[4]]);
  f:=x^2*(a^4+a*b*c-b^3)-x*(11*a^3*b-a*c^2+2*b^2*c)+
     64*a^2*b^2-27*a^3*c-b*c^2;
  Fac:=Factorization(UnivariatePolynomial(f));
  lambda1:=-Coefficient(Fac[1,1],0)/Coefficient(Fac[1,1],1);
  lambda2:=-Coefficient(Fac[2,1],0)/Coefficient(Fac[2,1],1);
  J1:=(a*lambda1^2-3*b*lambda1-3*c)^3/
      (a^2*(lambda1*a*c-lambda1*b^2-b*c));
  J2:=(a*lambda2^2-3*b*lambda2-3*c)^3/
      (a^2*(lambda2*a*c-lambda2*b^2-b*c));
  return J1,J2;
end function;
```

B.1.3 From a quotient parameterization to one integral parameterization

The 4 functions in this section are really straightforward and only included for the sake of completeness.

The following function calculates binary forms $\mathtt{NJ}, \mathtt{DJ} \in \mathbb{Z}[s,t]$ such that $\mathtt{J} = \mathtt{NJ}/\mathtt{DJ}$.

```
function NDJ(J);
```

```
  CfsN:=Coefficients(Numerator(J));
  CfsD:=Coefficients(Denominator(J));
  DenCfsN:= [ IntegerRing() |
              Denominator(CfsN[i]) : i in [ 1..#CfsN ] ];
  DenCfsD:= [ IntegerRing() |
              Denominator(CfsD[i]) : i in [ 1..#CfsD ] ];
  lcm:=LCM(LCM(DenCfsN),LCM(DenCfsD));
  NJ:=Evaluate(lcm*Numerator(J),[s,t,s,t]);
  DJ:=Evaluate(lcm*Denominator(J),[s,t,s,t]);
  return NJ,DJ;
end function;
```

A Chinese remainder theorem, convenient for us.

```
function Chinese(i,j,k);
  n:=k;
  while n mod 3 ne j mod 3 or n mod 2 ne i mod 2 do
    n:=n+5;
  end while;
  while n lt i or n lt j do
    n:=n+30;
  end while;
  return(n);
end function;
```

If the element `fn` (in some ring) is of the form ux, where u is a unit and x an `n`-th power, the following function returns u times an `n`-th root of x. (The Magma function `IsPower` does not always work properly.)

```
function nthroot(fn,n);
  Fac,f:=Factorization(fn);
  for k:= 1 to #Fac do
    f:=f*Fac[k,1]^(ExactQuotient(Fac[k,2],n));
  end for;
  return f;
end function;
```

Given binary forms $\mathtt{b3}, \mathtt{c5} \in \mathbb{Z}[s,t]$ (such that $\mathtt{b3}/\mathtt{c5}$ is a quotient parameterization) and $\mathtt{A}, \mathtt{B}, \mathtt{C} \in \mathbb{Z} - \{0\}$, the function outputs binary forms $\mathtt{a}, \mathtt{b}, \mathtt{c} \in \mathbb{Z}[s,t]$ such that $\mathtt{A} \cdot \mathtt{a}^2 + \mathtt{B} \cdot \mathtt{b}^3 = \mathtt{C} \cdot \mathtt{c}^5$ and $\mathtt{b3}/\mathtt{c5} = 1728 \cdot \mathtt{B} \cdot \mathtt{b}^3/(\mathtt{C} \cdot \mathtt{c}^5)$.

```
function abc(b3,c5,A,B,C);
  c5:=1728*c5;
  a2:=c5-b3;
  Ca2:=Content(a2);
  Cb3:=Content(b3);
  Cc5:=Content(c5);
  F:=Factorization(Ca2*Cb3*Cc5*A*B*C);
```

```
  mult:=Sign(LeadingCoefficient(a2));
  divi:=Sign(A);
  for i:=1 to #F do
    p:=F[i,1];
    n:=Chinese(Valuation(A,p)-Valuation(Ca2,p),
               Valuation(B,p)-Valuation(Cb3,p),
               Valuation(C,p)-Valuation(Cc5,p));
   if n ge 0 then
     mult:=mult*p^n;
   else
     divi:=divi*p^(-n);
   end if;
  end for;
  a2:=ExactQuotient(mult*a2,divi*A);
  b3:=ExactQuotient(mult*b3,divi*B);
  c5:=ExactQuotient(mult*c5,divi*C);
  a:=nthroot(a2,2);
  b:=nthroot(b3,3);
  c:=nthroot(c5,5);
  return([a,b,c]);
end function;
```

B.1.4 From one integral parameterization to all relevant integral parameterizations

A convenient matrix function.

```
function Mat(k,p);
  if k eq p then
    return Matrix(Integers(),2,2,[p,0,0,1]);
  else
    return Matrix(Integers(),2,2,[1,0,k,p]);
  end if;
end function;
```

Given three binary forms $\mathtt{a}, \mathtt{b}, \mathtt{c} \in \mathbb{Z}[s,t]$ the following function outputs `true` if there exists $s,t \in \mathbb{Z}$ such that $\mathtt{p} \nmid \gcd(\mathtt{a}(s,t), \mathtt{b}(s,t), \mathtt{c}(s,t))$, otherwise outputs `false`.

```
function HasCoprimeSpecialization(p,a,b,c);
  HasCS:=false;
  gcd:=GCD([Evaluate(a,[1,0]),
            Evaluate(b,[1,0]),
            Evaluate(c,[1,0])]);
  if not IsDivisibleBy(gcd,p) then
    HasCS:=true;
  end if;
```

```
  k:=0;
  while (not HasCS) and (k lt p) do
    gcd:=GCD([Evaluate(a,[k,1]),
              Evaluate(b,[k,1]),
              Evaluate(c,[k,1])]);
    if not IsDivisibleBy(gcd,p) then
      HasCS:=true;
    end if;
    k:=k+1;
  end while;
  return HasCS;
end function;
```

Given a prime p, a pair $((\mathtt{a},\mathtt{b},\mathtt{c}),\mathtt{M}) \in S_i$, $\mathtt{e} = C_{\mathtt{p}}(\mathtt{a},\mathtt{b},\mathtt{c})$ and a subset of P, list. This procedure, working w.r.t. the prime p of course, adds to list all integral parameterizations in P coming (i.e. by dividing out a power of p) from $((a',b',c'),M') \in S_j$ for some $j \geq i$ and with $M' = \mathtt{M}\prod_{j>i} M_{[a_j:b_j]}$ for some $[a_j : b_j] \in \mathbb{P}^1(\mathbb{F}_{\mathtt{p}})$, with the exception that a parameterization is not added if all $\mathbb{Z}_{(\mathtt{p})}$ specializations have p dividing the gcd. The procedure works recursively and the natural start is with M the identity and list empty.

```
procedure integralparam(p,a,b,c,M,e,~list);
  if IsDivisibleBy(e,60) then
    potentialparam:=true;
  else
    potentialparam:=false;
  end if;
  for k:=0 to p do
    M1:=M*Mat(k,p);
    m11:=Mat(k,p)[1,1];
    m12:=Mat(k,p)[1,2];
    m21:=Mat(k,p)[2,1];
    m22:=Mat(k,p)[2,2];
    if MatrixRing(FiniteField(p),2)!M1 ne 0 then
      a1:=Evaluate(a,[m11*s+m12*t,m21*s+m22*t]);
      b1:=Evaluate(b,[m11*s+m12*t,m21*s+m22*t]);
      c1:=Evaluate(c,[m11*s+m12*t,m21*s+m22*t]);
      e1:=Min([2*Valuation(Content(a1),p),
               3*Valuation(Content(b1),p),
               5*Valuation(Content(c1),p)]);
      if e1 gt e then
        integralparam(p,a1,b1,c1,M1,e1,~list);
        if IsDivisibleBy(e1,60) then
          potentialparam:=false;
        end if;
      end if;
    end if;
```

```
  end for;
  if potentialparam then
    a:=ExactQuotient(a,p^(e div 2));
    b:=ExactQuotient(b,p^(e div 3));
    c:=ExactQuotient(c,p^(e div 5));
      if HasCoprimeSpecialization(p,a,b,c) then
        list:=Append(list,[a,b,c]);
      end if;
  end if;
end procedure;
```

The following function returns a list with integral parameterizations such that all solutions obtained from the integral parameterizations $(\mathtt{p}^{15}\mathtt{a}, \mathtt{p}^{10}\mathtt{b}, \mathtt{p}^{6}\mathtt{b})$ and $(\mathtt{a}, \mathtt{b}, \mathtt{c})$ by specializing at rational values, can be obtained by specializing at values integral at p.

```
function localsols(p,a,b,c);
  e:=Min([2*Valuation(Content(a),p),
          3*Valuation(Content(b),p),
          5*Valuation(Content(c),p)]);
  list1:=[];
  integralparam(p,a,b,c,M0,e,~list1);
  list2:=[];
  integralparam(p,p^15*a,p^10*b,p^6*c,M0,e+30,~list2);
   return list1 cat list2;
end function;
```

The simplest explanation of the following short function is probably the code itself.

```
function bifurcation(list,i,F);
  p:=F[i,1];
  listnew:=[];
  for j:=1 to #list do
    listnew:=listnew cat
             localsols(p,list[j,1],list[j,2],list[j,3]);
  end for;
  if i lt #F then
    return bifurcation(listnew,i+1,F);
  else
    return listnew;
  end if;
end function;
```

B.1.5 From a polynomial to all integral parameterizations

Given binary forms $\mathtt{b3\_1}, \mathtt{c5\_1}, \mathtt{b3\_2}, \mathtt{c5\_2} \in \mathbb{Z}[s,t]$, such that $\mathtt{b3\_1}/\mathtt{c5\_1}$ and $\mathtt{b3\_2}/\mathtt{c5\_2}$ are quotient parameterizations, the function outputs `true` if these parameterizations are $\mathbb{Q}$-twists of each other, otherwise the function outputs `false`.

```
function Twists(b3_1,c5_1,b3_2,c5_2);
  twist:=false;
  b3:=0;
  c5:=0;
  k:=0;
  while b3 eq 0 or c5 eq 0 or b3 eq 1728*c5 do
    b3:=Evaluate(b3_1,[1,k]);
    c5:=Evaluate(c5_1,[1,k]);
    k:=k+1;
  end while;
  if
  HasRoot(PolynomialRing(Rationals())!
          UnivariatePolynomial(Evaluate(b3_2*c5-c5_2*b3,[s,1])))
  or
  HasRoot(PolynomialRing(Rationals())!
          UnivariatePolynomial(Evaluate(b3_2*c5-c5_2*b3,[1,t])))
  then
    twist:=true;
  end if;
  return twist;
end function;
```

Given a polynomial $F(t) := t^5 + \mathtt{a4} \cdot t^4 + \mathtt{a3} \cdot t^3 + \mathtt{a2} \cdot t^2 + \mathtt{a1} \cdot t + \mathtt{a0}$ and $\mathtt{A}, \mathtt{B}, \mathtt{C} \in \mathbb{Z} - \{0\}$, the following function returns a finite list of integral parameterizations to $\mathtt{A}x^2 + \mathtt{B}y^3 = \mathtt{C}z^5$ such that all solutions related to $F(t)$ can be obtained by integer specialization of one of these parameterizations.

```
function poltosols(a0,a1,a2,a3,a4,A,B,C);
  J1,J2:=param(a0,a1,a2,a3,a4);
  b3_1,c5_1:=NDJ(J1);
  list:=abc(b3_1,c5_1,A,B,C);
  a:=list[1]; b:=list[2]; c:=list[3];
  F:=Factorization(Content(Resultant(b,c,t)));
  list1:=bifurcation([[a,b,c]],1,F);
  b3_2,c5_2:=NDJ(J2);
  if not Twists(b3_1,c5_1,b3_2,c5_2) then
    list:=abc(b3_2,c5_2,A,B,C);
    a:=list[1];
    b:=list[2];
    c:=list[3];
    F:=Factorization(Content(Resultant(b,c,t)));
    list2:=bifurcation([[a,b,c]],1,F);
  else
    list2:=[];
  end if;
  return list1 cat list2;
end function;
```

Bibliography

[Bec] Sybilla Beckmann, *On extensions of number fields obtained by specializing branched coverings*, J. Reine Angew. Math. **419** (1991), 27–53.

[BD] Michael A. Bennett and Sander R. Dahmen, *On the Diophantine equation* $x^3 + Dy^3 = z^l$, in progress.

[BS] Michael A. Bennett and Chris M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.

[BVY] Michael A. Bennett, Vinayak Vatsal and Soroosh Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compositio Math. **140** (2004), 1399–1416.

[Beu1] Frits Beukers, *The diophantine equation* $Ax^p + By^q = Cz^r$, Duke Math J. **91** (1998), 61–88.

[Beu2] ——, *The generalized Fermat equation*, Lecture notes, January 20, 2006. See `http://www.math.uu.nl/people/beukers/Fermatlectures.pdf`

[Beu3] ——, *Gauss' hypergeometric function*, Arithmetic and geometry around hypergeometric functions, 23–42, Progr. Math., 260, Birkhäuser, Basel, 2007.

[BT] Frits Beukers and Robert Tijdeman, *On the multiplicities of binary complex recurrences*, Compositio Math. **51** (1984), no. 2, 193–213.

[BK] Bryan J. Birch and Willem Kuyk (editors), *Modular Functions of One Variable IV*, Lecture notes in Mathematics 467, Berlin-Heidelberg-New York, Springer, 1975.

[BCDT] Christophe Breuil, Brian Conrad, Fred Diamond and Richard Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** No. 4 (2001),843–939.

[Bru] Nils Bruin, *On powers as sums of two cubes*, in Algorithmic number theory (Leiden, 2000), 169–184, Lecture Notes in Comput. Sci., 1838, Springer, Verlag, 2000.

[BMS1] Yann Bugeaud, Maurice Mignotte and Samir Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) **163** (2006), no. 3, 969–1018.

[BMS2] ——, *Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation*, Compos. Math. **142** (2006), no. 1, 31–62.

[BMS3] ——, *A multi-Frey approach to some multi-parameter families of Diophantine equations*, to appear in Canad. J. Math.

[Cas] John W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, 13. Academic Press, Inc.[Harcourt Brace Jovanovich, Publishers], London-New York, 1978. xvi+413 pp. ISBN: 0-12-163260-1.

[Che] Imin Chen, *On the equation* $s^2 + y^{2p} = \alpha^3$, Math. Comp. **77** (2008), no. 262, 1223–1227.

[Coh1] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin Heidelberg, 1993.

[Coh2] ——, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, 193. Springer-Verlag, New York, 2000. xvi+578 pp. ISBN: 0-387-98727-4.

[CP] Pierre E. Conner and Robert Perlis, *A survey of trace forms of algebraic number fields*, Series in Pure Mathematics, 2. World Scientific Publishing Co., Singapore, 1984. ix+316 pp. ISBN: 9971-966-04-2; 9971-966-05-0.

[Cre1] John E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **4** (2001), 73 (electronic).

[Cre2] ——, *Elliptic Curve Data*, `http://modular.math.washington.edu/cremona/INDEX.html`

[CR] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Pure and applied mathematics Vol. XI, Interscience Publishers, New York-London, 1962.

[Dar] Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449.

[DG] Henri Darmon and Andrew Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), no. 6, 513–543.

[DM] Henri Darmon and Loïc Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.

[Del] Pierre Deligne, *Formes modulaires et répresentations l-adiques*, Séminaire Bourbaki, no. 355, Lecture Notes in Math. **179**, Springer-Verlag, Berlin Heidelberg New York, 1971, pp. 139–172.

[Dia] Fred Diamond, *The refined conjecture of Serre*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 22–37, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

[DI] Fred Diamond and John Im, *Modular forms and modular curves*, in Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), 39–133, CMS Conf. Proc., 17, Amer. Math. Soc., Providence, RI, 1995.

[DK] Fred Diamond and Kenneth Kramer, *Modularity of a familiy of elliptic curves*, Math. Res. Lett. **2** (1995), no. 3, 299–304.

[DS] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate texts in mathematics 228, Springer-Verlag, New York, 2005.

[Edi] Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594.

[Edw] Johnny Edwards, *A complete solution to* $X^2+Y^3+Z^5=0$, J. reine angew. Math. **571** (2004), 213–236.

[Ell] Jordan S. Ellenberg, *Galois representations attached to* $\mathbb{Q}$*-curves and the generalized Fermat equation* $A^4+B^2=C^p$, Amer. J. Math. **126** (2004), no. 4, 763–787.

[Fre] Gerhard Frey, *Links between stable elliptic curves and certain Diophantine equations*, Ann. Univ. Sarav. Ser. Math. **1** (1986), no. 1, iv+40 pp.

[HK] Emmanuel Halberstadt and Alain Kraus, *Sur les modules de torsion des courbes elliptiques*, Math. Ann. **10** (1998), 47–54.

[JR] John W. Jones and David P. Roberts, *Tables of Number Fields with Prescribed Ramification*, `http://math.la.asu.edu/~jj/numberfields/`

[Kat] Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. math. **62** (1981), 481–502.

[Kie] Ludwig Kiepert, *Auflösung der Gleichungen Fünften Grades*, J. für Math. **87** (1878), 114–133.

[Kin] R. Bruce King, *Beyond the quartic equation*, Birkhäuser Boston, Inc., Boston, MA, 1996. viii+149 pp. ISBN: 0-8176-3776-1.

[Kle] Felix Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Reprint of the 1884 original. Edited, with an introduction and commentary by Peter Slodowy. Birkhuser Verlag, Basel; B. G. Teubner, Stuttgart, 1993. xxviii+viii+343 pp. ISBN: 3-7643-2454-6.

[Kra1] Alain Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69**:4 (1990), 353–385.

[Kra2] ——, *Détermination du poids et du conducteur associé aux représentations des points de p-torsion d'une courbe elliptique*, Dissertationes Math. **344** (1997), 39 pp.

[Kra3] ——, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), no. 6, 1139–1161.

[Kra4] ——, *Sur l'équation* $a^3 + b^3 = c^p$, Experiment. Math. **7** (1998), no. 1, 1–13.

[Kra5] ——, *On the Equation* $x^p + y^q = z^r$*: A Survey*, The Ramanujan Journal **3** (1999), 315–333.

[KO] Alain Kraus and Joseph Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293**:2 (1992), 259–275.

[LZ] Sergei K. Lando and Alexander K. Zvonkin, *Graphs on surfaces and their applications*, With an appendix by Don B. Zagier, Encyclopaedia of Mathematical Sciences, 141, Low-Dimensional Topology, II, Springer-Verlag, Berlin, 2004. xvi+455 pp. ISBN: 3-540-00203-0.

[Lig] Gérard Ligozat, *Courbes Modulaires de genre 1*, Bull. Soc. Math. France, Mémoire **43** (1975), 1–80.

[Mar] Greg Martin, *Dimensions of the space of cusp forms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$, J. Number Theory **112** (2005), no. 2, 298–331.

[Maz1] Barry Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33–186.

[Maz2] ——, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[MV] Barry Mazur and Jacques Vélu, *Courbes de Weil de conducteur* 26, C. R. Acad. Sci. Paris Sér. A-B **275** (1972), A743–A745.

[Mer1] Loïc Merel, *Arithmetic of elliptic curves and diophantine equations*, J. Théor. Nombres Bordeaux **11** (1999), 173–200.

[Mer2] ——, *Normalizers of split Cartan subgroups and supersingular elliptic curves*, Diophantine geometry, 237–255, CRM Series, 4, Ed. Norm., Pisa, 2007.

[Mom] Fumiyuki Momose, *Rational points on the modular curves* $X_{\mathrm{split}}(p)$, Compositio Math. **52** (1984), no. 1, 115–137.

[MN] Jesús Montes and Enric Nart, *On a theorem of Ore*, J. Algebra **146** (1992), no. 2, 318–334.

[O'M] O. Timothy O'Meara, *Introduction to quadratic forms*, Die Grundlehren der mathematischen Wissenschaften, Bd. 117 Academic Press, Inc., Publishers, New York; Springer-Verlag, Berlin-Göttingen-Heidelberg 1963 xi+342 pp.

[Ore] Öystein Ore, *Newtonische Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), no. 1, 84–117.

[Pap] Ioannis Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 and 3*, J. Number Theory **44**:2 (1993), 119–152.

[Par] Pierre Parent, *Triviality of* $X_{\mathrm{split}}(N)(\mathbb{Q})$ *for certain congruence classes of* N, C. R. Math. Acad. Sci. Paris **336** (2003), no. 5, 377–380.

[PSS] Bjorn Poonen, Edward F. Schaeffer and Michael Stoll, *Twists of* $X(7)$ *and primitive solutions to* $x^2+y^3 = z^7$, Duke Math. J. **137** (2007), no. 1, 103–158.

[Reb] Marusia Rebolledo, *Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires*, Pacific J. Math. **234** (2008), no. 1, 167–184.

[Rib1] Kenneth A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

[Rib2] ——, *Report on mod l representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, in Motives, Proc. Symp. Pure Math. **55**:2 (1994), 639–676.

[RS1] Karl Rubin and Alice Silverberg, *Families of elliptic curves with constant mod p representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 148–161, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

[RS2] , ——, *Mod* 2 *representations of elliptic curves*, Proc. Amer. Math. Soc. **129** (2001), no. 1, 53–57.

[SchTij] Andrzej Schinzel and Robert Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith. **31** (1976), no. 2, 199–204.

[Ser1] Jean-Pierre Serre, *Propriété galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[Ser2] ——, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

[ST] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. Math. **88** (1968), 492–517.

[Sik] Samir Siksek, *The modular approach to Diophantine equations*, tutorial, February 15, 2007.

[Sil] Alice Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), 447–461, Springer, New York, 1997.

[Sil1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin, New York, 1986.

[Sil2] ——, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 151, Springer-Verlag, Berlin, New York, 1994.

[Tat] John Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in *Modular functions of one variable IV*, Lect. Notes in Math. 476, B. J. Birch and W. Kuyk, eds., Springer-Verlag, Berlin, 1975, 33–52.

[Tib] Steve Thiboutot, *Courbes elliptiques, représentations galoisiennes, et l'équation* $x^2 + y^3 = z^5$, Master's thesis, McGill Univ., Montreal 1996.

[Tau] Olga Taussky, *The discriminant matrices of an algebraic number field*, J. London Math. Soc. **43** (1968), 152–154.

[TW] Richard Taylor and Andrew Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), 553–572.

[Wil] Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.

Samenvatting

Een Diophantische vergelijking is een bepaald soort vergelijking (namelijk een polynoomvergelijking met gehele coëfficiënten) waarin de onbekenden gehele getallen moeten zijn. Diophantische vergelijkingen zijn vernoemd naar de Griekse wiskundige Diophantus van Alexandrië, die waarschijnlijk omstreeks de derde eeuw na Christus leefde. Voor elk geheel getal $n \geq 2$, is de vergelijking

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

waarin de onbekenden x, y en z gehele getallen moeten zijn, een voorbeeld van een interessante Diophantische vergelijking. Voor elke n kunnen we oplossingen vinden met $xyz = 0$. Voor $n = 2$ zijn er ook oplossingen met $xyz \neq 0$, zoals $(x, y, z) = (3, 4, 5), (x, y, z) = (5, 12, 13)$ of $(x, y, z) = (1855, 792, 2017)$. De Franse wiskundige Pierre de Fermat vermoedde rond 1638 dat voor $n \geq 3$ bovenstaande Diophantische vergelijking geen enkele oplossing heeft met $xyz \neq 0$, dit vermoeden is later bekend komen te staan als de laatste stelling van Fermat. In de kantlijn van een vertaling van het werk van Diophantus schreef Fermat dat hij een wonderbaarlijk bewijs voor deze stelling gevonden had, maar dat de kantlijn te smal was om het bewijs te bevatten. Bekend is dat Fermat voor het geval $n = 4$ een prachtig bewijs heeft geleverd, maar hoogstwaarschijnlijk heeft hij geen correct bewijs gevonden voor het algemene geval. Vele wiskundigen hebben nadien getracht een bewijs te vinden voor de laatste stelling van Fermat. Voortbouwend op het werk van vele anderen werd uiteindelijk in 1994 een bewijs gevonden door de Britse wiskundige Andrew Wiles. De methoden die hiervoor ontwikkeld zijn, zogenaamde modulaire methoden, zijn zeer krachtig en kunnen ook licht werpen op andere wiskundige vraagstukken.

In dit proefschrift zijn zowel verscheidene klassieke wiskundige methoden als moderne wiskundige methoden, namelijk modulaire methoden, gebruikt om zogenaamde gegeneraliseerde Fermat vergelijkingen op te lossen. Dit zijn Diophantische vergelijkingen in de onbekenden x, y en z van de vorm

$$ax^p + by^q = cz^r,$$

waarbij de coëfficiënten a, b en c gegeven gehele getallen ongelijk aan 0 zijn en de exponenten p, q en r gegeven gehele getallen groter dan 1 zijn. Het meest interessant zijn oplossingen waarvoor $xyz \neq 0$ en $\gcd(x, y, z) = 1$ (ggd staat voor grootste gemeenschappelijke deler), zulke oplossingen noemen we primitieve oplossingen.

In onderstaande tabel zijn de belangrijkste gegeneraliseerde Fermat vergelijkingen weergegeven waarvoor in dit proefschrift alle primitieve oplossingen bepaald zijn, samen met een referentie naar waar ze behandeld worden.

vergelijking	zie paragraaf
$x^2 + y^{10} = z^3$	3.3.1
$x^2 + y^{62} = z^3$	3.3.1
$x^3 + y^3 = z^5$,	3.3.2
$x^2 + y^3 = z^5$	4.4.1 en 5.4
$16x^2 + 9y^3 = z^5$	4.4.2
$16x^2 + 3y^3 = z^5$	4.4.2

We zullen nu de vergelijkingen uit de tabel kort bespreken. Voor alle oneven priemgetallen $l < 10^7$, behalve $l = 5$ en $l = 31$, was het bekend dat de vergelijking $x^2 + y^{2l} = z^3$ geen primitieve oplossingen heeft. Dat er ook voor $l = 5$ en $l = 31$ geen primitieve oplossingen zijn, is in dit proefschrift aangetoond. Voor alle priemgetallen l met $7 \leq l < 10000$, was het bekend dat met modulaire methoden aangetoond kan worden dat de vergelijking $x^3+y^3 = z^l$ geen primitieve oplossingen heeft (eigenlijk waren de gevallen $l = 7, l = 11$ en $l = 13$ nog niet eerder uitgewerkt, maar hier zijn geen nieuwe ideeën voor nodig). Voor $l = 5$ was het al wel bekend dat $x^3 + y^3 = z^l$ geen primitieve oplossingen heeft, maar in dit proefschrift is dit voor het eerst aangetoond door middel van modulaire methoden. De vergelijking $x^2+y^3 = z^5$ was ook al eerder opgelost, er zijn oneindig veel primitieve oplossingen en er zijn formules bekend die deze oplossingen beschrijven. In dit proefschrift is een nieuwe aanpak ontwikkeld voor deze vergelijking, met deze aanpak konden ook de laatste twee vergelijkingen uit de tabel worden opgelost. Een lange tijd hebben wiskundigen zich afgevraagd of er gehele getallen a, b en c bestaan met $abc \neq 0$ en $\gcd(a, b) = \gcd(b, c) = \gcd(c, a) = 1$ waarvoor de vergelijking $ax^2 + by^3 = cz^5$ geen primitieve oplossingen heeft. Dat zulke getallen bestaan is in dit proefschrift eindelijk aangetoond door te bewijzen dat de vergelijkingen $16x^2 + 9y^3 = z^5$ en $16x^2 + 3y^3 = z^5$ geen primitieve oplossingen hebben.

Behalve gegeneraliseerde Fermat vergelijkingen zijn er met behulp van modulaire methoden ook nog enige andere interessante Diophantische vergelijkingen opgelost in dit proefschrift. Zo is bijvoorbeeld aangetoond dat voor $l = 5$ en voor elk priemgetal l met $13 \leq l < 10^7$ de Diophantische vergelijking

$$x^2 - x - 2 = y^l$$

geen oplossingen heeft.

Er zijn nu veel resultaten genoemd, maar er is nog niet echt diep ingegaan op de methoden. In deze samenvatting willen we hier enkel nog over melden dat er prachtige meetkundige structuren, zoals regelmatige betegelingen van het hyperbolische vlak, achter schuil gaan. De lezer die hier meer over wil weten, is hierbij uitgenodigd om dit proefschrift en de referenties te bestuderen.

Acknowledgements

First of all I would like to thank my Ph.D. supervisor Frits Beukers for all his support. I am very grateful for the ideas and inspiration he provided me with and for the freedom he gave me in choosing research directions.

I would like to thank the members of the reading committee, Mike Bennett, Gunther Cornelissen, Bas Edixhoven, Samir Siksek and Jaap Top, for reading my thesis and for providing me with various helpful comments.

Since we are following the canonical order of acknowledgement, I would next like to thank of course all my (former) colleagues at the Department of Mathematics for creating a pleasant and interesting working environment. In particular I would like to thank the number theorists Oliver, Jeroen and Johnny, the geometers Pieter, Rogier and Alex, my (former) roommates Erik, Tammo Jan, Arthur and Jaap, and also Vincent, Charlene and Bas.

Many thanks to all my friends and family!! I would especially like to thank Annelie for not complaining too much during the write-up phase of my thesis, but above all, I would like to thank Annelie for all her love and support.

Curriculum vitae

Sander Dahmen was born on the 12th of January 1979 in Amersfoort, The Netherlands, where he also grew up and attended primary and secondary education. In 1997 he started to study mathematics and physics at Utrecht University and in 2003 he obtained his master's degree in both disciplines (cum laude). After a seven month intermezzo of following ski instructor courses, obtaining the Austrian *anwärter* ski instructor diploma and working as a ski instructor in Kitzbühel, Austria, Sander returned to mathematics. From 2004 to 2008 he worked as a Ph.D. student in number theory at Utrecht University. The research on Diophantine equations carried out in this period under the guidance of Frits Beukers has resulted in this thesis.