Computing elliptic curves over $\mathbb{Q}$ via Thue-Mahler equations and related problems

by

Adela Gherga

B.Sc. Mathematics, McMaster University, 2010

M.Sc. Mathematics, McMaster University, 2012

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Doctor of Philosophy

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES
(Mathematics)

The University of British Columbia
(Vancouver)

July 2019

Abstract

We present a practical and efficient algorithm for solving an arbitrary Thue-Mahler equation. This algorithm uses explicit height bounds with refined sieves, combining Diophantine approximation techniques of Tzanakis-de Weger with new geometric ideas. We begin by using methods of algebraic number theory to reduce the problem of solving the Thue-Mahler equation to the problem of solving a finite collection of related Diophantine equations. In the first part of this thesis, we establish the key results which allow us to drastically reduce the number of such Diophantine equations and subsequently reduce the running time.

In the second part of this thesis, we show that if $n \geq 3$ is a fixed integer, then there exists an effectively computable constant $c(n)$ such that if x, y and m are integers satisfying

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}, \ \ y > x > 1, \ m > n,$$

with $\gcd(m-1, n-1) > 1$, then $\max\{x, y, m\} < c(n)$. In case $n \in \{3, 4, 5\}$, we solve the equation completely, subject to this non-coprimality condition. In case $n = 5$, our resulting computations require a variety of innovations for solving Ramanujan-Nagell equations of the shape $f(x) = y^n$, where $f(x)$ is a given polynomial with integer coefficients (and degree at least two), and y is a fixed integer. In particular, we modify our Thue-Mahler algorithm and specialize our refinements to the case of Ramanujan-Nagell equations, enabling us to fully resolve the $n = 5$ case.

In the third part, we discuss an algorithm for finding all elliptic curves over $\mathbb{Q}$

with a given conductor. Though based on classical ideas derived from reducing the problem to one of solving associated Thue-Mahler equations, our approach, in many cases at least, appears to be reasonably efficient computationally. We provide details of the output derived from running the algorithm, concentrating on the cases of conductor p or p^2, for p prime, with comparisons to existing data.

Finally, we specialize the Thue-Mahler algorithm to degree 3, applying an analogue of Matshke-von K anel's elliptic logarithm sieve to construct a global sieve, leading to reduced search spaces. The algorithm is implemented in the Magma computer algebra system, and is part of an on-going collaborative project.

Lay Summary

Consider any collection of prime numbers $\{p_1, \ldots, p_v\}$ and any collection of integers $c, c_0, \ldots, c_n$. Our main result involves the *Thue-Mahler* equation

$$F(x, y) = c_0x^n + c_1x^{n-1}y + \cdots + c_{n-1}xy^{n-1} + c_ny^n = cp_1^{z_1} \cdots p_v^{z_v},$$

where the values x, y, and $z_1, \ldots, z_v$ are unknown. In particular, for any such equation, we know that there are only finitely many values of x, y, and $z_1, \ldots, z_n$ which satisfy it. In our work, we develop an algorithm to find all of these solutions for any given collection of primes and coefficients c_i. The solutions to these Thue-Mahler have many important mathematical applications, and we modify and refine our algorithm for use in those applications.

Contents

Acknowledgments

I am indebted to Dr. Michael A. Bennett for suggesting to me the line of research on which this thesis is based and for numerous comments and suggestions that helped me to improve this thesis.

This research was funded in part by a National Sciences and Engineering Research Council Postgraduate Scholarship.

Chapter 1

Introduction

A Diophantine equation is a polynomial equation in several variables defined over the integers. The term *Diophantine* refers to the Greek mathematician Diophantus of Alexandria, who studied such equations in the 3rd century A.D. Let $f(x_1, \ldots, x_n)$ be a polynomial with integer coefficients. We wish to study the set of solutions $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ to the equation

$$f(x_1, \ldots, x_n) = 0. \tag{1.1}$$

There are several different approaches for doing so, arising from three basic problems concerning Diophantine equations. The first such problem is to determine whether (1.1) has any solutions. Indeed, one of the most famous theorems in mathematics states that for $f(x, y, z) = x^n + y^n - z^n$, where $n \geq 3$, there are no solutions in the positive integers x, y, z. This equation is known as Fermat's Last Theorem and was proven by Wiles in 1995. Qualitative questions of this type are often studied using algebraic methods.

Suppose now that (1.1) is solvable, that is, has at least one solution. The second basic problem is to determine whether the number of solutions is finite or infinite. For example, consider the *Thue equation*,

$$f(x, y) = a, \tag{1.2}$$

where $f(x, y)$ is an integral binary form of degree $n \geq 3$ and a is a fixed nonzero rational integer. In 1909, Thue [108] proved that this equation has only finitely many solutions. This result followed from a sharpening of Liouville's inequality [64], an observation that algebraic numbers do not admit very strong approximation by rational numbers. That is, if α is a real algebraic number of degree $n \geq 2$ and p, q are integers, Liouville's observation states that

$$\left|\alpha - \frac{p}{q}\right| > \frac{c_1}{q^n}, \tag{1.3}$$

where $c_1 > 0$ is a value depending explicitly on α. The finitude of the number of solutions to (1.2) follows directly from a sharpening of (1.3) of the type

$$\left|\alpha - \frac{p}{q}\right| > \frac{\lambda(q)}{q^n}, \quad \lambda(q) \to \infty. \tag{1.4}$$

Indeed, if α is a real root of $f(x, 1)$ and $\alpha^{(i)}$, $i = 1, \ldots, n$ are its conjugates, it follows from (1.2) that

$$\prod_{i=1}^{n} \left|\alpha^{(i)} - \frac{x}{y}\right| = \frac{a}{|a_0||y|^n}$$

where a_0 is the leading coefficient of the polynomial $f(x, 1)$. If the Thue equation has integer solutions with arbitrarily large $|y|$, the product $\prod_{i=1}^{n} |\alpha^{(i)} - x/y|$ must take arbitrarily small values for solutions x, y of (1.2). As all the $\alpha^{(i)}$ are different, x/y must be correspondingly close to one of the real numbers $\alpha^{(i)}$, say α. Thus we obtain

$$\left|\alpha - \frac{x}{y}\right| < \frac{c_2}{|y|^n}$$

where c_2 depends only on a_0, n, and the conjugates $\alpha^{(i)}$ (cf. Chapter 4 of [103]). Comparison of this inequality with (1.4) shows that $|y|$ cannot be arbitrarily large, and so the number of solutions of the Thue equation is finite. Using this argument, an explicit bound can be constructed on the solutions of (1.2) provided that an effective inequality (1.4) is known. The sharpening of the Liouville inequality however, especially in effective form, proved to be very difficult.

In [108], Thue published a proof that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\frac{n}{2}+1+\varepsilon}}$$

has only finitely many solutions in integers $p, q > 0$ for all algebraic numbers α of degree $n \geq 3$ and any $\varepsilon > 0$. In essence, he obtained the inequality (1.4) with $\lambda(q) = c_3 q^{\frac{1}{2}n-1-\varepsilon}$, where $c_3 > 0$ depends on α and ε, thereby confirming that all Thue equations have only finitely many solutions (cf [103]). Unfortunately, Thue's arguments do not allow one to find the explicit dependence of c_3 on α and ε, and so the bound for the number of solutions of the Thue equation cannot be given in explicit form either. That is, Thue's proof is ineffective, meaning that it provides no means to find the solutions to (1.2).

Nonetheless, the investigation of Thue's equation and its generalizations was central to the development of the theory of Diophantine equations in the early 20th century when it was discovered that many Diophantine equations in two unknowns could be reduced to it. In particular, the thorough development and enrichment of Thue's method led Siegel [99] to his theorem on the finitude of the number of integral points on an algebraic curve of genus greater than zero. However, as Siegel's result relies on Thue's rational approximation to algebraic numbers, it too is ineffective.

Shortly following Thue's result, Goormaghtigh [45] conjectured that the only non-trivial integer solutions of the exponential Diophantine equation

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1} \tag{1.5}$$

satisfying $x > y > 1$ and $n, m > 2$ are

$$31 = \frac{2^5 - 1}{2 - 1} = \frac{5^3 - 1}{5 - 1} \quad \text{and} \quad 8191 = \frac{2^{13} - 1}{2 - 1} = \frac{90^3 - 1}{90 - 1}.$$

These correspond to the known solutions $(x, y, m, n) = (2, 5, 5, 3)$ and $(2, 90, 13, 3)$ to what is nowadays termed *Goormaghtigh's equation*. The Diophantine equation (1.5) asks for integers having all digits equal to one with respect to two distinct bases, yet whether it has finitely many solutions is still unknown. By fixing the exponents m and n however, Davenport, Lewis, and Schinzel [38] were able to prove that (1.5) has only finitely many solutions. Unfortunately, this result rests on Siegel's aforementioned finiteness theorem, and is therefore ineffective.

In 1933, Mahler [67] published a paper on the investigation of the Diophantine equation

$$f(x,y) = p_1^{z_1} \cdots p_v^{z_v}, \quad (x,y) = 1,$$

in which $S = \{p_1, \dots, p_v\}$ denotes a fixed set of prime numbers, $x, y, z_i \geq 0$, $i = 1, \dots, v$ are unknown integers, and $f(x,y)$ is an integral irreducible binary form of degree $n \geq 3$. Generalizing the classical result of Thue, Mahler proved that this equation has only finitely many solutions. Unfortunately, like Thue, Mahler's argument is also ineffective.

This leads us to the third basic problem regarding Diophantine equations and the main focus of this thesis: given a solvable Diophantine equation, determine all of its solutions. Until long after Thue's work, no method was known for the construction of bounds for the number of solutions of a Thue equation in terms of the parameters of the equation. Only in 1968 was such a method introduced by Baker [4], based on his theory of bounds for linear forms in the logarithms of algebraic numbers. Generalizing Baker's ground-breaking result to the p-adic case, Sprindžuk and Vinogradov [104] and Coates [25] proved that the solutions of any *Thue-Mahler equation*,

$$f(x,y) = ap_1^{z_1} \cdots p_v^{z_v}, \quad (x,y) = 1, \tag{1.6}$$

where a is a fixed integer, could, at least in principal, be effectively determined. The first practical method for solving the general Thue-Mahler equation (1.6) over $\mathbb{Z}$ is attributed to Tzanakis and de Weger (cf. [114], [110], [111], [112]), whose ideas were inspired in part by the method of Agrawal, Coates, Hunt, and van der Poorten [1] in their work to solve the specific Thue-Mahler equation

$$x^3 - x^2y + xy^2 + y^3 = \pm 11^{z_1}.$$

Using optimized bounds arising from the theory of linear forms in logarithms, a refined, automated version of this explicit method has since been implemented by Hambrook [48] as a Magma package [17].

As for Goormaghtigh's equation, when m and n are fixed and

$$\gcd(m-1, n-1) > 1, \tag{1.7}$$

Davenport, Lewis, and Schinzel [38] were able to replace Siegel's result by an effective argument due to Runge. This result was improved by Nesterenko and Shorey [81], and Bugeaud and Shorey [22] using Baker's theory of linear forms in logarithms. In either case, in order to deduce effectively computable bounds upon the polynomial variables x and y, one must impose the constraints upon m and n that either $m = n + 1$, or that the assumption (1.7) holds. In the extensive literature on this problem, there are a number of striking results that go well beyond what we have mentioned here. By way of example, work of Balasubramanian and Shorey [3] shows that equation (1.5) has at most finitely many solutions if we fix only the set of prime divisors of x and y, while Bugeaud and Shorey [22] prove an analogous finiteness result, under the additional assumption of (1.7), provided the quotient $(m-1)/(n-1)$ is bounded above. Additional results on special cases of equation (1.5) are available in, for example, [52], [60], [61],[97] and [62].

1.1 Statement of the results

The novel contributions of this thesis concern the development and implementation of efficient algorithms to determine all solutions of certain Goormaghtigh equations and Thue-Mahler equations. In particular, we follow [REF: BeGhKr] to prove that, in fact, under assumption (1.7), equation (1.5) has at most finitely many solutions which may be found effectively, even if we fix only a single exponent.

Theorem 1.1.1 (BeGhKr)**.** *If there is a solution in integers x, y, n and m to equa-*

tion (1.5)*, satisfying* (1.7)*, then*

$$x < (3d)^{4n/d} \leq 36^n. \tag{1.8}$$

In particular, if n is fixed, there is an effectively computable constant $c = c(n)$ such that $\max\{x, y, m\} < c$*.*

We note that the latter conclusion here follows immediately from (1.8), in conjunction with, for example, work of Baker ([REF]). The constants present in our upper bound (1.8) may be sharpened somewhat at the cost of increasing the complexity of our argument. By refining our approach, in conjunction with some new results from computational Diophantine approximation, we are able to achieve the complete solution of equation (1.5), subject to condition (1.7), for small fixed values of n.

Theorem 1.1.2 (BeGhKr)**.** *If there is a solution in integers x, y and m to equation* (1.5)*, with $n \in \{3, 4, 5\}$ and satisfying* (1.7)*, then*

$$(x, y, m, n) = (2, 5, 5, 3) \text{ and } (2, 90, 13, 3).$$

In the case $n = 5$ of Theorem (1.1.2) "off-the-shelf" techniques for finding integral points on models of elliptic curves or for solving *Ramanujan-Nagell* equations of the shape $F(x) = z^n$ (where F is a polynomial and z a fixed integer) do not apparently permit the full resolution of this problem in a reasonable amount of time. Instead, we sharpen the existing techniques of [TdW] and [Hambrook] for solving Thue-Mahler equations and specialize them to this problem.

A direct consequence and primary motivation for developing an efficient Thue-Mahler algorithm is the computation of elliptic curves over $\mathbb{Q}$. Let S be a finite set of rational primes. In 1963, Shafarevich [CITE] proved that there are at most finitely many $\mathbb{Q}$-isomorphism classes of elliptic curves defined over $\mathbb{Q}$ having good reduction outside S. The first effective proof of this statement was provided by Coates [CITE] in 1970 for the case $K = \mathbb{Q}$ and $S = \{2, 3\}$ using bounds for linear forms in p-adic and complex logarithms. Early attempts to make these results explicit for fixed sets of small primes overlap with the arguments of [COATES], in that they reduce the problem to that of solving a number of degree 3 Thue-Mahler equations of the form

$$F(x, y) = au,$$

where u is an integer whose prime factors all lie in S.

In the 1950's and 1960's, Taniyama and Weil asked whether all elliptic curves over $\mathbb{Q}$ of a given conductor N are related to modular functions. While this conjecture is now known as the Modularity Theorem, until its proof in 2001 [**?**], attempts to verify it sparked a large effort to tabulate all elliptic curves over $\mathbb{Q}$ of given conductor N. In 1966, Ogg ([**?**], [**?**]) determined all elliptic curves defined over $\mathbb{Q}$ with conductor of the form 2^a. Coghlan, in his dissertation [**?**], studied the curves of conductor 2^a3^b independently of Ogg, while Setzer [**?**] computed all $\mathbb{Q}$-isomorphism classes of elliptic curves of conductor p for certain small primes p. Each of these examples corresponds, via the [BR] approach, to cases with reducible forms. The first analysis on irreducible forms in (**??**) was carried out by Agrawal, Coates, Hunt and van der Poorten [**?**], who determined all elliptic curves of conductor 11 defined over $\mathbb{Q}$ to verify the (then) conjecture of Taniyama-Weil.

There are very few, if any, subsequent attempts in the literature to find elliptic curves of given conductor via Thue-Mahler equations. Instead, many of the approaches involve a completely different method to the problem, using modular forms. This method relies upon the Modularity Theorem of Breuil, Conrad, Diamond and Taylor [**?**], which was still a conjecture (under various guises) when these ideas were first implemented. Much of the success of this approach can be attributed to Cremona (see e.g. [**?**], [**?**]) and his collaborators, who have devoted decades of work to it. In fact, using this method, all elliptic curves over $\mathbb{Q}$ of conductor N have been determined for values of N as follows

- Antwerp IV (1972): $N \leq 200$
- Tingley (1975): $N \leq 320$
- Cremona (1988): $N \leq 600$

- Cremona (1990): $N \leq 1000$
- Cremona (1997): $N \leq 5077$
- Cremona (2001): $N \leq 10000$
- Cremona (2005): $N \leq 130000$
- Cremona (2014): $N \leq 350000$
- Cremona (2015): $N \leq 364000$
- Cremona (2016): $N \leq 390000$.

In this thesis, we follow [BeGhRe] wherein we return to techniques based upon solving Thue-Mahler equations, using a number of results from classical invariant theory. In particular, we illustrate the connection between elliptic curves over $\mathbb{Q}$ and cubic forms and subsequently describe an effective algorithm for determining all elliptic curves over $\mathbb{Q}$ having good reduction outside S. This result can be summarized as follows. If we wish to find an elliptic curves E of conductor $N = p_1^{a_1} \cdots p_v^{a_v}$ for some $a_i \in \mathbb{N}$, by Theorem 1 of [BeGhRe], there exists an integral binary cubic form F of discriminant $N_0 \mid 12N$ and relatively prime integers u, v satisfying

$$F(u,v) = w_0u^3 + w_1u^2v + w_2uv^2 + w_3v^3 = 2^{\alpha_1}3^{\beta_1}\prod_{p \mid N_0} p^{\kappa_p}$$

for some $\alpha_1, \beta_1, \kappa_p$. Then E is isomorphic over $\mathbb{Q}$ to the elliptic curve $E_{\mathcal{D}}$, where $E_{\mathcal{D}}$ is determined by the form F and (u, v). It is worth noting that Theorem 1 of [BeGhRe] very explicitly describes how to generate $E_{\mathcal{D}}$; once a solution (u, v) to the Thue-Mahler equation F is known, a quick computation of the Hessian and Jacobian discriminant of F evaluated at (u, v) yields the coefficients of $E_{\mathcal{D}}$. Using this theorem, all $E/\mathbb{Q}$ of conductor N may be computed by generating all of the relevant binary cubic forms, solving the corresponding Thue-Mahler equations, and outputting the elliptic curves that arise. The first and last steps of this process are straightforward. Indeed, Bennett and Rechnitzer describe an efficient algorithm for carrying out the first step REF. In fact, they having carried out a one-time computation of all irreducible forms that can arise in Theorem 1 of absolute discriminant bounded by 10^{10}. The bulk of the work is therefore concentrated in step 2, solving a large number of degree 3 Thue-Mahler equations.

Unfortunately, despite many refinements, [Hambrook's] MAGMA implementation of a Thue-Mahler solver encounters a multitude of bottlenecks which often yield unavoidable timing and memory problems, even when parallelization is considered. As our aim is to use the results of [BeGhRe] to generate all elliptic curves over $\mathbb{Q}$ of conductor $N < 10^6$, in its current state, the Hambrook algorithm is inefficient for this task, and in many cases, simply unusable due to its memory requirements. The main novel contribution of this thesis is therefore the efficient resolution of an arbitrary degree 3 Thue-Mahler equation and the implementation of this algorithm as a MAGMA package. This work is based on ideas of Matshke, von Kanel [CITE], and Siksek and is summarized in the following steps.

Step 1. Following [TdW] and [Hambrook], we reduce the problem of solving the given Thue-Mahler equation to the problem of solving a collection of finitely many S-unit equations in a certain algebraic number field K. These are equations of the form

$$\mu_0 y - \lambda_0 x = 1 \tag{1.9}$$

for some $\mu_0, \lambda_0 \in K$ and unknowns x, y. The collection of forms is such that if we know the solutions of each equation in the collection, then we can easily derive all of the solutions of the Thue-Mahler equation. This reduction is performed in two steps. First, (1.6) is reduced to a finite number of ideal equations over K. Here, we employ new results by Siksek [Cite?] to significantly reduce the number of ideal equations to consider. Next, we reduce each ideal equation to a number of certain S-unit equations (1.9) via a finite number of principalization tests. The method of [TdW] reduces (1.6) to $(m/2)h^v$ S-unit equations, where m is the number of roots of unity of K, h is the class number, and v is the number of rational primes $p_1, \ldots, p_v$. The method of Siksek that we employ gives only $m/2$ S-unit equations. The principle computational work here consists of computing an integral basis, a system of fundamental units, and a splitting field of K, as well as computing the class group of K and the factorizations of the primes $p_1, \ldots, p_v$ into prime ideals in the ring of integers of K.

The remaining steps are performed for each of the S-unit equations in our collection.

Step 2. In place of the logarithmic sieves used in [TdW] to derive a large upper bound, we work with the global logarithmic Weil height

$$h : \mathbb{G}_m(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}.$$

For a given (1.9), we show that the height $h(1/x)$ admits a decomposition into local heights at each place of K appearing in the S-unit equation. Using [CITE : Matshke, von Kanel], we generate a very large upper bound on the height $h(1/x)$, and subsequently, on the local heights. This step is a straightforward computation, whereas the analogous step in Hambrook and TdW is a complex and lengthy derivation which involves factoring rational primes into prime ideals in a splitting field of K and computing heights of certain elements of the splitting field.

Step 3. For each place of K appearing in (1.9), we drastically reduce the upper bounds derived in Step 2 by using computational Diophantine approximation techniques applied to the intersection of a certain ellipsoid and translated lattice. This technique involves using the Finke-Pohst algorithm to enumerate all short vectors in the intersection. Here, working with the Weil height $h(1/x)$ has the advantage that it leads to ellipsoids whose volumes are smaller than the ellipsoids implicitly used in [TdW] by a factor of $\sim r^{r/2}$ for r the number of places of K appearing in our S-unit equation. In this way, we reduce the number of short vectors appearing from the Fincke-Pohst algorithm, and consequently reduce our running time and memory requirements.

Step 5. Finally, we use a sieving procedure to find all the solutions of the Diophantine equation that live in the box defined by the bounds derived in the previous steps. To carry out this step, we run through all the possible solutions in the box and sieve out the vast majority of non-solutions. This is done via certain low-cost congruence tests. The candidate solutions passing this test are then verified directly against (1.9). Though we expect the bounds defining the box to be small, there can still be a very large number of possible solutions to check, especially if the number of rational primes involved in the Thue-Mahler equation is large. The computations performed on each individual candidate solution are relatively simple, but the sheer number of candidates often makes this step the computational bottleneck of the entire algorithm.

Step 6. Having performed Steps 2-5 for each S-unit equation in our collection, we now have all the solutions of each such equation, and we use this knowledge to determine all the solutions of the Thue-Mahler equation.

The reader will notice several parallels between this refined algorithm and the aforementioned Goormaghtigh equation solver in the case $n = 5$. In particular, both algorithms share the same setup and refinements of the [TdW] and [Hambrook] solver. For (1.5), however, we are left to solve

$$f(y) = x^m,$$

a Thue-Mahler-like equation of degree 4 in explicit values of x and unknown integers y and m. In this case, we are permitted simplifications which allow us to omit the Fincke-Pohst algorithm and final congruence sieves. Instead, for each x, we rely on only a few iterations of the LLL algorithm to reduce our initial bound on the exponents before entering a naive search to complete our computation. Of course, this algorithm can be refined further for efficiency, however, in the context of [BeGhKr], such improvements are not needed.

The outline of this thesis is as follows. ADD

Intro from Goormaghtigh: More than a century ago, Ratat [90] and Goormaghtigh [45] observed the identities

$$31 = \frac{2^5 - 1}{2 - 1} = \frac{5^3 - 1}{5 - 1} \quad \text{and} \quad 8191 = \frac{2^{13} - 1}{2 - 1} = \frac{90^3 - 1}{90 - 1}.$$

These correspond to the known solutions $(x, y, m, n) = (2, 5, 5, 3)$ and $(2, 90, 13, 3)$

to what is nowadays termed *Goormaghtigh's equation*

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}, \ \ y > x > 1, \ m > n > 2. \tag{1.10}$$

This is a classical example of a *polynomial-exponential equation* and shares a number of common characteristics with other frequently-studied Diophantine equations of this type, such as those of Catalan

$$x^m - y^n = 1, \ \ x, y, m, n > 1, \tag{1.11}$$

and Nagell-Ljunggren

$$\frac{x^m - 1}{x - 1} = y^n, \ \ x, y, n > 1, \ m > 2. \tag{1.12}$$

In a certain sense, however, equation (4.2) appears to be rather harder to treat than (1.11) or (1.12). Techniques from Diophantine approximation (specifically, bounds for linear forms in complex and p-adic logarithms) have been applied by Tijdeman [109] to show that equation (1.11) has at most finitely many solutions in the four variables x, y, m and n (a result subsequently sharpened by Mihăilescu [73] via a different method to solve (1.11) completely). Similarly, Shorey and Tijdeman [98] showed that equation (1.12) has at most finitely many solutions if any one of the variables x, y or m is fixed (though we do not have a like result for fixed odd n; the case where n is even was resolved earlier by Nagell [78] and Ljunggren [65]). In the case of equation (4.2), on the other hand, to obtain finiteness results with current technology, we apparently need to assume that two of the variables x, y, m and n are fixed (see [3] for references). In addition, if the two variables fixed are the exponents m and n, then in order to deduce effectively computable bounds upon the polynomial variables x and y, via either Runge's method (Davenport, Lewis and Schinzel [38]) or from bounds upon linear forms in logarithms (see e.g. Nesterenko and Shorey [81], and Bugeaud and Shorey [22]), we require constraints upon m and n, that either $m = n + 1$, or that

$$\gcd(m - 1, n - 1) = d > 1. \tag{1.13}$$

In the extensive literature on this problem, there are a number of striking results that go well beyond what we have mentioned here. By way of example, work of Balasubramanian and Shorey [3] shows that equation (4.2) has at most finitely many solutions if we fix only the set of prime divisors of x and y, while Bugeaud and Shorey [22] prove an analogous finiteness result, under the additional assumption of (4.1), provided the quotient $(m-1)/(n-1)$ is bounded above. Additional results on special cases of equation (4.2) are available in, for example, [52], [60], [61] and [62]. An excellent overview of results on this problem can be found in the survey of Shorey [97].

In this paper, we prove that, in fact, under assumption (4.1), equation (4.2) has at most finitely many solutions which may be found effectively, even if we fix only a single exponent.

Theorem 1.1.3. *If there is a solution in integers x, y, n and m to equation (4.2), satisfying (4.1), then*

$$x < (3d)^{4n/d} \leq 36^n. \tag{1.14}$$

In particular, if n is fixed, there is an effectively computable constant $c = c(n)$ such that $\max\{x, y, m\} < c$.

We note that the latter conclusion here follows immediately from (4.3), in conjunction with, for example, work of Baker [5]. The constants present in our upper bound (4.3) may be sharpened somewhat at the cost of increasing the complexity of our argument. By refining our approach, in conjunction with some new results from computational Diophantine approximation, we are able to achieve the complete solution of equation (4.2), subject to condition (4.1), for small fixed values of n.

Theorem 1.1.4. *If there is a solution in integers x, y and m to equation (4.2), with $n \in \{3, 4, 5\}$ and satisfying (4.1), then*

$$(x, y, m, n) = (2, 5, 5, 3) \ \textit{and} \ (2, 90, 13, 3).$$

Essentially half of the current paper is concerned with developing Diophantine approximation machinery for the case $n = 5$ in Theorem 4.0.2. Here, "off-the-shelf" techniques for finding integral points on models of elliptic curves or for solving *Ramanujan-Nagell* equations of the shape $F(x) = z^n$ (where F is a polynomial and z a fixed integer) do not apparently permit the full resolution of this problem in a reasonable amount of time. The new ideas introduced here are explored more fully in the general setting of *Thue-Mahler* equations in the forthcoming paper [44]. These are polynomial-exponential equations of the form $F(x, y) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where F is a binary form of degree three or greater and $p_1, \ldots, p_k$ are fixed rational primes. Here, we take this opportunity to specialize these refinements to the case of Ramanujan-Nagell equations, and to introduce some further sharpenings which enable us to complete the proof of Theorem 4.0.2.

We observe that, in case $n = 3$, Theorem 4.0.2 was obtained earlier by Yuan [118] (see also He [51]). The techniques employed in both [51] and [118], however, depend essentially upon the fact that $n = 3$ (whereby $n - 1 = 2$ and one can appeal to specialized techniques from the theory of quadratic fields) and cannot apparently be generalized to other values of n.

The title of this paper reflects the fact that the machinery of Padé approximation to binomial functions has been applied to the problem of solving equation (4.2) in earlier work of Bugeaud and Shorey [22]. We will employ these tools here rather differently.

The outline of this paper is as follows. In Section 4.1, we derive "good" rational approximations to certain algebraic numbers associated to solutions of (4.2). Section 4.2 contains relevant details about Padé approximation to the binomial function. In Sections 4.3 and 4.4, we find the proofs of Theorems 4.0.1 and 4.0.2, respectively. In the latter case, to treat small fixed values of n and x in equation (4.2), we appeal to a variety of techniques from computational Diophantine approximation. Most interestingly, in case $n = 5$, we sharpen existing techniques for solving Thue-Mahler equations, and specialize them to our problem. We note that this section may essentially be read independently of the rest of the paper. For each x, we restrict the problem to that of solving a number of related S-unit equations, where S is the set of primes dividing x. We then generate a large upper bound on the exponents of these equations using bounds for linear forms in logarithms, both Archimedean and non-Archimedean. Finally, unlike traditional examples of Thue-Mahler equations, where extensive use of geometric and p-adic reduction techniques are typically required, using only a few iterations of the LLL algorithm, we reduce this bound significantly, after which we apply a naive search to complete our computation. We will, in fact, employ two quite different algorithms for solving Thue-Mahler equations, one for which we must compute the class group of a number field and one which avoids this computation altogether. For a given value of x, one of these versions may be significantly faster than the other; we list some timings for examples to illustrate this difference.

Chapter 2

Preliminaries

2.1 Algebraic number theory

In this section we recall some basic results from algebraic number theory that we use throughout the remaining chapters. We refer to [71] and [83] for full details.

Let K be a finite algebraic extension of $\mathbb{Q}$ of degree $n = [K : \mathbb{Q}]$. There are n embeddings $\sigma : K \to \mathbb{C}$. These embeddings can be described by writing $K = \mathbb{Q}(\theta)$ for some $\theta \in \mathbb{C}$ and observing that θ can be sent to any one of its conjugates. Let s denote the number of real embeddings of K and let t denote the number of conjugate pairs of complex embeddings of K, where $n = s + 2t$. By Dirichlet's Unit Theorem, the group of units of K is the direct product of a finite cyclic group consisting of the roots of unity in K and a free abelian group of rank $r = s+t-1$. Equivalently, there exists a system of r independent units $\varepsilon_1, \ldots, \varepsilon_r$ such that the group of units of K is given by

$$\{\zeta \cdot \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \ : \ \zeta \text{ a root of unity}, a_i \in \mathbb{Z} \text{ for } i = 1, \ldots, r\}.$$

Any set of independent units that generate the torsion-free part of the unit group is called a system of *fundamental units*.

An element $\alpha \in K$ is called an *algebraic integer* if its minimal polynomial over $\mathbb{Z}$ is monic. The set of algebraic integers in K forms a ring, denoted $\mathcal{O}_K$. We refer to this ring as the *ring of integers* or *number ring* corresponding to the number field K. For any $\alpha \in K$, we define the *norm* of α as

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma: K \to \mathbb{C}} \sigma(\alpha)$$

where the product is taken over all embeddings σ of K. For algebraic integers, $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. The units are precisely the elements of norm ± 1. Two elements α, β of K are called *associates* if there exists a unit ε such that $\alpha = \varepsilon\beta$. Let $(\alpha)\mathcal{O}_K$ denote the ideal generated by α. Associated elements generate the same ideal, and distinct generators of an ideal are associated. There exist only finitely many non-associated algebraic integers in K with given norm.

Any element of the ring of integers can be written as a product of *irreducible* elements. These are non-zero non-unit elements of $\mathcal{O}_K$ which have no integral divisors but their own associates. Unfortunately, number rings are not alway unique factorization domains: this decomposition into irreducible elements may not be unique. However, every number ring is a Dedekind domain. This means that every ideal can be decomposed into a product of prime ideals and this decomposition is unique. A *principal* ideal is an ideal generated by a single element α. Two fractional ideals are called equivalent if their quotient is principal. It is well known that there are only finitely many equivalence classes of fractional ideals and the set of all such classes forms a finite abelian group called the *ideal class group*, $\mathrm{Cl}(K)$. The number of ideal classes, $\#\,\mathrm{Cl}(K)$, is called the *class number* of $\mathcal{O}_K$ and is denoted by h_K. For an ideal $\mathfrak{a}$, it is always true that $\mathfrak{a}^{h_K}$ is principal. The norm of the (integral) ideal $\mathfrak{a}$ is defined by $N_{K/\mathbb{Q}}(\mathfrak{a}) = \#\,(\mathcal{O}_K/\mathfrak{a})$. If $\mathfrak{a} = (\alpha)\mathcal{O}_K$ is a principal ideal, then $N_{K/\mathbb{Q}}(\mathfrak{a}) = \left|N_{K/\mathbb{Q}}(\alpha)\right|$.

Let L be a finite field extension of K with ring of integers $\mathcal{O}_L$. Every prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ *lies over* a unique prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. That is, $\mathfrak{P}$ divides $\mathfrak{p}$. The *ramification index* $e(\mathfrak{P}|\mathfrak{p})$ is the largest power to which $\mathfrak{P}$ divides $\mathfrak{p}$. The field $\mathcal{O}_L/\mathfrak{P}$ is an extension of finite degree $f(\mathfrak{P}|\mathfrak{p})$ over $\mathcal{O}_K/\mathfrak{p}$. We call $f(\mathfrak{P}|\mathfrak{p})$ the *inertial degree* of $\mathfrak{P}$ over $\mathfrak{p}$. For $\mathfrak{p}$ lying over the rational prime p, this is the integer such that

$$N_{K/\mathbb{Q}}(\mathfrak{p}) = p^{f(\mathfrak{p}|p)}.$$

The ramification index and inertial degree are multiplicative in a tower of fields. In particular, if $\mathfrak{P}$ lies over $\mathfrak{p}$ which lies over the rational prime p, then

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|p) \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p})f(\mathfrak{p}|p).$$

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ be the primes of $\mathcal{O}_L$ lying over a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Denote by $e(\mathfrak{P}_1|\mathfrak{p}), \ldots, e(\mathfrak{P}_m|\mathfrak{p})$ and $f(\mathfrak{P}_1|\mathfrak{p}), \ldots, f(\mathfrak{P}_m|\mathfrak{p})$ the corresponding ramification indices and inertial degrees. Then

$$\sum_{i=1}^{m} e(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{P}_i|\mathfrak{p}) = [L : K].$$

If L is normal over K and $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are two prime ideals lying over $\mathfrak{p}$, then $e(\mathfrak{P}_i|\mathfrak{p}) = e(\mathfrak{P}_j|\mathfrak{p})$ and $f(\mathfrak{P}_i|\mathfrak{p}) = f(\mathfrak{P}_j|\mathfrak{p})$. In this case, $\mathfrak{p}$ factors as

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_m)^e$$

in $\mathcal{O}_L$, where the $\mathfrak{P}_i$ are distinct prime ideals all having the same ramification degree e and inertial degree f over $\mathfrak{p}$. It follows that

$$mef = [L : K].$$

2.2 p-adic valuations

In this section we give a concise exposition of p-adic valuations. As references for this material we give [16] (especially Theorem 3 in Chapter 4, Section 2), [23] (especially Lemma 2.1 in Chapter 9), [50] (especially Chapter 18), [58] (especially Chapter 3, Section 2), and [80] (especially Theorem 6.1).

We denote the algebraic closure of $\mathbb{Q}_p$ by $\overline{\mathbb{Q}}_p$. The completion of $\overline{\mathbb{Q}}_p$ with respect to the absolute value of $\overline{\mathbb{Q}}_p$ is denoted by $\mathbb{C}_p$.

Let K be an arbitrary number field. A homomorphism $v : K^* \to \mathbb{R}_{\geq 0}$ of the multiplicative group of K into the group of positive real numbers is called a *valuation* if it satisfies the condition

$$v(x + y) \leq v(x) + v(y).$$

This definition may be extended to all of K by setting $v(0) = 0$. If

$$v(x + y) \leq \max(v(x), v(y))$$

holds for all $x, y \in K$, then v is called a *non-Archimedean valuation*. All remaining valuations on K are called *Archimedean*.

Every valuation v induces on K the structure of a metric topological space which may or may not be complete. We say that two valuations are *equivalent* if they define the same topology and we call an equivalence class of absolute values a *place* of K. It is an elementary result of topology that every metric space may be embedded in a complete metric space, and this can be done in an essentially unique way. For the field K, the resulting complete metric space may be given a field structure. Equivalently, there exists a field L with a valuation w such that L is complete in the topology induced by w. The field K is contained in L and the valuations v and w coincide in K. Moreover, the completion L of K is unique up to topological isomorphism.

For any non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ denote the exact power to which $\mathfrak{p}$ divides the ideal $\mathfrak{a}$. For fractional ideals $\mathfrak{a}$ this number may be negative. For $\alpha \in K$, we write $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ for $\mathrm{ord}_{\mathfrak{p}}\left((\alpha)\mathcal{O}_K\right)$. Every prime ideal defines a discrete non-Archimedean valuation on K via

$$v(x) := \left(\frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})}\right)^{\mathrm{ord}_{\mathfrak{p}}(x)}.$$

Furthermore, every embedding of K into the complex field defines an Archimedean valuation. Conversely, every discrete valuation on K arises in this way by a prime ideal of $\mathcal{O}_K$, while every Archimedean valuation of K is equivalent to $|\sigma(x)|$, where σ is an embedding of K into $\mathbb{C}$. Valuations defined by different prime ideals are non-equivalent, and two valuations defined by different embeddings of K into $\mathbb{C}$ are equivalent if and only if those embeddings are complex conjugated. The topology induced in K by a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is called the $\mathfrak{p}$-*adic topology*. The completion of K under this valuation is denoted by $K_\mathfrak{p}$ or K_v and called the $\mathfrak{p}$-*adic field*. Let V be the set of all valuations of an algebraic number field K. Then for every non-zero element $\alpha \in K$ we have

$$\prod_{v \in V} v(\alpha) = 1.$$

In the ring of integers of $\mathbb{Q}$, the prime ideals are generated by the rational primes p, and the resulting topology in the field $\mathbb{Q}$ is called the *p-adic topology*. The completion of $\mathbb{Q}$ under this valuation is denoted by $\mathbb{Q}_p$. If $v(x)$ is a non-trivial valuation of $\mathbb{Q}$, then either $v(x)$ is equivalent to the ordinary absolute value $|x|$, or it is equivalent to one of the p-adic valuations induced by rational primes. Analogous to $\operatorname{ord}_\mathfrak{p}$, for any prime p we define the p-adic order of $x \in \mathbb{Q}$ as the largest exponent of p dividing x. Then, the p-adic valuation v is defined as

$$v(x) = p^{-\operatorname{ord}_p(x)}.$$

If $K_\mathfrak{p}$ is a $\mathfrak{p}$-adic field, it is necessarily a finite extension of a certain $\mathbb{Q}_p$.

Consider now $K/\mathbb{Q}$ where $n = [K : \mathbb{Q}]$ and let $g(t)$ denote the minimal polynomial of K over $\mathbb{Q}$. Suppose p is a rational prime and let $g(t) = g_1(t) \cdots g_m(t)$ be the decomposition of $g(t)$ into irreducible polynomials $g_i(t) \in \mathbb{Q}_p[t]$ of degree $n_i = \deg g_i(t)$. The prime ideals in K dividing p are in one-to-one correspondence with $g_1(t), \ldots, g_m(t)$. More precisely, we have in K the following decomposition of $(p)\mathcal{O}_K$

$$(p)\mathcal{O}_K = \mathfrak{p}_1^{e(\mathfrak{p}_1|p)} \cdots \mathfrak{p}_m^{e(\mathfrak{p}_m|p)},$$

with $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ distinct prime ideals and ramification indices $e(\mathfrak{p}_1|p), \ldots, e(\mathfrak{p}_m|p) \in \mathbb{N}$. For $i = 1, \ldots, m$ the inertial degree of $\mathfrak{p}_i$ is denoted by $f(\mathfrak{p}_i|p)$. Then $n_i = e(\mathfrak{p}_i|p)f(\mathfrak{p}_i|p)$ and $K_{\mathfrak{p}_i} \simeq \mathbb{Q}_p(\theta_i)$, where $g(\theta_i) = 0$.

By $\overline{\mathbb{Q}_p}$ we denote the algebraic closure of $\mathbb{Q}_p$. There are n embeddings of K into $\overline{\mathbb{Q}_p}$, and each one fixes $\mathbb{Q}$ and maps θ to a root of g in $\overline{\mathbb{Q}_p}$. Let $\theta_i^{(1)}, \ldots, \theta_i^{(n_i)}$ denote the roots of $g_i(t)$ in $\overline{\mathbb{Q}_p}$. For $i = 1, \ldots, m$ and $j = 1, \ldots, n_i$, let σ_{ij} be the embedding of K into $\mathbb{Q}_p(\theta_i^{(j)})$ defined by $\theta \mapsto \theta_i^{(j)}$. The m classes of conjugate embeddings are $\{\sigma_{i1}, \ldots, \sigma_{in_i}\}$ for $i = 1, \ldots, m$. Note that σ_{ij} coincides with the embedding $K \hookrightarrow K_{\mathfrak{p}_i} \simeq \mathbb{Q}_p(\theta_i) \simeq \mathbb{Q}_p(\theta_i^{(j)})$.

For any finite extension L of $\mathbb{Q}_p$, the p-adic valuation v of $\mathbb{Q}_p$ extends uniquely to L as

$$v(x) = |N_{L/\mathbb{Q}_p}(x)|^{1/[L:\mathbb{Q}_p]}.$$

Here, we define the p-adic order of $x \in L$ by

$$\mathrm{ord}_p(x) = \frac{1}{[L:\mathbb{Q}_p]} \mathrm{ord}_p(N_{L/\mathbb{Q}_p}(x)).$$

This definition is independent of the field L containing x. So, since each element of $\overline{\mathbb{Q}_p}$ is by definition contained in some finite extension of $\mathbb{Q}_p$, this definition can be used to define the p-adic valuation v of any $x \in \overline{\mathbb{Q}_p}$. Every finite extension of $\mathbb{Q}_p$ is complete with respect to v, but $\overline{\mathbb{Q}_p}$ is not. The completion of $\overline{\mathbb{Q}_p}$ with respect to v is denoted by $\mathbb{C}_p$.

The m extensions of the p-adic valuation on $\mathbb{Q}$ to K are just multiples of the $\mathfrak{p}_i$-adic valuation on K:

$$\mathrm{ord}_p(x) = \frac{1}{e_i} \mathrm{ord}_{\mathfrak{p}_i}(x) \quad \text{for } i = 1, \ldots, m.$$

We also view these extensions as arising from various embeddings of K into $\overline{\mathbb{Q}_p}$. Indeed, the extension to $\mathbb{Q}_p(\theta_i^{(j)})$ of the p-adic valuation on $\mathbb{Q}_p$ induces a p-adic valuation on K via the embedding σ_{ij} as

$$v(x) = |N_{K_{\mathfrak{p}_i}/\mathbb{Q}_p}(\sigma_{ij}(x))|^{1/n_i}.$$

Here, as before, $n_i = \deg g_i(t) = [K_{\mathfrak{p}_i} : \mathbb{Q}_p]$. Furthermore,

$$\mathrm{ord}_p(x) = \mathrm{ord}_p(\sigma_{ij}(x)),$$

and we have

$$\operatorname{ord}_p(\sigma_{ij}(x)) = \frac{1}{e_i}\operatorname{ord}_{\mathfrak{p}_i}(x) \quad \text{for } i = 1, \dots, m,\ j = 1, \dots, n_i.$$

Of course, in the special case $x \in \mathbb{Q}_p$, we can write

$$x = \sum_{i=k}^{\infty} u_i p^i$$

where $k = \operatorname{ord}_p(x)$ and the p-adic digits u_i are in $\{0, \dots, p-1\}$ with $u_k \neq 0$. If $\operatorname{ord}_p(x) \geq 0$ then x is called a p-adic *integer*. The set of p-adic integers is denoted $\mathbb{Z}_p$. A p-adic *unit* is an $x \in \mathbb{Q}_p$ with $\operatorname{ord}_p(x) = 0$. For any p-adic integer α and $\mu \in \mathbb{N}_0$ there exists a unique rational integer $x^{(\mu)} = \sum_{i=0}^{\mu-1} u_i p^i$ such that

$$\operatorname{ord}_p(x - x^{(\mu)}) \geq \mu, \quad \text{and} \quad 0 \leq x^{(\mu)} \leq p^{\mu} - 1.$$

For $\operatorname{ord}_p(x) \geq k$ we also write $x \equiv 0 \mod p^k$.

2.3 p-adic logarithms

We have seen how to define $\operatorname{ord}_{\mathfrak{p}}$ and ord_p on algebraic extensions of $\mathbb{Q}$. For any $z \in \mathbb{C}_p$ with $\operatorname{ord}_p(z-1) > 0$, we can also define the p-adic logarithm of z by

$$\log_p(z) = -\sum_{i=1}^{\infty} \frac{(1-z)^i}{i}.$$

By the n^{th} term test, this series converges precisely in the region where $\operatorname{ord}_p(z-1) > 0$. Three important properties of the p-adic logarithm are

1. $\log_p(xy) = \log_p(x) + \log_p(y)$ whenever $\operatorname{ord}_p(x-1) > 0$ and $\operatorname{ord}_p(y-1) > 0$.

2. $\log_p(z^k) = k\log(p)$ whenever $\operatorname{ord}_p(z-1) > 0$ and $k \in \mathbb{Z}$.

3. $\operatorname{ord}_p(\log_p(z)) = \operatorname{ord}_p(z-1)$ whenever $\operatorname{ord}_p(z-1) > 1/(p-1)$.

Proofs of the first and last property can be found in [50] (pp. 264-265). The second property follows from the first.

We will use the following lemma to extend the definition of the p-adic logarithm to all p-adic units in $\overline{\mathbb{Q}_p}$.

Lemma 2.3.1. *Let z be a p-adic unit belonging to a finite extensions L of $\mathbb{Q}_p$. Let e and f be the ramification index and inertial degree of L.*

(a) There is a positive integer r such that $\mathrm{ord}_p(z^r - 1) > 0$.

(b) If r is the smallest positive integer having $\mathrm{ord}_p(z^r - 1) > 0$*, then r divides $p^f - 1$, and an integer q satisfies* $\mathrm{ord}_p(z^q - 1) > 0$ *if and only if it is a multiple of r.*

(c) If r is a nonzero integer with $\mathrm{ord}_p(z^r - 1) > 0$*, and if k is an integer with $p^k(p-1) > e$, then*

$$\mathrm{ord}_p(z^{rp^k} - 1) > \frac{1}{p-1}.$$

For z a p-adic unit in $\overline{\mathbb{Q}_p}$ we define

$$\log_p z = \frac{1}{q} \log_p z^q,$$

where q is an arbitrary non-zero integer such that $\mathrm{ord}_p(z^q - 1) > 0$. To see that this definition is independent of q, let r be the smallest positive integer with $\mathrm{ord}_p(z^r - 1) > 0$, note that q/r is an integer, and use the second property of p-adic logarithms above to write

$$\frac{1}{q} \log_p z^q = \frac{1}{r(q/r)} \log_p z^{r(q/r)} = \frac{1}{r} \log_p z^r.$$

Choosing q such that $\mathrm{ord}_p(z^q - 1) > 1/(p-1)$ helps to speed up and control the convergence of the series defining $\log_p$ (cf. [101] (pp. 28-30) and [28] (pp. 263-265)).

It is straightforward to see that Properties 1 and 2 above extend to the case where x, y, z are p-adic units. Combining this with Property 3, we obtain

Lemma 2.3.2. *Let $z_1, \ldots, z_m \in \overline{\mathbb{Q}_p}$ be p-adic units and let $b_1, \ldots, b_m \in \mathbb{Z}$. If*

$$\mathrm{ord}_p(z_1^{b_1} \cdots z_m^{b_m} - 1) > \frac{1}{p-1}$$

then

$$\mathrm{ord}_p(b_1 \log_p z_1 + \cdots + b_m \log_p z_m) = \mathrm{ord}_p(z_1^{b_1} \cdots z_m^{b_m} - 1).$$

2.4 The Weil height

Let K be a number field and at each place v of K, let K_v denote the completion of K at v. Then

$$\sum_{v|p} [K_v : \mathbb{Q}_v] = [K : \mathbb{Q}]$$

for all places p of $\mathbb{Q}$. We will use two absolute values $|\cdot|_v$ and $\|\cdot\|_v$ on K which we now define. If $v|\infty$, then $\|\cdot\|_v$ restricted to $\mathbb{Q}$ is the usual Archimedean absolute value; if $v|p$ for a rational prime p, then $\|\cdot\|_v$ restricted to $\mathbb{Q}$ is the usual p-adic valuation. We then set

$$|\cdot|_v = \|\cdot\|_v^{[K_v:\mathbb{Q}_v]/[K:\mathbb{Q}]}.$$

Let $x \in K$ and let $\log^+(\cdot)$ denote the real-valued function $\max\{\log(\cdot), 0\}$ on $\mathbb{R}_{\geq 0}$. We define the *logarithmic Weil height* $h(x)$ by

$$h(x) = \frac{1}{[K : \mathbb{Q}]} \sum_v \log^+ |x|_v,$$

where the sum is take over all places v of K. If x is an algebraic unit, then $|x|_v = 1$ for all non-Archimedean places v, and therefore $h(x)$ can be taken over the Archimedean places only. In particular, if $x \in \mathbb{Q}$, then with $x = p/q$ for $p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$, we have $h(x) = \log \max\{|p|, |q|\}$, and if $x \in \mathbb{Z}$ then $h(x) = \log |x|$.

2.5 Elliptic curves

Let K be a field of characteristic $\mathrm{char}(K) \neq 2, 3$. An *elliptic curve* E over K is a nonsingular curve of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

with $a_i \in K$ having a specified base point, $\mathcal{O} \in E$. An equation of the form (2.1) is called a *Weierstrass equation*. This equation is unique up to a coordinate transformation of the form

$$x = u^2x' + r, \qquad y = u^3y' + su^2x' + t,$$

with $r, s, t, u \in K, u \neq 0$. Applying several linear changes of variables and writing

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4, \quad \text{and} \quad c_6 = -b_2^3 + 36b_2b_4 + 9b_2b_4b_6,$$

E can be written as

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Associated to this curve are the quantities

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad \text{and} \quad j = c_4^3/\Delta,$$

where Δ is called the *discriminant* of the Weierstrass equation and the quantity j is called the *j-invariant* of the elliptic curve. The condition of being nonsingular is equivalent to Δ being non-zero. Two elliptic curves are isomorphic over $\bar{K}$, the algebraic closure of K, if and only if they both have the same j-invariant.

When $K = \mathbb{Q}$, the Weierstrass model (2.1) can be chosen so that Δ has minimal p-adic order for each rational prime p and $a_i \in \mathbb{Z}$. Suppose (2.1) is such a global minimal model for an elliptic curve E over $\mathbb{Q}$. Reducing the coefficients modulo a rational prime p yields a (possibly singular) curve over $\mathbb{F}_p$

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}, \tag{2.2}$$

where $\tilde{a_i} \in \mathbb{F}_p$. This "reduced" curve $\tilde{E}/\mathbb{F}_p$ is called the *reduction of E modulo p*. It is nonsingular provided that $\Delta \not\equiv 0 \mod p$, in which case it is an elliptic curve defined over $\mathbb{F}_p$. The curve E is said to have *good reduction* modulo p if $\tilde{E}/\mathbb{F}_p$ is nonsingular, otherwise, we say E has *bad reduction* modulo p.

The reduction type of E at a rational prime p is measured by the *conductor*,

$$N = \prod_p p^{f_p}$$

where the product runs over all primes p and $f_p = 0$ for all but finitely many primes. In particular, $f_p \neq 0$ if p does not divide Δ. Equivalently, E has bad reduction at p if and only if $p \mid N$. Suppose E has bad reduction at p so that $f_p \neq 0$. The reduction type of E at p is said to be *multiplicative* (E has a node over $\mathbb{F}_p$) or *additive* (E has a cusp over $\mathbb{R}_p$) depending on whether $f_p = 1$ or $f_p \geq 2$, respectively. The f_p, hence the conductor, are invariant under isogeny.

2.6 Cubic forms

Let a, b, c and d be integers and consider the binary cubic form

$$F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3.$$

Two such forms F_1 and F_2 are called *equivalent* if they are equivalent under the $GL_2(\mathbb{Z})$-action. That is, if there exist integers a_1, a_2, a_3, and a_4 such that

$$F_1(a_1x + a_2y, a_3x + a_4y) = F_2(x, y)$$

for all x, y, where $a_1 a_4 - a_2 a_3 = \pm 1$. In this case, we write $F_1 \sim F_2$. The *discriminant* D_F of such a form is given by

$$D_F = -27a^2d^2 + b^2c^2 + 18abcd - 4ac^3 - 4b^3d = a^4 \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

where α_1, α_2 and α_3 are the roots of the polynomial $F(x, 1)$. We observe that if $F_1 \sim F_2$, then $D_{F_1} = D_{F_2}$.

Associated to F is the Hessian $H_F(x, y)$, given by

$$\begin{aligned} H_F(x,y) &= -\frac{1}{4}\left(\frac{\partial^2 F}{\partial x^2}\frac{\partial^2 F}{\partial y^2} - \left(\frac{\partial^2 F}{\partial x \partial y}\right)^2\right) \\ &= (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2, \end{aligned}$$

and the Jacobian determinant of F and H_F, a cubic form $G_F(x, y)$ defined by

$$\begin{aligned} G_F(x,y) &= \frac{\partial F}{\partial x}\frac{\partial H_F}{\partial y} - \frac{\partial F}{\partial y}\frac{\partial H_F}{\partial x} \\ &= (-27a^2d + 9abc - 2b^3)x^3 + (-3b^2c - 27abd + 18ac^2)x^2y + \\ &\quad + (3bc^2 - 18b^2d + 27acd)xy^2 + (-9bcd + 2c^3 + 27ad^2)y^3. \end{aligned}$$

2.7 Lattices

An n-dimensional lattice is a discrete subgroup of $\mathbb{R}^n$ of the form

$$\Gamma = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z} \right\},$$

where $\mathbf{b}_1, \ldots, \mathbf{b_n}$ are vectors forming a basis for $\mathbb{R}^n$. We say that the vectors $\mathbf{b}_1, \ldots, \mathbf{b_n}$ form a *basis* for Γ, or that they generate Γ. Let B denote the matrix whose columns are the vectors $\mathbf{b}_1, \ldots, \mathbf{b_n}$. Any lattice element $\mathbf{v}$ may be expressed as $\mathbf{v} = B\mathbf{x}$ for some $\mathbf{x} \in \mathbb{Z}^n$. We call $\mathbf{v}$ the *embedded vector* and $\mathbf{x}$ the *coordinate vector*.

A *bilinear form* on a lattice Γ is a function $\Phi : \Gamma \times \Gamma \to \mathbb{Z}$ satisfying

1. $\Phi(\mathbf{u}, \mathbf{v} + \mathbf{w}) = \Phi(\mathbf{u}, \mathbf{v}) + \Phi(\mathbf{u}, \mathbf{w})$
2. $\Phi(\mathbf{u} + \mathbf{v}, \mathbf{w}) = \Phi(\mathbf{u}, \mathbf{w}) + \Phi(\mathbf{v}, \mathbf{w})$
3. $\Phi(a\mathbf{u}, \mathbf{w}) = a\Phi(\mathbf{u}, \mathbf{w})$
4. $\Phi(\mathbf{u}, a\mathbf{w}) = a\Phi(\mathbf{u}, \mathbf{w})$

for all $\mathbf{u}, \mathbf{v}$, and $\mathbf{w}$ in Γ and any $a \in \mathbb{Z}$.

Given a basis, we can define a specific bilinear form on our lattice Γ as part of its structure. This form describes a kind of distance between elements $\mathbf{u}$ and $\mathbf{v}$ and we say the lattice is *defined* by Φ. Associated to this bilinear form is a quadratic form $Q : \Gamma \to \mathbb{Z}$ defined by $Q(\mathbf{v}) = \Phi(\mathbf{v}, \mathbf{v})$. A lattice is called *positive definite* if its quadratic form is positive definite.

The bilinear forms (and their associated quadratic forms) that we will be using come from the usual inner product on vectors in $\mathbb{R}^n$. This is simply the dot product $\Phi(\mathbf{u}, \mathbf{v}) = \mathbf{u} \cdot \mathbf{v}$ for embedded vectors, $\mathbf{u}, \mathbf{v}$. For the coordinate vectors $\mathbf{x}, \mathbf{y}$ associated to these vectors, this translates to multiplication with the basis matrix. Precisely, if $\mathbf{u} = B\mathbf{x}$ and $\mathbf{v} = B\mathbf{y}$, we have $\Phi(\mathbf{u}, \mathbf{v}) = \mathbf{x}^T B^T B\mathbf{y}$.

If $\mathbf{v} = B\mathbf{x}$, the *norm* of the vector $\mathbf{v} \in \Gamma$ is defined to be the inner product $\Phi(\mathbf{v}, \mathbf{v})$. In terms of the corresponding coordinate vector $\mathbf{x}$, this is

$$\mathbf{v}^T \mathbf{v} = \mathbf{x}^T B^T B\mathbf{x}.$$

Equivalently, we write $\mathbf{x}^T A\mathbf{x}$ where $A = B^T B$ is the Gram matrix of Γ with basis B and bilinear form Φ. The entries of the matrix A are $a_{ij} = \Phi(\mathbf{b}_i, \mathbf{b}_j)$.

Two basis matrices B_1 and B_2 define the same lattice Γ if and only if there is a unimodular matrix U such that $B_1 U = B_2$. The bilinear form on Γ can be written with respect to either embedded or coordinate vectors. Using another basis to express the lattice elements is possible, and sometimes preferable. However, the Gram matrix is specific to the bilinear form on the lattice and should not change when operating on embedded vectors. If it is operating on coordinate vectors, the change of basis must be accounted for.

Chapter 3

Algorithms for Thue-Mahler Equations

In this chapter, we give some of primary algorithms needed to solve an arbitrary Thue-Mahler equation. The methods presented here follow somewhat [48] and [112], with new results and modifications from [44].

3.1 First steps

Fix a nonzero integer c and let $S = \{p_1, \ldots, p_v\}$ be a set of rational primes. Let

$$F(X,Y) = c_0 X^n + c_1 X^{n-1} Y + \cdots + c_{n-1} X Y^{n-1} + c_n Y^n$$

be an irreducible binary form over $\mathbb{Z}$ of degree $n \geq 3$. We want to solve the Thue–Mahler equation

$$F(X,Y) = c p_1^{Z_1} \cdots p_v^{Z_v} \tag{3.1}$$

for unknowns $X, Y, Z_1, \ldots, Z_v$ with $\gcd(X,Y) = 1$ and $Z_i \geq 0$ for $i = 1, \ldots, v$. To do so, we first reduce (3.1) to the special case where $c_0 = 1$ and $\gcd(c, p_i) = 1$ for $i = 1, \ldots, v$, loosely following [48].

As F is irreducible by assumption, at least one of the coefficients c_0 and c_n is nonzero. Hence, we may transform the given Thue–Mahler equation to one with $c_0 \neq 0$ by interchanging X and Y and by renaming the coefficients c_i appropriately. In particular, solving (3.1) is equivalent to solving

$$c_0'\overline{X}^n + c_1'\overline{X}^{n-1}\overline{Y} + \cdots + c_{n-1}'\overline{XY}^{n-1} + c_n'\overline{Y}^n = cp_1^{Z_1}\cdots p_v^{Z_v},$$

where $c_i' = c_{n-1}$ for $i = 0, \ldots, n$, $\overline{X} = Y$, and $\overline{Y} = X$.

Denote by $\mathcal{D}$ the set of all positive rational integers m dividing c_0 such that $\mathrm{ord}_p(m) \leq \mathrm{ord}_p(c)$ for each rational prime $p \notin S$. Equivalently, $\mathcal{D}$ is precisely the set of all possible integers d such that $d = \gcd(c_0, Y)$. To see this, let $q_1, \ldots, q_w$ denote the distinct prime divisors of a not contained in S. Then

$$c = \prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(c)}$$

for some integers $b_i > 0$. If $(X, Y, Z_1, \ldots, Z_v)$ is a solution of the Thue-Mahler equation in question, it follows that

$$F(X,Y) = cp_1^{Z_1}\ldots p_v^{Z_v} = \prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(c)+Z_i}.$$

Suppose $\gcd(c_0, Y) = d$. Since d divides $F(X,Y)$, it necessarily divides

$$\prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(c)+Z_i}.$$

In particular,

$$d = \prod_{i=1}^{w} q_i^{s_i} \cdot \prod_{i=1}^{v} p_i^{t_i}$$

for some non-negative integers $s_1, \ldots, s_w, t_1, \ldots, t_v$ such that

$$s_i \leq \min\{\mathrm{ord}_{q_i}(c), \mathrm{ord}_{q_i}(c_0)\} \quad \text{and} \quad t_i \leq \min\{\mathrm{ord}_{p_i}(c) + Z_i, \mathrm{ord}_{p_i}(c_0)\}.$$

From here, it is easy to see that $\mathrm{ord}_p(d) \leq \mathrm{ord}_p(c)$ for each rational prime $p \notin S$

so that $d \in \mathcal{D}$.

Conversely, suppose $d \in \mathcal{D}$ so that $\mathrm{ord}_p(d) \leq \mathrm{ord}_p(c)$ for all $p \notin S$. That is, the right-hand side of

$$\mathrm{ord}_p(d) \leq \mathrm{ord}_p(c) = \mathrm{ord}_p\left(\prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(c)}\right)$$

is non-trivial only at the primes $\{q_1, \ldots, q_w\}$. In particular,

$$d = \prod_{i=1}^{w} q_i^{s_i} \cdot \prod_{i=1}^{v} p_i^{t_i}$$

for non-negative integers $s_1, \ldots, s_w, t_1, \ldots, t_v$ such that

$$s_i \leq \min\{\mathrm{ord}_{q_i}(c), \mathrm{ord}_{q_i}(c_0)\} \quad \text{and} \quad t_i \leq \mathrm{ord}_{p_i}(c_0).$$

It follows that $d = \gcd(c_0, Y)$ for some solution $(X, Y, Z_1, \ldots, Z_v)$ of equation (3.1).

For any $d \in \mathcal{D}$, we define the rational numbers

$$u_d = c_0^{n-1}/d^n \quad \text{and} \quad c_d = \mathrm{sgn}(u_d c) \prod_{p \notin S} p^{\mathrm{ord}_p(u_d c)}.$$

On using that $d \in \mathcal{D}$, we see that the rational number c_d is in fact an integer coprime to S.

Suppose $(X, Y, Z_1, \ldots, Z_v)$ is a solution of (3.1) with $\gcd(X, Y) = 1$ and $d = \gcd(c_0, Y)$. Define the homogeneous polynomial $f(x, y) \in \mathbb{Z}[x, y]$ of degree n by

$$f(x, y) = x^n + C_1 x^{n-1} y + \cdots + C_{n-1} x y^{n-1} + C_n y^n,$$

where

$$x = \tfrac{c_0 X}{d}, \quad y = \tfrac{Y}{d} \quad \text{and} \quad C_i = c_i c_0^{i-1} \quad \text{for } i = 1, \ldots, n.$$

Since $\gcd(X, Y) = 1$, the numbers x and y are also coprime integers by definition of d. We observe that

$$f(x,y) = u_d F(X,Y) = u_d c \prod_{i=1}^{v} p_i^{Z_i} = c_d \prod_{p \in S} p^{Z_i + \mathrm{ord}_p(u_d c)}.$$

Setting $z_i = Z_i + \mathrm{ord}_p(u_d c)$ for all $i \in \{1, \ldots, v\}$, we obtain

$$f(x,y) = x^n + C_1 x^{n-1} y + \cdots + C_{n-1} x y^{n-1} + C_n y^n = c_d p_1^{z_1} \cdots p_v^{z_v}, \quad (3.2)$$

where $\gcd(x,y) = 1$ and $\gcd(c_d, p_i) = 1$ for all $i = 1, \ldots, v$.

Since there are only finitely many choices for $d = \gcd(c_0, Y)$, there are only finitely many choices for $\{c_d, u_d, d\}$. Then, solving (3.1) is equivalent to solving the finitely many Thue-Mahler equations (3.2) for each choice of $\{c_d, u_d, d\}$. For each such choice, the solution $\{x, y, z_1, \ldots, z_v\}$ is related to $\{X, Y, Z_1, \ldots, Z_v\}$ via

$$X = \frac{dx}{c_0}, \quad Y = dy \quad \text{and} \quad Z_i = z_i - \mathrm{ord}_p(u_d c).$$

Lastly, we observe that the polynomial $f(x,y)$ of (3.2) remains the same for any choice of $\{c_d, u_d, d\}$. Thus, to solve the family of equations (3.2), we need only to enumerate over every possible c_d. Now, if $\mathcal{C}$ denotes the set of all $\{c_d, u_d, d\}$ and $d_1, d_2 \in \mathcal{D}$, we may have $\{c_{d_1}, u_{d_1}, d_1\}, \{c_{d_2}, u_{d_2}, d_2\} \in \mathcal{C}$ where $c_{d_1} = c_{d_2}$. That is, d_1, d_2 may yield the same value of c_d, reiterating that we need only solve (3.2) for each distinct c_d.

3.2 The relevant algebraic number field

For the remainder of this chapter, we consider the Thue-Mahler equation

$$f(x,y) = x^n + C_1 x^{n-1} y + \cdots + C_{n-1} x y^{n-1} + C_n y^n = c p_1^{z_1} \cdots p_v^{z_v} \quad (3.3)$$

where $\gcd(x,y) = 1$ and $\gcd(c, p_i) = 1$ for $i = 1, \ldots, p_v$.

Following [112], put

$$g(t) = f(t, 1) = t^n + C_1 t^{n-1} + \cdots + C_{n-1} t + C_n$$

and note that $g(t)$ is irreducible in $\mathbb{Z}[t]$. Let $K = \mathbb{Q}(\theta)$ with $g(\theta) = 0$. Now (3.3) is equivalent to the norm equation

$$N_{K/\mathbb{Q}}(x - y\theta) = c p_1^{z_1} \dots p_v^{z_v}. \tag{3.4}$$

Let p_i be any rational prime and let

$$(p_i)\mathcal{O}_K = \prod_{j=1}^{m_i} \mathfrak{p}_{ij}^{e(\mathfrak{p}_{ij}|p_i)}$$

be the factorization of p_i into prime ideals in the ring of integers $\mathcal{O}_K$ of K. Let $f(\mathfrak{p}_{ij}|p_i)$ be the inertial degree of $\mathfrak{p}_{ij}$ over p_i. Since $N(\mathfrak{p}_{ij}) = p_i^{f_{ij}}$, (3.4) leads to finitely many ideal equations of the form

$$(x - y\theta)\mathcal{O}_K = \mathfrak{a} \prod_{j=1}^{m_1} \mathfrak{p}_{1j}^{z_{1j}} \cdots \prod_{j=1}^{m_v} \mathfrak{p}_{vj}^{z_{vj}} \tag{3.5}$$

where $\mathfrak{a}$ is an ideal of norm $|c|$ and the z_{ij} are unknown integers related to z_i by

$$\sum_{j=1}^{m_i} f(\mathfrak{p}_{ij}|p_i) z_{ij} = z_i$$

for $i \in \{1, \dots, v\}$.

Our first task is to cut down the number of variables appearing in (3.5). We will do this by showing that only a few prime ideals can divide $(x - y\theta)\mathcal{O}_K$ to a large power.

3.3 The prime ideal removing lemma

In this section, we establish some key results that will allow us to cut down the number of prime ideals that can appear to a large power in the factorization of $(x - y\theta)\mathcal{O}_K$. It is of particular importance to note that we do not appeal to the Prime Ideal Removing Lemma of Tzanakis and de Weger ([112]) here and instead apply the following results of [44].

Let $p \in \{p_1, \dots, p_v\}$. We will produce the following two finite lists L_p and M_p. The list L_p will consist of certain ideals $\mathfrak{b}$ of $\mathcal{O}_K$ supported at the prime ideals above p. The list M_p will consist of certain pairs $(\mathfrak{b}, \mathfrak{p})$ where $\mathfrak{b}$ is supported at the prime ideals above p and $\mathfrak{p}$ is a prime ideal lying over p satisfying $e(\mathfrak{p}|p) = f(\mathfrak{p}|p) = 1$. These lists will satisfy the following property: if $(x, y, z_1, \dots, z_v)$ is a solution to the Thue-Mahler equation (3.3) then

(i) either there is some $\mathfrak{b} \in L_p$ such that

$$\mathfrak{b} \mid (x - y\theta)\mathcal{O}_K, \qquad (x - y\theta)\mathcal{O}_K/\mathfrak{b} \text{ is coprime to } (p)\mathcal{O}_K; \tag{3.6}$$

(ii) or there is a pair $(\mathfrak{b}, \mathfrak{p}) \in M_p$ and a non-negative integer v_p such that

$$(\mathfrak{b}\mathfrak{p}^{v_p}) \mid (x - y\theta)\mathcal{O}_K, \qquad (x - y\theta)\mathcal{O}_K/(\mathfrak{b}\mathfrak{p}^{v_p}) \text{ is coprime to } (p)\mathcal{O}_K. \tag{3.7}$$

To generate the lists M_p, L_p we consider two affine patches, $p \nmid y$ and $p \mid y$. We begin with the following lemmata.

Lemma 3.3.1. *Let $(x, y, z_1, \dots, z_v)$ be a solution of (3.3) with $p \nmid y$, let t be a positive integer, and suppose $x/y \equiv u \pmod{p^t}$, where $u \in \{0, 1, 2, \dots, p^t - 1\}$. If $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_K$ lying over p, then*

$$\operatorname{ord}_{\mathfrak{q}}(x - y\theta) \geq \min\{\operatorname{ord}_{\mathfrak{q}}(u - \theta), t \cdot e(\mathfrak{q}|p)\}.$$

Moreover, if $\operatorname{ord}_{\mathfrak{q}}(u - \theta) < t \cdot e(\mathfrak{q}|p)$, then

$$\operatorname{ord}_{\mathfrak{q}}(x - y\theta) = \operatorname{ord}_{\mathfrak{q}}(u - \theta).$$

Lemma 3.3.2. *Let* $(x, y, z_1, \ldots, z_v)$ *be a solution of* (3.3) *with* $p \mid y$ *(and thus* $p \nmid x$*), let* t *be a positive integer, and suppose* $y/x \equiv u \pmod{p^t}$*, where* $u \in \{0, 1, 2, \ldots, p^t - 1\}$*. If* $\mathfrak{q}$ *is a prime ideal of* $\mathcal{O}_K$ *lying over* p*, then*

$$\operatorname{ord}_{\mathfrak{q}}(x - y\theta) \geq \min\{\operatorname{ord}_{\mathfrak{q}}(1 - \theta u), t \cdot e(\mathfrak{q}|p)\}.$$

Moreover, if $\operatorname{ord}_{\mathfrak{q}}(1 - \theta u) < t \cdot e(\mathfrak{q}|p)$*, then*

$$\operatorname{ord}_{\mathfrak{q}}(x - y\theta) = \operatorname{ord}_{\mathfrak{q}}(1 - \theta u).$$

Proof of Lemmas 3.3.1 and 3.3.2. Suppose $p \nmid y$. Thus $\operatorname{ord}_{\mathfrak{q}}(y) = 0$ and hence

$$\operatorname{ord}_{\mathfrak{q}}(x - y\theta) = \operatorname{ord}_{\mathfrak{q}}(x/y - \theta).$$

Since $x/y - \theta = u - \theta + x/y - u$, we have

$$\begin{aligned} \operatorname{ord}_{\mathfrak{q}}(x/y - \theta) &= \operatorname{ord}_{\mathfrak{q}}(u - \theta + x/y - u) \\ &\geq \min\{\operatorname{ord}_{\mathfrak{q}}(u - \theta), \operatorname{ord}_{\mathfrak{q}}(x/y - u)\}. \end{aligned}$$

By assumption,

$$\operatorname{ord}_{\mathfrak{q}}(x/y - u) \geq \operatorname{ord}_{\mathfrak{q}}(p^t) = t \cdot e(\mathfrak{q}|p),$$

completing the proof of Lemma 3.3.1. The proof of Lemma 3.3.2 is similar. □

The following algorithm computes the lists L_p and M_p that come from the first patch $p \nmid y$. We denote these respectively by $\mathcal{L}_p$ and $\mathcal{M}_p$.

Algorithm 3.3.3. To compute $\mathcal{L}_p$ and $\mathcal{M}_p$:

Step (1) Let

$$\mathcal{L}_p \leftarrow \emptyset, \qquad \mathcal{M}_p \leftarrow \emptyset,$$

$$t \leftarrow 1, \quad \mathcal{U} \leftarrow \{w : w \in \{0, 1, \ldots, p - 1\}\}.$$

Step (2) Let

$$\mathcal{U}' \leftarrow \emptyset.$$

Loop through the elements $u \in \mathcal{U}$. Let

$$\mathcal{P}_u = \{\mathfrak{q} \text{ lying above } p \ : \ \operatorname{ord}_{\mathfrak{q}}(u-\theta) \geq t \cdot e(\mathfrak{q}|p)\}$$

and

$$\mathfrak{b}_u = \prod_{\mathfrak{q}|p} \mathfrak{q}^{\min\{\operatorname{ord}_{\mathfrak{q}}(u-\theta), t\cdot e(\mathfrak{q}|p)\}} = (u-\theta)\mathcal{O}_K + p^t\mathcal{O}_K.$$

(i) If $\mathcal{P}_u = \emptyset$ then

$$\mathcal{L}_p \leftarrow \mathcal{L}_p \cup \{\mathfrak{b}_u\}.$$

(ii) Else if $\mathcal{P}_u = \{\mathfrak{p}\}$ with $e(\mathfrak{p}|p) = f(\mathfrak{p}|p) = 1$ and there is at least one $\mathbb{Z}_p$-root α of $g(t)$ satisfying $\alpha \equiv u \pmod{p^t}$, then

$$\mathcal{M}_p \leftarrow \mathcal{M}_p \cup \{(\mathfrak{b}_u, \mathfrak{p})\}.$$

(iii) Else

$$\mathcal{U}' \leftarrow \mathcal{U} \cup \{u + p^t w : w \in \{0, \dots, p-1\}\}.$$

Step (3) If $\mathcal{U}' \neq \emptyset$ then let

$$t \leftarrow t+1, \qquad \mathcal{U} \leftarrow \mathcal{U}',$$

and return to Step (2). Else output $\mathcal{L}_p$, $\mathcal{M}_p$.

Lemma 3.3.4. *Algorithm 3.3.3 terminates.*

Proof. Suppose otherwise. Write $t_0 = 1$ and $t_i = t_0 + i$ for $i = 1, 2, 3, \dots$. Then there is an infinite sequence of congruence classes $u_i \mod p^{t_i}$ such that $u_{i+1} \equiv u_i \mod p^{t_i}$, and such that the u_i fail the hypotheses of both (i) and (ii). This means that $\mathcal{P}_{u_i}$ is non-empty for every $i \in \mathbb{N}_{>0}$. By the pigeon-hole principle, some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ appears in infinitely many of the $\mathcal{P}_{u_i}$. Thus $\operatorname{ord}_{\mathfrak{p}}(u_i - \theta) \geq t_i \cdot e(\mathfrak{p}|p)$ infinitely often. However, the sequence $\{u_i\}_{i=1}^{\infty}$ converges to some $\alpha \in \mathbb{Z}_p$ so that $\alpha = \theta$ in $K_{\mathfrak{p}}$. This forces $e(\mathfrak{p}|p) = f(\mathfrak{p}|p) = 1$ and α to be a $\mathbb{Z}_p$-root of $g(t)$. In this case, $\mathfrak{p}$ corresponds to the factor $(t-\alpha)$ in the

p-adic factorisation of $g(t)$. There can be at most one such $\mathfrak{p}$, forcing $\mathcal{P}_{u_i} = \{\mathfrak{p}\}$ for all i. In particular, the hypothesis of (ii) are satisfied and we reach a contradiction. □

Lemma 3.3.5. *Let $p \in \{p_1, \dots, p_v\}$ and let $\mathcal{L}_p$, $\mathcal{M}_p$ be as given by Algorithm 3.3.3. Let $(x, y, z_1, \dots, z_v)$ be a solution to* (3.3). *Then*

- *either there is some $\mathfrak{b} \in \mathcal{L}_p$ such that* (3.6) *is satisfied;*
- *or there is some $(\mathfrak{b}, \mathfrak{p}) \in \mathcal{M}_p$ with $e(\mathfrak{p}|p) = f(\mathfrak{p}|p) = 1$ and integer $v_p \geq 0$ such that* (3.7) *is satisfied.*

Proof. Let

$$t_0 = 1 \quad \text{and} \quad \mathcal{U}_0 = \{w \; : \; w \in \{0, 1, \dots, p-1\}\}$$

be the initial values for t and $\mathcal{U}$ in the algorithm. Then $x/y \equiv u_0 \pmod{p^{t_0}}$ for some $u_0 \in \mathcal{U}_0$. Write $\mathcal{U}_i$ for the value of $\mathcal{U}$ after i iterations of the algorithm and let $t_i = t_0 + i$. As the algorithm terminates, $\mathcal{U}_i = \emptyset$ for some sufficiently large i. Hence there is some i such that $x/y \equiv u_i \mod p^{t_i}$ where $u_i \in \mathcal{U}_i$, but there is no element in $\mathcal{U}_{i+1}$ congruent to x/y modulo $p^{t_{i+1}}$. In other words, u_i must satisfy the hypotheses of either step (i) or (ii) of algorithm 3.3.3. Write $u = u_i$ and $t = t_i$ for $x/y \equiv u \mod p^t$ and consider the ideal $\mathfrak{b}_u$ generated in this step. By Lemma 3.3.1, $\mathfrak{b}_u$ divides $(x - y\theta)\mathcal{O}_K$. Furthermore, by definition of $\mathcal{P}_u$, if $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_K$ not contained in $\mathcal{P}_u$, then $(x - y\theta)\mathcal{O}_K/\mathfrak{b}_u$ is not divisible by $\mathfrak{q}$.

Suppose first that the hypothesis of (i) is satisfied: $\mathcal{P}_u = \emptyset$. The algorithm adds $\mathfrak{b}_u$ to the set $\mathcal{L}_p$, with the above remarks ensuring that (3.6) is satisfied.

Suppose next that the hypothesis of (ii) is satisfied: $\mathcal{P}_u = \{\mathfrak{p}\}$ where $e(\mathfrak{p}|p) = f(\mathfrak{p}|p) = 1$ and there is a unique $\mathbb{Z}_p$ root α of $g(t)$ such that $\alpha \equiv u \mod p^t$. The algorithm adds $(\mathfrak{b}_u, \mathfrak{p})$ to the set $\mathcal{M}_p$. By the above, $(x - y\theta)\mathcal{O}_K/\mathfrak{b}_u$ is an integral ideal, not divisible by any prime ideal $\mathfrak{q} \neq \mathfrak{p}$ lying over p. Thus there is some positive integer $v_p \geq 0$ such that (3.7) is satisfied, concluding the proof. □

Having computed the lists arising from the affine patch $p \nmid y$, we initialize L_p and

M_p as $\mathcal{L}_p$ and $\mathcal{M}_p$, respectively, and append to these lists the elements from the second patch, $p \mid y$, using the following algorithm.

Algorithm 3.3.6. To compute L_p and M_p.

Step (1) Let

$$L_p \leftarrow \mathcal{L}_p, \qquad M_p \leftarrow \mathcal{M}_p,$$

where $\mathcal{L}_p$, $\mathcal{M}_p$ are computed by Algorithm 3.3.3.

Step (2) Let

$$t \leftarrow 2, \qquad \mathcal{U} \leftarrow \{pw \ : \ w \in \{0, 1, \ldots, p-1\}\}.$$

Step (3) Let

$$\mathcal{U}' \leftarrow \emptyset.$$

Loop through the elements $u \in \mathcal{U}$. Let

$$\mathcal{P}_u = \{\mathfrak{q} \text{ lying above } p \ : \ \mathrm{ord}_{\mathfrak{q}}(1 - u\theta) \geq t \cdot e(\mathfrak{q}|p)\},$$

and

$$\mathfrak{b}_u = \prod_{\mathfrak{q}|p} \mathfrak{q}^{\min\{\mathrm{ord}_{\mathfrak{q}}(1-u\theta), t \cdot e(\mathfrak{q}|p)\}} = (1 - u\theta)\mathcal{O}_K + p^t \mathcal{O}_K.$$

(i) If $\mathcal{P}_u = \emptyset$ then

$$L_p \leftarrow L_p \cup \{\mathfrak{b}_u\}.$$

(ii) Else

$$\mathcal{U}' \leftarrow \mathcal{U}' \cup \{u + p^t w : w \in \{0, \ldots, p-1\}\}.$$

Step (4) If $\mathcal{U}' \neq \emptyset$ then let

$$t \leftarrow t + 1, \qquad \mathcal{U} \leftarrow \mathcal{U}',$$

and return to Step (3). Else output L_p, M_p.

Lemma 3.3.7. *Algorithm 3.3.6 terminates.*

Proof. Suppose that the algorithm does not terminate. Let $t_0 = 2$ and $t_i = t_0 + i$

for $i \in \mathbb{N}$. Then there is an infinite sequence of congruence classes $\{u_i\}_{i=0}^{\infty}$ and corresponding sets $\{\mathcal{P}_{u_i}\}_{i=0}^{\infty}$ such that $u_{i+1} \equiv u_i \mod t_i$ and $\mathcal{P}_{u_i} \neq \emptyset$ for all i. Moreover, $p \mid u_0$. Let α be the limit of $\{u_i\}_{i=0}^{\infty}$ in $\mathbb{Z}_p$. By the pigeon-hole principle, there is some ideal $\mathfrak{q}$ in $\mathcal{O}_K$ above p which appears in infinitely many sets $\mathcal{P}_{u_i}$. It follows that $\text{ord}_{\mathfrak{q}}(1 - u_i\theta) \geq t_i \cdot e(\mathfrak{q}|p)$ and thus $1 - \alpha\theta = 0$ in $K_{\mathfrak{q}}$. But as $p \mid u_0$, we have $\text{ord}_p(\alpha) \geq 1$, and so $\text{ord}_{\mathfrak{q}}(\theta) < 0$. This contradicts the fact that θ is an algebraic integer. Therefore the algorithm must terminate. □

Lemma 3.3.8. *Let $p \in \{p_1, \ldots, p_v\}$ and let L_p, M_p be as given by Algorithm 3.3.6. Let $(x, y, z_1, \ldots, z_v)$ be a solution to* (3.3). *Then*

- *either there is some $\mathfrak{b} \in L_p$ such that* (3.6) *is satisfied;*
- *or there is some $(\mathfrak{b}, \mathfrak{p}) \in M_p$ with $e(\mathfrak{p}|p) = f(\mathfrak{p}|p) = 1$ and integer $v_p \geq 0$ such that* (3.7) *is satisfied.*

Proof. Let $(x, y, z_1, \ldots, z_v)$ be a solution to (3.3). In view of Lemma 3.3.5 we may suppose $p \mid y$. Then $\text{ord}_{\mathfrak{q}}(x) = 0$ and $\text{ord}_{\mathfrak{q}}(x - y\theta) = \text{ord}_{\mathfrak{q}}(1 - (y/x)\theta)$ for any prime ideal $\mathfrak{q}$ lying over p. The remainder of the proof is analogous to the proof of Lemma 3.3.5. □

3.3.1 Computational remarks and refinements

In implementing Algorithms 3.3.3 and 3.3.6, we reduce the number of prime ideals appearing in the factorization of $(x - y\theta)\mathcal{O}_K$ to a large power. The Prime Ideal Removing Lemma, as originally stated in Tzanakis - de Weger outlines a similar process by comparing the valuations of $(x - y\theta)\mathcal{O}_K$ at two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ above p. Of course if $\mathfrak{p}_1 \mid (x - y\theta)\mathcal{O}_K$, we restrict the possible values for x and y modulo p. However any choice of x and y modulo p affects the valuations of $(x - y\theta)\mathcal{O}_K$ at all prime ideals above p. In the present refinement outlined by Lemma 3.3.1 and Lemma 3.3.2, we instead study the valuations of $(x - y\theta)\mathcal{O}_K$ at all prime ideals above p simultaneously. This presents us with considerably less ideal equations of the form 3.5 to resolve.

Moreover, this variant of the Prime Ideal Removing Lemma permits the following additional refinements:

- Let $\mathfrak{b} \in L_p$. If there exists a pair $(\mathfrak{b}', \mathfrak{p}) \in M_p$ with $\mathfrak{b}' \mid \mathfrak{b}$ and $\mathfrak{b}/\mathfrak{b}' = \mathfrak{p}^w$ for some $w \geq 0$, then we may delete $\mathfrak{b}$ from L_p. In doing so, the conclusion to Lemma 3.3.8 continues to hold.
- Suppose $(\mathfrak{b}, \mathfrak{p}), (\mathfrak{b}', \mathfrak{p}) \in M_p$ with $\mathfrak{b}' \mid \mathfrak{b}$, and $\mathfrak{b}/\mathfrak{b}' = \mathfrak{p}^w$ for some $w \geq 0$. Then, we may delete $(\mathfrak{b}, \mathfrak{p})$ from M_p without affecting the conclusion to Lemma 3.3.8.

3.4 Factorization of the Thue-Mahler equation

After applying Algorithm 3.3.3 and Algorithm 3.3.6, we are reduced to solving finitely many ideal equations of the form

$$(x - y\theta)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{u_1} \cdots \mathfrak{p}_\nu^{u_\nu} \tag{3.8}$$

in integer variables $x, y, u_1, \dots, u_\nu$ with $u_i \geq 0$ for $i = 1, \dots, \nu$, where $0 \leq \nu \leq v$. Here

- for $i \in \{1, \dots, \nu\}$, $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_K$ arising from Algorithm 3.3.3 and Algorithm 3.3.6 applied to $p \in \{p_1, \dots, p_v\}$, such that $(\mathfrak{b}, \mathfrak{p}_i) \in M_p$ for some ideal $\mathfrak{b}$;
- for $i \in \{\nu + 1, \dots, v\}$, the corresponding rational prime $p_i \in S$ yields $M_{p_i} = \emptyset$, in which case we set $u_i = 0$;
- $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ of norm $|c| \cdot p_1^{t_1} \cdots p_v^{t_v}$ such that $u_i + t_i = z_i$.

For each choice of $\mathfrak{a}$ and prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_\nu$, we reduce equation (3.8) to a number of so-called "S-unit equations". We present two different algorithms for doing so and outline the advantages and disadvantages of each. In practicality, we do not know a priori which of these two options is more efficient. Instead, we implement and use both algorithms simultaneously and selecting the most computationally efficient option as it appear.

3.4.1 Avoiding the class group $\mathrm{Cl}(K)$

For $i = 1, \ldots, \nu$ let h_i be the smallest positive integer for which $\mathfrak{p}_i^{h_i}$ is principal and let r_i be a positive integer satisfying $0 \leq r_i < h_i$. Let

$$\mathbf{a}_i = (a_{1i}, \ldots, a_{\nu i}).$$

where $a_{ii} = h_i$ and $a_{ji} = 0$ for $j \neq i$. We let A be the matrix with columns $\mathbf{a}_1, \ldots, \mathbf{a}_\nu$. Hence A is a $\nu \times \nu$ diagonal matrix over $\mathbb{Z}$ with diagonal entries h_i. Now, if (3.8) has a solution $\mathbf{u} = (u_1, \ldots, u_\nu)$, it necessarily must be of the form $\mathbf{u} = A\mathbf{n} + \mathbf{r}$, where $\mathbf{n} = (n_1, \ldots, n_\nu)$ and $\mathbf{r} = (r_1, \ldots, r_\nu)$. The vector $\mathbf{n}$ is comprised of integers n_i which we solve for. The vector $\mathbf{r}$ is comprised of the values r_i satisfying $0 \leq r_i < h_i$ for $i = 1, \ldots, \nu$.

Using the above notation, we let

$$\mathfrak{c}_i = \tilde{\mathfrak{p}}^{\mathbf{a}_i} = \mathfrak{p}_1^{a_{1i}} \cdot \mathfrak{p}_2^{a_{2i}} \cdots \mathfrak{p}_\nu^{a_{\nu i}} = \mathfrak{p}_i^{h_i}$$

for all $i \in \{1, \ldots, \nu\}$.

Thus, we can write (3.8) as

$$(x - y\theta)\mathcal{O}_K = \mathfrak{a}\tilde{\mathfrak{p}}^{\mathbf{u}} = (\mathfrak{a} \cdot \tilde{\mathfrak{p}}^{\mathbf{r}}) \cdot \mathfrak{c}_1^{n_1} \cdots \mathfrak{c}_\nu^{n_\nu}.$$

By definition of h_i, each $i \in \{1, \ldots, \nu\}$ yields an element $\gamma_i \in K^*$ such that

$$\mathfrak{c}_i = (\gamma_i)\mathcal{O}_K.$$

Furthermore, if $\mathbf{u}$ is a solution of (3.8) with corresponding vectors $\mathbf{n}, \mathbf{r}$, there exists some $\alpha \in K^*$ such that

$$\mathfrak{a} \cdot \tilde{\mathfrak{p}}^{\mathbf{r}} = (\alpha)\mathcal{O}_K.$$

3.4.2 Using the class group $\mathrm{Cl}(K)$

Let $\mathbf{u} = (u_1, \ldots, u_\nu)$ be a solution of (3.8) and consider the map

$$\phi : \mathbb{Z}^\nu \to \mathrm{Cl}(K), \qquad (x_1, \ldots, x_\nu) \mapsto [\mathfrak{p}_1]^{x_1} \cdots [\mathfrak{p}_\nu]^{x_\nu},$$

where $[\mathfrak{q}]$ denotes the equivalence class of the fractional ideal $\mathfrak{q}$. Since the product of $\mathfrak{a}$ and $\mathfrak{p}_1^{u_1} \cdots \mathfrak{p}_\nu^{u_\nu}$ defines a principal ideal, the map ϕ implies

$$\phi(\mathbf{u}) = [\mathfrak{a}]^{-1}.$$

In particular, if $[\mathfrak{a}]^{-1}$ does not belong to the image of ϕ then (3.8) has no solutions. We therefore suppose that $[\mathfrak{a}]^{-1}$ belongs to the image. Let $\mathbf{r} = (r_1, \ldots, r_\nu)$ denote a preimage of $[\mathfrak{a}]^{-1}$ and observe that $\mathbf{u} - \mathbf{r}$ belongs to the kernel of ϕ. The kernel is a subgroup of $\mathbb{Z}^v$ of rank ν. Let $\mathbf{a}_1, \ldots, \mathbf{a}_\nu$ be a basis for the kernel, where

$$\mathbf{a}_i = (a_{1i}, \ldots, a_{\nu i}) \quad \text{for } i = 1, \ldots, \nu.$$

Let

$$\mathbf{u} - \mathbf{r} = n_1 \mathbf{a}_1 + \cdots + n_\nu \mathbf{a}_\nu$$

for some integers $n_i \in \mathbb{Z}$ and let A denote the $\nu \times \nu$ matrix over $\mathbb{Z}$ with columns $\mathbf{a}_1, \ldots, \mathbf{a}_\nu$. It follows that $\mathbf{u} = A\mathbf{n} + \mathbf{r}$ where $\mathbf{n} = (n_1, \ldots, n_\nu)$.

For $\mathbf{a}_i = (a_{1i}, \ldots, a_{\nu i}) \in \mathbb{Z}^\nu$, we adopt the notation

$$\tilde{\mathfrak{p}}^{\mathbf{a}} := \mathfrak{p}_1^{a_{1i}} \cdot \mathfrak{p}_2^{a_{2i}} \cdots \mathfrak{p}_\nu^{a_{\nu i}}.$$

Let

$$\mathfrak{c}_1 = \tilde{\mathfrak{p}}^{\mathbf{a}_1}, \ldots, \mathfrak{c}_\nu = \tilde{\mathfrak{p}}^{\mathbf{a}_\nu}.$$

Thus, we can rewrite (3.8) as

$$(x - y\theta)\mathcal{O}_K = \mathfrak{a}\tilde{\mathfrak{p}}^{\mathbf{u}} = (\mathfrak{a} \cdot \tilde{\mathfrak{p}}^{\mathbf{r}}) \cdot \mathfrak{c}_1^{n_1} \cdots \mathfrak{c}_\nu^{n_\nu}.$$

Consider the ideal equivalence class of $(\mathfrak{a} \cdot \tilde{\mathfrak{p}}^{\mathbf{r}})$ in $\mathrm{Cl}(K)$ and note that

$$[\mathfrak{a} \cdot \tilde{\mathfrak{p}}^{\mathbf{r}}] = [\mathfrak{a}] \cdot [\mathfrak{p}_1]^{r_1} \cdots [\mathfrak{p}_\nu]^{r_\nu} = [\mathfrak{a}] \cdot \phi(r_1, \ldots, r_\nu) = [1]$$

as $\phi(r_1, \ldots, r_\nu) = [\mathfrak{a}]^{-1}$ by construction. This means

$$\mathfrak{a} \cdot \tilde{\mathfrak{p}}^{\mathbf{r}} = (\alpha)\mathcal{O}_K$$

for some $\alpha \in K^*$. Furthermore,

$$[\mathfrak{c}_i] = [\tilde{\mathfrak{p}}^{\mathbf{a}_i}] = \phi(\mathbf{a}_i) = [1] \quad \text{for } i = 1, \ldots, \nu,$$

as the $\mathbf{a}_i$ are a basis for the kernel of ϕ. For all $i \in \{1, \ldots, \nu\}$, we therefore have

$$\mathfrak{c}_i = (\gamma_i)\mathcal{O}_K$$

for some $\gamma_i \in K^*$.

3.4.3 The S-unit equation

Section 3.4.1 and Section 3.4.2 outline two different algorithms to reduce the ideal equation (3.8) to a number of certain "S-unit equations", which we define shortly. Regardless of which method we use, under both algorithms outlined above, equation (3.8) becomes

$$(x - y\theta)\mathcal{O}_K = (\alpha \cdot \gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu})\mathcal{O}_K \tag{3.9}$$

for some vector $\mathbf{n} = (n_1, \ldots, n_\nu) \in \mathbb{Z}^\nu$. The ideal generated by α in K has norm

$$|c| \cdot p_1^{t_1 + r_1} \cdots p_\nu^{t_\nu + r_\nu} p_{\nu+1}^{t_{\nu+1}} \cdots p_v^{t_v}$$

and the n_i are related to the z_i via

$$z_i = u_i + t_i = \sum_{j=1}^{\nu} n_j a_{ij} + r_i + t_i \quad \text{for } i = 1, \ldots, v.$$

where $u_i = r_i = 0$ for all $i \in \{\nu+1, \ldots, v\}$.

Fix a complete set of fundamental units $\{\varepsilon_1, \ldots, \varepsilon_r\}$ of $\mathcal{O}_K$. Here $r = s + t - 1$, where s denotes the number of real embeddings of K into $\mathbb{C}$ and t denotes the number of complex conjugate pairs of non-real embeddings of K into $\mathbb{C}$. Then, under either method, equation (3.8) reduces to a finite number of equations in K of the form

$$x - y\theta = \alpha\zeta\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}\gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu} \tag{3.10}$$

with unknowns $a_i \in \mathbb{Z}$, $n_i \in \mathbb{Z}$, and ζ in the set T of roots of unity in $\mathcal{O}_K$. Since T is finite, we treat ζ as another parameter.

Let $p \in \{p_1, \ldots, p_v, \infty\}$. Recall that $g(t)$ is an irreducible polynomial in $\mathbb{Z}[t]$ arising from (3.3) such that

$$g(t) = f(t, 1) = t^n + C_1 t^{n-1} + \cdots + C_{n-1}t + C_n.$$

Denote the roots of $g(t)$ in $\overline{\mathbb{Q}_p}$ (where $\overline{\mathbb{Q}_\infty} = \overline{\mathbb{R}} = \mathbb{C}$) by $\theta^{(1)}, \ldots, \theta^{(n)}$. Let $i_0, j, k \in \{1, \ldots, n\}$ be distinct indices and consider the three embeddings of K into $\overline{\mathbb{Q}_p}$ defined by $\theta \mapsto \theta^{(i_0)}, \theta^{(j)}, \theta^{(k)}$. We use $z^{(i)}$ to denote the image of z under the embedding $\theta \mapsto \theta^{(i)}$. From the Siegel identity

$$(\theta^{(i_0)} - \theta^{(j)})(x - y\theta^{(k)}) + (\theta^{(j)} - \theta^{(k)})(x - y\theta^{(i_0)}) + (\theta^{(k)} - \theta^{(i_0)})(x - y\theta^{(j)}) = 0,$$

applying the embeddings to $\beta = x - y\theta$ yields the so-called "S-unit equation"

$$\delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i} - 1 = \delta_2 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i}, \tag{3.11}$$

where

$$\delta_1 = \frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \cdot \frac{\alpha^{(k)}\zeta^{(k)}}{\alpha^{(j)}\zeta^{(j)}}, \quad \delta_2 = \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\alpha^{(i_0)}\zeta^{(i_0)}}{\alpha^{(j)}\zeta^{(j)}}$$

are constants.

To summarize, our original problem of solving (3.3) for $(x, y, z_1, \dots, z_v)$ has been reduced to solving finitely many equations of the form (3.11) for the variables $(x, y, n_1, \dots, n_\nu, a_1, \dots, a_r)$.

3.4.4 Computational remarks and comparisons

In Section 3.4.1, we follow closely the method of [112] to reduce the ideal equation (3.8) to the S-unit equation (3.11). To implement this reduction, we begin by computing all h_i for which $\mathfrak{p}_i^{h_i}$ is principal for $i = 1, \dots, \nu$. In doing so, we generate all possible values for r_i, the non-negative integer satisfying $0 \leq r_i < h_i$. We then generate every possible vector $\mathbf{r} = (r_1, \dots, r_\nu)$ and test the corresponding ideal product $\mathfrak{a} \cdot \tilde{\mathfrak{p}}^{\mathbf{r}}$ for principality. Those vectors which pass this test yield an S-unit equation (3.11). In the worst case scenario, this method reduces to h_K^ν such equations, where h_K is the class number of K. Moreover, this process needs to be applied to every ideal equation (3.8), yielding what may be a very large number of principalization tests and subsequent large number of S-unit equations to solve.

In contrast, the method in Section 3.4.2 reduces (3.8) to only $\#T/2$ S-unit equations to solve, where T is the set of roots of unity in K. In particular, the sum total of S-unit equations does not drastically increase. If $[\mathbf{a}]^{-1}$ is not in the image of ϕ, we reach a contradiction. If $[\mathbf{a}]^{-1}$ is in the image of ϕ then we obtain only $\#T/2$ corresponding equations (3.11). In particular, the number of principalization tests in this method is limited by the number of ideal equations (3.8), where each such equation yields only $(1 + \nu)$ tests.

However, when generating the vectors $\mathbf{r} = (r_1, \dots, r_\nu)$ using the class group, we observe that some of the integers r_i may be negative, so we do not expect α to be an algebraic integer in general. This can be problematic later in the algorithm when we compute the embedding of K into our p-adic fields. In those instances, the precision on our p-adic fields may not be high enough, and as a result, some non-zero elements of K may be erroneously mapped to 0. To avoid this, we force the r_i to be positive by adding sufficiently many multiples of the class number.

In most cases, the method described in Section 3.4.2 is far more efficient than that of Section 3.4.1. However, computing the class group may be a very costly computation. Indeed, for some Thue-Mahler equations, this may be the bottle-neck of the algorithm. In this case, it may happen that computing the class group will take longer than directly checking each potential S-unit equation arising from the alternative method. Unfortunately, we cannot know a piori how long computing $\mathrm{Cl}(K)$ will take in so much that we cannot know a priori how long solving all S-unit equations from the other algorithm will take. In practicality, generating the class group in Magma is a process which cannot be terminated without exiting the program. For this reason, we cannot simply apply a timeout in Magma if computing $\mathrm{Cl}(K)$ is exceeding what we deem a reasonable amount of time. Adding to this, Magma does not support parallelization, so we cannot implement both algorithms simultaneously. Our compromise to solve a single Thue-Mahler equation is to run two separate instances of Magma in parallel, each generating the S-unit equations using the two aforementioned algorithms. When one of these instances finishes, the other is forced to terminate. In this way, though far from ideal, we are able to select the most computationally efficient option.

3.5 A small upper bound for u_l in a special case

We now restrict our attention to those $p \in \{p_1, \dots, p_\nu\}$ and study the p-adic valuations of the numbers appearing in (3.11). In particular, for $l \in \{1, \dots, \nu\}$, we identify conditions in which $\sum_{j=1}^{\nu} n_j a_{lj}$ can be bounded by a small explicit constant, where a_{lj} is the $(l,j)^{\text{th}}$ entry of the matrix A derived in either Section 3.4.1 or Section 3.4.2. Recall that $u_l + r_l = \sum_{j=1}^{\nu} n_j a_{lj}$, where r_l is known, so that a bound on $\sum_{j=1}^{\nu} n_j a_{lj}$ yields a bound on the exponent u_l in (3.8).

Fix a rational prime $p_l \in \{p_1, \dots, p_\nu\}$ and recall that $z \in \mathbb{C}_{p_l}$ having $\mathrm{ord}_{p_l}(z) = 0$ is called a p_l-adic unit. Part (i) of the Corollary of Lemma 7.2 of [112] tells us that $\frac{\varepsilon_1^{(i_0)}}{\varepsilon_1^{(j)}}, \dots, \frac{\varepsilon_r^{(i_0)}}{\varepsilon_r^{(j)}}$ and $\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}, \dots, \frac{\varepsilon_r^{(k)}}{\varepsilon_r^{(j)}}$ are p_l-adic units.

Let $g_l(t)$ be the irreducible factor of $g(t)$ in $\mathbb{Q}_{p_l}[t]$ corresponding to the prime ideal $\mathfrak{p}_l$. Since $\mathfrak{p}_l$ has ramification index and residue degree equal to 1, $\deg(g_l(t)) = 1$.

We now choose $i_0 \in \{1, \ldots, 4\}$ so that $\theta^{(i_0)}$ is the root of $g_l(t)$. We fix this choice of index i_0 for the remainder of this chapter. The indices of j, k are fixed, but arbitrary.

Lemma 3.5.1.

(i) Let $i \in \{1, \ldots, \nu\}$. Then $\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}$ are p_l-adic units.

(ii) Let $i \in \{1, \ldots, \nu\}$. Then $\mathrm{ord}_{p_l}\left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right) = a_{li}$, where $\mathbf{a_i} = (a_{1i}, \ldots, a_{vi})$ is the i^{th} column of the matrix A of either Section 3.4.1 or Section 3.4.2.

Proof. Consider the factorization $g(t) = g_1(t) \cdots g_m(t)$ of $g(t)$ in $\mathbb{Q}_{p_l}[t]$. Note that $\theta^{(j)}$ is a root of some $g_h(t) \neq g_l(t)$. Let $\mathfrak{p}_h$ be the corresponding prime ideal above p_l and $e(\mathfrak{p}_h|p_l)$ be its ramification index. Then $\mathfrak{p} \neq \mathfrak{p}_l$ and since

$$(\gamma_i)\mathcal{O}_K = \mathfrak{p}_1^{a_{1i}} \cdots \mathfrak{p}_v^{a_{vi}},$$

we have

$$\mathrm{ord}_{p_l}(\gamma_i^{(j)}) = \frac{1}{e(\mathfrak{p}_h|p_l)}\,\mathrm{ord}_{\mathfrak{p}_h}(\gamma_i) = 0.$$

An analogous argument gives $\mathrm{ord}_{p_l}(\gamma_i^{(k)}) = 0$. On the other hand,

$$\mathrm{ord}_{p_l}(\gamma_i^{(i_0)}) = \frac{1}{e(\mathfrak{p}_l|p_l)}\,\mathrm{ord}_{\mathfrak{p}_l}(\gamma_i) = \mathrm{ord}_{\mathfrak{p}_l}(\mathfrak{p}_1^{a_{1i}} \cdots \mathfrak{p}_v^{a_{vi}}) = a_{li}.$$

□

The next lemma deals with a special case in which the sum $\sum_{j=1}^{\nu} n_j a_{lj}$ can be computed directly. This lemma is analogous to Lemma 7.3 of [112].

Recall the constants

$$\delta_1 = \frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \cdot \frac{\alpha^{(k)}\zeta^{(k)}}{\alpha^{(j)}\zeta^{(j)}}, \quad \delta_2 = \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\alpha^{(i_0)}\zeta^{(i_0)}}{\alpha^{(j)}\zeta^{(j)}}$$

of (3.11).

Lemma 3.5.2. *Let* $l \in \{1, \ldots, v\}$. *If* $\mathrm{ord}_{p_l}(\delta_1) \neq 0$, *then*

$$\sum_{i=1}^{\nu} n_i a_{li} = \min\{\mathrm{ord}_{p_l}(\delta_1), 0\} - \mathrm{ord}_{p_l}(\delta_2).$$

Proof. Apply the Corollary of Lemma 7.2 of [112] and Lemma 3.5.1 to both expressions of λ in (3.11). On the one hand, we obtain that $\mathrm{ord}_{p_l}(\lambda) = \min\{\mathrm{ord}_{p_l}(\delta_1), 0\}$, and on the other hand,

$$\begin{aligned} \mathrm{ord}_{p_l}(\lambda) &= \mathrm{ord}_{p_l}(\delta_2) + \sum_{i=1}^{\nu} \mathrm{ord}_{p_l} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}} \right)^{n_i} \\ &= \mathrm{ord}_{p_l}(\delta_2) + \sum_{i=1}^{\nu} n_i a_{li}. \end{aligned}$$

$\square$

For the remainder of this section, we assume $\mathrm{ord}_{p_l}(\delta_1) = 0$. Here, it is convenient to use the notation

$$b_1 = 1, \quad b_{1+i} = n_i \text{ for } i \in \{1, \ldots, \nu\},$$

and

$$b_{1+\nu+i} = a_i \text{ for } i \in \{1, \ldots, r\}.$$

Put

$$\alpha_1 = \log_{p_l} \delta_1, \quad \alpha_{1+i} = \log_{p_l} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}} \right) \text{ for } i \in \{1, \ldots, \nu\},$$

and

$$\alpha_{1+\nu+i} = \log_{p_l} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}} \right) \text{ for } i \in \{1, \ldots, r\}.$$

Define

$$\Lambda_l = \sum_{i=1}^{1+\nu+r} b_i \alpha_i.$$

Let L be a finite extension of $\mathbb{Q}_{p_l}$ containing $\delta_1, \frac{\gamma_1^{(k)}}{\gamma_1^{(j)}}, \ldots, \frac{\gamma_\nu^{(k)}}{\gamma_\nu^{(j)}}$, and $\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}, \ldots, \frac{\varepsilon_r^{(k)}}{\varepsilon_r^{(j)}}$. Since finite p_l-adic fields are complete, $\alpha_i \in L$ for $i = 1, \ldots, 1 + \nu + r$ as well. Choose $\phi \in \overline{\mathbb{Q}_{p_l}}$ such that $L = \mathbb{Q}_{p_l}(\phi)$ and $\operatorname{ord}_{p_l}(\phi) > 0$. Let $G(t)$ be the minimal polynomial of ϕ over $\mathbb{Q}_{p_l}$ and let s be its degree. For $i = 1, \ldots, 1+\nu+r$ write

$$\alpha_i = \sum_{h=1}^{s} \alpha_{ih}\phi^{h-1}, \quad \alpha_{ih} \in \mathbb{Q}_{p_l}.$$

Then

$$\Lambda_l = \sum_{h=1}^{s} \Lambda_{lh}\phi^{h-1}, \tag{3.12}$$

with

$$\Lambda_{lh} = \sum_{i=1}^{1+\nu+r} b_i\alpha_{ih}$$

for $h = 1, \ldots, s$.

Lemma 3.5.3. *For every $h \in \{1, \ldots, s\}$, we have*

$$\operatorname{ord}_{p_l}(\Lambda_{lh}) > \operatorname{ord}_{p_l}(\Lambda_l) - \frac{1}{2}\operatorname{ord}_{p_l}(\mathit{Disc}(G(t))).$$

Proof. Taking the images of (3.12) under conjugation $\phi \mapsto \phi^{(h)}$ $(h = 1, \ldots, s)$ yields

$$\begin{bmatrix} \Lambda_l^{(1)} \\ \vdots \\ \Lambda_l^{(s)} \end{bmatrix} = \begin{bmatrix} 1 & \phi^{(1)} & \cdots & \phi^{(1)s-1} \\ \vdots & \vdots & & \vdots \\ 1 & \phi^{(s)} & \cdots & \phi^{(s)s-1} \end{bmatrix} \begin{bmatrix} \Lambda_{l1} \\ \vdots \\ \Lambda_{ls} \end{bmatrix}$$

The $s \times s$ matrix $(\phi^{(h)i-1})$ above is invertible, with inverse

$$\frac{1}{\displaystyle\prod_{1 \le j < k \le s} (\phi^{(k)} - \phi^{(j)})} \begin{bmatrix} \gamma_{11} & \cdots & \gamma_{1s} \\ \vdots & & \vdots \\ \gamma_{s1} & \cdots & \gamma_{ss} \end{bmatrix},$$

where γ_{jk} is an integral polynomial in the entries of $(\phi^{(h)i-1})$. Since $\operatorname{ord}_{p_l}(\phi) > 0$ and $\operatorname{ord}_{p_l}(\phi^{(h)}) = \operatorname{ord}_{p_l}(\phi)$ for all $h = 1, \ldots, s$, it follows that $\operatorname{ord}_{p_l}(\gamma_{jk}) > 0$ for every γ_{jk}. Therefore, as

$$\Lambda_{lh} = \frac{1}{\prod_{1 \le j < k \le s} (\phi^{(k)} - \phi^{(j)})} \sum_{i=1}^{s} \gamma_{hi} \Lambda_l^{(i)},$$

we have

$$\begin{aligned}
\operatorname{ord}_{p_l}(\Lambda_{lh}) &= \min_{1 \le i \le s} \left\{ \operatorname{ord}_{p_l}(\gamma_{hi}) + \operatorname{ord}_{p_l}(\Lambda_l^{(i)}) \right\} - \frac{1}{2} \operatorname{ord}_{p_l}(\text{Disc}(G(t))) \\
&\ge \min_{1 \le i \le s} \operatorname{ord}_{p_l}(\Lambda_l^{(i)}) + \min_{1 \le i \le s} \operatorname{ord}_{p_l}(\gamma_{hi}) - \frac{1}{2} \operatorname{ord}_{p_l}(\text{Disc}(G(t))) \\
&= \operatorname{ord}_{p_l} \Lambda_l + \min_{1 \le i \le s} \operatorname{ord}_{p_l}(\gamma_{hi}) - \frac{1}{2} \operatorname{ord}_{p_l}(\text{Disc}(G(t)))
\end{aligned}$$

for every $h \in \{1, \ldots, s\}$. □

Lemma 3.5.4. *If*

$$\sum_{i=1}^{\nu} n_i a_{li} > \frac{1}{p_l - 1} - \operatorname{ord}_{p_l}(\delta_2),$$

then

$$\operatorname{ord}_{p_l}(\Lambda_l) = \sum_{i=1}^{\nu} n_i a_{li} + \operatorname{ord}_{p_l}(\delta_2).$$

Proof. Immediate from Lemma 2.3.2. □

Lemma 3.5.5.

(i) If $\operatorname{ord}_{p_l}(\alpha_1) < \min_{2 \le i \le 1+\nu+r} \operatorname{ord}_{p_l}(\alpha_i)$*, then*

$$\sum_{i=1}^{\nu} n_i a_{li} \le \max \left\{ \left\lfloor \frac{1}{p_l - 1} - \operatorname{ord}_{p_l}(\delta_2) \right\rfloor, \left\lceil \min_{2 \le i \le 1+\nu+r} \operatorname{ord}_{p_l}(\alpha_i) - \operatorname{ord}_{p_l}(\delta_2) \right\rceil - 1 \right\}$$

(ii) For all $h \in \{1, \ldots, s\}$*, if* $\operatorname{ord}_{p_l}(\alpha_{1h}) < \min_{2 \le i \le 1+\nu+r} \operatorname{ord}_{p_l}(\alpha_{ih})$*, then*

$$\sum_{i=1}^{\nu} n_i a_{li} \le \max \left\{ \left\lfloor \frac{1}{p_l - 1} - \operatorname{ord}_{p_l}(\delta_2) \right\rfloor, \left\lceil \min_{2 \le i \le 1+\nu+r} \operatorname{ord}_{p_l}(\alpha_{ih}) - \operatorname{ord}_{p_l}(\delta_2) + w_l \right\rceil - 1 \right\},$$

where
$$w_l = \frac{1}{2}\operatorname{ord}_{p_l}(\textit{Disc}(G(t))).$$

Proof.

(i) We prove the contrapositive. Suppose
$$\sum_{i=1}^{\nu} n_i a_{li} > \frac{1}{p_l - 1} - \operatorname{ord}_{p_l}(\delta_2),$$
and
$$\sum_{i=1}^{\nu} n_i a_{li} \geq \min_{2\leq i\leq 1+\nu+r} \operatorname{ord}_{p_l}(\alpha_i) - \operatorname{ord}_{p_l}(\delta_2).$$
Observe that
$$\begin{aligned}\operatorname{ord}_{p_l}(\alpha_1) &= \operatorname{ord}_{p_l}\left(\Lambda_l - \sum_{i=2}^{1+\nu+r} b_i\alpha_i\right)\\ &\geq \min\left\{\operatorname{ord}_{p_l}(\Lambda_l), \min_{2\leq i\leq 1+\nu+r}\operatorname{ord}_{p_l}(b_i\alpha_i)\right\}.\end{aligned}$$
Therefore, it suffices to show that
$$\operatorname{ord}_{p_l}(\Lambda_l) \geq \min_{2\leq i\leq 1+\nu+r}\operatorname{ord}_{p_l}(b_i\alpha_i).$$
By Lemma 2.3.2, the first inequality implies $\operatorname{ord}_{p_l}(\Lambda_l) = \sum_{i=1}^{\nu} n_i a_{li} + \operatorname{ord}_{p_l}(\delta_2)$, from which the result follows.

(ii) Similar to the proof of (i).

$\square$

3.6 Lattice-Based Reduction

At this point in solving the Thue-Mahler equation, we proceed to solve each S-unit equation (3.11) for the exponents $(n_1, \ldots, n_\nu, a_1, \ldots, a_r)$. To do so, we generate a very large upper bound on the exponents and reduce this bound via Diophantine approximation computations. The specific details of this process are described in Chapter 6 and Chapter 4. In general, from each S-unit equation, we generate several linear forms in logarithms to which we associate an integral lattice Γ. It will be important in this reduction process to enumerate all short vectors in these lattices. In this section, we describe two algorithms used in the short vector enumeration process.

3.6.1 The L^3-lattice basis reduction algorithm

Let Γ be an n-dimensional lattice with basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ equipped with a bilinear form $\Phi : \Gamma \times \Gamma \to \mathbb{Z}$. Recall that Φ defines a norm on Γ via the usual inner product on $\mathbb{R}^n$. For $i = 1, \ldots, n$, define the vectors $\mathbf{b}_i^*$ inductively by

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^*, \quad \mu_{ij} = \frac{\Phi(\mathbf{b}_i, \mathbf{b}_j^*)}{\Phi(\mathbf{b}_j^*, \mathbf{b}_j)},$$

where $\mu_{ij} \in \mathbb{R}$ for $1 \leq j < i \leq n$. This is the usual Gram-Schmidt process. The basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called *LLL-reduced* if

$$|\mu_{ij}| \leq \frac{1}{2} \quad \text{for } 1 \leq j < i \leq n,$$

$$\frac{3}{4} |\mathbf{b}_{i-1}^*|^2 \leq |\mathbf{b}_i^* + \mu_{ii-1} \mathbf{b}_{i-1}^*|^2 \quad \text{for } 1 < i \leq n,$$

where $|\cdot|$ is the usual Euclidean norm in $\mathbb{R}^n$,

$$|\mathbf{v}| = \Phi(\mathbf{v}, \mathbf{v}) = \mathbf{v}^T \mathbf{v}.$$

These properties imply that an LLL-reduced basis is approximately orthogonal, and that, generically, its constituent vectors are roughly of the same length. Every n-dimensional lattice has an LLL-reduced basis and such a basis can be computed very quickly using the so-called LLL algorithm ([63]). This algorithm takes as input an arbitrary basis for a lattice and outputs an LLL-reduced basis. The algorithm is typically modified to additionally output a unimodular matrix U such that $A = BU$, where B is the matrix whose column-vectors are the input basis and A is the matrix whose column-vectors are the LLL-reduced output basis. Several versions of this algorithm are implemented in Magma, including de Weger's exact integer version. ([114]).

We remark that a lattice may have more than one reduced basis, and that the ordering of the basis vectors is not arbitrary. The properties of reduced bases that are of most interest to us are the following. Let $\mathbf{v}$ a vector in $\mathbb{R}^n$ and denote by $l(\Gamma, \mathbf{v})$ the distance from $\mathbf{v}$ to the nearest point in the lattice Γ, viz.

$$l(\Gamma, \mathbf{v}) = \min_{\mathbf{u} \in \Gamma \setminus \{\mathbf{v}\}} |\mathbf{u} - \mathbf{v}|.$$

From an LLL-reduced basis for Γ, we can compute lower bounds for $l(\Gamma, \mathbf{v})$, according to the following results.

Lemma 3.6.1. *Let Γ be a lattice with LLL-reduced basis $\mathbf{c}_1, \ldots, \mathbf{c}_n$ and let $\mathbf{v}$ be a vector in $\mathbb{R}^n$.*

(a) If $\mathbf{v} = \mathbf{0}$, then $l(\Gamma, \mathbf{v}) \geq 2^{-(n-1)/2} |\mathbf{c}_1|$.

(b) Assume $\mathbf{v} = s_1 \mathbf{c}_1 + \cdots + s_n \mathbf{c}_n$, where $s_1, \ldots, s_n \in \mathbb{R}$ with not all $s_i \in \mathbb{Z}$. Put

$$J = \{j \in \{1, \ldots, n\} \ : \ s_j \notin \mathbb{Z}\}.$$

For $j \in J$, set

$$\delta(j) = \begin{cases} \max_{i > j} \|s_i\| |\mathbf{c}_i| & \text{if } j < n \\ 0 & \text{if } j = n, \end{cases}$$

where $\| \cdot \|$ denotes the distance to the nearest integer. We have

$$l(\Gamma, \mathbf{v}) \geq \max_{j \in J} \left(2^{-(n-1)/2} \|s_j\| |\mathbf{c}_1| - (n-j)\delta(j) \right).$$

Lemma 4.5.8 (a) is Proposition 1.11 in [63]; proofs can be found in [63], [114] (Section 3.4), or [101] (Section V.3). Lemma 4.5.8 (b) is a combination of Lemmas 3.5 and 3.6 in [114]. Note that the assumption in Lemma 4.5.8 (b) is equivalent to

$\mathbf{v} \notin \Gamma$.

We see that the vector $\mathbf{c}_1$ in a reduced basis is, in a very precise sense, not too far from being the shortest non-zero vector of Γ. As has already been mentioned, what makes this result so valuable is that there is a very simple and efficient algorithm to find a reduced basis in a lattice, namely the LLL algorithm.

3.6.2 The Fincke-Pohst algorithm

Sometimes it is not sufficient to have a lower bound for $l(\Gamma, \mathbf{v})$ only. It may be useful to know exactly all vectors $\mathbf{u} \in \Gamma$ such that $|\mathbf{u}| = \Phi(\mathbf{u}, \mathbf{u}) \leq C$ for a given constant C. This can be done efficiently using an algorithm of Fincke-Pohst (cf. [43], [27]). A version of this algorithm with some improvements due to Stehlé is implemented in Magma. As input this algorithm takes a matrix B, whose columns span the lattice Γ, and a constant $C > 0$. The output is a list of all lattice points $\mathbf{u} \in \Gamma$ with $|\mathbf{u}| \leq C$, apart from $\mathbf{u} = \mathbf{0}$. In this section, we outline the main steps in this algorithm.

We begin by letting B denote the basis matrix associated to the lattice Γ, with corresponding bilinear form Φ. We call a vector $\mathbf{u} \in \Gamma$ *small* if its norm $\Phi(\mathbf{u}, \mathbf{u})$ is less than a constant C. As an element of the lattice, $\mathbf{u} = B\mathbf{x}$ for some coordinate vector $\mathbf{x} \in \mathbb{Z}^n$. Let Q be the quadratic form associated to Φ and let $A = B^T B$. Now finding the short vectors $\mathbf{u} \in \Gamma$ is equivalent to solving

$$Q(\mathbf{x}) = \mathbf{x}^T A \mathbf{x} \leq C. \tag{3.13}$$

Let $\mathbf{x} = (x_1, \ldots, x_n)$. To solve this inequality, we first rearrange the terms of the quadratic form via quadratic completion. Here we assume that Γ is positive definite so that every nonzero element of the lattice has a positive norm. With this, we find the Cholesky decomposition $A = R^T R$, where R is an upper triangular matrix, and express Q as

$$Q(\mathbf{x}) = \sum_{i=1}^{n} q_{ii} \left(x_i + \sum_{j=i+1}^{n} q_{ij} x_j \right)^2 .$$

The coefficients q_{ij} are defined from R and stored in a matrix $\tilde{Q}$ for convenience. In particular,

$$q_{ij} = \begin{cases} \frac{r_{ij}}{r_{ii}} & \text{if } i < j \\ r_{ii}^2 & \text{if } i = j. \end{cases} \tag{3.14}$$

Since R is upper triangular, the matrix $\tilde{Q}$ is as well. This yields the following reformulation of (3.13)

$$\sum_{i=1}^{n} q_{ii} \left(x_i + \sum_{j=i+1}^{n} q_{ij} x_j \right)^2 \leq C.$$

From here we observe that the individual term $q_{nn} x_n^2$ must also be less than C. Specifically,

$$x_n^2 \leq \frac{C}{q_{nn}}$$

so that x_n is bounded above by $\sqrt{C/q_{nn}}$ and below by $-\sqrt{C/q_{nn}}$. This illustrates the first step in establishing bounds on a specific entry x_i. Adding more terms from the outer sum to this sequence, a pattern emerges. Let

$$U_k = \sum_{j=k+1}^{n} q_{kj} x_j,$$

where $U_n = 0$, and rewrite $Q(\mathbf{x})$ as

$$Q(\mathbf{x}) = \sum_{i=1}^{n} q_{ii} \left(x_i + \sum_{j=i+1}^{n} q_{ij} x_j \right)^2 = \sum_{i=1}^{n} q_{ii} \left(x_i + U_i \right)^2 .$$

In general,

$$q_{kk}(x_k + U_k)^2 \leq C - \sum_{i=k+1}^{n} q_{ii}(x_i + U_i)^2.$$

Let T_k denote the bound on the right-hand side,

$$T_k = C - \sum_{i=k+1}^{n} q_{ii}(x_i + U_i)^2.$$

We set $T_n = C$ and find each subsequent T_k by subtracting the next term from the outer summand,

$$T_k = T_{k+1} - q_{k+1,k+1}(x_{k+1} + U_{k+1})^2.$$

This yields the upper bound

$$q_{kk}(x_k + U_k)^2 \leq T_k$$

so that x_k is bounded above by $\sqrt{T_k/q_{kk}} - U_k$ and below by $-\sqrt{T_k/q_{kk}} - U_k$. In this way, we iteratively enumerate all vectors $\mathbf{x}$ satisfying $Q(\mathbf{x}) \leq C$, beginning with the entry x_n of $\mathbf{x}$ and working down towards x_1.

3.6.3 Computational remarks and translated lattices

Recall that the Cholesky decomposition of $A = B^T B$ yields the upper triangular matrix R where $A = R^T R$. It is noted in the [43] that if we label the columns of R by $\mathbf{r}_i$ and the rows of R^{-1} by $\mathbf{r}'_i$, then

$$x_k^2 = \left(\mathbf{r}'^T_k \cdot \sum_{i=1}^{n} x_i \mathbf{r}_i \right)^2 \leq \mathbf{r}'^T_k \mathbf{r}_k (\mathbf{x}^T R^T R \mathbf{x}) \leq |\mathbf{r}'_k|^2 C.$$

To reduce the search space, it is thus beneficial to reduce the rows of R^{-1}. Furthermore, rearranging the columns of R so that the shortest column vector is first helps reduce the total running time of the Fincke-Pohst algorithm. In particular, doing so leads to progressively smaller intervals in which x_k may exist.

We express this reduction with a unimodular matrix V^{-1} so that $R_1^{-1} = V^{-1}R^{-1}$. Applying an appropriate permutation matrix P, we then reorder the columns of R_1. Since $R_1 = RV$, this yields $R_2 = (RV)P$. Finally, we compute the solutions $\mathbf{y}$ to $\mathbf{y}^T R_2^T R_2 \mathbf{y} \leq C$ and recover the short vectors $\mathbf{x}$ satisfying the original inequality (3.13) via $\mathbf{x} = VP\mathbf{y}$.

As before, let Γ be an n-dimensional lattice with basis matrix B, quadratic form Φ, and associated bilinear form Q. In Section 3.6.2, it is noted that an implementation of the Fincke-Pohst algorithm is available in Magma. Unfortunately, this implementation does not support *translated* lattices, a variant of the Fincke-Pohst algorithm which we will need in Chapter 6. By a translated lattice, we mean the discrete subgroup of $\mathbb{R}^n$ of the form

$$\Gamma + \mathbf{w} = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i + \mathbf{w} \ : \ x_i \in \mathbb{Z} \right\},$$

where $\mathbf{b}_1, \ldots, \mathbf{b}_n$ form the columns of B and $\mathbf{w} \in \mathbb{R}^n$. In the remainder of this section, we describe how to modify the Fincke-Pohst algorithm and its refinements to support translated lattices.

Analogous to the non-translated case, any embedded vector $\mathbf{u}$ of $\Gamma + \mathbf{w}$ may be expressed as $\mathbf{u} = B\mathbf{x} + \mathbf{w}$ for a corresponding coordinate vector $\mathbf{x}$. In this case, we call the vector $\mathbf{u} \in \Gamma + \mathbf{w}$ *small* if

$$(\mathbf{x} - \mathbf{c})^T B^T B (\mathbf{x} - \mathbf{c}) \leq C \tag{3.15}$$

for some $C \geq 0$, where $\mathbf{c} = -\mathbf{w}$.

As in the usual short vectors process, we begin by applying Cholesky decomposition to the positive definite matrix $A = B^T B$ to obtain an upper triangular matrix R satisfying $A = R^T R$. We then generate the matrices R_1, R_2, V, and P described earlier in this section. This allows us to write $A = U^T G U$ for a unimodular matrix U and Gram matrix G given by

$$U = P^{-1} V^{-1} \quad \text{and} \quad G = R_2^T R_2.$$

Thus the inequality (3.15) becomes

$$(\mathbf{y}-\mathbf{d})^T G(\mathbf{y}-\mathbf{d}) \leq C \tag{3.16}$$

where

$$\mathbf{y} = U\mathbf{x} \quad \text{and} \quad \mathbf{d} = U\mathbf{c}.$$

To enumerate the vectors $\mathbf{y}$ which satisfy this inequality, we consider the bilinear form Q associated to the lattice Γ. We express this form as

$$Q(\mathbf{y}-\mathbf{d}) = \sum_{i=1}^{n} q_{ii} \left(y_i - d_i + \sum_{j=i+1}^{n} q_{ij}(y_j - d_j) \right)^2 .$$

As in the usual Fincke-Pohst algorithm, the coefficients q_{ij} are defined from the matrix R via equation (3.14). Let

$$U_k = -d_k + \sum_{j=k+1}^{n} q_{kj}(y_j - d_j),$$

where $U_n = -d_n$, and rewrite $Q(\mathbf{y}-\mathbf{d})$ as

$$Q(\mathbf{y}-\mathbf{d}) = \sum_{i=1}^{n} q_{ii} \left(y_i - d_i + \sum_{j=i+1}^{n} q_{ij}(y_j - d_j) \right)^2 = \sum_{i=1}^{n} q_{ii} \left(y_i + U_i \right)^2 .$$

From here, we proceed as in the usual Fincke-Pohst algorithm described in Section 3.6.2. Once we compute all vectors $\mathbf{y}$ which satisfy (3.16), we recover $\mathbf{x}$ using $\mathbf{x} = U^{-1}\mathbf{y}$.

As a final remark about Fincke-Pohst for translated lattices, it is worth noting that one could use the variant implemented in Magma simply by increasing the dimension of the lattice Γ and appropriately redefining the basis vectors $\mathbf{b}_i$. This is highly ill-advised as it increases the search space and subsequent running time of the algorithm.

Generally speaking, the use of Fincke-Pohst in our applications poses one of the main bottlenecks in solving Thue-Mahler and Thue-Mahler-like equations. Specifically, this algorithm often yields upwards of hundreds of millions of short vectors, each one needing to be stored and, in our case, appropriately manipulated. This creates both timing and memory problems, often leading to gigabytes of data usage. Deleting these vectors does not release the memory and, as with the class group function, Magma's built-in Fincke-Pohst process cannot be terminated without exiting the program. The primary advantage of implementing and using our own version of Fincke-Pohst, as described in this section, is therefore the ability to add a fail-stop should the number of vectors found become too large.

Chapter 4

Goormaghtigh Equations

Let m and n be integers such that $m > n > 2$, where either $m = n + 1$ or

$$\gcd(m-1, n-1) = d > 1m \tag{4.1}$$

and consider the Goormaghtigh's equation

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}, \;\; y > x > 1, \; m > n > 2. \tag{4.2}$$

In this chapter, we prove that, in fact, under assumption (4.1), equation (4.2) has at most finitely many solutions which may be found effectively, even if we fix only a single exponent.

Theorem 4.0.1. *If there is a solution in integers x, y, n and m to equation (4.2), satisfying (4.1), then*

$$x < (3d)^{4n/d} \leq 36^n. \tag{4.3}$$

In particular, if n is fixed, there is an effectively computable constant $c = c(n)$ such that $\max\{x, y, m\} < c$.

We note that the latter conclusion here follows immediately from (4.3), in conjunction with, for example, work of Baker [5]. The constants present in our upper bound (4.3) may be sharpened somewhat at the cost of increasing the complexity of our argument. By refining our approach, in conjunction with some new results from computational Diophantine approximation, we are able to achieve the complete solution of equation (4.2), subject to condition (4.1), for small fixed values of n.

Theorem 4.0.2. *If there is a solution in integers x, y and m to equation (4.2), with $n \in \{3, 4, 5\}$ and satisfying (4.1), then*

$$(x, y, m, n) = (2, 5, 5, 3) \ \textit{and} \ (2, 90, 13, 3).$$

Essentially half of the current chapter is concerned with developing Diophantine approximation machinery for the case $n = 5$ in Theorem 4.0.2. Here, "off-the-shelf" techniques for finding integral points on models of elliptic curves or for solving *Ramanujan-Nagell* equations of the shape $F(x) = z^n$ (where F is a polynomial and z a fixed integer) do not apparently permit the full resolution of this problem in a reasonable amount of time. The new ideas introduced here are explored more fully in the general setting of *Thue-Mahler* equations in the forthcoming paper [44]. These are polynomial-exponential equations of the form $F(x, y) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where F is a binary form of degree three or greater and $p_1, \ldots, p_k$ are fixed rational primes. Here, we take this opportunity to specialize these refinements to the case of Ramanujan-Nagell equations, and to introduce some further sharpenings which enable us to complete the proof of Theorem 4.0.2.

4.1 Rational approximations

In what follows, we will always assume that x, y, m and n are integers satisfying (4.2) with (4.1), and write

$$m - 1 = dm_0 \quad \text{and} \quad n - 1 = dn_0. \tag{4.4}$$

We note, for future use, that an appeal to Théorème II of Karanicoloff [57] (which, in our notation, states that the only solution to (4.2) with $n_0 = 1$ and $m_0 = 2$ in (4.4) is given by $(x, y, m, n) = (2, 5, 5, 3)$) allows us to suppose that either

$(x, y, m, n) = (2, 5, 5, 3)$, or that $m_0 \geq 3$ and $n_0 \geq 1$.

Our starting point, as in, for example, [22] and [81], is the observation that the existence of a solution to (4.2) with (4.1) implies a number of unusually good rational approximations to certain irrational algebraic numbers. One such approximation arises from rewriting (4.2) as

$$x \, \frac{x^{dm_0}}{x-1} - y \, \frac{y^{dn_0}}{y-1} = \frac{1}{x-1} - \frac{1}{y-1},$$

whereby

$$\left| \sqrt[d]{\frac{y(x-1)}{x(y-1)}} - \frac{x^{m_0}}{y^{n_0}} \right| < \frac{1}{y^{dn_0}}. \tag{4.5}$$

The latter inequality was used, in conjunction with lower bounds for linear forms in logarithms (in [81]) and with machinery based upon Padé approximation to binomial functions (in [22]), to derive a number of strong restrictions upon x, y and d satisfying equation (4.2).

Our argument will be somewhat different, as we consider instead a rational approximation to $\sqrt[d]{(x-1)/x}$ that is, on the surface, much less impressive than that to $\sqrt[d]{\frac{y(x-1)}{x(y-1)}}$ afforded by (4.5). The key additional idea is that we are able to take advantage of the arithmetic structure of our approximations to obtain very strong lower bounds for how well they can approximate $\sqrt[d]{(x-1)/x}$. This argument has its genesis in work of Beukers [12], [13].

For the remainder of this section, we will always assume that $x \geq 40$. From

$$\frac{y^n-1}{y-1} = y^{dn_0}\left(1 + \frac{1}{y} + \cdots + \frac{1}{y^{dn_0}}\right) \text{ and } \frac{x^m-1}{x-1} = x^{dm_0}\left(1 + \frac{1}{x} + \cdots + \frac{1}{x^{dm_0}}\right),$$

we thus have

$$y^{dn_0} < \frac{y^n-1}{y-1} = \frac{x^m-1}{x-1} < \frac{x}{x-1} \, x^{dm_0}$$

and

$$\frac{y}{y-1} \, x^{dm_0} \leq \frac{x+1}{x} \, x^{dm_0} < \frac{x^m-1}{x-1} = \frac{y^n-1}{y-1} < \frac{y}{y-1} \, y^{dn_0},$$

so that

$$x^{m_0} < y^{n_0} < \left(\frac{x}{x-1}\right)^{1/d} x^{m_0} \leq \sqrt{40/39}\, x^{m_0} < 1.013\, x^{m_0}. \tag{4.6}$$

We will rewrite (4.2) as

$$x^{dm_0} - \frac{(x-1)}{x} \sum_{j=0}^{dn_0} y^j = \frac{1}{x}.$$

From this equation, we will show that $\sqrt[d]{(x-1)/x}$ is well approximated by a rational number whose numerator is divisible by x^{m_0}.

If we define, as in Nesterenko and Shorey [81], $A_k(d)$ via

$$\left(1 - \frac{1}{X}\right)^{-1/d} = \sum_{k=0}^{\infty} A_k(d)\, X^{-k} = \sum_{k=0}^{\infty} \frac{d^{-1}(d^{-1}+1)\cdots(d^{-1}+k-1)}{k!}\, X^{-k},$$

then we can write

$$\sum_{j=0}^{dn_0} y^j = \left(\sum_{k=0}^{n_0} A_k(d) y^{n_0-k}\right)^d + \sum_{j=0}^{(d-1)n_0-1} B_j(d) y^j.$$

Here, the B_j are positive, monotone increasing in j, and satisfy

$$B_{(d-1)n_0-1}(d) = \frac{n}{n_0+1} A_{n_0}(d),$$

while, for the $A_k(d)$, we have the inequalities

$$\frac{d+1}{kd^2} \leq A_k(d) \leq \frac{d+1}{2d^2},$$

valid provided $k \geq 2$ (see displayed equation (14) of [81]).

We thus have

$$x^{dm_0} - \frac{(x-1)}{x} \left(\sum_{k=0}^{n_0} A_k(d) y^{n_0-k} \right)^d = \frac{1}{x} + \frac{x-1}{x} \sum_{j=0}^{(d-1)n_0-1} B_j(d) y^j \quad (4.7)$$

and so

$$0 < x^{dm_0} - \frac{(x-1)}{x} \left(\sum_{k=0}^{n_0} A_k(d) y^{n_0-k} \right)^d < \frac{(dn_0+1)(d+1)}{2(n_0+1)d^2} \frac{y}{y-1} y^{(d-1)n_0-1}. \quad (4.8)$$

Since

$$\frac{(dn_0+1)(d+1)}{2(n_0+1)d^2} < \frac{d+1}{2d} \leq \frac{3}{4},$$

from the fact that $n_0 \geq 1$ and $d \geq 2$, and since $y > x \geq 40$, we may conclude that

$$0 < x^{dm_0} - \frac{(x-1)}{x} \left(\sum_{k=0}^{n_0} A_k(d) y^{n_0-k} \right)^d < 0.769\, y^{(d-1)n_0-1}. \quad (4.9)$$

Applying the Mean Value Theorem,

$$0 < x^{m_0} - \sqrt[d]{\frac{x-1}{x}} \sum_{k=0}^{n_0} A_k(d) y^{n_0-k} < 0.769 \frac{y^{(d-1)n_0-1}}{dY^{d-1}}, \quad (4.10)$$

where Y lies in the interval

$$\left(\sqrt[d]{\frac{x-1}{x}} \sum_{k=0}^{n_0} A_k(d) y^{n_0-k}, x^{m_0} \right).$$

We thus have

$$Y^{d-1} > \left(\frac{x-1}{x} \right)^{(d-1)/d} y^{(d-1)n_0}$$

and so, from (4.10) and the fact that $d \geq 2$ and $x \geq 40$,

$$0 < x^{m_0} - \sqrt[d]{\frac{x-1}{x}} \sum_{k=0}^{n_0} A_k(d) y^{n_0-k} < \frac{0.779}{dy}. \quad (4.11)$$

Let us define

$$C(k,d) = d^k \prod_{p|d} p^{\mathrm{ord}_p(k!)},$$

where by $\mathrm{ord}_p(z)$ we mean the largest power of p that divides a nonzero integer z. Here, k and d positive integers with $d \geq 2$. Then we have

$$C(k,d) = d^k \prod_{p|d} p^{\left[\frac{k}{p}\right]+\left[\frac{k}{p^2}\right]+\cdots}$$

and hence it follows that

$$C(k,d) < \left(d \prod_{p|d} p^{1/(p-1)} \right)^k . \tag{4.12}$$

Further (see displayed equation (18) of Nesterenko and Shorey [81]), and critically for our purposes, $C(k,d)A_k(d)$ is an integer. Multiplying equation (4.7) by $C(n_0,d)$ and setting

$$P = C(n_0,d)\, x^{m_0} \quad \text{and} \quad Q = C(n_0,d) \sum_{k=0}^{n_0} A_k(d) y^{n_0-k}, \tag{4.13}$$

then P and Q are integers and, defining

$$\epsilon = P - \sqrt[d]{\frac{x-1}{x}} Q, \tag{4.14}$$

we thus have, from (4.11), that the following result holds.

Proposition 4.1.1. *Suppose that (x,y,m,n) is a solution in integers to equation (4.2), with (4.1) and $x \geq 40$. If we define ϵ via (4.14), then*

$$0 < \epsilon < \frac{0.779\, C(n_0,d)}{dy}. \tag{4.15}$$

Our next goal will be to construct a second linear form δ, in 1 and $\sqrt[d]{(x-1)/x}$, with the property that a particular linear combination of ϵ and δ is a (relatively large) nonzero integer, a fact we will use to derive a lower bound on ϵ. This argument, which will employ off-diagonal Padé approximants to the binomial function $\sqrt[d]{1+z}$, follows work of Beukers [12], [13].

To apply Proposition 4.1.1 and for our future arguments, we will have use of bounds upon the quantity $C(k, d)$.

Proposition 4.1.2. *If k is a positive integer, then*

$$2^k \leq C(k, 2) < 4^k$$

and

$$d^k \leq C(k, d) < (2d \log d)^k,$$

for $d > 2$.

We will postpone the proof of this result until Section 4.6; the upper bound here for large d may be sharpened somewhat, but this is unimportant for our purposes.

4.2 Padé approximants

In this section, we will define Padé approximants to $(1+z)^{1/d}$, for $d \geq 2$. Suppose that m_1 and m_2 are nonnegative integers, and set

$$I_{m_1,m_2}(z) = \frac{1}{2\pi i} \int_\gamma \frac{(1+zv)^{m_2}(1+zv)^{1/d}}{v^{m_1+1}(1-v)^{m_2+1}} \, dv,$$

where γ is a closed, counter-clockwise contour, containing $v = 0$ and $v = 1$. Applying Cauchy's residue theorem, we may write $I_{m_1,m_2}(z)$ as R_0+R_1, where

$$R_i = \mathrm{Res}_{v=i} \left(\frac{(1+zv)^{m_2}(1+zv)^{1/d}}{v^{m_1+1}(1-v)^{m_2+1}} \right).$$

Now

$$R_0 = \frac{1}{m_1!} \lim_{v \to 0} \frac{d^{m_1}}{dv^{m_1}} \frac{(1+zv)^{m_2}(1+zv)^{1/d}}{(1-v)^{m_2+1}} = P_{m_1,m_2}(z)$$

and

$$R_1 = \frac{1}{m_2!} \lim_{v \to 1} \frac{d^{m_2}}{dv^{m_2}} \frac{(1+zv)^{m_2}(1+zv)^{1/d}}{v^{m_1+1}} = -Q_{m_1,m_2}(z)\,(1+z)^{1/d},$$

where

$$P_{m_1,m_2}(z) = \sum_{k=0}^{m_1} \binom{m_2+1/d}{k} \binom{m_1+m_2-k}{m_2} z^k \tag{4.16}$$

and

$$Q_{m_1,m_2}(z) = \sum_{k=0}^{m_2} \binom{m_1-1/d}{k} \binom{m_1+m_2-k}{m_1} z^k. \tag{4.17}$$

Note that there are typographical errors in the analogous statement given in displayed equation (2.3) of [6]. We take $z = -1/x$. Arguing as in the proof of Lemma 4.1 of [6], we find that

$$|I_{m_1,m_2}(-1/x)| = \frac{\sin(\pi/d)}{\pi\, x^{m_1+m_2+1}} \int_0^1 \frac{v^{m_2+1/d}(1-v)^{m_1-1/d}dv}{(1-(1-v)/x)^{m_2+1}}. \tag{4.18}$$

Upon multiplying the identity

$$P_{m_1,m_2}(-1/x) - Q_{m_1,m_2}(-1/x)\sqrt[d]{\frac{x-1}{x}} = I_{m_1,m_2}(-1/x)$$

through by $x^{m_2}C(m_2,d)$, and setting

$$\delta = C_0P_1 - \sqrt[d]{\frac{x-1}{x}}\,Q_1,$$

where we write $m_0 = m_2 - m_1$,

$$C_0 = x^{m_0}C(m_2,d)/C(m_1,d), \quad P_1 = x^{m_1}C(m_1,d)P_{m_1,m_2}(-1/x)$$

and

$$Q_1 = x^{m_2}C(m_2,d)Q_{m_1,m_2}(-1/x), \tag{4.19}$$

it follows, from Lemma 3.1 of Chudnovsky [24], that C_0, P_1 and Q_1 are integers. Further, from (4.18),

$$|\delta| = \frac{\sin(\pi/d)\, C(m_2,d)}{\pi\, x^{m_1+1}} \int_0^1 \frac{v^{m_2+1/d}(1-v)^{m_1-1/d}dv}{(1-(1-v)/x)^{m_2+1}}. \tag{4.20}$$

Recall that P and Q are defined as in (4.13). Here and henceforth, we will assume that

$$m_2 - m_1 = m_0. \tag{4.21}$$

We have

Lemma 4.2.1. *If m_1 and m_2 are nonnegative integers satisfying (4.21), then it follows that $PQ_1 \neq C_0P_1Q$.*

Proof. Let p be a prime with $p \mid d$. Then

$$\mathrm{ord}_p(P) = n_0 \,\mathrm{ord}_p(d) + \mathrm{ord}_p(n_0!) + m_0 \,\mathrm{ord}_p(x),$$

$$\mathrm{ord}_p(P_1) = \mathrm{ord}_p(Q_1) = \mathrm{ord}_p(Q) = 0$$

and

$$\mathrm{ord}_p(C_0) = m_0 \,\mathrm{ord}_p(d) + \mathrm{ord}_p(m_2!) - \mathrm{ord}_p(m_1!) + m_0 \,\mathrm{ord}_p(x).$$

Since $m_2 - m_1 = m_0 > n_0$, we have

$$\mathrm{ord}_p\left(\frac{C_0P_1Q}{PQ_1}\right) = (m_0 - n_0)\,\mathrm{ord}_p(d) + \mathrm{ord}_p\left(\frac{m_2!}{m_1!n_0!}\right) > 0$$

so that

$$\mathrm{ord}_p(PQ_1 - C_0P_1Q) = \mathrm{ord}_p(PQ_1) = n_0 \,\mathrm{ord}_p(d) + \mathrm{ord}_p(n_0!) + m_0 \,\mathrm{ord}_p(x)$$

and, in particular, $PQ_1 - C_0P_1Q \neq 0$.

□

It follows from Lemma 4.2.1 and its proof that $PQ_1 - C_0 P_1 Q$ is a nonzero integer multiple of $C(n_0, d)\, x^{m_0}$, so that, from the definitions of ϵ and δ,

$$|\epsilon Q_1 - \delta Q| = |PQ_1 - C_0 P_1 Q| \geq C(n_0, d)\, x^{m_0}. \tag{4.22}$$

Now

$$Q = C(n_0, d) \sum_{k=0}^{n_0} A_k(d) y^{n_0 - k} < \frac{y}{y-1}\, C(n_0, d)\, y^{n_0} \leq 1.025\, C(n_0, d)\, y^{n_0},$$

since $y > x \geq 40$, and hence, from (4.6),

$$Q < 1.039\, C(n_0, d)\, x^{m_0}. \tag{4.23}$$

Combining (4.6), (4.15), (4.22) and (4.23), we thus have

Proposition 4.2.2. *Suppose that (x, y, m, n) is a solution in integers to equation (4.2), with (4.1) and $x \geq 40$. If m_0, n_0 and d are defined as in (4.4), and m_1 and m_2 are nonnegative integers satisfying (4.21), then for Q_1 and $|\delta|$ as given in (4.19) and (4.20), we may conclude that*

$$|Q_1| > 1.28\, d\, (1 - 1.039|\delta|)\, x^{m_0 + m_0/n_0}. \tag{4.24}$$

In the other direction, we will deduce two upper bounds upon $|Q_1|$; we will use one or the other depending on whether or not m_1 is "large", relative to x. The first result is valid for all choices of x.

Proposition 4.2.3. *If m_1, m_2 and x are integers with $m_2 > m_1 \geq 1$ and $x \geq 2$, define $\alpha = m_2/m_1$ and $|\delta|$ as in (4.20). Then*

$$|Q_1| < \sqrt[d]{\frac{x}{x-1}}\, \left(\frac{(\alpha+1)^2}{\alpha} \left(e\,(\alpha+1)\right)^{m_1} x^{m_2}\, C(m_2, d) + |\delta| \right). \tag{4.25}$$

If $x \geq m_1$, we will have use of the following slightly sharper bound.

Proposition 4.2.4. *If m_1 and m_2 are integers with $m_2 > m_1 \geq 0$ and $x \geq \frac{m_1 m_2}{m_1 + m_2}$,* *then*

$$|Q_1| < \frac{x}{x-1} \binom{m_1+m_2}{m_1} C(m_2,d)\, x^{m_2}.$$

Proof of Proposition 4.2.3. Let us write $\alpha = m_2/m_1 > 1$ and define

$$r(\alpha,u) = \frac{1}{2u}\left((\alpha+1)-(\alpha-1)u-\sqrt{((\alpha+1)-(\alpha-1)u)^2-4u}\right), \tag{4.26}$$

and

$$M(\alpha,x) = \frac{(1-r(\alpha,1/x)/x)^{\alpha}}{(1-r(\alpha,1/x))^{\alpha} r(\alpha,1/x)}. \tag{4.27}$$

Via the Mean Value Theorem,

$$\frac{1}{\alpha+1} < r(\alpha,1/x) < \frac{x}{(x-1)(\alpha+1)} \tag{4.28}$$

and so, from calculus,

$$M(\alpha,x) < \left(\frac{(x-1)\,(\alpha+1)-1}{(x-1)(\alpha+1)-x}\right)^{\alpha} \cdot (\alpha+1) < e\,(\alpha+1) \tag{4.29}$$

and

$$M(\alpha,x) > \left(1+\frac{x-1}{x\alpha}\right)^{\alpha} \left(\frac{x-1}{x}\right)\,(\alpha+1). \tag{4.30}$$

Arguing as in the proof of Lemma 3.1 of [6], we find that

$$|C_0P_1| \le \frac{(1-r(\alpha,1/x)/x)^{1/d}}{r(\alpha,1/x)(1-r(\alpha,1/x))}\, M(\alpha,x)^{m_1}\, x^{m_2}\, C(m_2,d),$$

whereby inequalities (4.28) and (4.29) imply that

$$|C_0P_1| < \frac{(\alpha+1)^2}{\alpha}\,(e\,(\alpha+1))^{m_1}\, x^{m_2}\, C(m_2,d).$$

Since $C_0P_1 = \sqrt[d]{\frac{x-1}{x}}\, Q_1 + \delta$, we conclude as desired. $\square$

Proof of Proposition 4.2.4. To bound Q_1 from above, we begin by noting that

$$x^{m_2}\left|Q_{m_1,m_2}(-1/x)\right| = \left|\sum_{k=0}^{m_2}\binom{m_1-1/d}{k}\binom{m_1+m_2-k}{m_1}(-1)^k x^{m_2-k}\right|. \tag{4.31}$$

Defining

$$f(k) = \binom{m_1-1/d}{k}\binom{m_1+m_2-k}{m_1},$$

it follows that, for $0 \le k \le m_2 - 1$,

$$f(k+1)/f(k) = \frac{(m_1-1/d-k)(m_2-k)}{(k+1)(m_1+m_2-k)}.$$

If $k \le m_1 - 1$, we thus have that

$$0 < f(k+1)/f(k) < \frac{(m_1-k)(m_2-k)}{(k+1)(m_1+m_2-k)} \le \frac{m_1 m_2}{m_1+m_2}. \tag{4.32}$$

If instead $k \ge m_1$,

$$\frac{(m_1-k-1)(m_2-k)}{(k+1)(m_1+m_2-k)} < f(k+1)/f(k) < 0. \tag{4.33}$$

It follows via calculus, in this case, that

$$|f(k+1)/f(k)| < \frac{(m_2-m_1+1)^2}{(m_2+m_1+1)^2}.$$

We thus have that $x^{m_2}\left|Q_{m_1,m_2}(-1/x)\right|$ is bounded above by

$$\binom{m_1+m_2}{m_1}x^{m_2} + \left|\binom{m_1-1/d}{m_1}\right|\binom{m_2}{m_1}\sum_{k=m_1+1}^{m_2} x^{m_2-k}$$

which implies the desired result. □

4.3 Proof of Theorem 4.0.1

To prove Theorem 4.0.1, we will work with Padé approximants to $(1+z)^{1/d}$, as in Section 4.2, of degrees m_1 and m_2 where we choose

$$m_1 = \left[\frac{m_0}{2n_0}\right] \quad \text{and} \quad m_2 = m_0 + \left[\frac{m_0}{2n_0}\right], \tag{4.34}$$

for m_0, n_0 and d as given in (4.4). Here $[x]$ denotes the greatest integer less than or equal to x. Let us assume further that $x \geq (3d)^{4n/d} \geq 6^6$. We will make somewhat different choices later, when we prove Theorem 4.0.2.

Our strategy will be as follows. We begin by showing that δ as given in (4.20) satisfies $|\delta| < \frac{1}{1.039}$, so that the lower bound upon $|Q_1|$ in Proposition 4.2.2 is nontrivial. From there, we will appeal to Proposition 4.2.3 to contradict Proposition 4.2.2.

4.3.1 Bounding δ

From the aforementioned Théorème II of Karanicoloff [57], we may suppose that $m_0 \geq 3$ and hence, arguing crudely, since $m_2 \geq m_0 \geq 3$ and $m_1 \geq 0$, we have

$$\int_0^1 \frac{v^{m_2+1/d}(1-v)^{m_1-1/d}dv}{(1-(1-v)/x)^{m_2+1}} < 1$$

and hence, from (4.20),

$$|\delta| < \frac{\sin(\pi/d)\, C(m_2, d)}{\pi\, x^{m_1+1}} \leq \frac{C(m_2, d)}{\pi\, x^{m_1+1}}. \tag{4.35}$$

From (4.34), $m_1 + 1 > \frac{m_0}{2n_0}$ and so, the assumption that $x \geq (3d)^{4n/d}$ yields the inequality

$$x^{m_1+1} > (3d)^{2m_0}.$$

Applying Proposition 4.1.2, if $d = 2$, it follows from $m_1 \leq \frac{m_0}{2n_0}$ that

$$|\delta| < \frac{1}{\pi} 4^{m_1} 3^{-2m_0} \leq \frac{8}{729\pi} < 0.01,$$

since $m_0 \geq 3$ and $n_0 \geq 1$. Similarly, if $d \geq 3$,

$$|\delta| < \frac{(2d \log d)^{m_0+m_1}}{(3d)^{2m_0}} \leq \frac{(2d \log d)^{m_0+\frac{m_0}{2n_0}}}{(3d)^{2m_0}} = \left(\frac{(2d \log d)^{1+\frac{1}{2n_0}}}{9d^2} \right)^{m_0} < 0.01,$$

again from $m_0 \geq 3$ and $n_0 \geq 1$. Appealing to Proposition 4.2.2, we thus have, in either case,

$$|Q_1| > 1.25\, d\, x^{m_0+m_0/n_0}. \tag{4.36}$$

4.3.2 Applying Proposition 4.2.3

We will next apply Proposition 4.2.3 to deduce an upper bound upon $|Q_1|$. To use this result, we must first separately treat the case when $m_1 = 0$. In this situation, Proposition 4.2.4 implies that

$$|Q_1| < \frac{x}{x-1}\, C(m_0, d)\, x^{m_0}.$$

Inequality (4.36) and $x \geq (3d)^{4n/d} > (3d)^{4n_0}$ thus lead to the inequalities

$$C(m_0, d) > d\, x^{m_0/n_0} > (3d)^{4m_0},$$

contradicting Proposition 4.1.2 in all cases.

Assuming now that $m_1 \geq 1$, combining Proposition 4.2.3 with (4.36), $d \geq 2$ and the fact that $\alpha = 1 + m_0/m_1 \geq 3$, implies that

$$x^{\frac{m_0}{n_0}-m_1} < \alpha\, C(m_2, d)\, (e\, (\alpha+1))^{m_1}.$$

Since $m_1 \leq m_0/2n_0$, $x \geq (3d)^{4n/d} > (3d)^{4n_0}$ and $\alpha = 1 + m_0/m_1$, it follows

that

$$(3d)^{2m_0} < (1 + m_0/m_1)\, C(m_0 + m_1, d)\, (e\,(2 + m_0/m_1))^{m_1}$$

and so

$$9d^2 < (1 + m_0/m_1)^{1/m_0}\, C(m_0 + m_1, d)^{1/m_0}\, (e\,(2 + m_0/m_1))^{m_1/m_0}. \quad (4.37)$$

If $d = 2$, Proposition 4.1.2 yields

$$36 < (1 + m_0/m_1)^{1/m_0}\, 4^{1+m_1/m_0}\, (e\,(2 + m_0/m_1))^{m_1/m_0}, \quad (4.38)$$

contradicting the fact that $m_0 \geq \max\{3, 2m_1\}$.

If $d \geq 3$, (4.37) and Proposition 4.1.2 lead to the inequality

$$9d^2 < (1 + m_0/m_1)^{1/m_0}\, (2d \log d)^{1+m_1/m_0}\, (e\,(2 + m_0/m_1))^{m_1/m_0},$$

whence

$$2.744 < \frac{9\sqrt{d}}{2\sqrt{2}(\log d)^{3/2}} < (1 + m_0/m_1)^{1/m_0}\, (e\,(2 + m_0/m_1))^{m_1/m_0}. \quad (4.39)$$

If $n_0 \geq 3$, then $m_0 \geq 6m_1$ and hence

$$(1 + m_0/m_1)^{1/m_0}\, (e\,(2 + m_0/m_1))^{m_1/m_0} < 2.4,$$

a contradiction, while, from the second inequality in (4.39), we find that $d \leq 1112$ or $d \leq 64$, if $n_0 = 1$ or $n_0 = 2$, respectively.

For these remaining values, we will argue somewhat more carefully. From (4.12) and (4.37),

$$9d^2 < (1 + m_0/m_1)^{1/m_0} \left(d \prod_{p|d} p^{1/(p-1)} \right)^{1+m_1/m_0} (e\,(2 + m_0/m_1))^{m_1/m_0}. \quad (4.40)$$

If $n_0 = 2$ (so that $m_0 \geq 4m_1$), we thus have

$$d^{3/4} < 0.34 \left(\prod_{p|d} p^{1/(p-1)} \right)^{5/4},$$

and hence, for $3 \leq d \leq 64$, a contradiction. Similarly, if $n_0 = 1$, we have from $m_0 \geq 3$ that either $(m_0, m_1) = (3, 1)$ or $m_0 \geq 4$. In the first case,

$$d^{2/3} < 0.43 \left(\prod_{p|d} p^{1/(p-1)} \right)^{4/3},$$

contradicting the fact that $d \leq 1112$. If $m_0 \geq 4$ (so that $m_1 \geq 2$), then (5.29) implies the inequality

$$d^{1/2} < \frac{e^{1/2} \cdot 2 \cdot 3^{1/2m_1}}{9} \left(\prod_{p|d} p^{1/(p-1)} \right)^{3/2}$$

and hence, after a short computation and using that $d \leq 1112$, either $d = 6$, $m_0 = 2m_1$ and $m_1 \leq 15$, or $d = 30$ and $(m_0, m_1) = (4, 2)$. In this last case,

$$x^6 Q_{2,6}(-1/x) = \sum_{k=0}^{6} \binom{2 - 1/30}{k} \binom{8 - k}{2} (-x)^{6-k}$$

and so $x^6 Q_{2,6}(-1/x)$ is equal to

$$28x^6 - \frac{413}{10}x^5 + \frac{1711}{120}x^4 + \frac{1711}{16200}x^3 + \frac{53041}{3240000}x^2 + \frac{3235501}{972000000}x + \frac{294430591}{524880000000} < 28x^6,$$

since $x \geq 6^6$. From $C(6, 30) = 52488000000$, we have that

$$|Q_1| < 1.47 \cdot 10^{13}\, x^6.$$

On the other hand, (4.36) implies that $|Q_1| > 37.5 \cdot x^8$, so that $x < 6.3 \cdot 10^5$, contradicting $x \geq (3d)^{4n/d} > 90^4$.

For $d = 6$, $2 \leq m_1 \leq 15$ and $m_0 = 2m_1$, we argue in a similar fashion, explicitly computing $Q_{m_1,m_2}(z)$ and finding that

$$|Q_1| < \kappa_{m_1} x^{3m_1},$$

where

m_1	κ_{m_1}	m_1	κ_{m_1}	m_1	κ_{m_1}
2	$1.89 \cdot 10^8$	7	$1.35 \cdot 10^{32}$	12	$1.60 \cdot 10^{57}$
3	$2.30 \cdot 10^{13}$	8	$1.24 \cdot 10^{37}$	13	$1.89 \cdot 10^{61}$
4	$9.86 \cdot 10^{17}$	9	$1.29 \cdot 10^{42}$	14	$1.79 \cdot 10^{66}$
5	$1.09 \cdot 10^{22}$	10	$6.02 \cdot 10^{46}$	15	$1.28 \cdot 10^{71}$
6	$5.88 \cdot 10^{27}$	11	$1.13 \cdot 10^{52}$		

With (4.36), we thus have

$$x^{m_1} < \frac{2}{15} \kappa_{m_1},$$

and so

$$x < \left(\frac{2}{15} \kappa_{m_1}\right)^{1/m_1} < 5.5 \cdot 10^4,$$

contradicting our assumption that $x \geq 18^{2n/3} \geq 18^{14/3} > 7.2 \cdot 10^5$. This completes the proof of Theorem 4.0.1.

4.4 Proof of Theorem 4.0.2 for x of moderate size

As can be observed from the proof of Theorem 4.0.1, the upper bound $x < (3d)^{4n/d}$ may, for fixed values of n (and hence d), be improved with a somewhat more careful argument. By way of example, for small choices of n, we may derive bounds of the shape $x < x_0(n)$, provided we assume that $m \geq m_0(n)$ for effectively computable m_0, where we have

n	$x_0(n)$	n	$x_0(n)$	n	$x_0(n)$	n	$x_0(n)$
3	38	5	676	7	11647	9	195712
4	80	6	230	8	492	10	72043.

To prove Theorem 4.0.2, we will begin by deducing slightly weaker versions of these bounds, for $n \in \{3, 4, 5\}$, where the corresponding values m_0 are amenable to explicit computation. Our arguments will closely resemble those of the preceding section, with slightly different choices of m_1 and m_2, and with a certain amount of additional care. Note that, from Theorem 4.0.1, we may assume that we are in one of the following cases

1. $n = 3,\ d = 2,\ n_0 = 1,\ 2 \leq x \leq 46655,$
2. $n = 4,\ d = 3,\ n_0 = 1,\ 2 \leq x \leq 122826,$
3. $n = 5,\ d = 2,\ n_0 = 2,\ 2 \leq x \leq 60466175,$
4. $n = 5,\ d = 4,\ n_0 = 1,\ 2 \leq x \leq 248831.$

Initially, we will suppose that $x \geq 40$ and, in all cases, that m_1 and m_2 are nonnegative integers satisfying (4.21). We will always, in fact, choose m_1 positive. Again setting $m_2 = \alpha m_1$, via calculus, we may bound the integral $\int_0^1 \frac{v^{m_2+1/d}(1-v)^{m_1-1/d}dv}{(1-(1-v)/x)^{m_2+1}}$ in (4.20) by

$$\left(\max_{v \in [0,1]} \frac{v^{(\alpha+1)/d}}{(1-(1-v)/x)^{(\alpha+d)/d}} \right) M(\alpha, x)^{1/d - m_1} < M(\alpha, x)^{1/d - m_1}.$$

From (4.20), it thus follows that

$$|\delta| < \frac{\sin(\pi/d)\, C(m_2, d)}{\pi\, x^{m_1+1}}\, M(\alpha, x)^{1/d - m_1}. \qquad (4.41)$$

4.4.1 Case (1) : $n = 3,\ d = 2,\ n_0 = 1,\ x \geq 40$

In this case, we will take

$$m_1 = \left\lceil \frac{2m_0}{7} \right\rceil \quad \text{and} \quad m_2 = m_0 + \left\lceil \frac{2m_0}{7} \right\rceil,$$

where by $\lceil x \rceil$ we mean the least integer that is $\geq x$, so that $m_1 \geq 2m_2/9$, i.e. $\alpha \leq 9/2$. From (4.41) and Proposition 4.1.2,

$$|\delta| < \frac{M(\alpha,x)^{1/2}}{\pi x} \left(\frac{4^\alpha}{x\, M(\alpha,x)} \right)^{m_1}.$$

Appealing to (4.30), since $x \geq 40$ and $\alpha \leq 9/2$, it follows that

$$\frac{4^\alpha}{x\, M(\alpha,x)} \leq \frac{4^\alpha}{\left(1+\frac{39}{40\alpha}\right)^\alpha 39\,(\alpha+1)} < 1,$$

whence, from (4.29),

$$|\delta| < \frac{M(\alpha,x)^{1/2}}{\pi x} < \frac{(e\,(\alpha+1))^{1/2}}{\pi x} < 0.031.$$

We may therefore apply Proposition 4.2.2 to conclude that

$$|Q_1| > 2.477\, x^{2m_0}. \tag{4.42}$$

From (4.25), Proposition 4.1.2, $\alpha \leq 9/2$ and $x \geq 40$, we have

$$|Q_1| < 6.81 \cdot 14.951^{m_1}\, (4x)^{m_0+m_1}$$

and so

$$x < \left(2.75 \cdot 14.951^{m_1}\, 4^{m_0+m_1}\right)^{\frac{1}{m_0-m_1}}. \tag{4.43}$$

We may check that $m_0 > 3.4m_1$ (so that $\alpha > 4.4$) whenever $m_0 \geq 96$ and hence, since the right hand side of (4.43) is monotone decreasing in m_0, may conclude that $x < 40$, a contradiction.

For $m_0 \leq 95$, we note that

$$\frac{m_1 m_2}{m_1+m_2} \leq m_1 = \left\lceil \frac{2m_0}{7} \right\rceil \leq \left\lceil \frac{2 \cdot 95}{7} \right\rceil = 28 < x$$

and hence may appeal to Proposition 4.2.4. It follows from (4.42) and $x \geq 40$

that

$$x < \left(\frac{C(m_2, 2)}{2.415} \binom{m_1 + m_2}{m_1} \right)^{\frac{1}{m_0 - m_1}}.$$

A short computation leads to the conclusion that $x < 40$, unless $m_0 = 4$ (in which case $x \leq 108$) or $m_0 = 18$ (whence $x \leq 40$). In the last case, we therefore have $x = 40$ and $m = 37$, and we may easily check that there are no corresponding solutions to equation (4.2). If $m_0 = 4$ (so that $m = 9$) and $40 \leq x \leq 108$, there are, similarly, no solutions to (4.2) with $n = 3$.

4.4.2 Case (2) : $n = 4,\ d = 3,\ n_0 = 1,\ x \geq 85$

We argue similarly in this case, choosing

$$m_1 = \left\lceil \frac{m_0}{3.23} \right\rceil \quad \text{and} \quad m_2 = m_0 + \left\lceil \frac{m_0}{3.23} \right\rceil,$$

so that $\alpha \leq 4.23$. From (4.41) and Proposition 4.1.2,

$$|\delta| < \frac{\sqrt{3}\, M(\alpha, x)^{1/3}}{2\,\pi x} \left(\frac{3^{3\alpha/2}}{x\, M(\alpha, x)} \right)^{m_1}.$$

Applying (4.30), $x \geq 85$ and $\alpha \leq 4.23$,

$$\frac{3^{3\alpha/2}}{x\, M(\alpha, x)} \leq \frac{3^{3\alpha/2}}{\left(1 + \frac{84}{85\alpha}\right)^{\alpha} 84\, (\alpha + 1)} < 1$$

and so

$$|\delta| < \frac{\sqrt{3}\, M(\alpha, x)^{1/3}}{2\,\pi x} < \frac{\sqrt{3}\, (e\, (\alpha + 1))^{1/3}}{2\,\pi x} < 0.008.$$

Proposition 4.2.2 thus implies

$$|Q_1| > 3.808\, x^{2m_0} \tag{4.44}$$

while (4.25), Proposition 4.1.2, $\alpha \leq 4.23$ and $x \geq 85$ give

$$|Q_1| < 6.5 \cdot 14.217^{m_1}\, (3\sqrt{3}\, x)^{m_0 + m_1}.$$

It follows that

$$x < \left(1.707 \cdot 14.217^{m_1} \, (3\sqrt{3})^{m_0+m_1}\right)^{\frac{1}{m_0-m_1}}. \tag{4.45}$$

We may check that $m_0 \geq 3.14 m_1$, for all $m_0 \geq 98$ (and $m_1 \geq 31$) and hence, for these m_0, we have $\alpha \geq 4.14$ and so

$$x < 1.707^{1/67} \cdot 14.217^{1/2.14} \cdot (3\sqrt{3})^{4.14/2.14},$$

which contradicts $x \geq 85$.

For $m_0 \leq 97$, we again find that

$$\frac{m_1 m_2}{m_1 + m_2} \leq m_1 = \left\lceil \frac{m_0}{3.23} \right\rceil \leq \left\lceil \frac{97}{3.23} \right\rceil = 31 < x$$

and hence, from Proposition 4.2.4, (4.44) and $x \geq 85$,

$$x < \left(\frac{C(m_2, 3)}{3.763} \binom{m_1 + m_2}{m_1} \right)^{\frac{1}{m_0-m_1}},$$

contradicting $x \geq 85$, unless we have $m_0 = 4$ and $x \leq 220$, or $m_0 = 7$ and $x \leq 138$, or $m_0 = 10$ and $x \leq 99$, or $m_0 = 13$ and $x \leq 110$, or $m_0 = 20$ and $x \leq 87$. In each case, we may verify that there are no solutions to equation (4.2). By way of example, if $m_0 = 4$, then $m = 13$ and a short computation reveals that, for $85 \leq x \leq 220$, there are no corresponding solutions to (4.2).

4.4.3 Case (3) : $n = 5, \ d = 2, \ n_0 = 2, \ x \geq 720$

In this case, we will take

$$m_1 = \left\lceil \frac{m_0}{5.906} \right\rceil \quad \text{and} \quad m_2 = m_0 + \left\lceil \frac{m_0}{5.906} \right\rceil,$$

so that $\alpha \leq 6.906$. From (4.41) and Proposition 4.1.2,

$$|\delta| < \frac{M(\alpha, x)^{1/2}}{\pi x} \left(\frac{4^{\alpha}}{x \, M(\alpha, x)} \right)^{m_1}.$$

Appealing to (4.30), since $x \geq 720$ and $\alpha \leq 6.906$, it follows that

$$\frac{4^\alpha}{x\,M(\alpha,x)} \leq \frac{4^\alpha}{\left(1+\frac{719}{720\alpha}\right)^\alpha \, 719\,(\alpha+1)} < 1,$$

whence, from (4.29),

$$|\delta| < \frac{M(\alpha,x)^{1/2}}{\pi x} < \frac{(e\,(\alpha+1))^{1/2}}{\pi x} < 0.003.$$

We may therefore apply Proposition 4.2.2 to conclude that

$$|Q_1| > 2.552\, x^{\frac{3}{2}m_0}. \tag{4.46}$$

On the other hand, from (4.25), Proposition 4.1.2, $\alpha \leq 6.906$ and $x \geq 720$ we have

$$|Q_1| < 9.058 \cdot 21.491^{m_1}\,(4x)^{m_0+m_1}.$$

It follows that

$$x < \left(3.550 \cdot 21.491^{m_1}\, 4^{m_0+m_1}\right)^{\frac{2}{m_0-2m_1}}.$$

We may check that $m_0 > 5.809m_1$ (so that $\alpha > 6.809$), for all $m_0 \geq 332$ and hence, for these m_0, we have

$$x < 3.550^{1/108} \cdot 21.491^{2/3.809} \cdot 4^{2+6/3.809}$$

which contradicts $x \geq 720$. For $m_0 \leq 331$,

$$\frac{m_1m_2}{m_1+m_2} \leq m_1 = \left\lceil \frac{m_0}{5.906} \right\rceil \leq \left\lceil \frac{331}{5.906} \right\rceil = 57 < x$$

and hence Proposition 4.2.4, (4.46) and $x \geq 720$ imply that

$$x < \left(\frac{C(m_2,2)}{2.548}\binom{m_1+m_2}{m_1}\right)^{\frac{2}{m_0-2m_1}},$$

contradicting $x \geq 720$, unless we have m_0 and $720 \leq x \leq x_0$ as follows :

m_0	x_0	m_0	x_0	m_0	x_0	m_0	x_0	m_0	x_0
3	63090	12	2780	19	992	31	834	54	836
6	578712	13	2531	20	909	36	859	55	723
7	12601	14	1177	24	1101	37	777	65	765
8	2605	15	755	25	847	42	849	71	768
9	762	18	1667	30	1103	48	767	83	734

Since we are assuming that m_0 is odd, because $\gcd(m-1, n-1) = 2$, this table reduces to the following:

m_0	x_0	m_0	x_0	m_0	x_0	m_0	x_0	m_0	x_0
3	63090	13	2531	25	847	55	723	83	734
7	12601	15	755	31	834	65	765		
9	762	19	992	37	777	71	768		

For these remaining triples $(x, n, m) = (x, 5, 2m_0 + 1)$, with $720 \leq x \leq x_0$, just as in the cases $n = 3$ and $n = 4$, we reach a contradiction upon explicitly verifying that there are no integers y satisfying equation (4.2).

4.4.4 Case (4) : $n = 5,\ d = 4,\ n_0 = 1,\ x \geq 300$

In this case, we will take

$$m_1 = \left\lceil \frac{m_0}{2.93} \right\rceil \quad \text{and} \quad m_2 = m_0 + \left\lceil \frac{m_0}{2.93} \right\rceil,$$

so that $\alpha \leq 3.93$. From (4.41) and Proposition 4.1.2,

$$|\delta| < \frac{\sqrt{2} M(\alpha, x)^{1/4}}{2\pi x} \left(\frac{8^{\alpha}}{x\, M(\alpha, x)} \right)^{m_1}.$$

Appealing to (4.30), since $x \geq 300$ and $\alpha \leq 3.93$, it follows that

$$\frac{8^\alpha}{x\,M(\alpha,x)} \leq \frac{8^\alpha}{\left(1+\frac{299}{300\alpha}\right)^\alpha 299\ (\alpha+1)} < 1,$$

whence, from (4.29),

$$|\delta| < \frac{\sqrt{2}M(\alpha,x)^{1/4}}{2\pi x} < \frac{\sqrt{2}(e\,(\alpha+1))^{1/4}}{2\pi x} < 0.002.$$

We may therefore apply Proposition 4.2.2 to conclude that

$$|Q_1| > 5.109\,x^{2m_0}. \tag{4.47}$$

On the other hand, from (4.25), Proposition 4.1.2, $\alpha \leq 3.93$ and $x \geq 300$ we have

$$|Q_1| < 6.19 \cdot 13.402^{m_1}\,(8x)^{m_0+m_1}.$$

It follows that

$$x < \left(1.212 \cdot 13.402^{m_1}\,8^{m_0+m_1}\right)^{\frac{1}{m_0-m_1}}.$$

We may check that $m_0 \geq 2.87m_1$ (so that $\alpha \geq 3.87$) for all $m_0 \geq 133$ (and hence for $m_1 \geq 46$) and hence, for these m_0, we have

$$x < 1.212^{1/87} \cdot 13.402^{1/1.87} \cdot 8^{3.87/1.87}$$

which contradicts $x \geq 300$.

For $m_0 \leq 132$,

$$\frac{m_1 m_2}{m_1+m_2} \leq m_1 = \left\lceil \frac{m_0}{2.93} \right\rceil \leq \left\lceil \frac{132}{2.93} \right\rceil = 46 < x$$

and hence Proposition 4.2.4, (4.47) and $x \geq 300$ imply that

$$x < \left(\frac{C(m_2,4)}{5.091}\binom{m_1+m_2}{m_1}\right)^{\frac{1}{m_0-m_1}}.$$

A short computation leads to the conclusion that $x < 300$ for all $m_0 \leq 132$, unless we have m_0 and $x \leq x_0$ as follows :

m_0	x_0	m_0	x_0	m_0	x_0
3	33791	7	350	15	343
4	600	9	502	18	315
6	1131	12	434		

In the remaining cases, we again reach a contradiction upon explicitly verifying that there are no integers y satisfying equation (4.2) (assuming thereby $x \geq 300$).

4.4.5 Treating the remaining small values of x for $n \in \{3, 4\}$

To deal with the remaining pairs (x, n) for $n \in \{3, 4, 5\}$, we can, in each case, reduce the problem to finding "integral points" on particular models of genus one curves. Such a reduction is not apparently available for larger values of n. In case $n \in \{3, 4\}$, this approach enables us to complete the proof of Theorem 4.0.2. When $n = 5$ (where we are left to treat values $2 \leq x < 720$), the resulting computations are much more involved. To complete them, we must work rather harder; we postpone the details to the next section.

Small values of x for $n = 3$

To complete the proof of Theorem 4.0.2 for $n = 3$, it remains to solve equation (4.2) with $2 \leq x \leq 39$. In this case, (4.2) becomes

$$y^2 + y + 1 = \frac{x^m - 1}{x - 1}, \tag{4.48}$$

whereby

$$\left(4(x-1)^2(2y+1)\right)^2 = 64(x-1)^3 x^m - 16(3x+1)(x-1)^3.$$

Writing $m = 3\kappa + \delta$ for $\kappa \in \mathbb{Z}$ and $\delta \in \{0, 1, 2\}$, we thus have

$$Y^2 = X^3 - k, \tag{4.49}$$

for

$$X = 4(x-1)x^{\kappa+\delta}, \;\; Y = 4(x-1)^2(2y+1)x^{\delta} \;\text{ and }\; k = 16(3x+1)(x-1)^3x^{2\delta}.$$

We solve equation (5.2.1) for the values of k arising from $2 \le x \le 39$ and $0 \le \delta \le 2$ rather quickly using Magma's *IntegralPoints* routine (see [17]). The only solutions we find with the property that $4(x-1)x^2 \mid X$ are those coming from trivial solutions corresponding to $m = 2$, together with $(x, \delta, X, |Y|)$ equal to one of

$$\begin{gathered}(2, 1, 128, 1448), (2, 2, 32, 176), (5, 2, 800, 22400), (8, 2, 3584, 213248),\\ (19, 2, 389880, 243441072), (26, 2, 11897600, 41038270000) \text{ or}\\ (27, 2, 227448, 108416880).\end{gathered}$$

Of these, only $(x, \delta, X, |Y|) = (2, 1, 128, 1448)$ and $(2, 2, 32, 176)$ have the property that $X = 4(x-1)x^t$ for t an integer, corresponding to the solutions $(x, y, m) = (2, 90, 13)$ and $(2, 5, 5)$ to equation (4.48), respectively.

Small values of x for $n = 4$

If $n = 4$ and we write $m = 2\kappa + \delta$, for $\kappa \in \mathbb{Z}$ and $\delta \in \{0, 1\}$, then (4.2) becomes

$$x^{\delta}(x^{\kappa})^2 = (x-1)(y^3 + y^2 + y + 1) + 1,$$

whereby

$$Y^2 = X^3 + x^{\delta}(x-1)X^2 + x^{2\delta}(x-1)^2X + x^{1+3\delta}\,(x-1)^2,$$

for

$$X = (x-1)x^{\delta}y \quad\text{and}\quad Y = (x-1)\,x^{\kappa+2\delta}.$$

Once again applying Magma's *IntegralPoints* routine, we find that the only points for $2 \leq x \leq 84$ and $\delta \in \{0,1\}$, and having $(x-1)x^2 \mid Y$ correspond to either trivial solutions to (4.2) with either $y = 0$ or $m = 4$, or have $\delta = 1$ and $(x, X, |Y|)$ among

$$(4, 48, 384), (9, 648, 17496), (16, 3840, 245760), (21, 1680, 79380),$$
$$(21, 465360, 317599380), (25, 15000, 1875000), (36, 45360, 9797760),$$
$$(41, 33620, 6320560), (49, 115248, 39530064), (64, 258048, 132120576),$$
$$(65, 10400, 1352000), (81, 524880, 382637520).$$

None of these triples lead to nontrivial solutions to (4.2) with $n = 4$.

4.5 Small values of x for $n = 5$

In case $n = 5$, solving equation (4.2) can, for a fixed choice of x, also be reduced to a question of finding integral points on a particular model of a genus 1 curve. Generally, for m odd, say $m = 2\kappa + 1$, we can rewrite (4.2) as

$$x\left(x^{\kappa}\right)^2 = (x-1)\left(y^4 + y^3 + y^2 + y + 1\right) + 1,$$

so that

$$\left(x^{\kappa+1}\right)^2 = \left(x^2 - x\right)\left(y^4 + y^3 + y^2 + y\right) + x^2.$$

Applying Magma's *IntegralQuarticPoints* routine, we may find solutions to the more general Diophantine equation

$$Y^2 = \left(x^2 - x\right)\left(y^4 + y^3 + y^2 + y\right) + x^2; \tag{4.50}$$

note that we always have, for each x, solutions $(y, Y) = (0, \pm x), (-1, \pm x)$ and $(x, \pm x^3)$.

Unfortunately, it does not appear that this approach is computationally efficient enough to solve equation (4.50) in a reasonable time for all values of x with $2 \leq x < 720$ (though it does work somewhat quickly for $2 \leq x \leq 59$ and various other $x < 720$). The elliptic curve defined by (4.50) has, in each case, rank at least

2 (the solutions corresponding to $(y, Y) = (0, x)$ and $(-1, x)$ are independent non-torsion points). Magma's *IntegralQuarticPoints* routine is based on bounds for linear forms in elliptic logarithms and hence requires detailed knowledge of the generators of the Mordell-Weil group. Thus, when the rank is much larger than 2, Magma's *IntegralQuarticPoints* routine can, in practice, work very slowly. This is the case, for example, when $x = 60$ (where the corresponding elliptic curve has rank 5 over $\mathbb{Q}$).

Instead, we will argue somewhat differently. We write (4.2) as

$$F_x(y, 1) = x^m, \tag{4.51}$$

where

$$F_x(y, z) = (x-1)(y^4 + y^3z + y^2z^2 + yz^3) + xz^4.$$

For the remainder of this section, we consider the homogeneous quartic form (4.51) for fixed x. Notably, we observe that this equation is a special case of the Thue-Mahler equation (3.1). In particular, if $x = p_1^{\alpha_1} \cdots p_v^{\alpha_v}$ is the prime factorization of x with $\alpha_i \geq 0$, then equation (4.51) becomes

$$F_x(y, 1) = p_1^{Z_1} \dots p_v^{Z_v} \tag{4.52}$$

where $Z_i = m\alpha_i$.

To find all solutions to this equation, we will use linear forms in p-adic logarithms to generate a very large upper bound on m. Then, applying several instances of the LLL lattice basis reduction algorithm, we will reduce the bound on m until it is sufficiently small enough that we may perform a brute force search efficiently. The remainder of this section is devoted to the details of this approach.

4.5.1 First steps and small bounds

Following arguments of Chapter 3 for solving Thue-Mahler equations, put $S = \{p_1, \dots, p_v\}$. This is the set of all distinct rational primes dividing x. As we seek only those solutions $(y, z, Z_1, \ldots, Z_v)$ to (4.52) for which $z = 1$, here and henceforth we write, for concision, $F(y) = F_x(y, 1)$.

Recall in Section 3.1 of Chapter 3 the set $\mathcal{D}$. This set consists of all positive rational integers m dividing $(x-1)$ such that $\mathrm{ord}_p(m) \leq \mathrm{ord}_p(c)$ for all primes $p \notin S$. In our case, $c = 1$ so that $\mathcal{D} = \{1\}$. Thus the only possible values for u_d, c_d are

$$u_d = (x-1)^3 \quad \text{and} \quad c_d = (x-1)^3.$$

Under the appropriate change of variables associated to u_d, c_d, this yields

$$g(t) = (x-1)^3 F\left(\frac{t}{x-1}\right) = t^4 + (x-1)t^3 + (x-1)^2 t^2 + (x-1)^3 t + x(x-1)^3.$$

Note that $g(t)$ is irreducible in $\mathbb{Z}[t]$. Writing $K = \mathbb{Q}(\theta)$ with $g(\theta) = 0$, it follows that (4.52) is equivalent to

$$N_{K/\mathbb{Q}}((x-1)y - \theta) = (x-1)^3 p_1^{Z_1} \ldots p_v^{Z_v}. \tag{4.53}$$

Let

$$(p_i)\mathcal{O}_K = \prod_{j=1}^{m_i} \mathfrak{p}_{ij}^{e(\mathfrak{p}_{ij}|p_i)}$$

be the factorization of p_i into prime ideals in the ring of integers $\mathcal{O}_K$ of K. In this decomposition, $e(\mathfrak{p}_{ij}|p_i)$ and $f(\mathfrak{p}_{ij}|p_i)$ denote the ramification index and residue degree of $\mathfrak{p}_{ij}$ respectively. Then, since $N(\mathfrak{p}_{ij}) = p_i^{f(\mathfrak{p}_{ij}|p_i)}$, equation (4.53) leads to finitely many ideal equations of the form

$$((x-1)y - \theta)\mathcal{O}_K = \mathfrak{a} \prod_{j=1}^{m_1} \mathfrak{p}_{1j}^{z_{1j}} \cdots \prod_{j=1}^{m_v} \mathfrak{p}_{vj}^{z_{vj}} \tag{4.54}$$

where $\mathfrak{a}$ is an ideal of norm $(x-1)^3$ and the z_{ij} are unknown integers related to m by $\sum_{j=1}^{m_i} f(\mathfrak{p}_{ij}|p_i) z_{ij} = Z_i = m\alpha_i$. Applying Algorithms 3.3.3 and 3.3.6, we reduce the number of prime ideals appearing to a large power in this equation. In doing so, we are reduced to solving finitely many equations of the form

$$((x-1)y-\theta)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{u_1}\cdots\mathfrak{p}_v^{u_v} \tag{4.55}$$

in integer variables $y, u_1, \ldots, u_v$ with $u_i \geq 0$ for $i = 1, \ldots, v$. Here

- for $i \in \{1, \ldots, v\}$, $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_K$ arising from Algorithm 3.3.3 and Algorithm 3.3.6 applied to $p \in \{p_1, \ldots, p_v\}$, such that $(\mathfrak{b}, \mathfrak{p}_i) \in M_p$ for some ideal $\mathfrak{b}$;
- for any $p_i \in S$ such that $M_{p_i} = \emptyset$, $\mathfrak{p}_i$ denotes the trivial ideal $\mathfrak{p}_i = (1)\mathcal{O}_K$;
- $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ of norm $(x-1)^3 \cdot p_1^{t_1}\cdots p_v^{t_v}$ such that $u_i + t_i = Z_i = m\alpha_i$.

Remark 4.5.1. Unlike in [112] and [44], if, after applying Algorithm 3.3.3 and Algorithm 3.3.6, we are in the situation that $u_i = 0$ for some i in $\{1, \ldots, v\}$, it follows that

$$m = \frac{Z_i}{\alpha_i} = \frac{u_i + t_i}{\alpha_i} = \frac{t_i}{\alpha_i}.$$

We iterate this computation over all $i \in \{1, \ldots, v\}$ such that $u_i = 0$ and take the smallest m as our bound. For all of the values of x that we are interested in, this bound on m is small enough that we may go directly to the final brute force search for solutions.

Following Remark 4.5.1, for the remainder of this paper, we assume that $u_i \neq 0$ for all $i = 1, \ldots, v$. Fix a complete set of fundamental units $\{\varepsilon_1, \ldots, \varepsilon_r\}$ of $\mathcal{O}_K$. Here $r = s + t - 1$, where s denotes the number of real embeddings of K into $\mathbb{C}$ and t denotes the number of complex conjugate pairs of non-real embeddings of K into $\mathbb{C}$. A quick computation in Maple shows that

$$g(t) = t^4 + (x-1)t^3 + (x-1)^2t^2 + (x-1)^3t + x(x-1)^3$$

has only complex roots for $x \geq 2$. It follows that we have no real embeddings of K into $\mathbb{R}$, two pairs of complex conjugate embeddings, and hence only one fundamental unit, ε_1.

Now, for each choice of $\mathfrak{a}$ and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_v$, we reduce each equation (4.55) to a number of so-called "S-unit equations" via either procedure outlined in Section 3.4.1 and Section 3.4.2 of Chapter 3. Regardless of which of these principalization methods is used, we arrive at finitely many equations of the form

$$(x-1)y-\theta = \alpha\zeta\varepsilon_1^{a_1}\gamma_1^{n_1}\cdots\gamma_v^{n_v} \tag{4.56}$$

with unknowns $a_1 \in \mathbb{Z}$, $n_i \in \mathbb{Z}_{\geq 0}$, and ζ in the set T of roots of unity in $\mathcal{O}_K$. Since T is also finite, we will treat ζ as another parameter. Moreover, we note that the ideal generated by α has norm

$$(x-1)^3 \cdot p_1^{t_1+r_1}\cdots p_v^{t_v+r_v}, \tag{4.57}$$

and the n_i are related to m via

$$m\alpha_i = Z_i = u_i + t_i = \sum_{j=1}^{v} n_j a_{ij} + r_i + t_i.$$

To summarize, our original problem of solving (4.52) is now reduced to the problem of solving finitely many equations of the form (4.57) for the variables

$$y, a_1, n_1, \ldots, n_v.$$

From here, we follow the arguments of Section 3.4.3 to deduce a so-called S-unit equation. In doing so, we eliminate the variable y and set ourselves the task of bounding the exponents $a_1, n_1, \ldots, n_v$.

In particular, let $p \in \{p_1, \ldots, p_v, \infty\}$. Denote the roots of $g(t)$ in $\overline{\mathbb{Q}_p}$ (where $\overline{\mathbb{Q}_\infty} = \overline{\mathbb{R}} = \mathbb{C}$) by $\theta^{(1)}, \ldots, \theta^{(4)}$. Let $i_0, j, k \in \{1, \ldots, 4\}$ be distinct indices and consider the three embeddings of K into $\overline{\mathbb{Q}_p}$ defined by $\theta \mapsto \theta^{(i_0)}, \theta^{(j)}, \theta^{(k)}$. We use $z^{(i)}$ to denote the image of z under the embedding $\theta \mapsto \theta^{(i)}$. Applying these embeddings to $\beta = (x-1)y - \theta$ yields

$$\lambda = \delta_1 \left(\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}\right)^{a_1} \prod_{i=1}^{v} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i} - 1 = \delta_2 \left(\frac{\varepsilon_1^{(i_0)}}{\varepsilon_1^{(j)}}\right)^{a_1} \prod_{i=1}^{v} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i}, \tag{4.58}$$

where

$$\delta_1 = \frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \cdot \frac{\alpha^{(k)}\zeta^{(k)}}{\alpha^{(j)}\zeta^{(j)}}, \quad \delta_2 = \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\alpha^{(i_0)}\zeta^{(i_0)}}{\alpha^{(j)}\zeta^{(j)}}$$

are constants.

Note that δ_1 and δ_2 are constants, in the sense that they do not depend upon $y, a_1, n_1, \ldots, n_v$.

Let $l \in \{1, \ldots, v\}$ and consider the prime $p = p_l$. From now on we make the following choice for the index i_0. Let $g_l(t)$ be the irreducible factor of $g(t)$ in $\mathbb{Q}_{p_l}[t]$ corresponding to the prime ideal $\mathfrak{p}_l$. Since $\mathfrak{p}_l$ has ramification index and residue degree equal to 1, $\deg(g_l[t]) = 1$. We choose $i_0 \in \{1, \ldots, 4\}$ so that $\theta^{(i_0)}$ is the root of $g_l(t)$. The indices of j, k are fixed, but arbitrary.

By Lemma 3.5.2, if $\mathrm{ord}_{p_l}(\delta_1) \neq 0$ for any $l \in \{1, \ldots, v\}$, then

$$\sum_{i=1}^{v} n_i a_{li} = \min\{\mathrm{ord}_{p_l}(\delta_1), 0\} - \mathrm{ord}_{p_l}(\delta_2).$$

For us, if this bound holds for any prime $p_l \in S$, it follows that

$$m = \frac{\sum_{j=1}^{v} n_j a_{lj} + r_l + t_l}{\alpha_l} = \frac{\min\{\mathrm{ord}_{p_l}(\delta_1), 0\} - \mathrm{ord}_{p_l}(\delta_2) + r_l + t_l}{\alpha_l}.$$

In particular, we iterate this computation over all $i \in \{1, \ldots, v\}$ for which Lemma 3.5.2 holds and take the smallest m as our bound on the solutions. We then compute all solutions below this bound using a simple brute force search.

For the remainder of this chapter, we may assume that $\mathrm{ord}_{p_l}(\delta_1) = 0$, since otherwise a reasonable bound is afforded by Lemma 3.5.2.

Following the notation of Section 3.5, we let

$$b_1 = 1, \quad b_{1+i} = n_i \text{ for } i \in \{1, \ldots, v\},$$

and

$$b_{v+2} = a_1.$$

Put

$$\alpha_1 = \log_{p_l} \delta_1, \quad \alpha_{1+i} = \log_{p_l} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(l)}} \right) \text{ for } i \in \{1, \ldots, v\},$$

and

$$\alpha_{v+2} = \log_{p_l} \left(\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(l)}} \right).$$

Define

$$\Lambda_l = \sum_{i=1}^{v+2} b_i \alpha_i.$$

Let L be a finite extension of $\mathbb{Q}_{p_l}$ containing δ_1, $\frac{\gamma_i^{(k)}}{\gamma_i^{(l)}}$ (for $i = 1, \ldots, v$), and $\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(l)}}$. Since finite p-adic fields are complete, $\alpha_i \in L$ for $i = 1, \ldots, v+2$ as well. Choose $\phi \in \overline{\mathbb{Q}_{p_l}}$ such that $L = \mathbb{Q}_{p_l}(\phi)$ and $\mathrm{ord}_{p_l}(\phi) > 0$. Let $G(t)$ be the minimal polynomial of ϕ over $\mathbb{Q}_{p_l}$ and let s be its degree. For $i = 1, \ldots, v+2$ write

$$\alpha_i = \sum_{h=1}^{s} \alpha_{ih} \phi^{h-1}, \quad \alpha_{ih} \in \mathbb{Q}_{p_l}.$$

Then

$$\Lambda_l = \sum_{h=1}^{s} \Lambda_{lh} \phi^{h-1}, \tag{4.59}$$

with

$$\Lambda_{lh} = \sum_{i=1}^{v+2} b_i \alpha_{ih}$$

for $h = 1, \ldots, s$.

We recall several important lemmata from Section 3.5 which we restate here.

Lemma 4.5.2. *For every $h \in \{1, \ldots, s\}$, we have*

$$\mathrm{ord}_{p_l}(\Lambda_{lh}) > \mathrm{ord}_{p_l}(\Lambda_l) - \frac{1}{2} \mathrm{ord}_{p_l}(\mathit{Disc}(G(t))).$$

Lemma 4.5.3. *If*

$$\sum_{i=1}^{v} n_i a_{li} > \frac{1}{p_l - 1} - \operatorname{ord}_{p_l}(\delta_2),$$

then

$$\operatorname{ord}_{p_l}(\Lambda_l) = \sum_{i=1}^{v} n_i a_{li} + \operatorname{ord}_{p_l}(\delta_2).$$

Lemma 4.5.4.

(i) If $\operatorname{ord}_{p_l}(\alpha_1) < \min_{2 \le i \le v+2} \operatorname{ord}_{p_l}(\alpha_i)$*, then*

$$\sum_{i=1}^{v} n_i a_{li} \le \max\left\{ \left\lfloor \frac{1}{p-1} - \operatorname{ord}_{p_l}(\delta_2) \right\rfloor, \left\lceil \min_{2 \le i \le v+2} \operatorname{ord}_{p_l}(\alpha_i) - \operatorname{ord}_{p_l}(\delta_2) \right\rceil - 1 \right\}$$

(ii) For all $h \in \{1, \dots, s\}$*, if* $\operatorname{ord}_{p_l}(\alpha_{1h}) < \min_{2 \le i \le v+2} \operatorname{ord}_{p_l}(\alpha_{ih})$*, then*

$$\sum_{i=1}^{v} n_i a_{li} \le \max\left\{ \left\lfloor \frac{1}{p-1} - \operatorname{ord}_{p_l}(\delta_2) \right\rfloor, \left\lceil \min_{2 \le i \le v+2} \operatorname{ord}_{p_l}(\alpha_{ih}) - \operatorname{ord}_{p_l}(\delta_2) + \nu_l \right\rceil - 1 \right\},$$

where

$$\nu_l = \frac{1}{2} \operatorname{ord}_{p_l}(\mathit{Disc}(G(t))).$$

Similar to Lemma 3.5.2, if Lemma 4.5.4 holds for p_l giving

$$\sum_{i=1}^{v} n_i a_{li} \le B_l$$

for some bound B_l as in the lemma, it follows that

$$m = \frac{\sum_{j=1}^{v} n_j a_{lj} + r_l + t_l}{\alpha_l} \le \frac{B_l + r_l + t_l}{\alpha_l}.$$

Again, we iterate this computation over all $l \in \{1, \dots, v\}$ for which Lemma 4.5.4 holds and take the smallest m as our bound on the solutions. We then compute all solutions below this bound using a simple naive search.

4.5.2 Bounding the $\sum_{j=1}^{v} n_j a_{ij}$

At this point, similar to [112], a very large upper bound for

$$\left(|a_1|, \sum_{j=1}^{v} n_j a_{1j}, \ldots, \sum_{j=1}^{v} n_j a_{vj}\right)$$

is derived using the theory of linear forms in logarithms. In practice, however, this requires that we compute the absolute logarithmic height of all terms of our so-called S-unit equation, (4.58). More often than not, this proves to be a computational bottleneck, and is best avoided whenever possible. In particular, the approach of Tzanakis and de Weger [112] requires the computation of the absolute logarithmic height of each algebraic number in the product of (4.58). Unfortunately, in many such instances, the fundamental units may be very large, with each coefficient having over 10^5 digits in their representation. Similarly, the generators of our principal ideals may also be very large, making elementary operations on them (such as division) a very time-consuming process. In the particular instance of $x = 60$, by way of example, each coefficient of α has in excess of 20,000 digits. As a result of this, computing the absolute logarithmic height of these elements, a process which must be done for each choice of parameters $\zeta, \mathfrak{a}, \mathfrak{p}_1, \ldots, \mathfrak{p}_v$, is computationally painful. Instead of this approach, we appeal to results of Bugeaud and Győry [21] to generate a (very large) upper bound for these quantities, which, while not sharp, will nevertheless prove adequate for our purposes. Following the notation of [21], we now describe this bound.

Arguing as in [21], put $Z_i = 4U_i + V_i$ with $U_i, V_i \in \mathbb{Z}$, $0 \leq V_i < 4$ for $i = 1, \ldots, v$ and let R_K and h_K be the regulator and class number of K, respectively. Let T be the set of all extensions to K of the places of $\{p_1, \ldots, p_v\}$. Let P denote $\max\{p_1, \ldots, p_v\}$, and let R_T denote the T-regulator of K. Further, let H be an upper bound for the maximum absolute value of the coefficients of F, namely $H = |x| = x$. Let $B = 3$, let $\log^* a$ denote $\max(\log(a), 1)$, and let

$$C_8 = \exp\left\{c_{24} P^N R_T (\log^* R_T) \left(\frac{\log^*(PR_T)}{\log^* P}\right)(R_K + vh_K + \log(HB'))\right\},$$

where $N = 24$, $B' \leq BHP^{4v} = 2xP^{4v}$, and

$$\begin{aligned} c_{24} &= 3^{v+1+25}(v+1)^{5(v+1)+12}N^{3(v+1)+16} \\ &= 3^{v+26}(v+1)^{5v+17}N^{3v+19}. \end{aligned}$$

Then, [21] shows that $p_i^{U_i} \leq C_8$. Now, $\log^*(PR_T)/\log^* P \leq 2\log^* R_T$, so that

$$C_8 \leq \exp\left\{c_{24}P^N R_T 2(\log^* R_T)^2(R_K + vh_K + \log(HB'))\right\}.$$

Lastly, we have, by [21] $R_T \leq R_K h_K (4\log^* P)^{4v}$. We note that the fundamental units of K may be very large, and so computing the regulator of K can be a very costly computation. To avoid this, we simply appeal to the upper bound of [21], namely

$$R_K < \frac{|\mathrm{Disc}(K)|^{1/2}(\log|\mathrm{Disc}(K)|)^3}{3!h_K}.$$

Now we have all of the components necessary to explicitly compute an upper bound on C_8, denoted C_9 in [21], from which it follows that

$$U_i \leq \frac{\log(C_9)}{\log p_i}$$

and hence

$$m\alpha_i = Z_i = 4U_i + V_i < \frac{4\log(C_9)}{\log(p_i)} + V_i < \frac{4\log(C_9)}{\log(p_i)} + 4.$$

We thus obtain the inequality

$$m < \frac{4\log(C_9)}{\alpha_i \log(p_i)} + \frac{4}{\alpha_i} = C_{10};$$

we compute this for all $p_i \in \{1, \ldots, v\}$ and select the smallest value of C_{10} as our bound on m.

From (4.57), it follows that

$$0 \leq \sum_{j=1}^{v} n_j a_{ij} = m\alpha_i - r_i - t_i \leq C_{10}\alpha_i - r_i - t_i.$$

At this point, converting this bound to a bound on m would yield far too large of an exponent to apply our brute force search. Instead, we must argue somewhat more carefully. Note that

$$||\mathbf{n}||_\infty = ||A^{-1}(\mathbf{u}-\mathbf{r})||_\infty \leq ||\mathbf{u}-\mathbf{r}||_\infty ||A^{-1}||_\infty,$$

and so

$$\max_{1\leq i\leq v} |n_i| \leq ||A^{-1}||_\infty \max_{1\leq i\leq v} \sum_{j=1}^{v} n_j a_{ij} \leq ||A^{-1}||_\infty \max_{1\leq i\leq v} (C_{10}\alpha_i - r_i - t_i) = C_{11}.$$

4.5.3 A bound for $|a_1|$

In this subsection, we establish an upper bound for $|a_1|$ by considering two cases separately. Our argument is based loosely on [112] but differs substantially in order to accommodate our new S-unit equation, which, unlike in [112], may now have negative exponents, n_i. In this subsection, $\theta^{(1)}, \ldots, \theta^{(4)}$ will denote the roots of $g(t)$ in $\mathbb{C}$. We order the roots of $g(t)$ in $\mathbb{C}$ so that

$$\theta^{(1)} = \overline{\theta^{3}} \quad \text{and} \quad \theta^{(2)} = \overline{\theta^{4}} \in \mathbb{C}.$$

Put

$$C_{12} = \left| \log \frac{(x-1)^3}{\min\limits_{1\leq i\leq 4} |\alpha^{(i)}\zeta^{(i)}|} + C_{10}\log x \right|$$

and

$$C_{13} = \sum_{j=1}^{v} \max_{1\leq i\leq 4} |\log|\gamma_j^{(i)}||$$

Set

$$C_{14} = \min\left(|\log|\varepsilon_1^{(1)}||, |\log|\varepsilon_1^{(2)}||\right)$$

and let C_{15} be any number satisfying $0 < C_{15} < \frac{C_{14}}{3}$. So we have

$$C_{14} - C_{15} > C_{14} - 3C_{15} > 0.$$

Lemma 4.5.5. *If* $\min\limits_{1 \le i \le 4} |(x-1)y - \theta^{(i)}| > e^{-C_{15}|a_1|}$*, we have*

$$|a_1| < \frac{C_{12} + C_{11}C_{13}}{C_{14} - 3C_{15}}.$$

Proof. Let $k \in \{1, 2\}$ be an index such that

$$C_{14} = \min\Big(|\log|\varepsilon_1^{(1)}||, |\log|\varepsilon_1^{(2)}||\Big) = |\log|\varepsilon_1^{(k)}||.$$

By (4.53),

$$|\beta^{(k)}| \cdot \prod_{i \ne k} |\beta^{(i)}| = (x-1)^3 \cdot p_1^{Z_1} \cdots p_v^{Z_v},$$

therefore

$$|(x-1)y - \theta^{(k)}| = |\beta^{(k)}| < (x-1)^3 \cdot x^{C_{10}} \cdot e^{3C_{15}|a_1|}.$$

Now,

$$|\varepsilon_1^{(k)a_1}| = \frac{|(x-1)y - \theta^{(k)}|}{|\alpha^{(k)}\zeta^{(k)}||\gamma_1^{(k)}|^{n_1} \cdots |\gamma_v^{(k)}|^{n_v}} < \frac{(x-1)^3 \cdot x^{C_{10}} \cdot e^{3C_{15}|a_1|}}{\min\limits_{1 \le i \le 4} |\alpha^{(i)}\zeta^{(i)}| \cdot |\gamma_1^{(k)}|^{n_1} \cdots |\gamma_v^{(k)}|^{n_v}}$$

from which it follows that

$$\log|\varepsilon_1^{(k)a_1}| < \log \frac{(x-1)^3}{\min\limits_{1 \le i \le 4} |\alpha^{(i)}\zeta^{(i)}|} + C_{10}\log x + 3C_{15}|a_1| - \sum_{j=1}^{v} n_j \log|\gamma_j^{(k)}|.$$

Taking absolute values yields

$$|a_1|C_{14} = |a_1||\log|\varepsilon_1^{(k)}| < C_{12} + 3C_{15}|a_1| + \sum_{j=1}^{v} |n_j| \log \gamma_j^{(k)}||.$$

Now

$$
\begin{aligned}
|a_1| &< \frac{C_{12} + \sum_{j=1}^{v} |n_j| |\log|\gamma_j^{(k)}||}{C_{14} - 3C_{15}} \\
&< \frac{C_{12} + C_{11} \sum_{j=1}^{v} |\log|\gamma_j^{(k)}||}{C_{14} - 3C_{15}} \\
&< \frac{C_{12} + C_{11}C_{13}}{C_{14} - 3C_{15}}.
\end{aligned}
$$

□

Now, put

$$C_{16} = \left\lfloor -\frac{1}{C_{15}} \log \min_{1 \le j \le t} |\mathrm{Im}(\theta^{(j)})| \right\rfloor.$$

Lemma 4.5.6. *If* $\min_{1 \le i \le n} |(x-1)y - \theta^{(i)}| \le e^{-C_{15}|a_1|}$, *then*

$$|a_1| \le C_{16}.$$

Proof.

$$e^{-C_{15}|a_1|} \ge |(x-1)y - \theta^{(i)}| \ge |\mathrm{Im}(\theta^{(i)})| \ge \min_{1 \le j \le t} |\mathrm{Im}(\theta^{(j)})|,$$

hence $|a_1| \le C_{16}$. □

It follows that

$$|a_1| \le \max\left\{ \frac{C_{12} + C_{11}C_{13}}{C_{14} - 3C_{15}}, C_{16} \right\}.$$

4.5.4 The reduction strategy

The upper bounds on

$$\left(|a_1|, \sum_{j=1}^{v} n_j a_{1j}, \ldots, \sum_{j=1}^{v} n_j a_{vj} \right)$$

are expected to be very large. Enumeration of the solutions by a naive search at this stage would be prohibitively expensive computationally. Instead, following the methods of [112], we reduce the above bound considerably by applying the LLL-algorithm to approximation lattices associated to the linear forms in logarithms obtained from (4.58).

In the standard algorithm for Thue-Mahler equations, this procedure is applied repeatedly to the real/complex and p-adic linear forms in logarithms until no further improvement on the bound is possible. The search space for solutions below this reduced bound can then be narrowed further using the Fincke-Pohst algorithm applied to the real/complex and p-adic linear forms in logarithms. Lastly, a sieving process and final enumeration of possibilities determines all solutions of the Thue-Mahler equation. In our situation however, after obtaining the above bounds, we apply the LLL algorithm for the p-adic linear forms in logarithms only.

In each step, we let N_l denote the current best upper bound on $\sum_{j=1}^{v} n_j a_{lj}$, let A_0 denote the current best upper bound on $|a_1|$, and let M denote the current best upper bound on m. We will use the notation

$$b_1 = 1, \quad b_{1+i} = n_i \text{ for } i \in \{1, \ldots, v\},$$

and

$$b_{v+2} = a_1$$

of Section Section 4.5.1 frequently. It will therefore be convenient to let B_l denote the current best upper bound for $|b_l|$ for $l = 1, \ldots, v+2$. Then

$$B_1 = 1 \quad \text{and} \quad B_{v+2} = A_0.$$

For $l = 1, \ldots, v$, using that

$$\sum_{j=1}^{v} n_j a_{lj} < N_l, \quad \text{for } l = 1, \ldots, v,$$

we compute

$$|n_l| \leq \max_{1 \leq i \leq v} |n_i| \leq ||A^{-1}||_\infty \max_{1 \leq i \leq v} \sum_{j=1}^{v} n_j a_{ij} \leq ||A^{-1}||_\infty \max_{1 \leq i \leq v} (N_i) = B_{l+1}.$$

For each $l \in \{1, \ldots, v\}$, our expectation is that the LLL algorithm will reduce the upper bound N_l to roughly $\log N_l$. Note that we expect the original upper bounds to be of size 10^{120} and hence a single application of our p_l-adic reduction procedure should yield a new bound N_l that is hopefully much smaller than 3000. Then we would have

$$m = \frac{\sum_{j=1}^{v} n_j a_{lj} + r_l + t_l}{\alpha_l} < \frac{N_l + r_l + t_l}{\alpha_l} = M < 3000$$

at which point we could simply search naively (i.e. by brute force) for all solutions arising from this S-unit equation. Of course, if this does not occur, we use our new upper bound on m, M, to reduce the bounds $N_1, \ldots, N_{l-1}, N_{l+1}, \ldots, N_v$ via

$$\sum_{j=1}^{v} n_j a_{ij} = m\alpha_i - r_i - t_i \leq M\alpha_i - r_i - t_i = N_i.$$

We then repeat this procedure with p_{l+1} until $M < 3000$. We note that for all x with $2 \leq x \leq 719$, the bound $m < 3000$ is, in each case, attained in 1 or 2 iterations of LLL.

Note also that if a bound on $\sum_{j=1}^{v} n_j a_{ij}$ is obtained via Lemma 4.5.4, then we similarly compute the bound M on m and enter the final search. We may do so because this bound always furnishes a bound on m that is smaller than 3000 for x with $2 \leq x \leq 719$.

Lastly, rather than testing each possible tuple $(|a_1|, |n_1|, \ldots, |n_v|)$ as in [112], our brute force search simply checks for solutions of (4.51) using the smallest bound obtained on m. Because of this, we may omit the reduction procedures on the real/complex linear forms in logarithms, and furthermore, we need only to reduce the bounds on $\sum_{j=1}^{v} n_j a_{ij}$ so that $M < 3000$.

4.5.5 The p_l-adic reduction procedure

In this section, we set some notation and give some preliminaries for the p_l-adic reduction procedures. Consider a fixed index $l \in \{1, \ldots, v\}$. Following Section 4.5.1, we have

$$\mathrm{ord}_{p_l}(\alpha_1) \geq \min_{2 \leq i \leq v+2} \mathrm{ord}_{p_l}(\alpha_i) \quad \text{and} \quad \mathrm{ord}_{p_l}(\alpha_{1h}) \geq \min_{2 \leq i \leq v+2} (\alpha_{ih}) \quad h = (1, \ldots, s).$$

Let I be the set of all indices $i' \in \{2, \ldots, v+2\}$ for which

$$\mathrm{ord}_{p_l}(\alpha_{i'}) = \min_{2 \leq i \leq v+2} \mathrm{ord}_{p_l}(\alpha_i).$$

We will identify two cases, the *special case* and the *general case*. The special case occurs when there is some index $i' \in I$ such that $\alpha_i/\alpha_{i'} \in \mathbb{Q}_{p_l}$ for $i = 1, \ldots, v+2$. The general case is when there is no such index.

In the special case, let $\hat{i}$ be an arbitrary index in I for which $\alpha_i/\alpha_{\hat{i}} \in \mathbb{Q}_{p_l}$ for every $i = 1, \ldots, v+2$. We further define

$$\beta_i = -\frac{\alpha_i}{\alpha_{\hat{i}}} \quad i = 1, \ldots, v+2,$$

and

$$\Lambda_l' = \frac{1}{\alpha_{\hat{i}}} \Lambda_l = \sum_{i=1}^{v+2} b_i(-\beta_i).$$

In the general case, we fix an $h \in \{1, \ldots, s\}$ arbitrarily. Then we let $\hat{i}$ be an index in $\{2, \ldots, v+2\}$ such that

$$\text{ord}_{p_l}(\alpha_{\hat{i}h}) = \min_{2 \leq i \leq v+2} (\alpha_{ih}),$$

and define

$$\beta_i = -\frac{\alpha_{ih}}{\alpha_{\hat{i}h}} \quad i = 1, \ldots, v+2,$$

and

$$\Lambda'_l = \frac{1}{\alpha_{\hat{i}h}} \Lambda_{lh} = \sum_{i=1}^{v+2} b_i(-\beta_i).$$

Now in both cases we have $\beta_i \in \mathbb{Z}_{p_l}$ for $i = 1, \ldots, v+2$.

Lemma 4.5.7. *Suppose*

$$\sum_{i=1}^{v} n_i a_{li} > \frac{1}{p_l - 1} - \text{ord}_{p_l}(\delta_2).$$

In the special case, we have

$$\text{ord}_{p_l}(\Lambda'_l) = \sum_{i=1}^{v} n_i a_{li} + d_l$$

with

$$d_l = \text{ord}_{p_l}(\delta_2) - \text{ord}_{p_l}(\alpha_{\hat{i}}).$$

In the general case we have

$$\text{ord}_{p_l}(\Lambda'_l) \geq \sum_{i=1}^{v} n_i a_{li} + d_l$$

with

$$d_l = \text{ord}_{p_l}(\delta_2) - \frac{1}{2}\text{ord}_{p_l}(\mathit{Disc}(G(t))) - \text{ord}_{p_l}(\alpha_{\hat{i}h}).$$

Proof. Immediate from Lemma 4.5.2 and Lemma 4.5.3. □

We now describe the p_l-adic reduction procedure. Let $\mu, W_2, \ldots, W_{v+2}$ denote positive integers. These are parameters that we will need to balance in order to obtain a good reduction for the upper bound of $\sum_{i=1}^{v} n_i a_{li}$. We will discuss how to choose these parameters later in this section. For each $x \in \mathbb{Z}_{p_l}$, let $x^{\{\mu\}}$ denote the unique rational integer in $[0, p_l^{\mu}-1]$ such that $\mathrm{ord}_{p_l}(x - x^{\mu}) \geq \mu$ (ie. $x \equiv x^{\{\mu\}} \pmod{p_l^{\mu}}$). Let Γ_μ be the $(v+1)$-dimensional lattice generated by the column vectors of the matrix

$$A_\mu = \begin{pmatrix} W_2 & & & & & & \\ & \ddots & & & 0 & & \\ & & W_{\hat{i}-1} & & & & \\ & & & W_{\hat{i}+1} & & & \\ & 0 & & & \ddots & & \\ W_{\hat{i}}\beta_2^{\{\mu\}} & \cdots & W_{\hat{i}}\beta_{\hat{i}-1}^{\{\mu\}} & W_{\hat{i}}\beta_{\hat{i}+1}^{\{\mu\}} & \cdots & W_{\hat{i}}\beta_{v+2}^{\{\mu\}} & W_{\hat{i}}p_l^{\mu} \end{pmatrix}.$$

Put

$$\lambda = \frac{1}{p_l^{\mu}} \sum_{i=1}^{v+2} b_i \left(-\beta_i^{\{\mu\}} \right)$$

and

$$\mathbf{y} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -W_{\hat{i}}\beta_1^{\mu} \end{pmatrix} \in \mathbb{Z}^{v+1}.$$

Of course, we must compute the β_i to p_l-adic precision at least μ in order to avoid errors here. We observe that $\mathbf{y} \in \Gamma_\mu$ if and only if $\mathbf{y} = \mathbf{0}$. To see that this is true, note that $\mathbf{y} \in \Gamma_\mu$ means there are integers $z_1, \ldots, z_{v+1}$ such that $\mathbf{y} = A_\mu [z_1, \ldots, z_{v+1}]^T$. The last equation of this equivalence forces $z_1 = \cdots = z_v = 0$ and $-\beta_1^{\{\mu\}} = z_{v+1} p_l^m$. Since $\beta_1^{\{\mu\}} \in [0, p_l^m - 1]$, we must then have $z_{v+1} = 0$ also. Hence $\mathbf{y} = \mathbf{0}$.

Put

$$Q = \sum_{i=2}^{v+2} W_i^2 B_i^2.$$

Lemma 4.5.8. *If* $\ell(\Gamma_\mu, \mathbf{y}) > Q^{1/2}$ *then*

$$\sum_{i=1}^{v} n_i a_{li} \leq \max\left\{\frac{1}{p_l - 1} - \mathrm{ord}_{p_l}(\delta_2), \mu - d_l - 1, 0\right\}$$

Proof. We prove the contrapositive. Assume

$$\sum_{i=1}^{v} n_i a_{li} > \frac{1}{p_l - 1} - \mathrm{ord}_{p_l}(\delta_2), \quad \sum_{i=1}^{v} n_i a_{li} > \mu - d_l \quad \text{and} \quad \sum_{i=1}^{v} n_i a_{li} > 0.$$

Consider the vector

$$\mathbf{x} = A_\mu \begin{pmatrix} b_2 \\ \vdots \\ b_{\hat{i}-1} \\ b_{\hat{i}+1} \\ \vdots \\ b_{v+2} \\ \lambda \end{pmatrix} = \begin{pmatrix} W_2 b_2 \\ \vdots \\ W_{\hat{i}-1} b_{\hat{i}-1} \\ W_{\hat{i}+1} b_{\hat{i}+1} \\ \vdots \\ W_{v+2} b_{v+2} \\ -W_{\hat{i}} b_{\hat{i}} \end{pmatrix} + \mathbf{y}.$$

By Lemma 6.6.2,

$$\mathrm{ord}_{p_l}\left(\sum_{i=1}^{v+2} b_i(-\beta_i)\right) = \mathrm{ord}_{p_l}(\Lambda_l') \geq \sum_{i=1}^{v} n_i a_{li} + d_l \geq \mu.$$

Since $\mathrm{ord}_{p_l}(\beta_i^{\{\mu\}} - \beta_i) \geq \mu$ for $i = 1, \ldots, v+2$, it follows that

$$\mathrm{ord}_{p_l}\left(\sum_{i=1}^{v+2} b_i(-\beta_i^{\{\mu\}})\right) \geq \mu,$$

so that $\lambda \in \mathbb{Z}$. Hence $\mathbf{x} \in \Gamma_\mu$. Now $\sum_{i=1}^{v} n_i a_{li} > 0$ so that there exists some i such that $n_i a_{li} \neq 0$, and in particular, $b_{1+i} = n_i \neq 0$. Thus we cannot have $\mathbf{x} = \mathbf{y}$.

Therefore,

$$\ell(\Gamma_\mu, \mathbf{y})^2 \leq |\mathbf{x} - \mathbf{y}|^2 = \sum_{i=2}^{v+2} W_i^2 b_i^2 \leq \sum_{i=2}^{v+2} W_i^2 |b_i|^2 \leq \sum_{i=2}^{v+2} W_i^2 B_i^2 = Q.$$

□

The reduction procedure works as follows. Taking A_μ as input, we first compute an LLL-reduced basis for Γ_μ. Then, we find a lower bound for $\ell(\Gamma_\mu, \mathbf{y})$. If the lower bound is not greater than $Q^{1/2}$ so that Lemma 4.5.8 does not give a new upper bound, we increase μ and try the procedure again. If we find that several increases of μ have failed to yield a new upper bound N_l and that the value of μ has become significantly larger than it was initially, we move onto the next $l \in \{1, \ldots, v\}$.

If the lower bound is greater than $Q^{1/2}$, Lemma 4.5.8 gives a new upper bound N_l for $\sum_{i=1}^{v} n_i a_{li}$ and hence for m

$$m = \frac{\sum_{j=1}^{v} n_j a_{lj} + r_l + t_l}{\alpha_l} < \frac{N_l + r_l + t_l}{\alpha_l} = M.$$

If $M < 3000$, we exit the algorithm and enter the brute force search. Otherwise, we update the bounds $N_1, \ldots, N_{l-1}, N_{l+1}, \ldots, N_v$ via

$$\sum_{j=1}^{v} n_j a_{ij} = m\alpha_i - r_i - t_i \leq M\alpha_i - r_i - t_i = N_i.$$

Then using

$$|n_l| \leq \max_{1 \leq i \leq v} |n_i| \leq ||A^{-1}||_\infty \max_{1 \leq i \leq v} \sum_{j=1}^{v} n_j a_{ij} \leq ||A^{-1}||_\infty \max_{1 \leq i \leq v} (N_i) = B_{l+1}.$$

we update the B_i and repeat the above procedure until $M < 3000$ or until no further improvement can be made on the B_i, in which case we move onto the next $l \in \{1, \ldots, v\}$.

4.5.6 Computational conclusions

Bottlenecks for this computation are generating the class group, generating the ring of integers of the splitting field of K (this is entirely because of a Magma issue and cannot be avoided) and generating the unit group.

An implementation of this algorithm is available at

http://www.nt.math.ubc.ca/BeGhKr/GESolverCode.

As before, we have, for each x, solutions $(x, y, m) = (x, -1, 1), (x, 0, 1)$, and $(x, x, 5)$. For x with $2 \leq x \leq 719$, we find additional solutions (x, y, m) among

$$(4, 1, 2), (5, 2, 3), (10, -2, 2), (10, -6, 4), (30, 2, 2), (60, -3, 2),$$
$$(120, 3, 2), (204, -4, 2), (340, 4, 2), (520, -5, 2).$$

Altogether, this computation took 3 weeks on a 16-core 2013 vintage MacPro, with the case $x = 710$ being the most time-consuming, taking roughly 5 days and 16 hours on a single core. This is the better timing attained for this value of x from our two approaches, computed using the class group to generate the S-unit equations. The most time-consuming job when computing the class group was $x = 719$, which took 10 days and 8 hours. However, using our alternate code, the better timing for $x = 719$ was only 2 hours. Without computing the class group, the most time-consuming process was $x = 654$, which took 2 days and 7 hours. However, this is the faster timing that was attained for this value of x, as computing the class group took roughly 4 days and 8 hours.

We list below some timings for our computation. These times are listed in seconds, with the second column indicating the algorithm requiring the computation of the class group, and the third column indicating the time taken by the algorithm which avoids the class group. In implementing these two algorithms, we terminated the latter algorithm if the program ran longer than its class group counterpart took. From these timings, it is clear that it is not always easy to predict which algorithm will prove faster.

x	Timing with $\mathrm{Cl}(K)$	Timing without $\mathrm{Cl}(K)$	Solutions
689	647.269	Terminated	$[-1,1],[0,1],[689,5]$
690	215306.420	Terminated	$[-1,1],[0,1],[690,5]$
691	456194.210	1821.049	$[-1,1],[0,1],[691,5]$
692	152385.640	Terminated	$[-1,1],[0,1],[692,5]$
693	36922.540	1908.230	$[-1,1],[0,1],[693,5]$
694	8288.190	Terminated	$[-1,1],[0,1],[694,5]$
695	362453.820	9786.649	$[-1,1],[0,1],[695,5]$
696	76273.470	Terminated	$[-1,1],[0,1],[696,5]$
697	14537.219	725.340	$[-1,1],[0,1],[697,5]$
698	451700.650	2708.920	$[-1,1],[0,1],[698,5]$

Full computational details are available at

http://www.nt.math.ubc.ca/BeGhKr/GESolverData,

including the timings obtained for each value of x, under both iterations of the algorithm.

This completes the proof of Theorem 4.0.2.

4.6 Bounding $C(k,d)$: the proof of Proposition 4.1.2

To complete the proof of Proposition 4.1.2, from (4.12), it remains to show that $\prod_{p|d} p^{1/(p-1)} < 2\log d$, provided $d > 2$. We verify this by explicit calculation for all $d \le d_0 = 10^5$.

Since $\log p/(p-1)$ is decreasing in p, if we denote by $\omega(d)$ the number of distinct prime divisors of d, we have

$$\sum_{p|d} \frac{\log p}{p-1} \le \sum_{p \le p_{\omega(d)}} \frac{\log p}{p-1}, \tag{4.60}$$

where p_k denotes the kth smallest prime. Since we have

$$\sum_{p \le p_{10}} \frac{\log p}{p-1} < \log(2\log(d_0)),$$

we may thus suppose that $\omega(d) \ge 11$, whereby

$$d \ge d_1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 = 200560490130.$$

The fact that

$$\sum_{p \le p_{21}} \frac{\log p}{p-1} < \log(2\log(d_1))$$

thus implies that $\omega(d) \ge 22$ and

$$d \ge d_2 = \prod_{1 \le i \le 22} p_i > 3 \cdot 10^{30}.$$

We iterate this argument, finding that

$$\sum_{p \le p_{\kappa(j)}} \frac{\log p}{p-1} < \log(2\log(d_j)),$$

so that

$$d \ge d_{j+1} = \prod_{1 \le i \le \kappa(j)+1} p_i,$$

for $j = 0, 1, 2, 3, 4$ and 5, where

$$\kappa(0) = 10,\ \kappa(1) = 21,\ \kappa(2) = 50,\ \kappa(3) = 130,\ \kappa(4) = 361 \text{ and } \kappa(5) = 1055.$$

We thus have that $\omega(d) \ge 1056$ and

$$d \ge \prod_{1 \le i \le 1056} p_i > e^{8316}.$$

We may thus apply Théorème 12 of of Robin [91] to conclude that

$$\omega(d) \leq \frac{\log d}{\log\log d} + 1.4573\,\frac{\log d}{(\log\log d)^2} < \frac{7\,\log d}{6\,\log\log d},$$

while the Corollary to Theorem 3 of Rosser-Schoenfeld yields

$$p_n < n(\log n + \log\log n) < \frac{10}{9} n \log n.$$

It follows that

$$p_{\omega(d)} < \frac{35}{27}\,\frac{\log d}{\log\log d} \log\left(\frac{7\,\log d}{6\,\log\log d}\right) < \frac{35}{27}\,\log d.$$

By Theorem 6 of Rosser-Schoenfeld, we have

$$\sum_{p<x} \frac{\log p}{p} < \log x - 1.33258 + \frac{1}{2\log x}, \tag{4.61}$$

for all $x \geq 319$. Also, if $j \geq 2$,

$$\int_k^\infty \frac{\log u}{u^j} du = \frac{(j-1)\log(k)+1}{(j-1)^2 k^{j-1}}. \tag{4.62}$$

For $2 \leq j \leq 10$, we have

$$\sum_{p<x} \frac{\log p}{p^j} < \sum_{p<10^6} \frac{\log p}{p^j} + \sum_{p>10^6} \frac{\log p}{p^j} < \sum_{p<10^6} \frac{\log p}{p^j} + \int_{10^6}^\infty \frac{\log u}{u^j} du,$$

whereby

$$\sum_{p<x} \frac{\log p}{p^j} < \sum_{p<10^6} \frac{\log p}{p^j} + \frac{(j-1)\log(10^6)+1}{(j-1)^2 10^{6(j-1)}}. \tag{4.63}$$

By explicit computation, from (4.63), we find that

$$\sum_{j=2}^{10} \sum_{p<x} \frac{\log p}{p^j} < 0.755, \tag{4.64}$$

while, from (4.62),

$$\sum_{j\geq 11}\sum_{p<x}\frac{\log p}{p^j}<\sum_{j\geq 11}\frac{(j-1)\log(2)+1}{(j-1)^2 2^{j-1}}<\sum_{j\geq 11}\frac{1}{(j-1)2^{j-1}}. \tag{4.65}$$

Evaluating this last sum explicitly, it follows that

$$\sum_{j\geq 2}\sum_{p<x}\frac{\log p}{p^j}<0.755+\log(2)-\frac{447047}{645120}<0.756,$$

whereby, from (4.61), if $x\geq 319$,

$$\sum_{p<x}\frac{\log p}{p-1}<\log x-0.489.$$

Applying this last inequality with $x=\frac{35}{27}\log d>\frac{35}{27}\cdot 8316=10780$, we conclude from our earlier arguments that

$$\sum_{p\mid d}\frac{\log p}{p-1}<\log\log d.$$

This completes the proof of Proposition 4.1.2.

4.7 Concluding remarks

The techniques employed in this chapter may be used, with very minor modifications, to treat equation (4.2), subject to condition (4.1), with the variables x and y integers (rather than just positive integers). Since

$$\frac{(-a-1)^3-1}{(-a-1)-1}=\frac{a^3-1}{a-1},$$

in addition to the known solutions $(x,y,m,n)=(2,5,5,3)$ and $(2,90,13,3)$ to (4.2), we also find $(x,y,m,n)=(2,-6,5,3)$ and $(2,-91,13,3)$, where we have assumed that $|y|>|x|>1$. Beyond these, a short computer search uncovers only three more integer tuples (x, y, m, n) satisfying

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}, \quad m > n \geq 3, \quad |y| > |x| > 1,$$

namely

$$(x, y, m, n) = (-2, -7, 7, 3), (-2, 6, 7, 3) \text{ and } (-6, 10, 5, 4).$$

Perhaps there are no others; we can prove this to be the case if, for example, $n = 3$, subject to (4.1). This result was obtained earlier as Corollary 4.1 of Yuan [117], though the statement there overlooks the solutions $(x, y, m, n) = (-2, 6, 7, 3), (2, -6, 5, 3)$ and $(2, -91, 13, 3)$.

Chapter 5

Computing Elliptic Curves over $\mathbb{Q}$

A classical result of Shafarevich [95] implies that, given fixed set of prime numbers S, there are only finitely many $\mathbb{Q}$-isomorphism classes of elliptic curves defined over $\mathbb{Q}$ with good reduction outside S. In 1970, Coates [25] proved an effective version of this theorem, using bounds for linear forms in p-adic and complex logarithms. Early attempts to make these results explicit, for fixed sets of small primes, overlap with the arguments of [25], in that they reduce the problem to solving a number of *Thue-Mahler equations*. These are Diophantine equations of the form

$$F(x, y) = u. \tag{5.1}$$

Here, F is a binary form of degree 3 or greater, with integer coefficients, and u is an S-*unit* – an integer whose prime factors are contained in S. The number of solutions in relatively prime integers x and y to equation (5.1), provided that F is irreducible, is known to be finite, via work of Mahler [67]. This generalizes a classical result of Thue [108] who had proved an analogous statement for the case of u fixed in equation (5.1). When F is a reducible form in $\mathbb{Z}[x, y]$, equation (5.1) is typically less difficult to solve; in the context of finding elliptic curves, this situation arises from consideration of elliptic curves with at least one nontrivial rational 2-torsion point. The first examples where all elliptic curves $E/\mathbb{Q}$ with good reduction outside a given set S were determined were for $S = \{2, 3\}$ by Coghlan [26] and Stephens [106] (see also [14]), and for $S = \{p\}$ for certain small primes p – see e.g. Setzer [94] and Neumann [82]. Each of these examples corresponds, via our approach, to cases with reducible forms. Agrawal, Coates, Hunt and van der Poorten [1] carried out the first analysis where irreducible forms in equation (5.1) were treated to find elliptic curves of given conductor (dealing with the case $S = \{11\}$). In this situation, the reduction to equation (5.1) is not particular involved, but subsequent computations are quite difficult; they use arguments from [25] and a range of techniques from computational Diophantine approximation.

It appears that there are very few subsequent attempts in the literature to compute elliptic curves of given conductor through the solution of Thue-Mahler equations. Instead, one finds a wealth of results which approach the problem via modular forms. This route relies upon the Modularity theorem (see Wiles [116] and Breuil, Conrad, Diamond and Taylor [18]), which was actually still conjectural when these ideas were first implemented. To find all $E/\mathbb{Q}$ of conductor N by this method, one computes the space of $\Gamma_0(N)$ modular symbols and the action of the Hecke algebra on it, and then searches for one-dimensional rational eigenspaces. After calculating a large number of Hecke eigenvalues, one is then able to extract corresponding elliptic curves. For a detailed description of how this technique works, the reader is directed to [30]. The great computational success of this approach can be primarily attributed to Cremona (see e.g. [29], [30]) and his collaborators; they have devoted many years of work to it and are responsible for the current state-of-the-art. In particular, at the time of writing in 2017, all $E/\mathbb{Q}$ of conductor $N \leq 400000$ have been determined by these methods.

In the chapter at hand, we return to techniques based upon solving Thue-Mahler equations, using a number of results from classical invariant theory. Our aim is to give a straightforward demonstration of the link between the conductors in question and the corresponding equations, and to make the Diophantine approximation problem that follows as easy to tackle as possible. It is worth noting here that these connections are quite straightforward for primes $p > 3$, but require careful analysis at the primes 2 and 3. We will demonstrate our approach for a number of specific conductors and sets S, and then focus our main computational efforts on curves with bad reduction at a single prime (i.e. curves of conductor p or p^2 for p prime). In these cases, the computations simplify significantly and we are able to find all curves of prime conductor up to 2×10^9 (10^{10} in the case of curves of positive discriminant) and conductor p^2 for $p \leq 5 \times 10^5$. We then extend these computations in the case of conductor p, for prime $p \leq 2 \times 10^{13}$, and conductor p^2 for prime $p \leq 10^{10}$. We are not, however, able to guarantee completeness for these extended computations (we will discuss this further in what follows).

5.1 Elliptic curves

Our basic problem is to find a model for each isomorphism class of elliptic curves over $\mathbb{Q}$ with a given conductor. Let $S = \{p_1, p_2, \ldots, p_k\}$ where the p_i are distinct primes, and fix a conductor $N = p_1^{\eta_1} \cdots p_k^{\eta_k}$ for $\eta_i \in \mathbb{N}$. Any curve of conductor N has a minimal model

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

with the a_i integral and discriminant

$$\Delta_E = (-1)^\delta p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

where the γ_i are positive integers satisfying $\gamma_i \geq \eta_i$, for each $i = 1, 2, \ldots, k$, and $\delta \in \{0, 1\}$.

Writing

$$b_2 = a_1^2 + 4a_2, \;\; b_4 = a_1a_3 + 2a_4, \;\; b_6 = a_3^2 + 4a_6, \;\; c_4 = b_2^2 - 24b_4$$

and

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

we have $1728\Delta_E = c_4^3 - c_6^2$ and $j_E = c_4^3/\Delta_E$. It follows that

$$c_6^2 = c_4^3 + (-1)^{\delta+1}2^6 \cdot 3^3 \cdot p_1^{\gamma_1} \cdots p_k^{\gamma_k}. \tag{5.2}$$

In fact, it is equation (5.2) that lies at the heart of our method (see also Cremona and Lingham [33] for an approach to the problem that takes as its starting point equation (5.2), but subsequently heads in a rather different direction).

Let $\nu_p(x)$ be the largest power of a prime p dividing a nonzero integer x. Since our model is minimal, we may suppose (via Tate's algorithm; see, for example, Papadopoulos [84]) that

$$\min\{3\nu_p(c_4), 2\nu_p(c_6)\} < 12 + 12\nu_p(2) + 6\nu_p(3),$$

for each prime p, while

$$\nu_p(N_E) \leq 2 + \nu_p(1728).$$

For future use, it will be helpful to have a somewhat more precise determination of the possible values of $\nu_p(c_4)$ and $\nu_p(c_6)$ we encounter. We compile this data from Papadopoulos [84] and summarize it in Tables 5.1, 5.2 and 5.3.

$\nu_2(c_4)$	$\nu_2(c_6)$	$\nu_2(\Delta_E)$	$\nu_2(N)$
0	0	≥ 0	$\min\{1, \nu_2(\Delta_E)\}$
≥ 4	3	0	0
≥ 4	5	4	2, 3 or 4
≥ 4	≥ 6	6	5 or 6
4	6	7	7
4	6	8	2, 3 or 4
4	6	9	5
4	6	10 or 11	3 or 4
4	6	≥ 12	4
5	7	8	7
≥ 6	7	8	2, 3 or 4

$\nu_2(c_4)$	$\nu_2(c_6)$	$\nu_2(\Delta_E)$	$\nu_2(N)$
5	≥ 8	9	8
≥ 6	8	10	6
6	≥ 9	12	5 or 6
6	9	≥ 14	6
7	9	12	5
≥ 8	9	12	4
6	9	13	7
7	10	14	7
7	≥ 11	15	8
≥ 8	10	14	6

Table 5.1: The possible values of $\nu_2(c_4), \nu_2(c_6), \nu_2(\Delta_E)$ and $\nu_2(N)$.

$\nu_3(c_4)$	$\nu_3(c_6)$	$\nu_3(\Delta_E)$	$\nu_3(N)$
0	0	≥ 0	$\min\{1, \nu_3(\Delta_E)\}$
1	≥ 3	0	0
≥ 2	3	3	2 or 3
2	4	3	3
2	≥ 5	3	2
2	3	4	4
2	3	5	3
2	3	≥ 6	2
≥ 3	4	5	5
3	5	6	4

$\nu_3(c_4)$	$\nu_3(c_6)$	$\nu_3(\Delta_E)$	$\nu_3(N)$
3	≥ 6	6	2
≥ 4	5	7	5
≥ 4	6	9	2 or 3
4	7	9	3
4	≥ 8	9	2
4	6	10	4
4	6	11	3
≥ 5	7	11	5
5	8	12	4
≥ 6	8	13	5

Table 5.2: The possible values of $\nu_3(c_4), \nu_3(c_6), \nu_3(\Delta_E)$ and $\nu_3(N)$.

$\nu_p(c_4)$	$\nu_p(c_6)$	$\nu_p(\Delta_E)$	$\nu_p(N)$
0	0	≥ 1	1
≥ 1	1	2	2
1	≥ 2	3	2
≥ 2	2	4	2
≥ 2	≥ 3	6	2

$\nu_p(c_4)$	$\nu_p(c_6)$	$\nu_p(\Delta_E)$	$\nu_p(N)$
2	3	≥ 7	2
≥ 3	4	8	2
3	≥ 5	9	2
≥ 4	5	10	2

Table 5.3: The possible values of $\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)$ and $\nu_p(N)$ when $p > 3$ is prime and $p \mid \Delta_E$.

5.2 Cubic forms : the main theorem and algorithm

Having introduced the notation we require for elliptic curves, we now turn our attention to cubic forms and our main result. Fix integers a, b, c and d, and consider the binary cubic form

$$F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3, \tag{5.3}$$

with discriminant

$$D_F = -27a^2d^2 + b^2c^2 + 18abcd - 4ac^3 - 4b^3d. \tag{5.4}$$

To any such form, we can associate a pair of covariants, the Hessian $H = H_F$:

$$H = H_F(x, y) = -\frac{1}{4}\left(\frac{\partial^2 F}{\partial x^2}\frac{\partial^2 F}{\partial y^2} - \left(\frac{\partial^2 F}{\partial x \partial y}\right)^2\right)$$

and the Jacobian determinant of F and H, a cubic form $G = G_F$ defined by

$$G = G_F(x, y) = \frac{\partial F}{\partial x}\frac{\partial H}{\partial y} - \frac{\partial F}{\partial y}\frac{\partial H}{\partial x}.$$

A quick computation reveals that, explicitly,

$$H = (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2$$

and

$$\begin{aligned} G = {} & (-27a^2d + 9abc - 2b^3)x^3 + (-3b^2c - 27abd + 18ac^2)x^2y \\ & +(3bc^2 - 18b^2d + 27acd)xy^2 + (-9bcd + 2c^3 + 27ad^2)y^3. \end{aligned}$$

These satisfy the syzygy

$$4H(x, y)^3 = G(x, y)^2 + 27D_F F(x, y)^2 \tag{5.5}$$

as well as the resultant identities:

$$\mathrm{Res}(F, G) = -8D_F^3 \quad \text{and} \quad \mathrm{Res}(F, H) = D_F^2. \tag{5.6}$$

Note here that we could just as readily work with $-G$ instead of G here (corresponding to taking the Jacobian determinant of H and F, rather than of F and H). Indeed, as we shall observe in Section 5.4.4, for our applications we will, in some sense, need to consider both possibilities.

Notice that if we set $(x, y) = (1, 0)$ and multiply through by $\mathcal{D}^6/4$ (for any rational

$\mathcal{D}$), then this syzygy can be rewritten as

$$(\mathcal{D}^2H(1,0))^3 - \left(\frac{\mathcal{D}^3}{2}G(1,0)\right)^2 = 1728 \cdot \frac{\mathcal{D}^6 D_F}{256}F(1,0)^2.$$

Given an elliptic curve with corresponding invariants c_4, c_6 and Δ_E, we will show that it is always possible to construct a binary cubic form F, with corresponding $\mathcal{D}$ for which

$$\mathcal{D}^2H(1,0) = c_4, \quad -\frac{1}{2}\mathcal{D}^3G(1,0) = c_6 \text{ and } \Delta_E = \frac{\mathcal{D}^6 D_F F(1,0)^2}{256}$$

(and hence equation (5.2) is satisfied). This is the basis of the proof of our main result, which provides an algorithm for computing all isomorphism classes of elliptic curves $E/\mathbb{Q}$ with conductor a fixed positive integer N. Though we state our result for curves with $j_E \neq 0$, the case $j_E = 0$ is easy to treat separately (see Section 5.2.1).

Theorem 5.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N = 2^\alpha 3^\beta N_0$, where N_0 is coprime to* 6 *and* $0 \leq \alpha \leq 8$, $0 \leq \beta \leq 5$. *Suppose further that $j_E \neq 0$. Then there exists an integral binary cubic form F of discriminant*

$$D_F = \mathit{sign}(\Delta_E)2^{\alpha_0}3^{\beta_0}N_1,$$

and relatively prime integers u and v with

$$F(u,v) = \omega_0u^3 + \omega_1u^2v + \omega_2uv^2 + \omega_3v^3 = 2^{\alpha_1} \cdot 3^{\beta_1} \cdot \prod_{p \mid N_0} p^{\kappa_p}, \tag{5.7}$$

such that E is isomorphic over $\mathbb{Q}$ to $E_{\mathcal{D}}$, where

$$E_{\mathcal{D}} \quad : \quad 3^{[\beta_0/3]}y^2 = x^3 - 27\mathcal{D}^2H_F(u,v)x + 27\mathcal{D}^3G_F(u,v) \tag{5.8}$$

and, for $[r]$ the greatest integer not exceeding a real number r,

$$\mathcal{D} = \prod_{p \mid \gcd(c_4(E),c_6(E))} p^{\min\{[\nu_p(c_4(E))/2],[\nu_p(c_6(E))/3]\}}. \tag{5.9}$$

The α_0, α_1, β_0, β_1 and N_1 are nonnegative integers satisfying $N_1 \mid N_0$,

$$(\alpha_0, \alpha_1) = \begin{cases} (2,0) \textit{ or } (2,3) & \textit{if } \alpha = 0, \\ (3, \geq 3) \textit{ or } (2, \geq 4) & \textit{if } \alpha = 1, \\ (2,1), (4,0) \textit{ or } (4,1) & \textit{if } \alpha = 2, \\ (2,1), (2,2), (3,2), (4,0) \textit{ or } (4,1) & \textit{if } \alpha = 3, \\ (2, \geq 0), (3, \geq 2), (4,0) \textit{ or } (4,1) & \textit{if } \alpha = 4, \\ (2,0) \textit{ or } (3,1) & \textit{if } \alpha = 5, \\ (2, \geq 0), (3, \geq 1), (4,0) \textit{ or } (4,1) & \textit{if } \alpha = 6, \\ (3,0) \textit{ or } (4,0) & \textit{if } \alpha = 7, \\ (3,1) & \textit{if } \alpha = 8 \end{cases}$$

and

$$(\beta_0, \beta_1) = \begin{cases} (0,0) & \textit{if } \beta = 0, \\ (0, \geq 1) \textit{ or } (1, \geq 0) & \textit{if } \beta = 1, \\ (3,0), (0, \geq 0) \textit{ or } (1, \geq 0) & \textit{if } \beta = 2, \\ (\beta, 0) \textit{ or } (\beta, 1) & \textit{if } \beta \geq 3. \end{cases}$$

The κ_p are nonnegative integers with

$$\nu_p(\Delta_E) = \begin{cases} \nu_p(D_F) + 2\kappa_p & \textit{if } p \nmid \mathcal{D}, \\ \nu_p(D_F) + 2\kappa_p + 6 & \textit{if } p \mid \mathcal{D} \end{cases} \tag{5.10}$$

and

$$\kappa_p \in \{0, 1\} \quad \textit{whenever} \quad p^2 \mid N_1. \tag{5.11}$$

Further, we have

$$\textit{if} \quad \beta_0 \geq 3, \quad \textit{then} \;\; 3 \mid \omega_1 \textit{ and } 3 \mid \omega_2, \tag{5.12}$$

and

$$\textit{if } \nu_p(N) = 1, \textit{ for } p \geq 3, \textit{ then } p \mid D_F F(u, v). \tag{5.13}$$

Here, as we shall make explicit in the next subsection, the form F corresponding to the curve E in Theorem 5.2.1 determines the 2-division field of E. This connection was noted by Rubin and Silverberg [92] in a somewhat different context – they proved that if K is a field of characteristic $\neq 2, 3$, $F(u, v)$ is a binary cubic form defined over K, E is an elliptic curve defined by $y^2 = F(x, 1)$, and E_0 is another elliptic curve over K with the property that $E[2] \cong E_0[2]$ (as Galois modules), then E_0 is isomorphic to the curve

$$y^2 = x^3 - 3H_F(u, v)x + G_F(u, v),$$

for some $u, v \in K$.

5.2.1 Remarks

Before we proceed, there are a number of observations we should make regarding Theorem 5.2.1.

Historical comments

Theorem 5.2.1 is based upon a generalization of classical work of Mordell [75] (see also Theorem 3 of Chapter 24 of Mordell [77]), in which the Diophantine equation

$$X^2 + kY^2 = Z^3$$

is treated through reduction to binary cubic forms and their covariants, under the assumption that X and Z are coprime. That this last restriction can, with some care, be eliminated, was noted by Sprindzuk (see Chapter VI of [103]). A similar approach to this problem can be made through the invariant theory of binary quartic forms, where one is led to solve, instead, equations of the shape

$$X^2 + kY^3 = Z^3.$$

We will not carry out the analogous analysis here.

2-division fields and reducible forms

It might happen that the form F whose existence is guaranteed by Theorem 5.2.1 is reducible over $\mathbb{Z}[x, y]$. This occurs precisely when the elliptic curve E has a nontrivial rational 2-torsion point. This follows from the more general fact that the cubic form $F(u, v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 u v^2 + \omega_3 v^3$ corresponding to an elliptic curve E has the property that the splitting field of $F(u, 1)$ is isomorphic to the 2-division field of E. This is almost immediate from the identity

$$\begin{aligned} 3^3\, \omega_0^2\, F\left(\tfrac{x-\omega_1}{3\omega_0}, 1\right) &= x^3 + (9\omega_0\omega_2 - 3\omega_1^2)x + 27\omega_0^2\omega_3 - 9\omega_0\omega_1\omega_2 + 2\omega_1^3 \\ &= x^3 - 3H_F(1,0)x + G_F(1,0). \end{aligned}$$

Indeed, from (5.8), the elliptic curve defined by the equation $y^2 = x^3 - 3H_F(1,0)x + G_F(1,0)$ is a quadratic twist of that given by the model $y^2 = x^3 - 27c_4(E)x - 54c_6(E)$, and hence also of E (whereby they have the same 2-division field).

Imprimitive forms

It is also the case that the cubic forms arising need not be primitive (in the sense that $\gcd(\omega_0, \omega_1, \omega_2, \omega_3) = 1$). This situation can occur if each of the coefficients of F is divisible by some integer $g \in \{2, 3, 6\}$. Since the discriminant is a quartic form in the coefficients of F, for this to take place one requires that

$$D_F \equiv 0 \mod g^4.$$

This is a necessary but not sufficient condition for the form F to be imprimitive. It follows, if we wish to restrict attention to primitive forms in Theorem 5.2.1, that the possible values for $\nu_p(D_F)$ that can arise are

$$\nu_2(D_F) \in \{0, 2, 3, 4\}, \quad \nu_3(D_F) \in \{0, 1, 3, 4, 5\} \quad \text{and} \quad \nu_p(D_F) \in \{0, 1, 2\}, \quad \text{for } p > 3. \tag{5.14}$$

Possible twists

We note that necessarily

$$\mathcal{D} \mid 2^3 \cdot 3^2 \cdot \prod_{p \mid N_0} p, \tag{5.15}$$

so that, given N, there is a finite set of $E_{\mathcal{D}}$ to consider (we can restrict our attention to quadratic twists of the curve defined via $y^2 = x^3 - 3H_F(1,0)x + G_F(1,0)$, by squarefree divisors of $6N$). In case we are dealing with squarefree conductor N (i.e. for semistable curves E), then, from Tables 5.1, 5.2 and 5.3, it follows that $\mathcal{D} \in \{1, 2\}$.

Necessity, but not sufficiency

If we search for elliptic curves of conductor N, say, there may exist a cubic form F for which the corresponding Thue-Mahler equation (5.7) has a solution, where all of the conditions of Theorem 5.2.1 are satisfied, but for which the corresponding $E_{\mathcal{D}}$ has conductor $N_{E_{\mathcal{D}}} \neq N$ for all possible $\mathcal{D}$. This can happen when certain local conditions at primes dividing $6N$ are not met; these local conditions are, in practice, easy to check and only a minor issue when performing computations. Indeed, when producing tables of elliptic curves of conductor up to some given bound, we will, in many cases, apply Theorem 5.2.1 to find all curves with good reduction outside a fixed set of primes – in effect, working with multiple conductors simultaneously. For such a computation, the conductor of every twist $E_{\mathcal{D}}$ we encounter will be of interest to us.

Special binary cubic forms

If, for a given binary form $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, 3 divides both the coefficients b and c (say $b = 3b_0$ and $c = 3c_0$), then $27 \mid D_F$ and, consequently, we can write $D_F = 27\widetilde{D}_F$, where

$$\widetilde{D}_F = -a^2d^2 + 6ab_0c_0d + 3b_0^2c_0^2 - 4ac_0^3 - 4b_0^3d.$$

One can show that the set of binary cubic forms with $b \equiv c \equiv 0 \mod 3$ is closed within the larger set of all binary cubic forms in $\mathbb{Z}[x, y]$, under the action of either $\mathrm{SL}_2(\mathbb{Z})$ or $\mathrm{GL}_2(\mathbb{Z})$. Also note that for such forms we have

$$\widetilde{H}_F(x, y) = \frac{H_F(x, y)}{9} = (b_0^2 - ac_0)x^2 + (b_0c_0 - ad)xy + (c_0^2 - b_0d)y^2$$

and $\widetilde{G}_F(x, y) = G_F(x, y)/27$, so that

$$\begin{aligned}\widetilde{G}_F(x, y) = (-a^2d + 3ab_0c_0 - 2b_0^3)x^3 + 3(-b_0^2c_0 - ab_0d + 2ac_0^2)x^2y \\ +3(b_0c_0^2 - 2b_0^2d + ac_0d)xy^2 + (-3b_0c_0d + 2c_0^3 + ad^2)y^3.\end{aligned}$$

The syzygy now becomes

$$4\widetilde{H}_F(x, y)^3 = \widetilde{G}_F(x, y)^2 + \widetilde{D}_F F(x, y)^2. \tag{5.16}$$

We note, from Theorem 5.2.1, that we will be working exclusively with forms of this shape whenever we wish to treat elliptic curves of conductor $N \equiv 0 \mod 3^3$.

The case $j_E = 0$

This case is treated over a general number field in Proposition 4.1 of Cremona and Lingham [33]. The elliptic curves $E/\mathbb{Q}$ with $j_E = 0$ and a given conductor N are particularly easy to determine, since a curve with this property is necessarily isomorphic over $\mathbb{Q}$ to a *Mordell* curve with a model of the shape $Y^2 = X^3 - 54c_6$ where $c_6 = c_6(E)$. Such a model is minimal except possibly at 2 and 3 and has discriminant $-2^6 \cdot 3^9 \cdot c_6^2$ (whereby any primes $p > 2$ which divide c_6 necessarily also divide N). Here, without loss of generality, we may suppose that c_6 is sixth-power-free. Further, from Tables 5.1, 5.2, and 5.3, we have that $\nu_2(N) \in$

$\{0, 2, 3, 4, 6\}$, that $\nu_3(N) \in \{2, 3, 5\}$, and that $\nu_p(N) = 2$ whenever $p \mid N$ for $p > 3$. Given a positive integer N satisfying these constraints, it is therefore a simple matter to check to see if there are elliptic curves $E/\mathbb{Q}$ with conductor N and j-invariant 0. One needs only to compute the conductors of the curves given by $Y^2 = X^3 - 54c_6$ for each sixth-power-free integer (positive or negative) c_6 dividing $64N^3$.

5.2.2 The algorithm

It is straightforward to convert Theorem 5.2.1 into an algorithm for finding all $E/\mathbb{Q}$ of conductor N. We can proceed as follows.

1. Begin by finding all $E/\mathbb{Q}$ of conductor N with $j_E = 0$, as outlined in Section 5.2.1.

2. Next, compute $\mathrm{GL}_2(\mathbb{Z})$-representatives for every binary form F with discriminant

$$\Delta_F = \pm 2^{\alpha_0} 3^{\beta_0} N_1$$

for each divisor N_1 of N_0, and each possible pair (α_0, β_0) given in the statement of Theorem 5.2.1 (see (5.14) for specifics). We describe an algorithm for listing these forms in Section 5.4.

3. Solve the corresponding Thue-Mahler equations, finding pairs of integers (u, v) such that $F(u, v)$ is an S-unit, where $S = \{p \text{ prime } : p \mid N\} \cup \{2\}$ and $F(u, v)$ satisfies the additional conditions given in the statement of Theorem 5.2.1.

4. For each cubic form F and pair of integers (u, v), consider the elliptic curve

$$E_1 \quad : \quad y^2 = x^3 - 27H_F(u, v)x + 27G_F(u, v)$$

and all its quadratic twists by squarefree divisors of $6N$. Output those curves with conductor N (if any).

The first, second and fourth steps here are straightforward; the first and second can be done efficiently, while the fourth is essentially trivial. The main bottleneck is step (3). While there is a deterministic procedure for carrying this out (see Tzanakis and de Weger [111], [112]), it is both involved and, often, computationally taxing. An earlier implementation of this method in Magma due to Hambrook [48] has subsequently been refined by the second author [**?**]; the most up-to-date version of this code (which we will reference here and henceforth as UBC-TM) is available at

http://www.nt.math.ubc.ca/BeGhRe/Code/UBC-TMCode

We give a number of examples of this general procedure in Section 5.5. In Section 5.6, we show that in the special cases where the conductor is prime or the square of a prime, the Thue-Mahler equations (5.7) (happily) reduce to Thue equations (i.e. the exponents on the right hand side of (5.7) are absolutely bounded). This situation occurs because, for such elliptic curves, a very strong form of Szpiro's conjecture (bounding the minimal discriminant of an elliptic curve from above in terms of its conductor) is known to hold. Thue equations can be solved by routines that are computationally much easier than is currently the case for Thue-Mahler equations; such procedures have been implemented in Pari/GP [85] and Magma [17]. Further, in this situation, it is possible to apply a much more computationally efficient argument to find all such elliptic curves heuristically but not, perhaps, completely (see Section 5.7).

5.3 Proof of Theorem 5.2.1

Proof. Given an elliptic curve $E/\mathbb{Q}$ of conductor $N = 2^\alpha 3^\beta N_0$ and invariants $c_4 = c_4(E) \neq 0$ and $c_6 = c_6(E)$, we will construct a corresponding cubic form F explicitly. In fact, our form F will have the property that its leading coefficient will be supported on the primes dividing $6N$, i.e. that

$$F(1,0) = 2^{\alpha_1} \cdot 3^{\beta_1} \cdot \prod_{p \mid N_0} p^{\kappa_p}.$$

Define $\mathcal{D}$ as in (5.9), i.e. take $\mathcal{D}$ to be the largest integer whose square divides c_4 and whose cube divides c_6. We then set

$$X = c_4/\mathcal{D}^2 \quad \text{and} \quad Y = c_6/\mathcal{D}^3,$$

whereby, from (5.2),

$$Y^2 = X^3 + (-1)^{\delta+1} M, \tag{5.17}$$

for

$$M = \mathcal{D}^{-6} \cdot 2^6 \cdot 3^3 \cdot |\Delta_E|.$$

Note that the assumption that $c_4(E) \neq 0$ ensures that both the j-invariant $j_E \neq 0$ and that $X \neq 0$.

It will prove useful to us later to understand precisely the possible common factors among $X, Y, \mathcal{D}$ and M. For any $p > 3$, we have $\nu_p(N) \leq 2$. When $\nu_p(N) = 1$, from Table 5.3 we find that

$$(\nu_p(\mathcal{D}), \nu_p(X), \nu_p(Y), \nu_p(M)) = (0, 0, 0, \geq 1), \tag{5.18}$$

while, if $\nu_p(N) = 2$, then either

$$\nu_p(\mathcal{D}) = 1 \text{ and } \min\{\nu_p(X), \nu_p(Y)\} = 0,\ \nu_p(M) = 0, \tag{5.19}$$

or

$$\nu_p(\mathcal{D}) \leq 1,\ (\nu_p(X), \nu_p(Y), \nu_p(M)) = (0, 0, \geq 1), (\geq 1, 1, 2), (1, \geq 2, 3) \text{ or } (\geq 2, 2, 4). \tag{5.20}$$

Things are rather more complicated for the primes 2 and 3; we summarize this in Tables 5.4 and 5.5 (which are, in turn, compiled from the data in Tables 5.1 and 5.2).

$\nu_2(N)$	$(\nu_2(X), \nu_2(Y), \nu_2(M), \nu_2(\mathcal{D}))$
0	$(\geq 2, 0, 0, 1)$ or $(0, 0, 6, 0)$
1	$(0, 0, \geq 7, 0)$
2	$(\geq 2, 2, 4, 1), (\geq 2, 1, 2, 2)$ or $(0, 0, 2, 2)$
3	$(\geq 2, 2, 4, 1), (\geq 2, 1, 2, 2)$ or $(0, 0, t, 2), t = 2, 4$ or 5
4	$(\geq 2, 2, 4, 1), (\geq 2, 1, 2, 2), (\geq 2, 0, 0, 3)$ or $(0, 0, t, 2), t = 2$ or $t \geq 4$
5	$(\geq 0, \geq 0, 0, 2), (0, \geq 0, 0, 3), (0, 0, 3, 2)$ or $(1, 0, 0, 3)$
6	$(\geq 0, \geq 0, 0, 2), (0, \geq 0, 0, 3), (\geq 2, 2, 4, 2), (\geq 2, 1, 2, 3)$ or $(0, 0, \geq 2, 3)$
7	$(0, 0, 1, 2), (0, 0, 1, 3), (1, 1, 2, 2)$ or $(1, 1, 2, 3)$
8	$(1, \geq 2, 3, 2)$ or $(1, \geq 2, 3, 3)$.

Table 5.4: The possible values of $\nu_2(N), \nu_2(X), \nu_2(Y), \nu_2(M)$ and $\nu_2(D)$

$\nu_3(N)$	$(\nu_3(X), \nu_3(Y), \nu_3(M), \nu_3(\mathcal{D}))$
0	$(1, \geq 3, 3, 0)$ or $(0, 0, 3, 0)$
1	$(0, 0, \geq 4, 0)$
2	$(\geq 0, 0, 0, 1), (0, \geq 2, 0, 1), (0, 0, \geq 3, 1), (1, \geq 3, 3, 1), (\geq 0, 0, 0, 2)$ or $(0, \geq 2, 0, 2)$
3	$(\geq 0, 0, 0, 1), (\geq 0, 0, 0, 2), (0, 1, 0, 1), (0, 1, 0, 2), (0, 0, 2, 1)$ or $(0, 0, 2, 2)$
4	$(0, 0, 1, 1), (0, 0, 1, 2), (1, 2, 3, 1)$ or $(1, 2, 3, 2)$
5	$(\geq 1, 1, 2, 1), (\geq 1, 1, 2, 2), (\geq 2, 2, 4, 1)$ or $(\geq 2, 2, 4, 2)$.

Table 5.5: The possible values of $\nu_3(N), \nu_3(X), \nu_3(Y), \nu_3(M)$ and $\nu_3(D)$

We will construct a cubic form

$$F_1(x, y) = ax^3 + 3b_0x^2y + 3c_0xy^2 + dy^3,$$

one coefficient at a time; our main challenge will be to ensure that the a, b_0, c_0 and d we produce are actually integral rather than just rational. The form F whose existence is asserted in the statement of Theorem 5.2.1 will turn out to be either F_1 or $F_1/3$.

Let us write

$$M = M_1 \cdot M_2$$

where M_2 is the largest integer divisor of M that is coprime to X, so that

$$M_1 = \prod_{p \,|\, X} p^{\nu_p(M)} \quad \text{and} \quad M_2 = \prod_{p \nmid X} p^{\nu_p(M)}.$$

We define

$$a_1 = \prod_{p | M_1} p^{\left[\frac{\nu_p(M)-1}{2}\right]} \tag{5.21}$$

and set

$$a_2 = \begin{cases} 3^{-1} \prod_{p | M_2} p^{\left[\frac{\nu_p(M)}{2}\right]} & \text{if } \nu_3(X) = 0, \ \nu_3(M) = 2t, \ t \in \mathbb{Z}, t \geq 2, \\ \prod_{p | M_2} p^{\left[\frac{\nu_p(M)}{2}\right]} & \text{otherwise.} \end{cases} \tag{5.22}$$

Define $a = a_1 \cdot a_2$. It follows that $a_1^2 \mid M_1$ and, from (5.18), (5.19), (5.20), and Tables 5.4 and 5.5, that both

$$a_1 \mid X \quad \text{and} \quad a_1^2 \mid Y.$$

We write $X = a_1 \cdot X_1$ and observe that $a_2^2 \mid M_2$. Note that a_2 is coprime to X and hence to a_1. Since $a^2 \mid M$, we may thus define a positive integer K via $K = M/a^2$, so that (5.17) becomes

$$Y^2 - X^3 = (-1)^{\delta+1} K a^2.$$

From the fact that $\gcd(a_2, X) = 1$ and $X \neq 0$, we may choose B so that

$$a_2 B \equiv -Y/a_1 \mod X^3,$$

whereby

$$aB + Y \equiv 0 \mod a_1 X^3. \tag{5.23}$$

Note that, since $a_1^2 \mid Y$ and $a_1 \mid X$, it follows that $a_1 \mid B$. Let us define

$$b_0 = \frac{aB + Y}{X}, \quad c_0 = \frac{b_0^2 - X}{a} \quad \text{and} \quad d = \frac{b_0 c_0 - 2B}{a}. \tag{5.24}$$

We now demonstrate that these are all integers. That $b_0 \in \mathbb{Z}$ is immediate from (5.23). Since $b_0 X - Y = aB$, we know that $b_0 X \equiv Y \mod a$. Squaring both sides thus gives

$$b_0^2 X^2 \equiv Y^2 \equiv X^3 + (-1)^{\delta+1} K a^2 \equiv X^3 \mod a_1 \cdot a_2,$$

and, since $\gcd(a_2, X) = 1$,

$$b_0^2 \equiv X \mod a_2.$$

From (5.23), we have $b_0 \equiv 0 \mod a_1 X^2$, whereby, since $a_1 \mid X$,

$$b_0^2 \equiv X \equiv 0 \mod a_1.$$

The fact that $\gcd(a_1, a_2) = 1$ thus allows us to conclude that $b_0^2 \equiv X \mod a$ and hence that $c_0 \in \mathbb{Z}$.

It remains to show that d is an integer. Let us rewrite ad as

$$ad = b_0 c_0 - 2B = \left(\frac{aB + Y}{aX}\right)\left(\left(\frac{aB + Y}{X}\right)^2 - X\right) - 2B,$$

so that

$$ad = \left(\frac{aB + Y}{aX}\right)\left(\frac{(-1)^{\delta+1} K a^2 + 2aBY + a^2 B^2}{X^2}\right) - 2B.$$

Expanding, we find that

$$X^3 d = (-1)^{\delta+1} KY + 3YB^2 + aB^3 + (-1)^{\delta+1} 3KaB. \tag{5.25}$$

We wish to show that

$$(-1)^{\delta+1} KY + 3YB^2 + aB^3 + (-1)^{\delta+1} 3KaB \equiv 0 \mod X^3.$$

From (5.23), we have that

$$(-1)^{\delta+1}KY+3YB^2+aB^3+(-1)^{\delta+1}3KaB \equiv 2Y\left(B^2+(-1)^{\delta}K\right) \mod a_1X^3.$$

Multiplying congruence (5.23) by $aB - Y$ (which, from our prior discussion, is divisible by a_1^2), we find that

$$a^2B^2 \equiv Y^2 \equiv X^3 + (-1)^{\delta+1}Ka^2 \mod a_1^3X^3$$

and hence, dividing through by a_1^2,

$$a_2^2B^2 \equiv a_1X_1^3 + (-1)^{\delta+1}Ka_2^2 \mod a_1X^3.$$

It follows that

$$B^2 + (-1)^{\delta}K \equiv a_2^{-2}a_1X_1^3 \mod a_1X^3, \tag{5.26}$$

and so, since $a_1^2 \mid Y$,

$$Y\left(B^2+(-1)^{\delta}K\right) \equiv 0 \mod X^3,$$

whence we conclude that d is an integer, as desired.

With these values of a, b_0, c_0 and d, we can then confirm (with a quick computation) that the cubic form

$$F_1(x,y) = ax^3 + 3b_0x^2y + 3c_0xy^2 + dy^3$$

has discriminant

$$D_{F_1} = \frac{108}{a^2}(X^3 - Y^2) = (-1)^{\delta} \cdot 2^2 \cdot 3^3 \cdot K$$

We also note that

$$F_1(1,0) = a, \quad \widetilde{H}_{F_1}(1,0) = b_0^2 - ac_0 = X$$

and
$$-\frac{1}{2}\widetilde{G}_{F_1}(1,0) = \frac{1}{2}(a^2d - 3ab_0c_0 + 2b_0^3) = Y,$$
where $\widetilde{G}_F$ and $\widetilde{H}_F$ are as in Section 5.2.1.

Summarizing Table 5.5, we find that we are in one of the following four cases :

(i) $\nu_3(X) = 1,\ \nu_3(Y) = 2,\ \nu_3(M) = 3$ and $\nu_3(N) = 4$,

(ii) $\nu_3(X) \geq 2,\ \nu_3(Y) = 2,\ \nu_3(M) = 4,\ \nu_3(N) = 5$,

(iii) $\nu_3(M) \leq 2$ and $\nu_3(N) \geq 2$, or

(iv) $\nu_3(M) \geq 3$ and either $\nu_3(XY) = 0$ or $\nu_3(X) = 1,\ \nu_3(Y) \geq 3$.

In cases (i), (ii), and (iii), we choose $F = F_1$, i.e.
$$(\omega_0, \omega_1, \omega_2, \omega_3) = (a, 3b_0, 3c_0, d),$$
so that
$$F(1,0) = a,\quad D_F = (-1)^\delta 2^2{\cdot}3^3{\cdot}K,\quad c_4 = \mathcal{D}^2\widetilde{H}_F(1,0)\quad \text{and}\quad c_6 = -\frac{1}{2}\mathcal{D}^3\widetilde{G}_F(1,0).$$
It follows that E is isomorphic over $\mathbb{Q}$ to the curve
$$y^2 = x^3 - 27c_4x - 54c_6 = x^3 - 3\mathcal{D}^2H_F(1,0)x + \mathcal{D}^3G_F(1,0).$$

In case (iv), observe that, from definitions (5.21) and (5.22),
$$\nu_3(a) = \left[\frac{\nu_3(M)-1}{2}\right] \quad \text{and} \quad \nu_3(K) = \nu_3(M) - 2\nu_3(a), \tag{5.27}$$
so that $3 \mid a$ and $3 \mid K$. From equation (5.25), $3 \mid X^3d$. If $\nu_3(X) = 0$ this implies that $3 \mid d$. On the other hand, if $\nu_3(X) = 1$, then, from (5.26), we may conclude that $3 \mid B$. Since each of a, B and K is divisible by 3, while $\nu_3(X) = 1$ and $\nu_3(Y) \geq 3$, equation (5.25) once again implies that $3 \mid d$. In this case, we can therefore write $a = 3a_0$ and $d = 3d_0$, for integers a_0 and d_0 and set $F = F_1/3$, i.e.

take

$$(\omega_0, \omega_1, \omega_2, \omega_3) = (a_0, b_0, c_0, d_0).$$

We have

$$F(1,0) = a/3, \quad D_F = (-1)^\delta 2^2 \cdot K/3, \quad c_4 = \mathcal{D}^2 H_F(1,0) \quad \text{and} \quad c_6 = -\frac{1}{2}\mathcal{D}^3 G_F(1,0).$$

The curve E is now isomorphic over $\mathbb{Q}$ to the model

$$y^2 = x^3 - 27c_4 x - 54c_6 = x^3 - 27\mathcal{D}^2 H_F(1,0)x + 27\mathcal{D}^3 G_F(1,0).$$

Since $|D_F|/D_F = (-1)^\delta$ and $a^2 K \mid 1728\Delta_E$, we may write

$$F(1,0) = 2^{\alpha_1} \cdot 3^{\beta_1} \cdot \prod_{p \mid N_0} p^{\kappa_p} \quad \text{and} \quad D_F = (|\Delta_E|/\Delta_E) 2^{\alpha_0} 3^{\beta_0} N_1,$$

for nonnegative integers $\alpha_0, \alpha_1, \beta_0, \beta_1, \kappa_p$ and a positive integer N_1, divisible only by primes dividing N_0. More explicitly, we have

$$\alpha_0 = \nu_2(K) + 2 \quad \text{and} \quad \beta_0 = \nu_3(K) + \begin{cases} 3 & \text{in case (i), (ii) or (iii), or} \\ -1 & \text{in case (iv),} \end{cases}$$

and

$$\alpha_1 = \nu_2(a) \quad \text{and} \quad \beta_1 = \nu_3(a) + \begin{cases} 0 & \text{in case (i), (ii) or (iii), or} \\ -1 & \text{in case (iv).} \end{cases}$$

It remains for us to prove that these integers satisfy the conditions listed in the statement of the theorem. It is straightforward to check this, considering in turn each possible triple (X, Y, M) from (5.18), (5.19), (5.20), and Tables 5.4 and 5.5, and using the fact that $K = M/a^2$.

In particular, if $p > 3$, we have $\nu_p(\Delta_E) = 6\nu_p(\mathcal{D}) + \nu_p(D_F) + 2\kappa_p$. From Table

5.3 and (5.9), we have $\nu_p(\mathcal{D}) \leq 1$, whereby (5.10) follows. Further,

$$\nu_p(a) = \begin{cases} \left[\frac{\nu_p(M)-1}{2}\right] & \text{if } p \mid X, \\ \left[\frac{\nu_p(M)}{2}\right] & \text{if } p \nmid X, \end{cases} \tag{5.28}$$

and so, if $p \nmid X$,

$$\nu_p(M) - 2\nu_p(a) \leq 1.$$

Since $a^2K = M$, if $p^2 \mid D_F$, then $\nu_p(N) = 2$ and it follows that we are in case (5.20), with $p \mid X$. We may thus conclude that $\nu_p(M) \in \{2, 3, 4\}$ and hence, from (5.28), that $\nu_p(a) \leq 1$. This proves (5.11).

For (5.12), note that, in cases (i), (ii) and (iii), we clearly have that $3 \mid \omega_1$ and $3 \mid \omega_2$. In case (iv), from (5.27),

$$\beta_0 = \nu_3(D_F) = \nu_3(K) - 1 = \nu_3(M) - 2\left[\frac{\nu_3(M)-1}{2}\right] - 1 \in \{0, 1\}.$$

Finally, to see (5.13), note that if $\nu_p(N) = 1$, for $p > 3$, then we have (5.18) and hence

$$\nu_p(D_F) + 2\nu_p(F(u,v)) = \nu_p(M) \geq 1,$$

whereby $p \mid D_F$ or $p \mid F(u,v)$. We may also readily check that the same conclusion obtains for $p = 3$ (since, equivalently, $\beta_0 + \beta_1 \geq 1$). This completes the proof of Theorem 5.2.1.

$\square$

To illustrate this argument, suppose we consider the elliptic curve (denoted 109a1 in Cremona's database) defined via

$$E \quad : \quad y^2 + xy = x^3 - x^2 - 8x - 7,$$

with $\Delta_E = -109$. We have

$$c_4(E) = 393 \quad \text{and} \quad c_6(E) = 7803,$$

so that $\gcd(c_4(E), c_6(E)) = 3$. It follows that

$$\mathcal{D} = 1,\ X = 393,\ Y = 7803,\ \delta = 1,\ M = 2^6 \cdot 3^3 \cdot 109,$$

and hence we have

$$M_1 = 3^3,\ M_2 = 2^6 \cdot 109,\ a_1 = 3,\ a_2 = 2^3,\ a = 2^3 \cdot 3 \text{ and } K = 3 \cdot 109.$$

We solve the congruence $8B \equiv -2601 \mod 393^3$ to find that we may choose $B = 7586982$, so that

$$b_0 = 463347, \quad c_0 = 8945435084 \quad \text{and} \quad d = 172701687278841.$$

We are in case (iv) and thus set

$$F(x, y) = 8x^3 + 463347x^2y + 8945435084xy^2 + 57567229092947y^3,$$

with discriminant $D_F = -4 \cdot 109$,

$$G_F(1, 0) = -15606 = -2c_6(E) \quad \text{and} \quad H_F(1, 0) = 393 = c_4(E).$$

The curve E is thus isomorphic to the model

$$E_{\mathcal{D}} \ :\ y^2 = x^3 - 27\mathcal{D}^2H_F(1, 0)x + 27\mathcal{D}^3G_F(1, 0) = x^3 - 10611x - 421362. \tag{5.29}$$

We observe that the form F is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to a "reduced" form (see Section 5.4 for details), given by

$$\tilde{F}(x, y) = x^3 + 3x^2y + 4xy^2 + 6y^3.$$

In fact, this is the only form (up to $\mathrm{GL}_2(\mathbb{Z})$-equivalence) of discriminant $\pm 4 \cdot 109$. We can check that the solutions to the Thue equation $\tilde{F}(u, v) = 8$ are given by $(u, v) = (2, 0)$ and $(u, v) = (-7, 3)$. The minimal quadratic twist of

$$y^2 = x^3 - 27H_{\tilde{F}}(2, 0)x + 27G_{\tilde{F}}(2, 0)$$

has conductor $2^5 \cdot 109$ and hence cannot correspond to E. For the solution $(u, v) = (-7, 3)$, we find that the curve given by the model

$$y^2 = x^3 - 27H_{\tilde{F}}(-7, 3)x + 27G_{\tilde{F}}(-7, 3) = x^3 - 10611x + 421362,$$

is the quadratic twist by -1 of the curve (5.29). This situation arises from the fact that G_F is an $\mathrm{SL}_2(\mathbb{Z})$-covariant, but not a $\mathrm{GL}_2(\mathbb{Z})$-covariant of F (we will discuss this more in the next section).

5.4 Finding representative forms

As Theorem 5.2.1 illustrates, we are able to tabulate elliptic curves over $\mathbb{Q}$ with good reduction outside a given set of primes, by finding a set of representatives for $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary cubic forms with certain discriminants, and then solving a number of Thue-Mahler equations. In this section, we will provide a brief description of techniques to find distinguished *reduced* representatives for equivalence classes of cubic forms over a given range of discriminants. For both positive and negative discriminants, the notion of *reduction* arises from associating a particular definite quadratic form to a given cubic form.

5.4.1 Irreducible Forms

For forms of positive discriminant, there is a well developed classical theory of reduction dating back to work of Hermite [53], [54] and, later, Davenport (see e.g. [34], [35] and [37]). We can actually apply this method to both reducible and irreducible forms. Initially, though, we will assume the forms are irreducible, since we will treat the elliptic curves corresponding to reducible forms by a somewhat different approach (see Section 5.4.2). Note that when one speaks of "irreducible, reduced forms", as Davenport observes, "the terminology is unfortunate, but can hardly be avoided" ([36], page 184).

In each of Belabas [7], Belabas and Cohen [8] and Cremona [31], we find very efficient algorithms for computing cubic forms of both positive and negative discriminant, refining classical work of Hermite, Berwick and Mathews [11], and Julia [55]. These are readily translated into computer code to loop over valid (a, b, c, d)-values (with corresponding forms $ax^3 + bx^2y + cxy^2 + dy^3$). The running time in each case is linear in the upper bound X. Realistically, this step (finding representatives for our cubic forms) is highly unlikely to be the bottleneck in our computations.

5.4.2 Reducible forms

One can make similar definitions of reduction for reducible forms (see [9] for example). However, for our purposes, it is sufficient to note that a reducible form is equivalent to

$$F(x, y) = bx^2y + cxy^2 + dy^3 \quad \text{with} \quad 0 \leq d \leq c,$$

which has discriminant

$$\Delta_F = b^2(c^2 - 4bd).$$

To find all elliptic curves with good reduction outside $S = \{p_1, p_2, \ldots, p_k\}$, corresponding to reducible cubics in Theorem 5.2.1 (i.e. those E with at least one rational 2-torsion point), it is enough to find all such triples (b, c, d) for which there exist integers x and y so that both

$$b^2(c^2 - 4bd) \quad \text{and} \quad bx^2y + cxy^2 + dy^3$$

are S^*-units (with $S^* = S \cup \{2\}$). For this to be true, it is necessary that each of the integers

$$b, \quad c^2 - 4bd, \quad y \quad \text{and} \quad \mu = bx^2 + cxy + dy^2$$

is an S^*-unit. Taking the discriminant of μ as a function of x, we thus require

that

$$(c^2 - 4bd)y^2 + 4b\mu = Z^2, \tag{5.30}$$

for some integer Z. This is an equation of the shape

$$X + Y = Z^2 \tag{5.31}$$

in S^*-units X and Y.

An algorithm for solving such equations is described in detail in Chapter 7 of de Weger [114] (see also [115]); it relies on bounds for linear forms in p-adic and complex logarithms and various reduction techniques from Diophantine approximation. An implementation of this is available at

http://www.nt.math.ubc.ca/BeGhRe/Code/UBC-TMCode.

While *a priori* equation (5.31) arises as only a necessary condition for the existence of an elliptic curve of the desired form, given any solution to (5.31) in S^*-units X and Y and integer Z, the curves

$$E_1(X,Y) \quad : \quad y^2 = x^3 + Zx^2 + \frac{X}{4}x$$

and

$$E_2(X,Y) \quad : \quad y^2 = x^3 + Zx^2 + \frac{Y}{4}x$$

have nontrivial rational 2-torsion (i.e. the point corresponding to $(x,y) = (0,0)$) and discriminant X^2Y and XY^2, respectively (and hence good reduction at all primes outside S^*).

Though a detailed analysis of running times for solving equations of the shape (5.31), or for solving more general cubic Thue-Mahler equations, has not to our knowledge been carried out, our experience from carrying out such computations for several thousand sets S is that, typically, the former can be done significantly faster than the latter. By way of example, solving (5.31) for $S = \{2,3,5,7,11\}$ takes only a few hours on a laptop, while treating the analogous problem of determining all elliptic curves over $\mathbb{Q}$ with trivial rational 2-torsion and good reduction outside S (see Section 5.5.4) requires many thousand machine-hours.

5.4.3 Computing forms of fixed discriminant

For our purposes, we will typically compute and tabulate a large list of irreducible forms of absolute discriminant bounded by a given positive number X (of size up to 10^{12} of so, beyond which storage becomes problematical). In certain situations, however, we will want to compute all forms of a given fixed, larger discriminant (perhaps up to size 10^{15}). To carry this out and find desired forms of the shape $ax^3 + bx^2y + cxy^2 + dy^3$, we can argue as in, for example, Cremona [31], to restrict our attention to $O(X^{3/4})$ triples (a, b, c). From (5.4), the definition of D_F, we have that

$$d = \frac{9abc - 2b^3 \pm \sqrt{4(b^2 - 3ac)^3 - 27a^2 D_F}}{27a^2}$$

and hence it remains to check that the quantity $4(b^2-3ac)^3-27a^2D_F$ is an integer square, that the relevant conditions modulo $27a^2$ are satisfied, and that a variety of further inequalities from [31] are satisfied. The running time for finding forms with discriminants of absolute value of size X via this approach is of order $X^{3/4}$.

5.4.4 $\mathbf{GL}_2(\mathbb{Z})$ vs $\mathbf{SL}_2(\mathbb{Z})$

One last observation which is very important to make before we proceed, is that while G_F^2 is $\mathrm{GL}_2(\mathbb{Z})$-covariant, the same is not actually true for G_F (it is, however, an $\mathrm{SL}_2(\mathbb{Z})$-covariant). This may seem like a subtle point, but what it means for us in practice is that, having found our $\mathrm{GL}_2(\mathbb{Z})$-representative forms F and corresponding curves of the shape $E_{\mathcal{D}}$ from Theorem 5.2.1, we need, in every case, to also check to see if

$$\tilde{E}_{\mathcal{D}} \quad : \quad 3^{[\beta_0/3]}y^2 = x^3 - 27\mathcal{D}^2 H_F(u,v)x - 27\mathcal{D}^3 G_F(u,v),$$

the quadratic twist of $E_{\mathcal{D}}$ by -1, yields a curve of the desired conductor.

5.5 Examples

In this section, we will describe a few applications of Theorem 5.2.1 to computing all elliptic curves of a fixed conductor N, or all curves with good reduction outside a given set of primes S. We restrict our attention to examples with composite conductors, since the case of conductors p and p^2, for p prime, will be treated at length in Section 5.6 (and subsequently). For the examples in Sections 5.5.1, 5.5.2, 5.5.2 and 5.5.2, since the conductors under discussion are not "square-full", there are necessarily no curves E encountered with $j_E = 0$.

In our computations in this section, we executed all jobs in parallel via the shell tool [107]. We note that our Magma code lends itself easily to parallelization, and we made full use of this fact throughout.

We carried out a one-time computation of all irreducible cubic forms that can arise in Theorem 5.2.1, of absolute discriminant bounded by 10^{10}. This computation took slightly more than 3 hours on a cluster of 40 cores; roughly half this time was taken up with sorting and organizing output files. There are 996198693 classes of irreducible cubic forms of positive discriminant and 3079102475 of negative discriminant in the range in question; storing them requires roughly 120 gigabytes. We could also have tabulated and stored representatives for each class of reducible form of absolute discriminant up to 10^{10}, but chose not to since our approach to solving equation (5.31) does not require them.

5.5.1 Cases without irreducible forms

We begin by noting an obvious corollary to Theorem 5.2.1 that, in many cases, makes it a relatively routine matter to determine all elliptic curves of a given conductor, provided we can show the nonexistence of certain corresponding cubic forms.

Corollary 5.5.1. *Let N be a square-free positive integer with $\gcd(N, 6) = 1$ and suppose that there do not exist irreducible binary cubic forms in $\mathbb{Z}[x, y]$ of discriminant $\pm 4N_1$, for each positive integer $N_1 \mid N$. Then every elliptic curve over $\mathbb{Q}$ of conductor N_1, for each $N_1 \mid N$, has nontrivial rational 2-torsion.*

We will apply this result to a pair of examples (chosen somewhat arbitrarily). Currently, such an approach is feasible for forms of absolute discriminant (and hence potentially conductors) up to roughly 10^{15}. We observe that, among the positive integers $N < 10^8$ satisfying

$$\nu_2(N) \leq 8, \ \ \nu_3(N) \leq 5 \ \ \text{and} \ \ \nu_p(N) \leq 2 \ \text{ for } \ p > 3,$$

i.e. those for which there might actually exist elliptic curves $E/\mathbb{Q}$ of conductor N, we find that 708639 satisfy the hypotheses of Corollary 5.5.1.

It is somewhat harder to modify the statement of Corollary 5.5.1 to include reducible forms (with corresponding elliptic curves having nontrivial rational 2-torsion). One of the difficulties one encounters is that there actually do exist reducible forms of, by way of example, discriminant $4p$ for every $p \equiv 1 \mod 8$; writing $p = 8k + 1$, for instance, the form

$$F(x, y) = 2x^2y + xy^2 - ky^3$$

has this property.

Conductor $2655632887 = 31 \cdot 9007 \cdot 9511$

In the notation of Theorem 5.2.1, we have $\alpha = \beta = 0$ and hence $\alpha_0 = 2$ and $\beta_0 = 0$, so that, in order for there to be an elliptic curve with trivial rational 2-torsion and this conductor, we require the existence of an irreducible cubic form of discriminant $4N_1$ where $N_1 \mid 31 \cdot 9007 \cdot 9511$, i.e. discriminant $\pm 4 \cdot 31^{\delta_1} \cdot 9007^{\delta_2} \cdot 9511^{\delta_3}$, for $\delta_i \in \{0, 1\}$. We check that there are no such forms, directly from our table of forms, except for the possibility of $D_F = \pm 4 \cdot 31 \cdot 9007 \cdot 9511$, which exceeds 10^{10} in absolute value. For these latter possibilities, we argue as in Section 5.4.3 to show that no such forms exist. We may thus appeal to Corollary 5.5.1.

For the possible cases with rational 2-torsion, we solve $X + Y = Z^2$ with X and Y S-units for $S = \{2, 31, 9007, 9511\}$. The solutions to this equation with $X \geq Y$,

$Z > 0$ and $\gcd(X, Y)$ squarefree are precisely those with

$$\begin{aligned}(X,Y) \quad = \quad & (2,-1),(2,2),(8,1),(32,-31),(62,2),(256,-31),(961,128),\\ & (992,-31),(3968,1),(76088,-9007),(294841,8) \text{ and } (492032,-9007).\end{aligned}$$

A short calculation confirms that each elliptic curve arising from these solutions via quadratic twist has bad reduction at the prime 2 (and, in particular, cannot have conductor 2655632887). There are thus no elliptic curves over $\mathbb{Q}$ with conductor 2655632887. Observe that these calculations in fact ensure that there do not exist elliptic curves over $\mathbb{Q}$ with conductor dividing 2655632887.

Full computational details are available at

http://www.nt.math.ubc.ca/BeGhRe/Examples/2655632887-data.

We should observe that it is much more challenging computationally to try to extend this argument to tabulate curves E with good reduction outside $S = \{31, 9007, 9511\}$. To do this, we would have to first determine whether or not there exist irreducible cubic forms of discriminant, say, $D_F = \pm 4 \cdot 31^2 \cdot 9007^2 \cdot 9511^2 > 2.8 \times 10^{19}$. This appears to be at or beyond current computational limits.

Conductor $3305354359 = 41 \cdot 409 \cdot 439 \cdot 449$

For there to exist an elliptic curve with trivial rational 2-torsion and conductor 3305354359, we require the existence of an irreducible cubic form of discriminant $\pm 4 \cdot 41^{\delta_1} \cdot 409^{\delta_2} \cdot 439^{\delta_3} \cdot 449^{\delta_4}$, with $\delta_i \in \{0, 1\}$. We check that, again, there are no such forms (once more employing a short auxiliary computation in the case $D_F = \pm 4 \cdot 41 \cdot 409 \cdot 439 \cdot 449$). If we solve $X + Y = Z^2$ with X and Y S-units for $S = \{2, 41, 409, 439, 449\}$, we find that the solutions to this equation with $X \geq Y$,

$Z > 0$ and $\gcd(X, Y)$ squarefree are precisely

$$(X,Y) = (2,-1),(2,2),(8,1),(41,-16),(41,-32),(41,8),(82,-1),(128,41),(409,-328),\\
(409,32),(439,2),(449,-328),(449,-8),(512,449),(818,82),(898,2),\\
(3272,449),(3362,2),(7184,41),(16769,-128),(16769,-14368),(18409,-16384),\\
(33538,-18409),(36818,818),(41984,41),(68921,-57472),(183641,-1312),\\
(183641,-56192),(183641,41984),(359102,898),(403202,-33538),\\
(403202,-359102),(403202,17999),(737959,183641),(754769,-6544),\\
(6858521,-919552),(8265641,-16) \text{ and } (7095601778,-5610270178).$$

Once again, a short calculation confirms that each elliptic curve arising from these solutions via twists has even conductor. There are thus no elliptic curves over $\mathbb{Q}$ with conductor 3305354359.

Full computational details are available at

http://www.nt.math.ubc.ca/BeGhRe/Examples/3305354359-data.

5.5.2 Cases with fixed conductor (and corresponding irreducible forms)

Conductor $399993 = 3 \cdot 11 \cdot 17 \cdot 23 \cdot 31$

We next choose an example where full data is already available for comparison in the LMFDB [66]. In particular, there are precisely 10 isogeny classes of curves of this conductor (labelled $399993a$ to $399993j$ in the LMFDB), containing a total of 21 isomorphism classes. Of these, 7 isogeny classes (and 18 isomorphism classes) have nontrivial rational 2-torsion.

According to Theorem 5.2.1, the curves arise from consideration of cubic forms of discriminant discriminant $\pm 4K$, where $K \mid 3 \cdot 11 \cdot 17 \cdot 23 \cdot 31$. The (reduced) irreducible cubic forms $F(u, v)$ of these discriminants are as follows, where $F(u,v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 u v^2 + \omega_3 v^3$.

$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F	$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F
$(1,1,1,3)$	$-4\cdot 3\cdot 17$	$(2,4,-6,-3)$	$4\cdot 3\cdot 17\cdot 23$
$(1,2,2,2)$	$-4\cdot 11$	$(2,5,2,6)$	$-4\cdot 3\cdot 17\cdot 23$
$(1,2,2,6)$	$-4\cdot 11\cdot 17$	$(3,3,-8,-2)$	$4\cdot 3\cdot 23\cdot 31$
$(1,4,-16,-2)$	$4\cdot 11\cdot 17\cdot 31$	$(3,3,44,66)$	$-4\cdot 3\cdot 11\cdot 17\cdot 23\cdot 31$
$(1,8,-2,42)$	$-4\cdot 3\cdot 17\cdot 23\cdot 31$	$(3,4,10,14)$	$-4\cdot 11\cdot 23\cdot 31$
$(1,11,-12,-6)$	$4\cdot 3\cdot 11\cdot 17\cdot 31$	$(3,7,5,7)$	$-4\cdot 3\cdot 23\cdot 31$
$(2,0,7,1)$	$-4\cdot 23\cdot 31$	$(4,17,10,28)$	$-4\cdot 11\cdot 17\cdot 23\cdot 31$
$(2,1,14,-2)$	$-4\cdot 11\cdot 17\cdot 31$		

In each case, we are thus led to solve the Thue-Mahler equation

$$F(u,v) = 2^{3\delta}3^{\beta_1}11^{\kappa_{11}}17^{\kappa_{17}}23^{\kappa_{23}}31^{\kappa_{31}}, \tag{5.32}$$

where $\gcd(u,v)=1$, $\delta\in\{0,1\}$ and β_1, κ_{11}, κ_{17}, κ_{23} and κ_{31} are arbitrary non-negative integers. Applying (5.13), in order to find a curve of conductor 399993, we require additionally that, for a corresponding solution to (5.32),

$$F(u,v)\,D_F \equiv 0 \mod 3\cdot 11\cdot 17\cdot 23\cdot 31. \tag{5.33}$$

We readily check that the congruence $F(u,v)\equiv 0 \mod p$ has only the solution $u\equiv v\equiv 0 \mod p$ for the following forms F and primes p (whereby (5.33) cannot be satisfied by coprime integers u and v for these forms) :

$(\omega_0,\omega_1,\omega_2,\omega_3)$	p	$(\omega_0,\omega_1,\omega_2,\omega_3)$	p
$(1,1,1,3)$	$11,23$	$(2,0,7,1)$	$3,17$
$(1,2,2,2)$	$3,23,31$	$(2,5,2,6)$	$11,31$
$(1,4,-16,-2)$	$3,23$	$(3,3,-8,-2)$	11
$(1,8,-2,42)$	11	$(4,17,10,28)$	3
$(1,11,-12,-6)$	23		

For the remaining 6 forms under consideration, we appeal to UBC-TM. The only solutions we find satisfying (5.33) are as follows.

$(\omega_0, \omega_1, \omega_2, \omega_3)$	(u, v)
$(1, 2, 2, 6)$	$(-1851, 892), (14133, -3790)$
$(2, 1, 14, -2)$	$(13, -5), (-29, -923)$
$(2, 4, -6, -3)$	$(10, -3), (64, 49), (-95, 199), (-3395, 1189),$
	$(3677, -1069), (5158, 4045), (-23546, 57259), (-77755, 30999)$
$(3, 3, 44, 66)$	$(1, 0), (1, 2), (-3, 4), (3, -2), (-11, 9), (25, -3),$
	$(231, 2), (-317, 240), (489, 61), (1263, -878), (6853, -4119)$
$(3, 7, 5, 7)$	$(1, 12), (-29, 26), (78, 1), (423, -160)$
$(3, 4, 10, 14)$	$(-41, 84), (95, -69), (307, 90)$

From these, we compute the conductors of $E_{\mathcal{D}}$ in (5.8), where $\mathcal{D} \in \{1, 2\}$, together with their twists by -1. The only curves with conductor 399993 arise from the form F with $(\omega_0, \omega_1, \omega_2, \omega_3) = (2, 4, -6, -3)$ and the solutions

$$(u, v) \in \{(10, -3), (5158, 4045), (-23546, 57259)\}.$$

In each case, $\mathcal{D} = 2$. The solution $(u, v) = (10, -3)$ corresponds to, in the notation of the LMFBD, curve 399993.j1, $(u, v) = (5158, 4045)$ to 399993.i1, and $(u, v) = (-23546, 57259)$ to 399993.h1. Note that every form and solution we consider leads to elliptic curves with good reduction outside $\{2, 3, 11, 17, 23, 31\}$, just not necessarily of conductor 399993. By way of example, if $(\omega_0, \omega_1, \omega_2, \omega_3) = (2, 4, -6, -3)$ and $(u, v) = (-77755, 30999)$, we find curves with minimal quadratic twists of conductor

$$2^5 \cdot 3 \cdot 11 \cdot 17 \cdot 23 \cdot 31 = 2^5 \cdot 399993.$$

To determine the curves of conductor 399993 with nontrivial rational 2-torsion, we are led to solve the equation $X + Y = Z^2$ in S-units X and Y, and integers Z, where $S = \{2, 3, 11, 17, 23, 31\}$. We employ Magma code available at

http://nt.math.ubc.ca/BeGhRe/Code/UBC-TMCode to find precisely 2858 solutions with $X \geq |Y|$ and $\gcd(X, Y)$ squarefree (this computation took slightly less than 2 hours). Of these, 1397 have $Z > 0$, with Z largest for the solution corresponding to the identity

$$48539191572432 - 40649300451407 = 2^4 \cdot 3^4 \cdot 11 \cdot 23^7 - 17^5 \cdot 31^5 = 2808895^2.$$

As in subsection 5.4.2, we attach to each solution a pair of elliptic curves $E_1(X, Y)$ and $E_2(X, Y)$. Of these, the only twists we find to have conductor 399993 are the quadratic twists by t of $E_i(X, Y)$ given in the following table. Note that there is some duplication – the curve labelled 399993.f2 in the LMFDB, for example, arises from three distinct solutions to $X + Y = Z^2$.

X	Y	E_i	t	LMFDB	X	Y	E_i	t	LMFDB
16192	-4743	E_1	-1	$399993.g2$	534336	-506447	E_2	2	$399993.e1$
16192	-4743	E_2	2	$399993.g1$	1311552	-527	E_1	1	$399993.a2$
23529	18496	E_1	-2	$399993.f2$	1311552	-527	E_2	-2	$399993.a1$
23529	18496	E_2	1	$399993.f3$	1414017	-1045568	E_1	2	$399993.b2$
116281	-75072	E_1	2	$399993.f4$	1414017	-1045568	E_2	-1	$399993.b1$
116281	-75072	E_2	-1	$399993.f2$	6305121	3027904	E_1	2	$399993.c1$
371008	4761	E_1	1	$399993.f2$	6305121	3027904	E_2	-1	$399993.c2$
371008	4761	E_2	-2	$399993.f1$	6988113	18496	E_1	2	$399993.c2$
519777	-131648	E_1	2	$399993.d2$	6988113	18496	E_2	-1	$399993.c3$
519777	-131648	E_2	-1	$399993.d1$	7745089	-2731968	E_1	2	$399993.c4$
534336	-506447	E_1	-1	$399993.e2$	7745089	-2731968	E_2	-1	$399993.c2$

Full computational details are available at

http://www.nt.math.ubc.ca/BeGhRe/Examples/399993-data.

Conductor $10^6 - 1$

We next treat a slightly larger conductor, which is not available in the LMFDB currently (but probably within computational range). We have

$$10^6 - 1 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37.$$

From Theorem 5.2.1, we thus need to consider binary cubic forms $F(u,v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 uv^2 + \omega_3 v^3$ of discriminant $D_F = \pm 108 N_1$, where $N_1 \mid 7 \cdot 11 \cdot 13 \cdot 37$ and $\omega_1 \equiv \omega_2 \equiv 0 \mod 3$. The irreducible forms of this shape are as follows.

$(\omega_0, \omega_1, \omega_2, \omega_3)$	D_F	p	$(\omega_0, \omega_1, \omega_2, \omega_3)$	D_F	p
$(1,0,-6,-2)$	$108 \cdot 7$	37	$(2,3,-78,-26)$	$108 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	none
$(1,0,21,16)$	$-108 \cdot 11 \cdot 37$	$7,13$	$(2,3,6,3)$	$-108 \cdot 7$	$11,37$
$(1,0,30,2)$	$-108 \cdot 7 \cdot 11 \cdot 13$	none	$(2,3,6,8)$	$-108 \cdot 37$	7
$(1,3,3,3)$	-108	$7,13,37$	$(2,6,-12,1)$	$108 \cdot 11 \cdot 13$	7
$(1,3,6,16)$	$-108 \cdot 37$	7	$(2,6,21,88)$	$-108 \cdot 11 \cdot 13 \cdot 37$	none
$(1,3,12,26)$	$-108 \cdot 7 \cdot 13$	none	$(2,12,0,13)$	$-108 \cdot 7 \cdot 11 \cdot 13$	none
$(1,3,33,117)$	$-108 \cdot 7 \cdot 11 \cdot 37$	none	$(2,21,-6,80)$	$-108 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	none
$(1,6,-36,-34)$	$108 \cdot 7 \cdot 13 \cdot 37$	11	$(3,3,18,20)$	$-108 \cdot 7 \cdot 11 \cdot 13$	none
$(1,6,3,6)$	$-108 \cdot 37$	7	$(4,6,15,14)$	$-108 \cdot 13 \cdot 37$	11
$(1,6,9,26)$	$-108 \cdot 11 \cdot 13$	none	$(5,6,27,14)$	$-108 \cdot 7 \cdot 11 \cdot 37$	none
$(1,9,0,74)$	$-108 \cdot 7 \cdot 13 \cdot 37$	none	$(5,9,3,21)$	$-108 \cdot 7 \cdot 11 \cdot 37$	none
$(1,12,12,14)$	$-108 \cdot 13 \cdot 37$	11	$(7,0,12,14)$	$-108 \cdot 7 \cdot 11 \cdot 37$	none
$(2,0,-18,-5)$	$108 \cdot 11 \cdot 37$	13	$(10,3,42,-16)$	$-108 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	none
$(2,0,3,3)$	$-108 \cdot 11$	$7,37$	$(10,6,12,3)$	$-108 \cdot 13 \cdot 37$	none
$(2,0,15,3)$	$-108 \cdot 7 \cdot 37$	$11,13$	$(11,6,12,6)$	$-108 \cdot 7 \cdot 11 \cdot 13$	none
$(2,0,18,7)$	$-108 \cdot 13 \cdot 37$	11	$(21,12,27,20)$	$-108 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	none

Here, we list primes p for which a local obstruction exists modulo p to finding coprime integers u and v satisfying (5.13). It is worth noting at this point that the restriction to forms with $\omega_1 \equiv \omega_2 \equiv 0 \mod 3$ that follows from the fact that we are considering a conductor divisible by 3^3 is a helpful one. There certainly can and do exist irreducible forms F with $108 \mid D_F$ that fail to satisfy $\omega_1 \equiv \omega_2 \equiv 0 \mod 3$.

We are thus left to treat 17 Thue-Mahler equations which we solve using UBC-TM; see

http://www.nt.math.ubc.ca/BeGhRe/Examples/999999-data

for computational details. From (5.13), we require that $D_F F(u,v) \equiv 0 \mod 7 \cdot 11 \cdot 13 \cdot 37$; the only solutions we find satisfying this constraint are as follows.

$(\omega_0, \omega_1, \omega_2, \omega_3)$	(u, v)
$(1, 0, 30, 2)$	$(-1, 21), (1, 16), (27, 25)$
$(1, 3, 33, 117)$	$(26, -7)$
$(1, 9, 0, 74)$	$(-19, 2)$
$(2, 3, -78, -26)$	$(-1, 3), (-3, 2), (-5, -1), (9, -1), (13, 2), (-17, -58), (-39, -61),$
	$(-57, -10), (-59, 9), (65, -6), (79, -330), (159, -23)$
$(2, 6, 21, 88)$	$(3, 1), (165, -43)$
$(2, 12, 0, 13)$	$(-1, 9), (18, 23)$
$(2, 21, -6, 80)$	$(1, -10), (2, 1), (4, -3), (4, -1), (17, 1),$
	$(19, -5), (21, -2), (138, -11), (1356, -127)$
$(3, 3, 18, 20)$	$(9, 13), (97, -12)$
$(5, 6, 27, 14)$	$(14, 1), (19, 6), (-21, 44)$
$(5, 9, 3, 21)$	$(-1, 2), (6, 1), (8, -3), (-649, 284), (1077, -464)$
$(7, 0, 12, 14)$	$(-1, 5), (-7, 9), (301, -62), (-459, 553)$
$(10, 3, 42, -16)$	$(1, 1), (1, 2), (2, -1), (3, 1), (4, -17), (20, 19), (-22, -69), (127, 339)$
$(10, 6, 12, 3)$	$(2, -1), (5, -13), (-12, 83), (-24, 89), (81, -107), (125, -437)$
$(11, 6, 12, 6)$	$(-1, 22), (47, -72), (223, -429)$
$(21, 12, 27, 20)$	$(1, -3), (1, 0), (1, 5), (4, -9), (4, 3), (9, -29),$
	$(19, -15), (29, -40), (316, -455), (551, -805)$

The only ones of these for which we find an $E_{\mathcal{D}}$ in (5.8) of conductor 999999 are as follows, where $E_{\mathcal{D}}$ is isomorphic over $\mathbb{Q}$ to a curve with model

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

$(\omega_0, \omega_1, \omega_2, \omega_3)$	(u, v)	$\mathcal{D}$	a_1	a_2	a_3	a_4	a_6
$(1, 0, 30, 2)$	$(27, 25)$	6	0	0	1	-40395	5402579
$(1, 0, 30, 2)$	$(27, 25)$	-2	0	0	1	-363555	-145869640
$(5, 6, 27, 14)$	$(14, 1)$	1	1	-1	0	14700	55223
$(5, 6, 27, 14)$	$(14, 1)$	-3	1	-1	1	1633	-2590
$(5, 9, 3, 21)$	$(-1, 2)$	6	0	0	1	30	2254
$(5, 9, 3, 21)$	$(-1, 2)$	-2	0	0	1	270	-60865
$(10, 6, 12, 3)$	$(125, -437)$	2	0	0	1	-17205345	-27554570341
$(10, 6, 12, 3)$	$(125, -437)$	-6	0	0	1	-1911705	1020539642
$(21, 12, 27, 20)$	$(4, 3)$	-1	1	-1	0	12432	-164125
$(21, 12, 27, 20)$	$(4, 3)$	3	1	-1	1	1381	5618

Each of these listed curves has trivial rational 2-torsion. To search for curves of conductor 999999 with nontrivial rational 2-torsion, we solve the equation $X + Y = Z^2$ in S-units X and Y, and integers Z, where $S = \{2, 3, 7, 11, 13, 37\}$. We find that there are precisely 4336 solutions with $X \geq |Y|$ and $\gcd(X, Y)$ squarefree. Of these, 2136 have $Z > 0$, with Z largest for the solution corresponding to the identity

$$103934571636753 - 68209863326528 = 3^{15} \cdot 11 \cdot 13 \cdot 37^3 - 2^6 \cdot 7^{13} \cdot 11 = 5977015^2.$$

Once again, we attach to each solution a pair of elliptic curves $E_1(X, Y)$ and $E_2(X, Y)$. We find 505270 isomorphism classes of $E/\mathbb{Q}$ with good reduction outside of $\{2, 3, 7, 11, 13, 37\}$ and nontrivial rational 2-torsion. None of them have conductor 999999, whereby we conclude that there are precisely 10 isomorphism classes of elliptic curves over $\mathbb{Q}$ with conductor $10^6 - 1$. Checking that these curves each have distinct traces of Frobenius a_{47} shows that they are nonisogenous.

Conductor $10^9 - 1$

This example is chosen to be somewhat beyond the current scope of the LMFDB. We have

$$10^9 - 1 = 3^4 \cdot 37 \cdot 333667$$

and so, applying Theorem 5.2.1, we are led to consider binary cubic forms of discriminant $\pm 4 \cdot 3^4 \cdot 37^{\delta_1} \cdot 333667^{\delta_2}$, where $\delta_i \in \{0,1\}$. These include imprimitive forms with the property that each of its coefficients ω_i is divisible by 3. For such forms, from Theorem 5.2.1, we necessarily have $\beta_1 \in \{0,1\}$ and hence $\beta_1 = 1$. Dividing through by 3, we may thus restrict our attention to primitive forms of discriminant $\pm 4 \cdot 3^\kappa \cdot 37^{\delta_1} \cdot 333667^{\delta_2}$, where $\delta_i \in \{0,1\}$ and $\kappa \in \{0,4\}$. For the irreducible forms, we have, by slight abuse of notation (since, for the F listed here with $D_F \not\equiv 0 \mod 3$, the form whose existence is guaranteed by Theorem 5.2.1 is actually $3F$), the following.

$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F	p	$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F	p
$(1,1,-3,-1)$	$4 \cdot 37$	333667	$(5,14,19,54)$	$-4 \cdot 333667$	37
$(1,4,52,250)$	$-4 \cdot 333667$	37	$(6,18,168,323)$	$-4 \cdot 3^4 \cdot 333667$	37
$(1,9,37,279)$	$-4 \cdot 333667$	none	$(6,27,42,356)$	$-4 \cdot 3^4 \cdot 333667$	37
$(1,21,117,2135)$	$-4 \cdot 3^4 \cdot 333667$	37	$(6,54,-48,115)$	$-4 \cdot 3^4 \cdot 333667$	37
$(2,0,3,1)$	$-4 \cdot 3^4$	37	$(10,18,96,229)$	$-4 \cdot 3^4 \cdot 333667$	37
$(2,17,-26,-31)$	$4 \cdot 333667$	37	$(26,9,102,4)$	$-4 \cdot 3^4 \cdot 333667$	none
$(4,30,117,665)$	$-4 \cdot 3^4 \cdot 333667$	37	$(27,7,70,32)$	$-4 \cdot 37 \cdot 333667$	none
$(4,35,14,216)$	$-4 \cdot 37 \cdot 333667$	none	$(31,9,87,-25)$	$-4 \cdot 3^4 \cdot 333667$	none
$(5,6,9,6)$	$-4 \cdot 3^4 \cdot 37$	none	$(49,51,63,55)$	$-4 \cdot 3^4 \cdot 333667$	none
$(5,7,19,51)$	$-4 \cdot 333667$	37	$(52,55,72,37)$	$-4 \cdot 37 \cdot 333667$	none

Once again, we list primes p for which a local obstruction exists modulo p to finding coprime integers u and v satisfying (5.13). There are thus 8 Thue-Mahler equations left to solve. In the (four) cases where $D_F \not\equiv 0 \mod 3$, these take the shape

$$F(u,v) = 2^{3\delta_1} \cdot 37^{\gamma_1} \cdot 333667^{\gamma_2},$$

where $\delta_1 \in \{0, 1\}$, γ_1 and γ_2 are nonnegative integers, and u and v are coprime integers. For the remaining F, the analogous equation is

$$F(u, v) = 2^{3\delta_1} \cdot 3^{\delta_2} \cdot 37^{\gamma_1} \cdot 333667^{\gamma_2},$$

where $\delta_i \in \{0, 1\}$, $\gamma_1, \gamma_2 \in \mathbb{Z}^+$ and $u, v \in \mathbb{Z}$ with $\gcd(u, v) = 1$. We solve these equations using the UBC-TM Thue-Mahler solver. The only cases where we find that

$$D_F F(u, v) \equiv 0 \mod 37 \cdot 333667$$

occur for $(\omega_0, \omega_1, \omega_2, \omega_3) = (4, 35, 14, 216)$ and $(u, v) = (-8, 1)$ or $(u, v) = (-2, 1)$, for $(\omega_0, \omega_1, \omega_2, \omega_3) = (27, 7, 70, 32)$ and $(u, v) = (1, -2)$ or $(2, -1)$, and for $(\omega_0, \omega_1, \omega_2, \omega_3) = (52, 55, 72, 37)$ and $(u, v) = (0, 1)$ or $(-3, 5)$. In each case, all resulting twists have bad reduction at 2 (and hence cannot have conductor $10^9 - 1$).

To search for curves with nontrivial rational 2-torsion and conductor $10^9 - 1$, we solve the equation $X + Y = Z^2$ in S-units X and Y, and integers Z, where $S = \{2, 3, 37, 333667\}$. There are precisely 98 solutions with $X \geq |Y|$ and $\gcd(X, Y)$ squarefree. Of these, 41 have $Z > 0$, with Z largest for the solution coming from the identity

$$27027027 - 101306 = 3^4 \cdot 333667 - 2 \cdot 37^3 = 5189^2.$$

These correspond via twists to elliptic curves of conductor as large as $2^8 \cdot 3^2 \cdot 37^2 \cdot 333667^2$, but none of conductor $10^9 - 1$. There thus exist no curves $E/\mathbb{Q}$ of conductor $10^9 - 1$.

Full computational details are available at

http://www.nt.math.ubc.ca/BeGhRe/Examples/999999999-data.

5.5.3 Curves with good reduction outside $\{2, 3, 23\}$: an example of Koutsianis and of von Kanel and Matchke

This case was worked out by Koutsianis [59] (and also by von Kanel and Matschke [56], who actually computed $E/\mathbb{Q}$ with good reduction outside $\{2, 3, p\}$ for all prime $p \leq 163$), by rather different methods from those employed here. We include it here to provide an example where we determine all $E/\mathbb{Q}$ with good reduction outside a specific set S, which is of somewhat manageable size in terms of the set of cubic forms encountered. Our data agrees with that of [56] and [59].

To begin, we observe that the elliptic curves with good reduction outside $\{2, 3, 23\}$ and j-invariant 0 are precisely those with models of the shape

$$E \quad : \quad Y^2 = X^3 \pm 2^a 3^b 23^c, \quad \text{where } \; 0 \leq a, b, c \leq 5.$$

Appealing to (5.14), we next look through our precomputed list to find all the irreducible primitive cubic forms of discriminant $\pm 2^\alpha 3^\beta 23^\gamma$, where

$$\alpha \in \{0, 2, 3, 4\}, \quad \beta \in \{0, 1, 3, 4, 5\} \quad \text{and} \quad \gamma \in \{0, 1, 2\}.$$

The imprimitive forms we need consider correspond to primitive forms F with either $\nu_2(D_F) = 0$ or $\nu_3(D_F) \in \{0, 1\}$. We find precisely 95 irreducible, primitive cubic forms of the desired discriminants.

$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F	$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F	$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F
$(1,0,-18,-6)$	$2^2\cdot3^5\cdot23$	$(2,0,3,4)$	$-2^3\cdot3^5$	$(4,9,24,29)$	$-2^2\cdot3^4\cdot23^2$
$(1,0,-3,-1)$	3^4	$(2,3,6,4)$	$-2^2\cdot3^5$	$(4,12,12,27)$	$-2^4\cdot3^3\cdot23^2$
$(1,0,3,2)$	$-2^3\cdot3^3$	$(2,3,12,8)$	$-2^4\cdot3^3\cdot23$	$(4,12,12,73)$	$-2^4\cdot3^5\cdot23^2$
$(1,0,6,2)$	$-2^2\cdot3^5$	$(2,3,36,29)$	$-2^3\cdot3^4\cdot23^2$	$(4,18,9,24)$	$-2^2\cdot3^5\cdot23^2$
$(1,0,6,4)$	$-2^4\cdot3^4$	$(2,3,36,98)$	$-2^3\cdot3^5\cdot23^2$	$(4,18,27,48)$	$-2^2\cdot3^5\cdot23^2$
$(1,0,9,6)$	$-2^4\cdot3^5$	$(2,5,8,15)$	$-2^3\cdot3\cdot23^2$	$(5,6,7,4)$	$-2^3\cdot23^2$
$(1,0,33,32)$	$-2^2\cdot3^4\cdot23^2$	$(2,6,-12,-1)$	$2^2\cdot3^5\cdot23$	$(5,6,15,8)$	$-2^3\cdot3^5\cdot23$
$(1,1,2,1)$	-23	$(2,6,6,5)$	$-2^2\cdot3^5$	$(5,9,12,10)$	$-2^2\cdot3^5\cdot23$
$(1,1,8,6)$	$-2^2\cdot23^2$	$(2,6,6,25)$	$-2^2\cdot3^3\cdot23^2$	$(5,12,18,20)$	$-2^4\cdot3^5\cdot23$
$(1,3,-9,-4)$	$3^5\cdot23$	$(2,6,27,117)$	$-2^3\cdot3^5\cdot23^2$	$(5,18,30,46)$	$-2^2\cdot3^5\cdot23^2$
$(1,3,-6,-4)$	$2^2\cdot3^3\cdot23$	$(2,9,-6,-4)$	$2^2\cdot3^5\cdot23$	$(5,24,-3,26)$	$-2^4\cdot3^5\cdot23^2$
$(1,3,-3,-2)$	$3^3\cdot23$	$(2,9,0,-4)$	$2^4\cdot3^3\cdot23$	$(6,3,12,-7)$	$-2^3\cdot3^3\cdot23^2$
$(1,3,-6,-2)$	$2^3\cdot3^5$	$(2,9,48,185)$	$-2^4\cdot3^5\cdot23^2$	$(6,3,12,16)$	$-2^4\cdot3^3\cdot23^2$
$(1,3,3,3)$	$-2^2\cdot3^3$	$(2,12,24,85)$	$-2^2\cdot3^5\cdot23^2$	$(6,6,9,13)$	$-2^3\cdot3^3\cdot23^2$
$(1,3,3,5)$	$-2^4\cdot3^3$	$(2,18,-15,31)$	$-2^3\cdot3^5\cdot23^2$	$(6,9,12,23)$	$-2^3\cdot3^4\cdot23^2$
$(1,3,3,7)$	$-2^2\cdot3^5$	$(3,0,3,2)$	$-2^4\cdot3^4$	$(6,18,18,29)$	$-2^2\cdot3^5\cdot23^2$
$(1,3,3,13)$	$-2^4\cdot3^5$	$(3,4,12,12)$	$-2^4\cdot3\cdot23^2$	$(7,6,9,4)$	$-2^3\cdot3^4\cdot23$
$(1,3,18,50)$	$-2^3\cdot3^5\cdot23$	$(3,6,4,6)$	$-2^2\cdot3\cdot23^2$	$(7,15,3,17)$	$-2^2\cdot3^5\cdot23^2$
$(1,6,-24,-4)$	$2^4\cdot3^5\cdot23$	$(3,6,9,8)$	$-2^3\cdot3^3\cdot23$	$(8,9,12,13)$	$-2^2\cdot3^4\cdot23^2$
$(1,6,3,32)$	$-2^3\cdot3^5\cdot23$	$(3,9,9,7)$	$-2^4\cdot3^5$	$(8,15,18,21)$	$-2^3\cdot3^4\cdot23^2$
$(1,6,6,16)$	$-2^4\cdot3^3\cdot23$	$(3,9,9,49)$	$-2^2\cdot3^5\cdot23^2$	$(9,9,3,31)$	$-2^4\cdot3^5\cdot23^2$
$(1,6,12,54)$	$-2^2\cdot3^3\cdot23^2$	$(3,18,36,116)$	$-2^4\cdot3^5\cdot23^2$	$(10,6,15,1)$	$-2^3\cdot3^3\cdot23^2$
$(1,6,12,100)$	$-2^4\cdot3^3\cdot23^2$	$(3,27,9,29)$	$-2^4\cdot3^5\cdot23^2$	$(11,6,12,2)$	$-2^2\cdot3^3\cdot23^2$
$(1,9,-12,-16)$	$2^4\cdot3^5\cdot23$	$(4,0,-18,-3)$	$2^4\cdot3^5\cdot23$	$(11,15,15,17)$	$-2^2\cdot3^5\cdot23^2$
$(1,9,-9,-3)$	$2^2\cdot3^5\cdot23$	$(4,0,6,1)$	$-2^4\cdot3^5$	$(12,9,36,16)$	$-2^4\cdot3^5\cdot23^2$
$(1,9,27,165)$	$-2^2\cdot3^5\cdot23^2$	$(4,2,8,3)$	$-2^4\cdot23^2$	$(12,36,36,35)$	$-2^4\cdot3^5\cdot23^2$
$(1,9,27,303)$	$-2^4\cdot3^5\cdot23^2$	$(4,3,6,2)$	$-2^2\cdot3^3\cdot23$	$(13,9,18,12)$	$-2^2\cdot3^5\cdot23^2$
$(1,12,9,18)$	$-2^4\cdot3^5\cdot23$	$(4,3,12,10)$	$-2^3\cdot3^5\cdot23$	$(13,15,27,7)$	$-2^2\cdot3^5\cdot23^2$
$(1,12,12,44)$	$-2^4\cdot3^3\cdot23^2$	$(4,3,18,13)$	$-2^3\cdot3^3\cdot23^2$	$(21,9,27,11)$	$-2^4\cdot3^5\cdot23^2$
$(1,15,3,-7)$	$2^4\cdot3^5\cdot23$	$(4,3,18,36)$	$-2^2\cdot3^5\cdot23^2$	$(23,30,36,20)$	$-2^4\cdot3^5\cdot23^2$
$(2,0,3,1)$	$-2^2\cdot3^4$	$(4,4,9,1)$	$-2^4\cdot23^2$	$(24,27,36,16)$	$-2^4\cdot3^5\cdot23^2$
$(2,0,3,2)$	$-2^3\cdot3^4$	$(4,6,3,12)$	$-2^2\cdot3^3\cdot23^2$		

In each case, we solve the corresponding Thue-Mahler equation specified by Theorem 5.2.1. For example, if $D_F = \pm 2^4 \cdot 3^t \cdot 23^2$, with $t \geq 3$, then we actually need only solve the (eight) Thue equations of the shape

$$F(u, v) = 2^{\delta_1} 3^{\delta_2} 23^{\delta_3}, \quad \text{where} \quad \delta_i \in \{0, 1\}.$$

For all other discriminants, we must treat "genuine" Thue-Mahler equations (where at least one of the exponents on the right-hand-side of equation (5.7) is, *a priori*, unconstrained). Details of this computation are available at

http://www.nt.math.ubc.ca/BeGhRe/Examples/2-3-23-data.

In total, we found precisely 730 solutions to these equations, leading, after twisting, to 3856 isomorphism classes of $E/\mathbb{Q}$ with good reduction outside $\{2, 3, 23\}$ and trivial rational 2-torsion.

Once again, to find the curves with nontrivial rational 2-torsion, we solved $X+Y = Z^2$ in S-units X and Y, and integers Z, where $S = \{2, 3, 23\}$. There are precisely 118 solutions with $X \geq |Y|$ and $\gcd(X, Y)$ squarefree (this computation took less than 1 hour). Of these, 55 have $Z > 0$, with Z largest for the solution coming from the identity

$$89424 - 23 = 2^4 \cdot 3^5 \cdot 23 - 23 = 299^2.$$

These correspond via twists to elliptic curves of conductor as large as $2^8 \cdot 3^2 \cdot 23^2$, a total of 1664 isomorphism classes. There thus exist a total of 5520 isomorphism classes (in 3968 isogeny classes) of elliptic curves $E/\mathbb{Q}$ with good reduction outside $\{2, 3, 23\}$. Note that $432 = 2 \times 6^3$ of these have $j_E = 0$.

5.5.4 Curves with good reduction outside $\{2, 3, 5, 7, 11\}$: an example of von Kanel and Matschke

This is the largest computation carried out along these lines by von Kanel and Matschke [56] (and also a very substantial computation via our approach, taking many thousand machine hours on 80 cores).

As in the preceding example, note that the curves with models of the shape

$$E \ : \ Y^2 = X^3 \pm 2^a 3^b 5^c 7^d 11^e, \ \ 0 \le a, b, c, d, e \le 5$$

are precisely the $E/\mathbb{Q}$ with good reduction outside $\{2, 3, 5, 7, 11\}$ and j-invariant 0. We next proceed by searching our precomputed list for all irreducible primitive cubic forms of discriminant $2^\alpha 3^\beta M$, where

$$\alpha \in \{0, 2, 3, 4\}, \ \ \beta \in \{0, 1, 3, 4, 5\} \ \ \text{and} \ \ M \mid 5^2 \cdot 7^2 \cdot 11^2.$$

The imprimitive forms we need consider again correspond to primitive forms F with either $\nu_2(D_F) = 0$ or $\nu_3(D_F) \in \{0, 1\}$. We encounter 1796 irreducible cubic forms, which we tabulate at

http://www.nt.math.ubc.ca/BeGhRe/Examples/2-3-5-7-11-data

where details on the resulting Thue-Mahler computation may also be found. Confirming the results of von Kanel and Matschke [56], we find that there exist a total of 592192 isomorphism classes (in 453632 isogeny classes) of elliptic curves $E/\mathbb{Q}$ with good reduction outside $\{2, 3, 5, 7, 11\}$, including $15552 = 2 \times 6^5$ with $j_E = 0$.

5.6 Good reduction outside a single prime

For the remainder of this chapter, we will focus our attention on the case of elliptic curves with bad reduction at a single prime, i.e. curves of conductor p or p^2, for p prime. In this case, our approach simplifies considerably and rather than being required to solve Thue-Mahler equations, the problem reduces to one of solving *Thue* equations, i.e. equations of the shape $F(x, y) = m$, where F is a form and m is a fixed integer. While, once again, we do not have a detailed computational complexity analysis of either algorithms for solving Thue equations or more general algorithms for solving Thue-Mahler equations, computations to date strongly support the contention that the former is, usually, much, much faster than the latter, particularly if the set of primes S considered for the Thue-Mahler equations is anything other than tiny. Since none of these conductors are divisible by 9, we may always suppose that $j_E \neq 0$. We note that the data we have produced in these cases totals several terabytes. As a result, we have not yet determined how best to make it publicly available; interested readers should contact the authors for further details.

5.6.1 Conductor $N = p$

Suppose that E is a curve with conductor $N = p$ prime with invariants c_4 and c_6. From Tables 5.1, 5.2 and 5.3, we necessarily have one of

$$\begin{aligned}
&(\nu_2(c_4), \nu_2(c_6)) = (0,0) \text{ or } (\geq 4, 3), \text{ and } \nu_2(\Delta_E) = 0, \text{ or} \\
&(\nu_3(c_4), \nu_3(c_6)) = (0,0) \text{ or } (1, \geq 3), \text{ and } \nu_3(\Delta_E) = 0, \text{ or} \\
&(\nu_p(c_4), \nu_p(c_6)) = (0,0) \text{ and } \nu_p(\Delta_E) \geq 1.
\end{aligned}$$

From this we see that $\mathcal{D} = 1$ or 2. Theorem 5.2.1 then implies that there is a cubic form of discriminant ± 4 or $\pm 4p$, and integers u, v, with

$$F(u,v) = p^{\kappa_p} \text{ or } 8p^{\kappa_p}, \quad c_4 = \mathcal{D}^2 H_F(u,v) \quad \text{and} \quad c_6 = -\frac{1}{2}\mathcal{D}^3 G_F(u,v),$$

for $\mathcal{D} \in \{1,2\}$ and κ_p a nonnegative integer. Note that, while the smallest absolute discriminant for an irreducible cubic form in $\mathbb{Z}[x,y]$ is 23, there do exist reducible cubic forms of discriminants 4 and -4 which we must consider.

Appealing to Théorème 2 of Mestre and Oesterlé [72] (and using [18]), we can actually restrict the choices for n dramatically. In fact, we have 3 possibilities – either $p \in \{11, 17, 19, 37\}$, or $p = t^2 + 64$ for some integer t, or, in all other cases, $\Delta_E = \pm p$. There are precisely 14 isomorphism classes of $E/\mathbb{Q}$ with conductor in $\{11, 17, 19, 37\}$; one may consult Cremona [29] for details. If we can write $p = t^2 + 64$ for an integer t (which we may, without loss of generality, assume to satisfy $t \equiv 1 \mod 4$), then the (2-isogenous) curves defined by

$$y^2 + xy = x^3 + \frac{t-1}{4} \cdot x^2 - x$$

and

$$y^2 + xy = x^3 + \frac{t-1}{4} \cdot x^2 + 4x + t$$

have rational points of order 2 given by $(x, y) = (0, 0)$ and $(x, y) = (-t/4, t/8)$, respectively, and discriminants $t^2 + 64$ and $-(t^2 + 64)^2$, respectively. In the final case (in which $\Delta_E = \pm p$), we have (using the notation of Section 5.2 and, in particular, appealing to (5.10) which, in this case yields the equation $1 = \nu_p(\Delta_E) = \nu_p(D_F) + 2\kappa_p$)

$$\alpha_0 = 2,\ \alpha_1 \in \{0, 3\},\ \beta_0 = \beta_1 = 0,\ \kappa_p = 0 \quad \text{and} \quad N_1 \in \{1, p\}.$$

Theorem 5.2.1 thus tells us that to determine the elliptic curves of conductor p, we are led to to find all binary cubic forms (reducible and irreducible) F of discriminant ± 4 and $\pm 4p$ and then solve the Thue equations

$$F(x, y) = 1 \quad \text{and} \quad F(x, y) = 8.$$

Since for any solution (x, y) to the equation $F(x, y) = 1$, we have $F(2x, 2y) = 8$, we may thus restrict our attention to the equation $F(x, y) = 8$ (where we assume that $\gcd(x, y) \mid 2$).

5.6.2 Conductor $N = p^2$

In case E has conductor $N = p^2$, we have that either E is a either a quadratic twist of a curve of conductor p, or we have $\nu_p(\Delta_E) \in \{2, 3, 4\}$. To see this, note that, via Table 5.3, $p \mid c_4$, $p \mid c_6$ and $\mathcal{D} \mid 2p$, and we may suppose that $(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta_E))$ is one of

$$(\geq 1, 1, 2), (1, \geq 2, 3), (\geq 2, 2, 4), (\geq 2, \geq 3, 6), (2, 3, \geq 7), (\geq 3, 4, 8), (3, \geq 5, 9), (\geq 4, 5, 10).$$

In each case with $\nu_p(c_6(E)) \geq 3$, denote by E_1 the quadratic twist of E by $(-1)^{(p-1)/2}p$. For curves E with

$$(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta_E)) = (\geq 2, \geq 3, 6),$$

one may verify that E_1 has good reduction at p and hence conductor 1, a contradiction. If we have

$$(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta_E)) = (2, 3, \geq 7),$$

then

$$(\nu_p(c_4(E_1)), \nu_p(c_6(E_1)), \nu_p(\Delta_{E_1})) = (0, 0, \nu_p(\Delta_E) - 6)$$

and so E_1 has conductor p. In the remaining cases, where

$$(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta_E)) \in \{(\geq 3, 4, 8), (3, \geq 5, 9), (\geq 4, 5, 10)\},$$

we check that

$$(\nu_p(c_4(E_1)), \nu_p(c_6(E_1)), \nu_p(\Delta_{E_1})) \in \{(\geq 1, 1, 2), (1, \geq 2, 3), (\geq 2, 2, 4)\}.$$

It follows that, in order to determine all isomorphism classes of $E/\mathbb{Q}$ of conductor p^2, it suffices to carry out the following program.

- Find all curves of conductor p.
- Find $E/\mathbb{Q}$ with minimal discriminant $\Delta_E \in \{\pm p^2, \pm p^3, \pm p^4\}$, and then
- consider all appropriate quadratic twists of these curves.

The fact that we can essentially restrict attention to $E/\mathbb{Q}$ with minimal discriminant

$$\Delta_E \in \{\pm p^2, \pm p^3, \pm p^4\} \tag{5.34}$$

(once we have all curves of conductor p) was noted by Edixhoven, de Groot and Top in Lemma 1 of [39]. To find the E satisfying (5.34), Theorem 5.2.1 (with specific appeal to (5.10)) leads us to consider Thue equations of the shape

$$F(x, y) = 8 \text{ for } F \text{ a form of discriminant } \pm 4p^2, \tag{5.35}$$

$$F(x, y) = 8p \text{ for } F \text{ a form of discriminant } \pm 4p \tag{5.36}$$

c_4	c_6	p	Δ_E	N_E
4353	287199	17	17	17
33	-81	17	17	17
t^2+48	$-t(t^2+72)$	t^2+64	t^2+64	t^2+64
273	4455	17	17^2	17
t^2-192	$-t(t^2+576)$	t^2+64	$-(t^2+64)^2$	t^2+64
1785	75411	7	7^3	7^2
105	1323	7	-7^3	7^2
33	12015	17	-17^4	17

Table 5.6: All curves of conductor p and p^2, for p prime, corresponding to reducible forms (i.e. with nontrivial rational 2-torsion). Note that t is any integer so that t^2+64 is prime. For the sake of brevity, we have omitted curves that are quadratic twists by $\pm p$ of curves of conductor p.

and

$$F(x,y) = 8p \ \text{ for } F \text{ a form of discriminant } \pm 4p^2, \tag{5.37}$$

corresponding to $\Delta_E = \pm p^2$, $\pm p^3$ and $\pm p^4$, respectively.

5.6.3 Reducible forms

To find all elliptic curves $E/\mathbb{Q}$ with conductor p or p^2 arising from reducible forms, via Theorem 5.2.1 we are led to solve equations

$$F(x,y) = 8p^n \quad \text{with} \quad n \in \mathbb{Z} \quad \text{and} \quad \gcd(x,y) \mid 2, \tag{5.38}$$

where F is a reducible binary cubic form of discriminant ± 4, $\pm 4p$ and $\pm 4p^2$. This is an essentially elementary, though rather painful, exercise. Alternatively, we may observe that curves of conductor p or p^2 arising from reducible cubic forms are exactly those with at least one rational 2-torsion point. We can then use Theorem I of Hadano [46] to show that the only such p are $p = 7, 17$ and $p = t^2 + 64$ for integer t. In any case, after some rather tedious but straightforward work, we can show that the elliptic curves of conductor p or p^2 corresponding to reducible forms, are precisely those given in Table 5.6 (up to quadratic twists by $\pm p$).

5.6.4 Irreducible forms : conductor p

A quick search demonstrates that there are no irreducible cubic forms of discriminant ± 4. Consequently if we wish to find elliptic curves of conductor p coming from irreducible cubics in Theorem 5.2.1, we need to solve equations of the shape $F(x, y) = 8$ for all cubic forms of discriminant $\pm 4p$. An almost immediate consequence of this is the following.

Proposition 5.6.1. *Let $p > 17$ be prime. If there exists an elliptic curve $E/\mathbb{Q}$ of conductor p, then either $p = t^2 + 64$ for some integer t, or there exists an irreducible binary cubic form of discriminant $\pm 4p$.*

On the other hand, if we denote by $h(K)$ the class number of a number field K, classical results of Hasse [49] imply the following.

Proposition 5.6.2. *Let $p \equiv \pm 1 \mod 8$ be prime and $\delta \in \{0, 1\}$. If there exists an irreducible cubic form of discriminant $(-1)^\delta 4p$, then*

$$h\left(\mathbb{Q}(\sqrt{(-1)^\delta p})\right) \equiv 0 \mod 3.$$

Combining Propositions 5.6.1 and 5.6.2, we thus have

Corollary 5.6.3 (Theorem 1 of Setzer [94])**.** *Let $p \equiv \pm 1 \mod 8$ be prime. If there exists an elliptic curve $E/\mathbb{Q}$ of conductor p, then either $p = t^2 + 64$ for some integer t, or we have*

$$h\left(\mathbb{Q}(\sqrt{p})\right) \cdot h\left(\mathbb{Q}(\sqrt{-p})\right) \equiv 0 \mod 3.$$

We remark that Proposition 5.6.1 is actually a rather stronger criterion for guaranteeing the non-existence of elliptic curves of conductor p than Corollary 5.6.3. Indeed, by way of example, we may readily check that there are no irreducible cubic forms of discriminant $\pm 4p$ for

$$p \in \{23, 31, 199, 239, 257, 367, 439\},$$

(and hence no elliptic curves of conductor p for these primes) while, in each case, we have that $3 \mid h\left(\mathbb{Q}(\sqrt{p})\right) \cdot h\left(\mathbb{Q}(\sqrt{-p})\right)$.

5.6.5 Irreducible forms : conductor p^2

As noted earlier, to determine all elliptic curves of conductor p^2 for p prime, arising via Theorem 5.2.1 from irreducible cubics, it suffices to find those of conductor p and those of conductor p^2 with $\Delta_F = \pm p^2, \pm p^3$ and $\pm p^4$ (and subsequently twist them). We explore these cases below.

Elliptic curves of discriminant $\pm p^3$

To find elliptic curves of discriminant $\pm p^3$, we need to solve Thue equations of the shape $F(x, y) = 8p$, where F runs over all cubic forms of discriminant $\Delta_F = \pm 4p$. These forms are already required to compute curves of conductor p. Now, we can either proceed directly to solve $F(x, y) = 8p$ or transform the problem into one of solving a pair of new Thue equations of the shape $G_i(x, y) = 8$. In practice, we used the former when solving rigorously and the latter when solving heuristically (see Section 5.7.3).

We now describe this transformation. Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a reduced form of discriminant $\pm 4p$. Since $p \mid \Delta_F$, we have

$$F(x, y) \equiv a(x - r_0 y)^2(x - r_1 y) \mod p,$$

where we must have that $p \nmid a$, since F is a reduced form (which implies that $1 \leq a < p$). Comparing coefficients of x shows that

$$2r_0 + r_1 \equiv -b/a \mod p, \ \ r_0^2 + 2r_0 r_1 \equiv c/a \mod p$$

and

$$r_0^2 r_1 \equiv -d/a \mod p.$$

Multiply the first two of these by a and add them to get

$$3ar_0^2 + 2br_0 + c \equiv 0 \mod p.$$

We can solve this for r_0 and hence r_1:

$$(r_0, r_1) \equiv (3a)^{-1} (-b \pm t, -b \mp 2t) \mod p,$$

where we require that t satisfies $t^2 \equiv b^2 - 3ac \mod p$. Finding square roots modulo p can be done efficiently via the Tonelli-Shanks algorithm, for example (see e.g. Shanks [96]), and almost trivially if, say, $p \equiv 3 \mod 4$. Once we have these (r_0, r_1), we can readily check which pair satisfies $r_0^2 r_1 \equiv -d/a \mod p$.

Now if $F(x, y) = 8p$ then we must have either

$$x \equiv r_0 y \mod p \quad \text{or} \quad x \equiv r_1 y \mod p.$$

In either case, write $x = r_i y + pu$, which maps the equation $F(x, y) = 8p$ to a pair of equations of the shape

$$G_i(u, y) = 8,$$

where

$$G_i(u, y) = ap^2u^3 + (3apr_i + bp)u^2y + (3ar_i^2 + 2br_i + c)uy^2 + \frac{1}{p}(ar_i^3 + br_i^2 + cr_i + d)y^3.$$

Notice that $\Delta_{G_i} = p^2 \Delta_F$. In practice, for our deterministic approach, we will actually solve the equation $F(x, y) = 8p$ directly. For our heuristic approach (where a substantial increase in the size of the form's discriminant is not especially problematic), we will reduce to consideration of the equations $G_i(x, y) = 8$.

A (conjecturally infinite) family of forms and solutions

We note that there are families of primes for which we can guarantee that the equation $F(x, y) = 8p$ has solutions. By way of example, define a quartic form

$p_{r,s}$ via

$$p_{r,s} = r^4 + 9r^2s^2 + 27s^4.$$

Then for a given r, s and $p = p_{r,s}$ the cubic form

$$F(x,y) = sx^3 + rx^2y - 3sxy^2 - ry^3$$

has discriminant $4p$. Additionally one can readily verify the polynomial identities

$$F(2r^2/s + 6s, -2r) = 8p \quad \text{and} \quad F(6s, -18s^2/r - 2r) = 8p.$$

If we set $s \in \{1,2\}$ in the first of these, or $r \in \{1,2\}$ in the second, then we arrive at four one-parameter families of forms of discriminant $4p$ for which the equation $F(x,y) = 8p$ has a solution, namely:

$$\begin{aligned}(p,x,y) = {} & (r^4 + 9r^2 + 27, 2r^2 + 6, -2r), (r^4 + 36r^2 + 432, r^2 + 12, -2r), \\ & (27s^4 + 9s^2 + 1, 6s, -18s^2 - 2), (27s^4 + 36s^2 + 16, 6s, -9s^2 - 4).\end{aligned}$$

Similarly, if we define

$$p_{r,s} = r^4 - 9r^2s^2 + 27s^4$$

then the form

$$F(x,y) = sx^3 + rx^2y + 3sxy^2 + ry^3$$

has discriminant $-4p$, and the equation $F(x,y) = 8p$ has solutions

$$(x,y) = (-2r^2/s + 6s, 2r) \text{ and } (6s, -18s^2/r + 2r)$$

and hence we again find (one parameter) families of primes corresponding to either $r \in \{1,2\}$ or $s \in \{1,2\}$:

$$\begin{aligned}(p,x,y) = &(r^4 - 9r^2 + 27, -2r^2 + 6, 2r), (r^4 - 36r^2 + 432, -r^2 + 12, 2r),\\ &(27s^4 - 9s^2 + 1, 6s, -18s^2 + 2), (27s^4 - 36s^2 + 16, 6s, -9s^2 + 4).\end{aligned}$$

We expect that each of the quartic families described here attains infinitely many prime values, but proving this is beyond current technology.

Elliptic curves of discriminant p^2 and p^4

To find elliptic curves of discriminant p^2 and p^4 via Theorem 5.2.1, we need to solve Thue equations $F(x,y) = 8$ and $F(x,y) = 8p$, respectively, for cubic forms F of discriminant $4p^2$. Such forms are quite special and it turns out that they form a 2-parameter family.

Indeed, in order for there to exist a cubic form of discriminant $4p^2$, it is necessary and sufficient that we are able to write $p = r^2 + 27s^2$ for positive integers r and s, whereby F is equivalent to the form

$$F_{r,s}(x,y) = sx^3 + rx^2y - 9sxy^2 - ry^3.$$

To see this, note that the existence of an irreducible cubic form of discriminant $4p^2$ for prime p necessarily implies that of a (cyclic) cubic field of discriminant p^2 and field index 2. From Silvester, Spearman and Williams [100], there is a unique such field up to isomorphism, which exists precisely when the prime p can be represented by the quadratic form $r^2 + 27s^2$. We conclude as desired upon observing that

$$D_{F_{r,s}} = 4\left(r^2 + 27s^2\right)^2.$$

It remains, then, to solve the Thue equations

$$F_{r,s}(x,y) = 8 \quad \text{and} \quad F_{r,s}(x,y) = 8p.$$

We can transform the problem of solving the second of these equations to one of solving a related Thue equation of the form $G_{r,s}(x, y) = 8$. This transformation is quite similar to the one described in the previous subsection.

First note that we may assume that $p \nmid y$, since otherwise, we would require that $p \mid sx$, contradicting the facts that $s < \sqrt{p}$ and $p^2 \nmid F$. Since $p^2 \mid \Delta_F$, it follows that the congruence

$$su^3 + ru^2 - 9su - r \equiv 0 \mod p$$

has a unique solution modulo p; one may readily check that this satisfies $u \equiv 9s/r \mod p$:

$$su^3 + ru^2 - 9su - r \equiv -r^{-3} \cdot (r^2 - 27s^2)(r^2 + 27s^2) \equiv 0 \mod p.$$

Consequently, we know that $x \equiv uy \mod p$. Substituting $x = uy + vp$ into F gives

$$F_{r,s}(uy + vp, y) = a_0v^3 + b_0v^2y + c_0vy^2 + d_0y^3$$

so, with a quick renaming of variables, we obtain

$$G_{r,s}(x, y) = a_0x^3 + b_0x^2y + c_0xy^2 + d_0y^3 = 8,$$

where

$$a_0 = sp^2, \quad b_0 = (3us+r)p, \quad c_0 = 3u^2s+2ru-9s \quad \text{and} \quad d_0 = (u^3s+ru^2-9us-r)/p.$$

A little algebra confirms that

$$\Delta_{G_{r,s}} = 4p^4.$$

As noted in the previous subsection, we have solved $F_{r,s}(x, y) = 8p$ directly in our deterministic approach, while we solved equation $G_{r,s}(x, y) = 8$ for our heuristic method.

Elliptic curves of discriminant $-p^2$ and $-p^4$

Elliptic curves of discriminant $-p^2$ and $-p^4$ can be found through Theorem 5.2.1 by solving the Thue equations $F(x,y) = 8$ and $F(x,y) = 8p$, respectively, this time for cubic forms F of discriminant $-4p^2$. As in the cases treated in the preceding subsection, these forms can be described as a 2-parameter family. Specifically, such forms arise precisely when there exist integers r and s such that $p = |r^2 - 27s^2|$, in which case the form F is equivalent to

$$F_{r,s}(x,y) = sx^3 + rx^2y + 9sxy^2 + ry^3.$$

The primes p for which we can write $p = |r^2 - 27s^2|$ are those with $p \equiv \pm 1 \mod 12$. To see this, note first that if $p \equiv 1 \mod 3$ and $p = |r^2 - 27s^2|$, then necessarily $p = r^2 - 27s^2$, so that $p \equiv 1 \mod 4$, while, if $p \equiv -1 \mod 3$ and $p = |r^2 - 27s^2|$, then $p = 27s^2 - r^2$ so that $p \equiv -1 \mod 4$. It follows that necessarily $p \equiv \pm 1 \mod 12$. To show that this is sufficient to have $p = |r^2 - 27s^2|$ for integers r and s, we appeal to the following.

Proposition 5.6.4. *If $p \equiv 1 \mod 12$ is prime, there exist positive integers r and s such that*

$$r^2 - 27s^2 = p, \quad \textit{with} \quad r < \frac{3}{2}\sqrt{6p} \quad \textit{and} \quad s < \frac{5}{18}\sqrt{6p}.$$

If $p \equiv -1 \mod 12$ is prime, there exist positive integers r and s such that

$$r^2 - 27s^2 = -p, \quad \textit{with} \quad r < \frac{5}{2}\sqrt{2p} \quad \textit{and} \quad s < \frac{1}{2}\sqrt{2p}.$$

This result is, in fact, an almost direct consequence of the following.

Theorem 5.6.5 (Theorem 112 from Nagell [79])**.** *If $p \equiv 1 \mod 12$ is prime, there exist positive integers u and v such that*

$$p = u^2 - 3v^2, \quad u < \sqrt{3p/2} \quad \textit{and} \quad v < \sqrt{p/6}.$$

If $p \equiv -1 \mod 12$ *is prime, there exist positive integers* u *and* v *such that*

$$-p = u^2 - 3v^2, \ \ u < \sqrt{p/2} \ \ \textit{and} \ \ v < \sqrt{p/2}.$$

Proof of Proposition 5.6.4. If $p \equiv \pm 1 \mod 12$, Theorem 5.6.5 guarantees the existence of integers u and v such that $p = |u^2 - 3v^2|$. If $3 \mid v$ then we set $r = u, s = v/3$. Clearly $3 \nmid u$, so if $3 \nmid v$ then we have (replacing v by $-v$ is necessary) that $u \equiv v \mod 3$. If we now set $r = 2u + 3v$ and $s = (2v + u)/3$, then it follows that

$$|r^2 - 27v^2| = |(2u + 3v)^2 - 3(2v + u)^2| = |u^2 - 3v^2| = p$$

and hence either

$$|r| \leq 2\sqrt{3p/2} + 3\sqrt{p/6} = \frac{3}{2}\sqrt{6p} \ \ \text{and} \ \ |s| \leq \frac{1}{3}(2\sqrt{p/6} + \sqrt{3p/2}) = \frac{5}{18}\sqrt{6p},$$

or

$$|r| \leq 2\sqrt{p/2} + 3\sqrt{p/2} = \frac{5}{2}\sqrt{2p} \ \ \text{and} \ \ |s| \leq \frac{1}{3}(2\sqrt{p/2} + \sqrt{p/2}) = \frac{1}{2}\sqrt{2p}.$$

□

Again, we are able to reduce the problem of solving $F_{r,s}(x, y) = 8p$ to that of treating a related equation $G_{r,s}(x, y) = 8$. As before, note that if $u \equiv -9s/r \mod p$, then

$$su^3 + ru^2 + 9su + r \equiv r^{-3}(r^2 - 27s^2)(r^2 + 27s^2) \equiv 0 \mod p.$$

Again, write $x = r_0y + vp$ so that, after renaming v, we have

$$G_{r,s}(x, y) = a_0x^3 + b_0x^2y + c_0xy^2 + d_0y^3 = 8,$$

where

$$a_0 = sp^2, \ \ b_0 = (3us+r)p, \ \ c_0 = 3u^2s+2ru+9s \ \ \text{and} \ \ d_0 = (u^3s+ru^2+9us+r)/p.$$

Note that, in contrast to the case where $p = r^2 + 27s^2$, here p is represented by an indefinite quadratic form and so the presence of infinitely many units in $\mathbb{Q}(\sqrt{3})$ implies that a given representation is not unique. If, however, we have two solutions to the equation $|r^2 - 27s^2| = p$, say (r_1, s_1) and (r_2, s_2), then the corresponding forms

$$s_1x^3 + r_1x^2y + 9s_1xy^2 + r_1y^3 \text{ and } s_2x^3 + r_2x^2y + 9s_2xy^2 + r_2y^3$$

may be shown to be $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

5.7 Computational details

As noted earlier, the computations required to generate curves of prime conductor p (and subsequently conductor p^2) fall into a small number of distinct parts.

5.7.1 Generating the required forms

To find the irreducible forms potentially corresponding to elliptic curves of prime conductor $p \leq X$ for some fixed positive real X, arguing as in Section 5.4, we tabulated all reduced forms $F(x, y) = ax^3 + bx^2y + cxy^2 + d$ with discriminants in $(0, 4X]$ and $[-4X, 0)$, separately. As each form was generated, we checked to see if it actually satisfied the desired definition of reduction. Of course, this does not only produce forms with discriminant $\pm 4p$ – as each form was produced, we kept only those whose discriminant was in the appropriate range, and equal to $\pm 4p$ for some prime p. Checking primality was done using the Miller-Rabin primality test (see [74], [89]; to make this deterministic for the range we require, we appeal to [102]). While it is straightforward to code the above in computer algebra packages such as `sage` [93], `maple` [70] or Magma [17], we instead implemented it in `c++` for speed. To avoid possible numerical overflows, we used the `CLN` library [47] for `c++`.

We computed forms of discriminant $\pm 4p$ in two separate runs — first to $p \leq 10^{12}$ and then a second run to $p \leq 2 \times 10^{13}$. In the first of these, we constructed all the forms and explicitly saved them to files. Constructing all the required positive discriminant forms took approximately 40 days of CPU time on a modern server, and about 300 gigabytes of disc space. Thankfully, the computation is easily parallelised and it only took about 1 day of real time. We split the jobs by running a manager which distributed a-values to the other cores. The output from each a-value was stored as a tab-delimited text file with one tuple of p, a, b, c, d on each line. Generating all forms of negative discriminant took about 3 times longer and required about 900 gigabytes of disc space. The distribution of forms is heavily weighted to small values of a. To allow us to spread the load across many CPUs we actually split the task into 2 parts. We first ran $a \geq 3$, with the master node distributing a-values to the other cores. We then ran $a = 1$ and 2 with the master node distributing b-values to the other cores. The total CPU time was about three times longer than for the positive case (there being essentially three times as many forms), but more real-time was required due to these complications. Thus generating all forms took less than 1 week of real time but required about 1.2 terabytes of disc space.

These forms were then sorted by discriminant while keeping positive and negative discriminant forms separated. Sorting a terabyte of data is a non-trivial task, and in practice we did this by first sorting[1] the forms for each a-value and then splitting them into files of discriminants in the ranges $[n \times 10^9, (n+1) \times 10^9)$ for $n \in [0, 999]$. Finally, all the files of each discriminant range were sorted together. This process for positive and negative discriminant forms took around two days of real time. We found 9247369050 forms of positive discriminant $4p$ and 27938060315 of negative discriminant $-4p$, with p bounded by 10^{12}. Of these, 475831852 and 828238359, respectively had $F(x, y) = 8$ solvable (by the heuristic method described below), leading to 159552514 and 276339267 elliptic curves of positive and negative discriminant, respectively, with prime conductor up to 10^{12}.

The second run to $p \leq 2 \times 10^{13}$ required a different workflow due to space constraints. Saving all forms to disc was simply impractical — we estimated it to re-

[1] Using the standard unix `sort` command and taking advantage of multiple cores.

quire over 20 terabytes of space! Because of this we combined the form-generation code with the heuristic solution method (see below) and kept only those forms $F(x, y)$ for which solutions to $F(x, y) = 8$ existed. Since only a small fraction of forms (asymptotically likely 0) have solutions, the disc space required was considerably less. Indeed to store all the required forms took about 250 and 400 gigabytes for positive and negative forms respectively. This then translated into about 65 and 115 gigabytes of positive and negative discriminant curves, respectively, with prime conductor up to 2×10^{13}. This second computation took roughly 20 times longer than the first, requiring about 4 months of real-time. This led to a final count of 1738595275 and 3011354026 (isomorphism classes of) curves of positive and negative discriminant, respectively, with prime conductor up to 2×10^{13}.

5.7.2 Complete solution of Thue equations : conductor p

For each form encountered, we needed to solve the Thue equation

$$ax^3 + bx^2y + cxy^2 + dy^3 = 8$$

in integers x and y with $\gcd(x, y) \in \{1, 2\}$. We approached this in two distinct ways.

To solve the Thue equation rigorously, we appealed to by now well-known arguments of Tzanakis and de Weger [110], based upon lower bounds for linear forms in complex logarithms, together with lattice basis reduction; these are implemented in several computer algebra packages, including Magma [17] and Pari/GP [85]. The main computational bottleneck in this approach is typically that of computing the fundamental units in the corresponding cubic fields; for computations p of size up to 10^9 or so, we encountered no difficulties with any of the Thue equations arising (in particular, the fundamental units occurring can be certified without reliance upon the Generalized Riemann Hypothesis).

We ran this computation in Magma [17], using its built-in Thue equation solver. Due to memory consumption issues, we fed the forms into Magma in small batches, restarting Magma after each set. We saved the output as a tuple

$$p, a, b, c, d, n, \{(x_1, y_1), \ldots, (x_n, y_n)\},$$

where p, a, b, c, d came from the form, n counts the number of solutions of the Thue equation and (x_i, y_i) the solutions. These solutions can then be converted into corresponding elliptic curves in minimal form using Theorem 5.2.1 and standard techniques.

For positive discriminant, this approach works without issue for $p < 10^{10}$. For forms of negative discriminant $-4p$, however, the fundamental unit ϵ_p in the associated cubic field can be extremely large (i.e. $\log|\epsilon_p|$ can be roughly of size $\sqrt{p}$). For this reason, finding all negative discriminant curves with prime conductor exceeding $2 \cdot 10^9$ or so proves to be extremely time-consuming. Consequently, for large p, we turned to a non-exhaustive method, which, though it finds solutions to the Thue equation, is not actually guaranteed to find them all.

5.7.3 Non-exhaustive, heuristic solution of Thue equations

If we wish to find all "small" solutions to a Thue equation (which, subject to various well-accepted conjectures, might actually prove to be all solutions), there is an obvious and very computationally efficient approach we can take, based upon the idea that, given any solution to the equation $F(x, y) = m$ for fixed integer m, we necessarily either have that x and y are (very) small, relative to m, or that x/y is a convergent in the infinite simple continued fraction expansion to a root of the equation $F(x, 1) = 0$.

Such techniques were developed in detail by Pethő [87], [88]; in particular, he provides a precise and computationally efficient distinction between "large" and "small" solutions. Following this, for each form F under consideration, we expanded the roots of $F(x, 1) = 0$ to high precision, again using the `CLN` library for `c++`. We then computed the continued fraction expansion for each real root, along with its associated convergents. Each convergent x/y was then substituted into $F(x, y)$ and checked to see if $F(x, y) = \pm 1, \pm 8$. Replacing (x, y) by one of

$(-x, -y), (2x, 2y)$ or $(-2x, -2y)$, if necessary, then provided the required solutions of $F(x, y) = 8$. The precision was chosen so that we could compute convergents x/y with $|x|, |y| \leq 2^{128} \approx 3.4 \times 10^{38}$. We then looked for solutions of small height using a brute force search over a relatively small range of values.

To "solve" $F(x, y) = 8$ by this method, for all forms with discriminant $\pm 4p$ with $p \leq 10^{12}$, took about 1 week of real time using 80 cores. The resulting solutions files (in which we stored also forms with no corresponding solutions) required about 1.5 terabytes of disc space. Again, the files were split into files of absolute discriminant (or more precisely absolute discriminant divided by 4) in the ranges $[n \times 10^9, (n + 1) \times 10^9)$ for $n \in [0, 999]$. For the second computation run to $p \leq 2 \times 10^{13}$, we combined the form-generation and heuristic-solutions steps, storing only forms which had solutions. This produced about 235 and 405 gigabytes of data for positive and negative discriminants, respectively.

5.7.4 Conversion to curves

Once one has a tuple (a, b, c, d, x, y), one then computes $G_F(x, y)$ and $H_F(x, y)$, appeals to Theorem 5.2.1 and checks twists. This leaves us with a list of pairs (c_4, c_6) corresponding to elliptic curves. It is now straightforward to derive a_1, a_2, a_3, a_4 and a_6 for a corresponding elliptic curve in minimal form (see e.g. Cremona [30]). For each curve, we saved a tuple $p, a_1, a_2, a_3, a_4, a_6, \pm 1$ with the last entry being the sign of the discriminant of the form used to generate the curve (which coincides with the sign of the discriminant of the curve). We then merged the curves with positive and negative discriminants and added the curves with prime conductor arising from reducible forms (i.e. of small conductor or for primes of the form $t^2 + 64$). After sorting by conductor, this formed a single file of about 17 gigabytes for all curves with prime conductor $p < 10^{12}$ and about 180 gigabytes for all curves with conductor $p < 2 \times 10^{13}$.

5.7.5 Conductor p^2

The conductor p^2 computation was quite similar, but was split further into parts.

Twisting conductor p

The vast majority of curves of conductor p^2 that we encountered arose as quadratic twists of curves of conductor p. To compute these, we took all curves with conductor $p \leq 10^{10}$ and calculated the invariants c_4 and c_6. The twisted curve then has corresponding c-invariants

$$c_4' = p^2 c_4 \quad \text{and} \quad c_6' = (-1)^{(p-1)/2} p^3 c_6.$$

The minimal a-invariants were then computed as for curves of conductor p.

We wrote a simple c++ program to read curves of conductor p and then twist them, recompute the a-invariants and output them as a tuple $p^2, a_1, a_2, a_3, a_4, a_6, \pm 1$. The resulting code only took a few minutes to process the approximately 1.1×10^7 curves.

Solving $F(x, y) = 8p$ with F of discriminant $\pm 4p$

There was no need to retabulate forms for this computation; we reused the positive and negative forms of discriminant $\pm 4p$ with $p \leq 10^{10}$ from the conductor-p computations. We subsequently rigorously solved the corresponding equations $F(x, y) = 8p$ for $p \leq 10^8$. To solve the Thue equation $F(x, y) = 8p$ for $10^8 < p \leq 10^{10}$, using the non-exhaustive, heuristic method, we first converted the equation to a pair of new Thue equations of the form $G_i(u, y) = 8$ as described in Section 5.6.5 and then applied Pethő's solution search method (where we searched for solutions to these new equations with $|y|$ bounded by 2^{128} and $|u| = |(x - r_i y)/p|$ bounded in such way as to guarantee that our original $|x|$ is also bounded by 2^{128}).

The solutions were then processed into curves as for the conductor p case above, and the resulting curves were twisted by $\pm p$ in order to obtain more curves of conductor p^2.

Solving $F(x, y) \in \{8, 8p\}$ with F of discriminant $\pm 4p^2$

To find forms of discriminant $4p^2$ with $p \leq 10^{10}$ we need only check to see which primes are of the form $p = r^2 + 27s^2$ in the desired range. To do so, we simply looped over r and s values and then again checked primality using Miller-Rabin. As each prime was found, the corresponding p, r, s tuple was converted to a form as in Section 5.6.5, and the Thue equations $F(x, y) = 8$ and $F(x, y) = 8p$ were solved, using the rigorous approach for $p < 10^6$ and the non-exhaustive method described previously for $10^6 < p \leq 10^{10}$. Again, in the latter situation, the equation $F(x, y) = 8p$ was converted to a new equation $G(x, y) = 8$ as described in Section 5.6.5. The process for forms of discriminant $-4p^2$ was very similar, excepting that more care is required with the range of r and s (appealing to Proposition 5.6.4). The non-exhaustive method solving both $F(x, y) = 8$ and $F(x, y) = 8p$ for positive and negative forms took a total of approximately 5 days of real time on a smaller server of 20 cores. The rigorous approach, even restricted to prime $p < 10^6$ was much, much slower.

The solutions were then converted to curves as with the previous cases and each resulting curve was twisted by $\pm p$ to find other curves of conductor p^2.

5.8 Data

5.8.1 Previous work

The principal prior work on computing table of elliptic curves of prime conductor was carried out in two lengthy computations, by Brumer and McGuinness [19] in the late 1980s and by Stein and Watkins [105] slightly more than ten years later. For the first of these computations, the authors fixed the a_1, a_2 and a_3 invariants (12 possibilities) and looped over a_4 and a_6 chosen to make the corresponding discriminant small. By this approach, they were able to find 311243 curves of prime conductor $p < 10^8$ (representing approximately 99.6% of such curves). In the latter case, the authors looped instead over c_4 and c_6, subject to (necessary) local conditions. They obtained a large collection of elliptic curves of general conductor to 10^8, and 11378912 of those with prime conductor to 10^{10} (which we estimate to be slightly in excess of 99.8% of such curves).

5.8.2 Counts : conductor p

By way of comparison, we found the following numbers of isomorphism classes of elliptic curves over $\mathbb{Q}$ with prime conductor $p \leq X$:

X	$\Delta_E > 0$	$\Delta_E < 0$	Ratio^2	Total	Expected	Total / Expected
10^3	33	51	2.3884	84	68	1.2353
10^4	129	228	3.1239	357	321	1.1122
10^5	624	1116	3.1986	1740	1669	1.0425
10^6	3388	5912	3.0450	9300	9223	1.0084
10^7	19605	34006	3.0087	53611	52916	1.0131
10^8	114452	198041	2.9941	312493	311587	1.0029
10^9	685278	1187686	3.0038	1872964	1869757	1.0017
2×10^9	1178204	2040736	3.0001	3218940	3216245	1.0008
10^{10}	4171055	7226982	3.0021	11398037	11383665	1.0013
10^{11}	25661634	44466339	3.0026	70127973	70107401	1.0003
10^{12}	159552514	276341397	2.9997	435893911	435810488	1.0002
10^{13}	999385394	1731017588	3.0001	2730402982	2730189484	1.00008
2×10^{13}	1738595275	3011354026	3.0000	4749949301	4749609116	1.00007

The data above the line is rigorous; for positive discriminant, we actually have a rigorous result to 10^{10}. For the positive forms this took about one week of real time using 80 cores. Unfortunately, the negative discriminant forms took significantly longer, roughly 2 months of real time using 80 cores. Heuristics given by Brumer and McGuinness [19] suggest that the number of elliptic curves of negative discriminant of absolute discriminant up to X should be asymptotically $\sqrt{3}$ times as many as those of positive discriminant in the same range – here we report the square of this ratio in the given ranges. The aforementioned heuristic count of Brumer and McGuinness suggests that the expected number of E with prime $N_E \leq X$ should be

$$\frac{\sqrt{3}}{12}\left(\int_1^\infty \frac{1}{\sqrt{u^3-1}}du + \int_{-1}^\infty \frac{1}{\sqrt{u^3+1}}du\right)\ \mathrm{Li}(X^{5/6}),$$

which we list (after rounding) in the table above. It should not be surprising that this "expected" number of curves appears to slightly undercount the actual number, since it does not take into account the roughly $\sqrt{X}/\log X$ curves of conductor $p = n^2 + 64$ and discriminant $-p^2$ (counting only curves of discriminant $\pm p$).

5.8.3 Counts : conductor p^2

To compile the final list of curves of conductor p^2, we combined the five lists of curves: twists of curves of conductor p, curves from forms of discriminant $+4p$ and $-4p$, and curves from discriminant $+4p^2$ and $-4p^2$. The list was then sorted and any duplicates removed. The resulting list is approximately one gigabyte in size. The counts of curves are as follows; here we list numbers of isomorphism classes of curves of conductor p^2 for p prime with $p \leq X$.

X	$\Delta_E > 0$	$\Delta_E < 0$	Total	Ratio^2
10^3	53	93	146	3.0790
10^4	191	322	513	2.8421
10^5	764	1304	2068	2.9132
10^6	3764	6356	10120	2.8515
10^7	20539	35096	55635	2.9198
10^8	116894	200799	317693	2.9508
10^9	691806	1195262	1887068	2.9851
10^{10}	4189445	7247980	11437425	2.9931

Subsequently we decided that we should recompute the discriminants of these curves as a sanity check, by reading the curves into `sage` and using its built-in elliptic curve routines to compute and then factor the discriminant. This took about one day on a single core.

The only curves of genuine interest are those that do not arise from twisting, i.e. those of discriminant $\pm p^2$, $\pm p^3$ and $\pm p^4$. In the last of these categories, we found only 5 curves, of conductors 11^2, 43^2, 431^2, 433^2 and 33013^2. The first four of these were noted by Edixhoven, de Groot and Top [39] (and are of small enough conductor to now appear in Cremona's tables). The fifth, satisfying

$$(a_1, a_2, a_3, a_4, a_6) = (1, -1, 1, -1294206576, 17920963598714),$$

has discriminant 33013^4. For discriminants $\pm p^2$ and $\pm p^3$, we found the following numbers of curves, for conductors p^2 with $p \leq X$:

X	$\Delta_E = -p^2$	$\Delta_E = p^2$	$\Delta_E = -p^3$	$\Delta_E = p^3$
10^3	12	4	7	4
10^4	36	24	9	5
10^5	80	58	12	9
10^6	203	170	17	15
10^7	519	441	24	23
10^8	1345	1182	32	36
10^9	3738	3203	48	58
10^{10}	10437	9106	60	86

It is perhaps worth observing that the majority of these curves arise from, in the case of discriminant $\pm p^2$, forms with, in the notation of Sections 5.6.5 and 5.6.5, either r or s in $\{1, 8\}$. Similarly, for $\Delta_E = \pm p^3$, most of the curves we found come from forms in the eight one-parameter families described in Section 5.6.5. We are unaware of a heuristic predicting the number of curves of conductor p^2 up to X that do not arise from twisting curves of conductor p.

5.8.4 Thue equations

It is noteworthy that all solutions we encountered to the Thue equations $F(x, y) = 8$ and $F(x, y) = 8p$ under consideration satisfied $|x|, |y| < 2^{30}$. The "largest" such solution corresponded to the equation

$$355x^3 + 293x^2y - 1310xy^2 - 292y^3 = 8,$$

where we have

$$(x, y) = (188455233, -82526573).$$

This leads to the elliptic curve of conductor 948762329069,

$$E \quad : \quad y^2 + xy + y = x^2 - 2x^2 + a_4x + a_6,$$

with

$$a_4 = -1197791024934480813341$$

and

$$a_6 = 15955840837175565243579564368641.$$

Note that this curve does not actually correspond to a particularly impressive abc or Hall conjecture (see Section 5.9 for the definition of this term) example.

In the following table, we collect data on the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary cubic forms of discriminant $4p$ or $-4p$ for p in $[0, X]$, denoted $P_3(0, X)$ and $P_3(-X, 0)$, respectively. We also provide counts for those forms where the corresponding equation $F(x, y) = 8$ has at least one integer solution, denoted $P_3^*(0, X)$ and $P_3^*(-X, 0)$ for positive and negative discriminant forms, respectively.

X	$P_3(0,X)$	$P_3^*(0,X)$	$P_3(-X,0)$	$P_3^*(-X,0)$
10^3	23	22	78	61
10^4	204	163	740	453
10^5	1851	1159	6104	2641
10^6	16333	7668	53202	16079
10^7	147653	49866	466601	97074
10^8	1330934	314722	4126541	582792
10^9	12050910	1966105	36979557	3530820
2×10^9	23418535	3408656	71676647	6080245
10^{10}	109730653	12229663	334260481	21576585
10^{11}	1004607003	76122366	3045402451	133115651
10^{12}	9247369050	475831852	27938060315	828238359

Due to space limitations we did not compute these statistics in the second large computational run.

Our expectation is that the number of forms for which the equation $F(x,y) = 8$ has solutions with absolute discriminant up to X is $o(X)$ (i.e. this occurs for essentially "zero" percent of forms; a first step in proving something is this direction can be found in recent work of Akhtari and Bhargava [2]).

5.8.5 Elliptic curves with the same prime conductor

One might ask how many isomorphism classes of curves of a given prime conductor can occur. If one accepts recent heuristics that predict that the Mordell-Weil rank of $E/\mathbb{Q}$ is absolutely bounded (see e.g. [86] and [113]), then this number should also be so bounded. As noted by Brumer and Silverman [20], there are 13 curves of conductor 61263451. Up to $p < 10^{12}$, the largest number we encountered was for $p = 530956036043$, with 20 isogeny classes, corresponding to

$(a_1, a_2, a_3, a_4, a_6)$ as follows :

$$(0,-1,1,-1003,37465)\,,(0,-1,1,-1775,45957)\,,(0,-1,1,-38939,2970729)\,,$$
$$(0,-1,1,-659,-35439)\,,(0,-1,1,2011,4311)\,,(0,-2,1,-27597,-1746656)\,,$$
$$(0,-2,1,57,35020)\,,(1,-1,0,-13337473,18751485796)\,,(0,0,1,-13921,633170)\,,$$
$$(0,0,1,-30292,-2029574)\,,(0,0,1,-6721,-214958)\,,(0,0,1,-845710,-299350726)\,,$$
$$(0,0,1,-86411851,309177638530)\,,(0,0,1,-10717,428466)\,,(1,-1,0,-5632177,5146137924)\,,$$
$$(1,-1,0,878,33379)\,,(1,-1,1,1080,32014)\,,(1,-2,1,-8117,-278943)\,,$$
$$(1,-3,0,-2879,71732)\,,(1,-3,0,-30415,-2014316)\,.$$

All have discriminant $-p$. Elkies [40] found examples of rather larger conductor with more curves, including 21 classes for $p = 14425386253757$ and discriminant p, and 24 classes for $p = 998820191314747$ and discriminant $-p$. Our computations confirm, with high likelihood, that, for $p < 2 \times 10^{13}$, the number of isomorphism classes of elliptic curves of conductor a fixed prime p is at most 21.

5.8.6 Rank and discriminant records

In the following table, we list the smallest prime conductor with a given Mordell-Weil rank. These were computed by running through our data, using Rubinstein's upper bounds for analytic ranks (as implemented in Sage) to search for candidate curves of "large" rank which were then checked using mwrank [32]. The last entry corresponds to a curve of rank 6 with minimal positive prime discriminant; we have not yet ruled out the existence of a rank 6 curve with smaller absolute (negative) discriminant.

N	$(a_1, a_2, a_3, a_4, a_6)$	sign(Δ_E)	$rk(E(\mathbb{Q})$
37	$(0, 0, 1, -1, 0)$	$+$	1
389	$(0, 1, 1, -2, 0)$	$+$	2
5077	$(0, 0, 1, -7, 6)$	$+$	3
501029	$(0, 1, 1, -72, 210)$	$+$	4
19047851	$(0, 0, 1, -79, 342)$	$-$	5
6756532597	$(0, 0, 1, -547, -2934)$	$+$	6

It is perhaps noteworthy that the curve listed here of rank 6 has the smallest known minimal discriminant for such a curve (see Table 4 of Elkies and Watkins [42]).

If we are interested in similar records over all curves, including composite conductors, we have

N	$(a_1, a_2, a_3, a_4, a_6)$	sign(Δ_E)	$rk(E(\mathbb{Q})$
37	$(0, 0, 1, -1, 0)$	$+$	1
389	$(0, 1, 1, -2, 0]$	$+$	2
5077	$(0, 0, 1, -7, 6)$	$+$	3
234446	$(1, -1, 0, -79, 289)$	$+$	4
19047851	$(0, 0, 1, -79, 342)$	$-$	5
5187563742	$(1, 1, 0, -2582, 48720)$	$+$	6
382623908456	$(0, 0, 0, -10012, 346900)$	$+$	7

Here, the curves listed above the line are proven to be those of smallest conductor with the given rank. Those listed below the line have the smallest known conductor for the corresponding rank. It is our belief that the techniques of this chapter should enable one to determine whether the curve listed here of rank 5 has the smallest conductor of any curve with this property.

5.9 Completeness of our data

As a final result, we will present something that might, optimistically, be viewed as evidence that our "heuristic" approach, in practice, enables us to actually find all elliptic curves of prime conductor $p < 2 \times 10^{13}$.

A conjecture of Hall, admittedly one that without modification is widely disbelieved at present, is that if x and y are integers for which $x^3 - y^2$ is nonzero, then the *Hall ratio*

$$\mathcal{H}_{x,y} = \frac{|x|^{1/2}}{|x^3 - y^2|}$$

is absolutely bounded. The pair (x, y) corresponding to the largest known Hall ratio comes from the identity

$$5853886516781223^3 - 447884928428402042307918^2 = 1641843,$$

noted by Elkies [41], with $\mathcal{H}_{x,y} > 46.6$. All other examples known currently have $\mathcal{H}_{x,y} < 7$. We prove the following.

Proposition 5.9.1. *If there is an elliptic curve E with conductor $p < 2 \times 10^{13}$, corresponding via Theorem 5.2.1 to a cubic form F and $u, v \in \mathbb{Z}$, such that*

$$F(u, v) = 8 \quad \textit{and} \quad \max\{|u|, |v|\} \geq 2^{128},$$

then

$$\mathcal{H}_{c_4(E),c_6(E)} > 1.5 \times 10^6. \tag{5.39}$$

In other words, if there is an elliptic curve E with conductor $p < 2 \times 10^{13}$ that we have missed in our heuristic search, then we necessarily have inequality (5.39) (and hence a record-setting Hall ratio).

Proof. The main idea behind our proof is that the roots of the Hessian $H_F(x, 1)$ have no particularly good reason to be close to those of the polynomial $F(x, 1)$. It follows that, if we have relatively large integers u and v satisfying the Thue equation $F(u, v) = 8$ (so that u/v is close to a root of $F(x, 1) = 0$), our expectation is that not only does $H_F(u,v)$ fail to be small, but, in fact, we should have inequalities of the order of

$$H_F(u,v) \gg (\max\{|u|,|v|\})^2 \quad \text{and} \quad G_F(u,v) \gg (\max\{|u|,|v|\})^3$$

(where the Vinogradov symbol hides a possible dependence on p). Since

$$c_4(E) = \mathcal{D}^2 H_F(u,v) \text{ and } c_6(E) = -\frac{1}{2}\mathcal{D}^3 G_F(u,v),$$

where $\mathcal{D} \in \{1,2\}$, these would imply that

$$\mathcal{H}_{c_4(E),c_6(E)} \gg_p \frac{1}{p}\max\{|u|,|v|\}.$$

In fact, for forms (and curves) of positive discriminant, we can deduce inequalities of the shape

$$\mathcal{H}_{c_4(E),c_6(E)} \gg_p p^{-3/4}\min\{|u|,|v|\} \gg p^{-5/4}\max\{|u|,|v|\},$$

where the implicit constants are absolute. For curves of negative discriminant, we have a slightly weaker result :

$$\mathcal{H}_{c_4(E),c_6(E)} \gg_p p^{-1}\min\{|u|,|v|\} \gg p^{-3/2}\max\{|u|,|v|\}.$$

To make this argument precise, let us write, for concision, $c_4 = c_4(E)$ and $c_6 = c_6(E)$. From the identity $|c_4^3 - c_6^2| = 1728p$, we have a Hall ratio

$$\mathcal{H}_{c_4,c_6} = \frac{|c_4|^{1/2}}{1728p} > \frac{|c_4|^{1/2}}{3.456 \times 10^{16}} \geq \frac{|H_F(u,v)|^{1/2}}{3.456 \times 10^{16}}.$$

Our goal will thus be to obtain a lower bound upon $|H_F(u,v)|$ – we claim that, in fact, $|H_F(u,v)| > 3 \times 10^{45}$, whereby this Hall ratio exceeds 1.5×10^6, as stated. Suppose that we have a cubic form F and integers u and v with $D_F = \pm 4p$ for p prime,

$$\max\{|u|,|v|\} \geq 2^{128} \quad \text{and} \quad 2 \times 10^9 < p < 2 \times 10^{13}. \tag{5.40}$$

Notice that $F(u,0) = \omega_0 u^3 = 8$ and hence (5.40) implies that $v \neq 0$.

Write

$$F(u,v) = \omega_0(u - \alpha_1 v)(u - \alpha_2 v)(u - \alpha_3 v)$$

and suppose that

$$|u - \alpha_1 v| = \min\{|u - \alpha_i v|,\ i = 1, 2, 3\}.$$

We may further assume, without loss of generality, that the form F is reduced. From (5.6), we have

$$\omega_0^2\ |H_F(\alpha_1, 1)\, H_F(\alpha_2, 1)\, H_F(\alpha_3, 1)| = 16\, p^2. \tag{5.41}$$

For future use, we note that the main result of Mahler [68] implies the inequality

$$|\omega_0| \prod_{i=1}^{3} \max\{1, |\alpha_i|\} \leq |\omega_0| + |\omega_1| + |\omega_2| + |\omega_3|. \tag{5.42}$$

Let us assume first that $D_F > 0$, whereby H_F has negative discriminant ($D_{H_F} = -3D_F$). Since F is reduced, we have

$$|\omega_1\omega_2 - 9\omega_0\omega_3| \leq \omega_1^2 - 3\omega_0\omega_2 \leq \omega_2^2 - 3\omega_1\omega_3,$$

and hence the identity

$$(\omega_1\omega_2 - 9\omega_0\omega_3)^2 - 4(\omega_1^2 - 3\omega_0\omega_2)(\omega_2^2 - 3\omega_1\omega_3) = -3D_F \tag{5.43}$$

yields the inequalities

$$D_F \geq (\omega_1^2 - 3\omega_0\omega_2)(\omega_2^2 - 3\omega_1\omega_3) \geq (\omega_1^2 - 3\omega_0\omega_2)^2. \tag{5.44}$$

Since (5.43) and $D_F > 0$ imply that $\omega_1^2 - 3\omega_0\omega_2 \neq 0$, we may write

$$\frac{H_F(\alpha_1, 1)}{\omega_1^2 - 3\omega_0\omega_2} = \left(\alpha_1 - \frac{9\omega_0\omega_3 - \omega_1\omega_2 + \sqrt{-3D_F}}{2(\omega_1^2 - 3\omega_0\omega_2)}\right)\left(\alpha_1 - \frac{9\omega_0\omega_3 - \omega_1\omega_2 - \sqrt{-3D_F}}{2(\omega_1^2 - 3\omega_0\omega_2)}\right).$$

Defining

$$\Gamma_1 = \alpha_1 - \frac{9\omega_0\omega_3 - \omega_1\omega_2}{2(\omega_1^2 - 3\omega_0\omega_2)} \quad \text{and} \quad \Gamma_2 = \frac{\sqrt{3D_F}}{2(\omega_1^2 - 3\omega_0\omega_2)},$$

we have

$$H_F(\alpha_1, 1) = \left(\omega_1^2 - 3\omega_0\omega_2\right)\left(\Gamma_1^2 + \Gamma_2^2\right)$$

and so

$$|H_F(\alpha_1, 1)| > \frac{3D_F}{4(\omega_1^2 - 3\omega_0\omega_2)}. \tag{5.45}$$

Since α_1 is "close" to u/v, it follows that the same is true for $H_F(\alpha_1, 1)$ and $H_F(u/v, 1) = v^{-2}H_F(u, v)$. To make this precise, note that, via the Mean Value Theorem,

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| = \left|2(\omega_1^2 - 3\omega_0\omega_2)y + \omega_1\omega_2 - 9\omega_0\omega_3\right| \left|\alpha_1 - \frac{u}{v}\right|, \tag{5.46}$$

for some y lying between α_1 and u/v. We thus have

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| \leq (\omega_1^2 - 3\omega_0\omega_2)\left(2\left(|\alpha_1| + \left|\alpha_1 - \frac{u}{v}\right|\right) + 1\right)\left|\alpha_1 - \frac{u}{v}\right|. \tag{5.47}$$

To derive an upper bound upon $\left|\alpha_1 - \frac{u}{v}\right|$, we can argue as in the proof of Theorem 2 of Pethő [88] to obtain the inequality

$$\left|\alpha_1 - \frac{u}{v}\right| \leq 2^{7/3} D_F^{-1/6} v^{-2}. \tag{5.48}$$

Since $|v| \geq 1$ and $D_F = 4p > 8 \times 10^9$, we thus have that

$$\left|\alpha_1 - \frac{u}{v}\right| < 0.12. \tag{5.49}$$

We may suppose that F is reduced, whereby, crudely, from Lemma **??**,

$$|\omega_0| \leq \frac{2D_F^{1/4}}{3\sqrt{3}} \quad \text{and} \quad |\omega_1| \leq \frac{3\omega_0}{2} + \left(\sqrt{D_F} - \frac{27\omega_0^2}{4}\right)^{1/2} < \left(1 + \frac{1}{\sqrt{3}}\right) D_F^{1/4}.$$

From Proposition 5.5 of Belabas and Cohen [8],

$$|\omega_2| \leq \left(\frac{35+13\sqrt{13}}{216}\right)^{1/3} D_F^{1/3} \text{ and } |\omega_3| \leq \frac{4}{27} D_F^{1/2},$$

whence, after a little computation, we find that

$$|\omega_0| + |\omega_1| + |\omega_2| + |\omega_3| < D_F^{1/2} = 2p^{1/2}.$$

From (5.42), it follows that

$$|\alpha_1| \leq |\omega_0| + |\omega_1| + |\omega_2| + |\omega_3| < 2p^{1/2},$$

whereby inequalities (5.49) and (5.40) thus yield

$$|u/v| < 2p^{1/2} + 0.12 < 2^{23.1},$$

and so, again appealing to (5.40), $\min\{|u|, |v|\} > 2^{104}$. Returning to inequality (5.47), we find that, after applying (5.44),

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| \leq 2p^{1/2} \left(4p^{1/2} + 1.24\right) 2^{7/3} (2p)^{-1/6} v^{-2}.$$

From $p < 2 \times 10^{13}$ and $|v| > 2^{104}$, it follows that

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| < 10^{-50}.$$

Combining this with (5.44) and (5.45) yields the inequality

$$|H_F(u/v, 1)| > \frac{2p}{|\omega_1^2 - 3\omega_0\omega_2|},$$

whence

$$|H_F(u, v)| = v^2 \, |H_F(u/v, 1)| > \frac{2v^2 p}{|\omega_1^2 - 3\omega_0\omega_2|} \geq v^2 \sqrt{p},$$

where the last inequality follows from (5.44). From (5.40) and the fact that $|v| >$

2^{104}, we conclude that

$$|H_F(u,v)| > 10^{67}.$$

Next, suppose that F has negative discriminant, so that H_F has positive discriminant $D_{H_F} = -3D_F$. If $\omega_1^2 - 3\omega_0\omega_2 = 0$, then, from (5.43), we have that

$$3p = -(\omega_1^2 - 3\omega_0\omega_2)(\omega_2^2 - 3\omega_1\omega_3),$$

which implies that

$$\max\left\{|\omega_1^2 - 3\omega_0\omega_2|, |\omega_2^2 - 3\omega_1\omega_3|\right\} \geq p.$$

On the other hand, from Lemma 6.4 of Belabas and Cohen [8], we have

$$\begin{gathered}|\omega_0| \leq \tfrac{2^{3/2}p^{1/4}}{3^{3/4}},\ |\omega_1| \leq \tfrac{2^{3/2}p^{1/4}}{3^{1/4}},\ \max\{|\omega_0\omega_2^3|, |\omega_1^3\omega_3|\} \leq \tfrac{(11+5\sqrt{5})p}{2}, \\ |\omega_1\omega_2| \leq \tfrac{8p^{1/2}}{3^{1/2}} \ \text{ and } \ |\omega_0\omega_3| \leq \tfrac{2p^{1/2}}{3^{1/2}},\end{gathered} \tag{5.50}$$

whereby a short calculation, together with the fact that $p > 2 \times 10^9$, yields a contradiction. We may thus suppose that $\omega_1^2 - 3\omega_0\omega_2 \neq 0$. We have

$$H_F(\alpha_i, 1) = (\omega_1^2 - 3\omega_0\omega_2)(\alpha_i - \beta_1)(\alpha_i - \beta_2),$$

where

$$\beta_j = \frac{9\omega_0\omega_3 - \omega_1\omega_2 + (-1)^j\sqrt{12p}}{2(\omega_1^2 - 3\omega_0\omega_2)} \quad \text{for} \quad j \in \{1,2\}.$$

It follows that

$$|\beta_j| \leq |\omega_1^2 - 3\omega_0\omega_2|^{-1} 44 \cdot 3^{-1/2} p^{1/2}$$

and, again from (5.42),

$$|\omega_0\alpha_i| \leq |\omega_0| + |\omega_1| + |\omega_2| + |\omega_3|,$$

whereby

$$|\omega_0\alpha_i| \leq \frac{2^{3/2}p^{1/4}}{3^{3/4}} + \frac{2^{3/2}p^{1/4}}{3^{1/4}} + \frac{2^{2/3}\left(11+5\sqrt{5}\right)^{1/3}p^{1/2}}{3^{1/2}|\omega_0|} + \frac{2p^{1/2}}{3^{1/2}|\omega_0|},$$

whence we find that

$$|\alpha_i| \leq \frac{3.4\,p^{1/4}}{|\omega_0|} + \frac{2.1\,p^{1/2}}{|\omega_0|^2} < \frac{6.4\,p^{1/2}}{|\omega_0|^2}.$$

From (5.41), we thus have

$$|H_F(\alpha_1,1)| \geq \omega_0^{-2}(\omega_1^2-3\omega_0\omega_2)^{-2}\min\left\{\frac{\omega_0^2}{3.2}, \frac{|\omega_1^2-3\omega_0\omega_2|}{12.8}\right\}^2.$$

If $|\omega_1^2-3\omega_0\omega_2| > 4\omega_0^2$, it follows that

$$|H_F(\alpha_1,1)| \geq \frac{\omega_0^2}{10.24\,(\omega_1^2-3\omega_0\omega_2)^2}$$

and so

$$|H_F(\alpha_1,1)| \geq \frac{1}{10.24\,(2^3 3^{-1/2}p^{1/2} + 2^{2/3}3^{1/2}\left(11+5\sqrt{5}\right)^{1/3}p^{1/2})^2}$$

which implies that

$$|H_F(\alpha_1,1)| > \frac{1}{1561\,p}. \tag{5.51}$$

If, conversely, $|\omega_1^2-3\omega_0\omega_2| \leq 4\omega_0^2$, then

$$|H_F(\alpha_1,1)| \geq \frac{1}{163.84\,\omega_0^2} > \frac{1}{253\sqrt{p}}$$

and hence (5.51) holds in either case.

Now if $\alpha_1 \notin \mathbb{R}$, then, via Mahler [69],

$$|\mathrm{Im}(\alpha_1)| \geq \frac{1}{18}\left(|\omega_0|+|\omega_1|+|\omega_2|+|\omega_3|\right)^{-2} > \frac{\omega_0^2}{738\,p},$$

so that

$$\left|\alpha_1 - \frac{u}{v}\right| > \frac{\omega_0^2}{738\,p}$$

and hence

$$8 = |\omega_0||v|^3 \left|\alpha_1 - \frac{u}{v}\right| \left|\alpha_2 - \frac{u}{v}\right| \left|\alpha_3 - \frac{u}{v}\right| > |\omega_0||v|^3 \left(\frac{\omega_0^2}{738\,p}\right)^3.$$

It follows that

$$|v| < 1476p < 2.952 \times 10^{16},$$

via (5.40). Since $\max\{|u|,|v|\} > 2^{128}$, we thus have

$$|u/v| > 1.15 \times 10^{22}.$$

From

$$|\alpha_1| < 6.4p^{1/2} < 6.4\left(2 \times 10^{13}\right)^{1/2} < 3 \times 10^7,$$

we may thus conclude that

$$\left|\alpha_1 - \frac{u}{v}\right| > 1.14 \times 10^{22}$$

and so

$$8 \geq \left(1.14 \times 10^{22}\right)^3,$$

an immediate contradiction.

We may thus suppose that $\alpha_1 \in \mathbb{R}$ (so that $\alpha_2, \alpha_3 \notin \mathbb{R}$). It follows from Mahler [69] that

$$\left|\alpha_i - \frac{u}{v}\right| > \frac{\omega_0^2}{738\,p}, \quad \text{for} \quad i \in \{2,3\},$$

and so

$$\left|\alpha_1 - \frac{u}{v}\right| < \frac{8}{|\omega_0||v|^3}\left(\frac{738p}{\omega_0^2}\right)^2. \tag{5.52}$$

Appealing to (5.40) and the inequalities $|\alpha_1| < 3 \times 10^7$ and $|v| \geq 1$, we thus have that

$$|u/v| < 1.75 \times 10^{33} + 3 \times 10^7 < 1.76 \times 10^{33},$$

and so, from $\max\{|u|,|v|\} > 2^{128}$, $|v| > 1.9 \times 10^5$. Inequality (5.52) thus now implies

$$|u/v| < 2.6 \times 10^{17},$$

whence $|v| > 1.3 \times 10^{21}$. Substituting this a third time into (5.52),

$$\left|\alpha_1 - \frac{u}{v}\right| < 10^{-30},$$

so that $|u/v| < 3.1 \times 10^7$ and $|v| > 10^{31}$. One final use of (5.52) thus yields the inequality

$$\left|\alpha_1 - \frac{u}{v}\right| < 10^{-59}.$$

Appealing to (5.40), (5.46), (5.50), and the fact that $|\alpha_1| < 3 \times 10^7$, we thus have, after a little work,

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| < 3.4 \times 10^{-44}.$$

With (5.51), this implies that

$$|H_F(u/v, 1)| > \frac{1}{1562\,p}$$

and so

$$|H_F(u,v)| = v^2\,|H_F(u/v,1)| > \frac{v^2}{1562p} > \frac{10^{62}}{3124 \times 10^{13}} > 3 \times 10^{45},$$

as claimed. □

5.10 Concluding remarks

Many of the techniques of this chapter can be generalized to potentially treat the problem of determining elliptic curves of a given conductor over a number field K. In case K is an imaginary quadratic field of class number 1, then, in fact, such an approach works without any especially new ingredients.

Chapter 6

Towards Efficient Resolution of Thue-Mahler Equations

Let a denote a nonzero integer and let $S = \{p_1, \ldots, p_v\}$ be a set of rational primes. In this section, we specialize the results of Chapter 3 to the degree 3 Thue–Mahler equation

$$F(X,Y) = c_0X^3 + c_1X^2Y + c_2XY^2 + c_3Y^3 = ap_1^{Z_1} \cdots p_v^{Z_v}, \tag{6.1}$$

where $(X,Y) \in \mathbb{Z}^2$, $\gcd(X,Y) = 1$, and $Z_i \geq 0$ for $i = 1, \ldots, v$. In particular, to enumerate the set of solutions $\{X, Y, Z_1, \ldots, Z_v\}$ to this equation, we follow Section 3.4 to reduce the problem of solving (6.1) to solving finitely many so-called "S-unit" equations

$$\lambda = \delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i} - 1 = \delta_2 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i}, \tag{6.2}$$

where

$$\delta_1 = \frac{\theta^{(i_0)} - \theta^{(j)}}{\theta^{(i_0)} - \theta^{(k)}} \cdot \frac{\alpha^{(k)}\zeta^{(k)}}{\alpha^{(j)}\zeta^{(j)}}, \quad \delta_2 = \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\alpha^{(i_0)}\zeta^{(i_0)}}{\alpha^{(j)}\zeta^{(j)}}$$

are constants. Here, we adopt the notation of Chapter 3 and recall that we reduce (6.1) to a homogenous equation of the form

$$f(x,y) = x^3 + C_1x^2y + C_2xy^2 + C_3y^3 = cp_1^{z_1} \cdots p_v^{z_v}, \tag{6.3}$$

where $\gcd(x,y) = 1$ and $\gcd(c,p_i) = 1$ for $i = 1,\dots,p_v$. Moreover, we set

$$g(t) = f(t,1) = t^3 + C_1t^2 + C_2t + C_3 \tag{6.4}$$

so that $K = \mathbb{Q}(\theta)$ with $g(\theta) = 0$. Recall that ζ in (6.2) denotes a root of unity in K, while $\{\varepsilon_1,\dots,\varepsilon_r\}$ is a set of fundamental units of $\mathcal{O}_K$. In this case, as K is a degree 3 extension of $\mathbb{Q}$, we either have 3 real embeddings of K into $\mathbb{C}$, or one real embedding of K into $\mathbb{C}$ and a pair of complex conjugate embeddings of K into $\mathbb{C}$. Thus either $r = 1$ or $r = 2$.

In this section, we describe new techniques to solve equation (6.2) via a global Weil height. This work is part of the on-going collaborative project [44]. Notably, the ideas presented in this chapter do not yet yield a full degree 3 Thue-Mahler solver. Indeed, for the time being, only those Thue-Mahler equations with $r = 2$ are considered. However, when $r = 1$, the general setup established in this chapter remains the same.

6.1 Decomposition of the Weil height

The sieves of [112] involve logarithms which are of local nature. To obtain a global sieve, we work instead with the global logarithmic Weil height. This height is invariant under conjugation and admits a decomposition into local heights which can be related to complex and p-adic logarithms.

Let $n_1,\dots,n_\nu,a_1,\dots,a_r$ be a solution to (6.2) and consider the Weil height of

$$\frac{\delta_2}{\lambda} = \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(j)}}{\varepsilon_i^{(i_0)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{n_i}.$$

Given the global Weil height of δ_2/λ, or all the local heights of δ_2/λ, we will construct several ellipsoids 'containing' $n_1, \ldots, n_\nu, a_1, \ldots, a_r$ such that the volume of the ellipsoids are as small as possible. We begin by computing the height of δ_2/λ.

Let L be the splitting field of K. Recall that for cubic extensions K, the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to either the alternating group A_3 or the symmetric group S_3.

Lemma 6.1.1. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and let $\mathfrak{P}$ denote an ideal of $\mathcal{O}_L$ lying above it. Suppose $\sigma_{i_0} : L \to L$, $\theta \mapsto \theta^{(i_0)}$ and $\sigma_j : L \to L$, $\theta \mapsto \theta^{(j)}$ are two automorphisms of L such that (i_0, j, k) forms a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ of order 3. Let $\mathfrak{P}^{(i_0)} = \sigma_{i_0}(\mathfrak{P})$ and $\mathfrak{P}^{(j)} = \sigma_j(\mathfrak{P})$ be the prime ideals lying over $\mathfrak{p}^{(i_0)}$, $\mathfrak{p}^{(j)}$ respectively. For $i = 1, \ldots, \nu$,*

$$\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)\mathcal{O}_L = \left(\prod_{\mathfrak{P}|\mathfrak{p}_1} \frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_1^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_1^{(i_0)})}}\right)^{a_{1i}} \cdots \left(\prod_{\mathfrak{P}|\mathfrak{p}_\nu} \frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_\nu^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_\nu^{(i_0)})}}\right)^{a_{\nu i}}$$

where $\mathfrak{P}^{(j)} \neq \mathfrak{P}^{(i_0)}$ for all $\mathfrak{P}$ lying above $\mathfrak{p}$ in K.

Proof. Since

$$(\gamma_i)\mathcal{O}_K = \mathfrak{p}_1^{a_{1i}} \cdots \mathfrak{p}_\nu^{a_{\nu i}},$$

for $i = 1, \ldots, \nu$, where

$$\mathfrak{p}_i\mathcal{O}_L = \prod_{\mathfrak{P}|\mathfrak{p}_i} \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p}_i)},$$

it holds that

$$(\gamma_i)\mathcal{O}_L = \left(\prod_{\mathfrak{P}|\mathfrak{p}_1} \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p}_1)}\right)^{a_{1i}} \cdots \left(\prod_{\mathfrak{P}|\mathfrak{p}_\nu} \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p}_\nu)}\right)^{a_{\nu i}}.$$

Let $\mathfrak{P}^{(i_0)}, \mathfrak{P}^{(j)}$ denote the ideal $\mathfrak{P}$ under the automorphisms of L

$$\sigma_{i_0} : L \to L, \quad \theta \mapsto \theta^{(i_0)} \quad \text{and} \quad \sigma_j : L \to L, \quad \theta \mapsto \theta^{(j)},$$

respectively. That is, $\mathfrak{P}^{(i_0)} = \sigma_{i_0}(\mathfrak{P})$ and $\mathfrak{P}^{(j)} = \sigma_j(\mathfrak{P})$. Then

$$\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)\mathcal{O}_L = \left(\prod_{\mathfrak{P}|\mathfrak{p}_1} \frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_1^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_1^{(i_0)})}}\right)^{a_{1i}} \cdots \left(\prod_{\mathfrak{P}|\mathfrak{p}_\nu} \frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_\nu^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_\nu^{(i_0)})}}\right)^{a_{\nu i}}.$$

To show that $\mathfrak{P}^{(j)} \neq \mathfrak{P}^{(i_0)}$ for all $\mathfrak{P}$ lying above $\mathfrak{p}$ in K, we consider the decomposition group of $\mathfrak{P}$,

$$D(\mathfrak{P}|p) = \{\sigma \in G \ : \ \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Iterating through all possible decompositions of $\mathfrak{p}$ in L, we observe that $\mathfrak{P}^{(i_0)} \neq \mathfrak{P}^{(j)}$ whenever $D(\mathfrak{P}_i|p)$ does not have cardinality 2. Since (i_0, j, k) forms an order 3 subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, it cannot coincide with $D(\mathfrak{P}|p)$ and therefore cannot lead to $\mathfrak{P}^{(i_0)} = \mathfrak{P}^{(j)}$. $\square$

For the remainder of this paper, we assume that (i_0, j, k) are automorphisms of L selected as in Lemma 6.1.1.

Lemma 6.1.2. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and let $\mathfrak{P}$ denote an ideal of $\mathcal{O}_L$ lying above it. Let $\mathfrak{P}^{(i_0)} = \sigma_{i_0}(\mathfrak{P})$ and $\mathfrak{P}^{(j)} = \sigma_j(\mathfrak{P})$ be the prime ideals lying over $\mathfrak{p}^{(i_0)}$, $\mathfrak{p}^{(j)}$ respectively. We have*

$$\mathrm{ord}_{\mathfrak{P}}\left(\frac{\delta_2}{\lambda}\right) = \begin{cases} (u_l - r_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}) & \text{if } \mathfrak{P}^{(j)} \mid p_l,\ p_l \in \{p_1, \ldots, p_\nu\} \\ (r_l - u_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)}) & \text{if } \mathfrak{P}^{(i_0)} \mid p_l,\ p_l \in \{p_1, \ldots, p_\nu\} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Lemma 6.1.1, we have

$$\begin{aligned}
\left(\frac{\delta_2}{\lambda}\right)\mathcal{O}_L &= \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{n_1}\cdots\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{n_\nu}\mathcal{O}_L \\
&= \left(\prod_{\mathfrak{P}|\mathfrak{p}_1}\frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_1^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_1^{(i_0)})}}\right)^{\sum_{i=1}^{\nu} n_i a_{1i}}\cdots\left(\prod_{\mathfrak{P}|\mathfrak{p}_\nu}\frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_\nu^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_\nu^{(i_0)})}}\right)^{\sum_{i=1}^{\nu} n_i a_{\nu i}} \\
&= \left(\prod_{\mathfrak{P}|\mathfrak{p}_1}\frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_1^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_1^{(i_0)})}}\right)^{u_1-r_1}\cdots\left(\prod_{\mathfrak{P}|\mathfrak{p}_\nu}\frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_\nu^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_\nu^{(i_0)})}}\right)^{u_\nu-r_\nu}.
\end{aligned}$$

It follows that

$$\mathrm{ord}_{\mathfrak{P}}\left(\frac{\delta_2}{\lambda}\right) = \begin{cases} (u_l-r_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}) & \text{if } \mathfrak{P}^{(j)} \mid p_l,\ p_l\in\{p_1,\ldots,p_\nu\} \\ (r_l-u_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)}) & \text{if } \mathfrak{P}^{(i_0)} \mid p_l,\ p_l\in\{p_1,\ldots,p_\nu\} \\ 0 & \text{otherwise.}\end{cases}$$

□

Let $\log^+(\cdot)$ denote the real valued function $\max(\log(\cdot),0)$ on $\mathbb{R}_{\geq 0}$.

Proposition 6.1.3. *The height* $h\left(\frac{\delta_2}{\lambda}\right)$ *admits a decomposition*

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu}\log(p_l)|u_l-r_l| + \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\}. \tag{6.5}$$

For ease of notation, let $S^* = S\cup\{v : L\to\mathbb{C}\}$ and write

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in S^*} h_v\left(\frac{\delta_2}{\lambda}\right).$$

By Proposition 6.1.3, when $v = p_l$ is a finite place,

$$h_v\left(\frac{\delta_2}{\lambda}\right) = \log(p_l)|u_l-r_l|,$$

whereas we write

$$h_v\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[L:K]}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}$$

for all infinite places $v = w$. Finally, let m denote the number of embeddings of L into $\mathbb{C}$, $m = \#\{v : L \to \mathbb{C}\}$.

Proof of Proposition 6.1.3. Since $\frac{\delta_2}{\lambda} \in L$, the definition of the absolute logarithmic Weil height gives

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[L:\mathbb{Q}]}\sum_{w\in M_L}\log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\}$$

where $||z||_w$ is the usual norms and M_L is a set of inequivalent absolute values on L. In particular, if $w : L \to \mathbb{C}$ is an infinite place, we obtain

$$\log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} = \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}.$$

Writing $z = \frac{\delta_2}{\lambda}$ and $w = \mathfrak{P}$ a finite place, we have

$$\log\max\{\|z\|_w, 1\} = \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{\mathrm{ord}_{\mathfrak{P}}(z)}}\right), 0\right\}.$$

By Lemma 6.1.2,

$$\mathrm{ord}_{\mathfrak{P}}\left(\frac{\delta_2}{\lambda}\right) = \begin{cases} (u_l - r_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}) & \text{if } \mathfrak{P}^{(j)} \mid p_l,\ p_l \in \{p_1,\ldots,p_\nu\} \\ (r_l - u_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)}) & \text{if } \mathfrak{P}^{(i_0)} \mid p_l,\ p_l \in \{p_1,\ldots,p_\nu\} \\ 0 & \text{otherwise.} \end{cases}$$

That is, for $\mathfrak{P}^{(j)} \mid p_l$ where $p_l \in \{p_1, \ldots, p_\nu\}$, we have

$$\begin{aligned}\log\max\{||z||_w, 1\} &= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{\mathrm{ord}_{\mathfrak{P}}(z)}}\right), 0\right\}\\ &= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{(u_l - r_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)})}}\right), 0\right\}\\ &= \max\left\{-(u_l - r_l)f(\mathfrak{P}^{(j)} \mid p_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)})\log(p_l), 0\right\}.\end{aligned}$$

Moreover, for $p_l \in \{p_1, \ldots, p_\nu\}$, there is one unique prime ideal $\mathfrak{p}_l$ in the ideal equation (3.8) lying above p_l in K. Hence, each $\mathfrak{P}$ lying over p_l must also lie over $\mathfrak{p}_l$. Now,

$$\begin{aligned}\sum_{\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}} \log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} &= \sum_{\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}} \max\left\{-(u_l - r_l)f(\mathfrak{P}^{(j)} \mid p_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)})\log(p_l), 0\right\}\\ &= \max\left\{(r_l - u_l)\log(p_l), 0\right\} f(\mathfrak{p}_l^{(j)} \mid p_l)[L : \mathbb{Q}(\theta^{(j)})]\\ &= \max\left\{(r_l - u_l)\log(p_l), 0\right\} f(\mathfrak{p}_l^{(j)} \mid p_l)[L : K],\end{aligned}$$

where the last inequality follows from $K = \mathbb{Q}(\theta) \cong \mathbb{Q}(\theta^{(j)})$.

Similarly, for $\mathfrak{P}^{(i_0)} \mid p_l$ where $p_l \in \{p_1, \ldots, p_\nu\}$, we have

$$\begin{aligned}\log\max\{\|z\|_w, 1\} &= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{\mathrm{ord}_{\mathfrak{P}}(z)}}\right), 0\right\}\\ &= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{(r_l - u_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)})}}\right), 0\right\}\\ &= \max\left\{-(r_l - u_l)f(\mathfrak{P}^{(i_0)} \mid p_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)})\log(p_l), 0\right\},\end{aligned}$$

and so

$$\sum_{\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)}} \log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} = \max\left\{(u_l - r_l)\log(p_l), 0\right\} f(\mathfrak{p}_l^{(i_0)} \mid p_l)[L : K].$$

Lastly, if $w = \mathfrak{P}$ such that $\mathfrak{P} \neq \mathfrak{P}^{(i_0)}, \mathfrak{P}^{(j)}$, we have

$$\log\max\{\|z\|_w, 1\} = \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{\mathrm{ord}_{\mathfrak{P}}(z)}}\right), 0\right\} = 0.$$

Putting this all together, we obtain

$$\begin{aligned} h\left(\frac{\delta_2}{\lambda}\right) &= \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[L:\mathbb{Q}]}\sum_{\mathfrak{P}\in\mathcal{O}_L \text{ finite}}\log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_{\mathfrak{P}}, 1\right\} \\ &= \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu}\log(p_l)|u_l - r_l|. \end{aligned}$$

□

6.2 Initial height bounds

We seek solutions to equaition (6.2). We recall this equation presently,

$$\lambda = \delta_1\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i} - 1 = \delta_2\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i}.$$

To simplify notation, we write

$$\tilde{y} = \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}, \quad \tilde{x} = \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i}$$

so that equation (6.2) becomes

$$\delta_1\tilde{y} - \delta_2\tilde{x} = 1. \tag{6.6}$$

Let $z = \frac{1}{\tilde{x}} = \frac{\delta_2}{\lambda}$ and denote by Σ the set of pairs $(\tilde{x}, \tilde{y})$ satisfying (6.6). That is, Σ denotes the set of tuples $(n_1, \ldots, n_\nu, a_1, \ldots, a_r)$ corresponding to $(\tilde{x}, \tilde{y})$ which satisfy (6.6).

Let $\mathbf{l}, \mathbf{h} \in \mathbb{R}^{\nu+m}$ with $\mathbf{0} \leq \mathbf{l} \leq \mathbf{h}$. Then we define $\Sigma(\mathbf{l}, \mathbf{h})$ as the set of all

$(\tilde{x}, \tilde{y}) \in \Sigma$ such that $\left(h_v\left(\frac{\delta_2}{\lambda}\right)\right) \leq \mathbf{h}$ and such that $\left(h_v\left(\frac{\delta_2}{\lambda}\right)\right) \not\leq \mathbf{l}$, and write $\Sigma(\mathbf{h}) = \Sigma(\mathbf{l}, \mathbf{h})$ if $\mathbf{l} = \mathbf{0}$. Additionally, for each place w, we denote by $\Sigma_w(\mathbf{l}, \mathbf{h})$ the set of all $(\tilde{x}, \tilde{y}) \in \Sigma(\mathbf{h})$ such that $h_w(z) > l_w$.

Recall the minimal polynomial $g(t)$ of K, (6.4), derived from

$$f(x, y) = x^3 + C_1x^2y + C_2xy^2 + C_3y^3 = cp_1^{z_1} \cdots p_v^{z_v}.$$

For $S = \{p_1, \ldots, p_v\}$, let $N_S = \prod_{p \in S} p$ and set

$$b_S = 1728N_S^2 \prod_{p \notin S} p^{\min(2, \mathrm{ord}_p(b))}$$

for any integer b. In particular, we take $b = 432\Delta c^2$ with Δ the discriminant of f. Denote by $h(f - c)$ the maximum logarithmic Weil heights of the coefficients of the polynomial $f - c$,

$$h(f - c) = \max(\log|C_1|, \log|C_2|, \log|C_3|, \log|c|).$$

Now, setting

$$\Omega = 2b_S \log(b_S) + 172h(f - c),$$

we obtain, by Corollary J (ii) of [56], the following height bound on any solution (x, y) of (6.3)

$$\max(h(x), h(y)) \leq \Omega.$$

To translate this result for use with our logarithmic Weil height (6.5), we have the following lemma.

Lemma 6.2.1. *Let* $\mathbf{m} = (n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{r+\nu}$ *be any solution of* (6.2) *and let*

$$\Omega' = 2h(\alpha) + 4\Omega + 2h(\theta) + 2\log(2). \tag{6.7}$$

If $\mathbf{h} \in \mathbb{R}^{\nu+m}$ *with* $\mathbf{h} = (\Omega')$, *then* $\mathbf{m} \in \Sigma(h)$.

Proof. Let $(\tilde{x}, \tilde{y}) \in \Sigma$. We show that the corresponding value $z = \frac{1}{\tilde{x}} = \frac{\delta_2}{\lambda}$ arising from this choice of $\tilde{x}, \tilde{y}$ satisfies

$$\mathbf{0} < \left(h_v \left(\frac{\delta_2}{\lambda} \right) \right) \leq \mathbf{h}.$$

As stated earlier, any solution x, y of $f(x,y) = cp_1^{z_1} \cdots p_v^{z_v}$ satisfies

$$\max(h(x), h(y)) \leq \Omega.$$

Taking the height of

$$\beta = x - y\theta = \alpha\zeta\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \cdot \gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu},$$

we obtain

$$h(\beta) = h(x) + h(\theta) + h(y) + \log 2 \leq 2\Omega + h(\theta) + \log 2.$$

In particular, as $h(\beta) = h(\beta^{(i)})$,

$$h(\beta^{(i)}) \leq 2\Omega + h(\theta) + \log 2.$$

Now,

$$\delta_2 \tilde{x} = \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\alpha^{(i_0)}\zeta^{(i_0)}}{\alpha^{(j)}\zeta^{(j)}} \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}} \right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}} \right)^{n_i} = \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}},$$

meaning that $\tilde{x}$ may be written as

$$\tilde{x} = \frac{\beta^{(i_0)}}{\beta^{(j)}} \cdot \frac{\alpha^{(j)}\zeta^{(j)}}{\alpha^{(i_0)}\zeta^{(i_0)}}.$$

Hence,

$$h(\tilde{x}) = 2h(\beta) + 2h(\alpha) \leq 4\Omega + 2h(\theta) + 2\log 2 + 2h(\alpha) = \Omega'.$$

Finally, we observer that

$$h(z) = h(1/\tilde{x}) \leq \Omega'.$$

Together with $h_v\left(\frac{\delta_2}{\lambda}\right) \leq h\left(\frac{\delta_2}{\lambda}\right)$, this implies

$$h_v\left(\frac{\delta_2}{\lambda}\right) \leq \Omega'.$$

Of course, by definition, we have $h_v\left(\frac{\delta_2}{\lambda}\right) \geq 0$, so that $(\tilde{x}, \tilde{y}) \in \Sigma(h)$ as required. $\square$

6.3 Coverings of Σ

From Section 6.2, we now know that all solutions $(\tilde{x}, \tilde{y}) \in \Sigma$ satisfy $\mathbf{m} \in \Sigma(h)$ if $\mathbf{h} = (\Omega')$. In the notation of Section 6.2, we have the following result.

Lemma 6.3.1. *Let* $\mathbf{l}, \mathbf{h} \in \mathbb{R}^{\nu+m}$ *with* $\mathbf{0} \leq \mathbf{l} \leq \mathbf{h}$. *It holds that* $\Sigma(\mathbf{h}) = \Sigma(\mathbf{l}, \mathbf{h}) \cup \Sigma(\mathbf{l})$ *and* $\Sigma(\mathbf{l}, \mathbf{h}) = \cup_{v \in S^*} \Sigma_v(\mathbf{l}, \mathbf{h})$.

Proof. Suppose $(\tilde{x}, \tilde{y}) \in \Sigma(\mathbf{h})$. By definition this means, $(h_v(z)) \leq \mathbf{h}$ and that $h_v(z) > 0$ for at least one coordinate v. Since $\mathbf{0} \leq \mathbf{l} \leq \mathbf{h}$, it follows that either $(h_v(z)) \leq \mathbf{l}$ or $(h_v(z)) \nleq \mathbf{l}$. That is, either all coordinates satisfy $h_v(z) \leq l_v$, or there is at least one coordinate for which $h_v(z) > l_v$. This means that either $(\tilde{x}, \tilde{y}) \in \Sigma(\mathbf{l})$ or $(\tilde{x}, \tilde{y}) \in \Sigma(\mathbf{l}, \mathbf{h})$, and so $\Sigma(\mathbf{h}) \subseteq \Sigma(\mathbf{l}, \mathbf{h}) \cup \Sigma(\mathbf{l})$.

Conversely, suppose $(\tilde{x}, \tilde{y}) \in \Sigma(\mathbf{l}, \mathbf{h}) \cup \Sigma(\mathbf{l})$. It follows that either $(h_v(z)) \leq \mathbf{h}$ and $(h_v(z)) \nleq \mathbf{l}$ or $(h_v(z)) \leq \mathbf{l}$ and $(h_v(z)) \nleq \mathbf{0}$. In either case, this means that $(h_v(z)) \leq \mathbf{h}$ and $(h_v(z)) \nleq \mathbf{0}$. Hence $(\tilde{x}, \tilde{y}) \in \Sigma(\mathbf{h})$ and $\Sigma(\mathbf{h}) \supseteq \Sigma(\mathbf{l}, \mathbf{h}) \cup \Sigma(\mathbf{l})$.

To prove the second equality, let $(\tilde{x}, \tilde{y}) \in \Sigma(\mathbf{l}, \mathbf{h})$. Then there exists $w \in S^*$ with $h_w(z) > l_w$ so that $(\tilde{x}, \tilde{y})$ lies in $\Sigma_w(\mathbf{l}, \mathbf{h})$. Hence $\Sigma(\mathbf{l}, \mathbf{h}) \subseteq \cup_{v \in S^*} \Sigma_v(\mathbf{l}, \mathbf{h})$. Lastly, since each set $\Sigma_v(\mathbf{l}, \mathbf{h})$ is contained in $\Sigma(\mathbf{l}, \mathbf{h})$ it follows that $\Sigma(\mathbf{l}, \mathbf{h}) = \cup_{v \in S^*} \Sigma_v(\mathbf{l}, \mathbf{h})$ as required. $\square$

Let $\mathbf{h}_0 = (\Omega', \ldots, \Omega')$ denote the vector consisting of the initial bound Ω'. By Proposition 6.2.1, every solution of (6.2) is contained in $\mathbf{h}_0$. Therefore, we write $\Sigma = \Sigma(\mathbf{h}_0)$. Consider the pairs $(\mathbf{l}_n, \mathbf{h}_n) \in \mathbb{R}^{\nu+m} \times \mathbb{R}^{\nu+m}$ with $\mathbf{0} \leq \mathbf{l}_n \leq \mathbf{h}_n$ and

$\mathbf{h}_{n+1} = \mathbf{l}_n$ for $n = 0, \ldots, N$. Then we can cover Σ:

$$\Sigma = \Sigma(\mathbf{l}_N) \cup \big(\cup_{n=0}^{N} \cup_{v \in S^*} \Sigma_v(\mathbf{l}_n, \mathbf{h}_n)\big).$$

Indeed this follows directly by applying Lemma 6.3.1 N times. In particular, Lemma 6.3.1 gives

$$\Sigma = \Sigma(\mathbf{h}_0), \quad \Sigma(\mathbf{h}) = \Sigma(\mathbf{l}, \mathbf{h}) \cup \Sigma(\mathbf{l}) \quad \text{and} \quad \Sigma(\mathbf{l}, \mathbf{h}) = \cup_{v \in S^*} \Sigma_v(\mathbf{l}, \mathbf{h}).$$

After choosing a good sequence of lower and upper bounds $\mathbf{l}_n, \mathbf{h}_n$ covering the whole space Σ, we are reduced to computing $\Sigma_v(\mathbf{l}, \mathbf{h})$ for each $v \in S^*$. In the following section, we construct the ellipsoids associated to each $\Sigma_v(\mathbf{l}, \mathbf{h})$, after which we describe the sieve allowing us to compute the solutions of each $\Sigma_v(\mathbf{l}, \mathbf{h})$.

6.4 Construction of the ellipsoids

In Section 6.3, we establish that for a suitable pair of vectors $\mathbf{l}, \mathbf{h}$, solving (6.2) reduces to computing $\Sigma_v(\mathbf{l}, \mathbf{h})$ for each $v \in S^*$. In this section, we construct the ellipsoids associated to each $\Sigma_v(\mathbf{l}, \mathbf{h})$, which will subsequently allow us to compute all solutions of $\Sigma_v(\mathbf{l}, \mathbf{h})$.

We begin with the quadratic form $q_f = A^T D^2 A$ on $\mathbb{Z}^\nu$, where D^2 is a $\nu \times \nu$ diagonal matrix with diagonal entries $\lfloor \frac{\log(p_i)^2}{\log(2)^2} \rfloor$ for $p_i \in S$. Recall that A is the matrix generated in either Section 3.4.1 or Section 3.4.1. As A is invertible, our choice of entries in D guarantees that this quadratic form is positive definite. This will become very important later in the sieve when we will need to apply many instances of the Fincke-Pohst algorithm.

Lemma 6.4.1. *For any solution* $(x, y, n_1, \ldots, n_\nu, a_1, \ldots, a_r)$ *of* (6.2) *with* $\mathbf{n} = (n_1, \ldots, n_\nu)$, *we have*

$$\frac{\log(2)^2}{[K:\mathbb{Q}]} q_f(\mathbf{n}) < \frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l)^2 |u_l - r_l|^2.$$

Proof. Recall from Section 3.4.1 and Section 3.4.2 that

$$A\mathbf{n} = \mathbf{u} - \mathbf{r}.$$

Assume first that $2 \notin S$ so that

$$q_f(\mathbf{n}) = (A\mathbf{n})^{\mathrm{T}} D^2 A\mathbf{n} = (\mathbf{u}-\mathbf{r})^{\mathrm{T}} D^2 (\mathbf{u}-\mathbf{r}) = \sum_{l=1}^{\nu} \left\lfloor \frac{\log(p_l)^2}{\log(2)^2} \right\rfloor |u_l - r_l|^2.$$

Multiplication by $\frac{\log(2)^2}{[K:\mathbb{Q}]}$ then gives

$$\frac{\log(2)^2}{[K:\mathbb{Q}]} q_f(\mathbf{n}) = \frac{\log(2)^2}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \left\lfloor \frac{\log(p_l)^2}{\log(2)^2} \right\rfloor |u_l - r_l|^2 \leq \frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l)^2 |u_l - r_l|^2,$$

where all terms in the summand are positive.

If $2 \in S$, we have

$$q_f(\mathbf{n}) = (A\mathbf{n})^{\mathrm{T}} D^2 A\mathbf{n} = |u_1 - r_1|^2 + \sum_{l=2}^{\nu} \left\lfloor \frac{\log(p_l)^2}{\log(2)^2} \right\rfloor |u_l - r_l|^2.$$

It follows that

$$\begin{aligned} \frac{\log(2)^2}{[K:\mathbb{Q}]} q_f(\mathbf{n}) &\leq \frac{\log(2)^2}{[K:\mathbb{Q}]} \left(|u_1 - r_1|^2 + \sum_{l=2}^{\nu} \frac{\log(p_l)^2}{\log(2)^2} |u_l - r_l|^2 \right) \\ &= \frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l)^2 |u_l - r_l|^2. \end{aligned}$$

□

We now briefly re-examine the decomposition of $h\left(\frac{\delta_2}{\lambda}\right)$ into local heights,

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]} \sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}.$$

In particular, for every finite place v, Lemma 6.4.1 tells us that any bound h_v on

$h_v\left(\frac{\delta_2}{\lambda}\right)$ yields a bound on $\frac{\log(2)^2}{[K:\mathbb{Q}]}q_f(\mathbf{n})$. In the remainder of this section, we build analogous bounds on the exponents $a_1, \ldots, a_r$ of the fundamental units.

Recall $r = 1$ or $r = 2$ for the degree 3 Thue-Mahler equation (6.3) in question. Choose a set I of embeddings $L \to \mathbb{C}$ of cardinality r. For $r = 1$, this is simply

$$R = \left(\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right|\right).$$

Clearly, as long as we choose ι_1 such that $\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right| \neq 0$, this matrix is invertible.

When $r = 2$, we let I be the set of embeddings $L \to \mathbb{C}$ of cardinality 2 such that for any $\alpha \in K$, it holds that $I\alpha^{(i_0)} \cup I\alpha^{(j)} = \mathrm{Gal}(L/\mathbb{Q})\alpha$. Let R be the 2×2 matrix

$$R = \begin{pmatrix} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right| & \log\left|\left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1}\right| \\ \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2}\right| & \log\left|\left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2}\right| \end{pmatrix}.$$

Lemma 6.4.2. *When $r = 2$, the matrix R has an inverse,*

$$R^{-1} = \begin{pmatrix} \overline{r}_{11} & \overline{r}_{12} \\ \overline{r}_{21} & \overline{r}_{22} \end{pmatrix}.$$

Proof. Suppose that $\mathbf{m} \in \mathbb{Z}^r$ satisfies $R\mathbf{m} = \mathbf{0}$. Then for each $\iota \in I$ it holds that

$$\sum_{i=1}^{r} m_{\varepsilon_i} \log\left|\left(\frac{\varepsilon_i^{(j)}}{\varepsilon_i^{(i_0)}}\right)^{\iota_1}\right| = 0,$$

and hence

$$\prod_{i=1}^{r}\left|\left(\frac{\varepsilon_i^{(j)}}{\varepsilon_i^{(i_0)}}\right)^{\iota_1}\right|^{m_{\varepsilon_i}} = 1.$$

This together with $I(i) \cup I(j) = Gal(L/\mathbb{Q})$ implies that all conjugates of $\alpha = \prod_{i=1}^{r} \varepsilon_i^{m_{\varepsilon_i}}$ have the same absolute value. Since all ε_i are units of $\mathcal{O}_K$, it follows that $|\alpha|^{[L:\mathbb{Q}]} = N(\alpha) = 1$ and hence α is a root of unity in K. On using that the elements ε_i are multiplicatively independent, we obtain that $\mathbf{m} = \mathbf{0}$. Then linear algebra gives $R^{-1} \in \mathbb{R}^{r\times r}$, completing the proof. $\square$

For the remainder of this chapter, we specialize to the real case, $r = 2$. The setup for $r = 1$ follows closely the work described here, yet poses other difficulties when defining the corresponding sieves. This case is treated in the on-going results of [44].

Now, for any solution $(x, y, n_1, \ldots, n_\nu, a_1, a_2)$ of (6.2), set

$$\varepsilon = \begin{pmatrix} a_1 & a_2 \end{pmatrix}^{\mathrm{T}}.$$

We have

$$R\varepsilon = \begin{pmatrix} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1\ a_2}\right| \\ \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2\ a_2} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2\ a_2}\right| \end{pmatrix}.$$

Since R is invertible with $R^{-1} = (\overline{r}_{nm})$, we find

$$\varepsilon = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} \overline{r}_{11}\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1\ a_2}\right| + \overline{r}_{12}\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2\ a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2\ a_2}\right| \\ \overline{r}_{21}\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1\ a_2}\right| + \overline{r}_{22}\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2\ a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2\ a_2}\right| \end{pmatrix},$$

giving

$$a_l = \overline{r}_{l1}\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1\ a_2}\right| + \overline{r}_{l2}\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2\ a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2\ a_2}\right|$$

for $l = 1, 2$.

To estimate $|a_l|$, we begin to estimate the sum on the right hand side. For this, we consider

$$\frac{\delta_2}{\lambda} = \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{a_1} \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{a_2} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{n_i}.$$

For any embedding $\iota : L \to \mathbb{C}$, we have

$$\left(\frac{\delta_2}{\lambda}\right)^{\iota} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\, n_i} = \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota\, a_1} \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota\, a_2}.$$

Taking absolute values, we obtain

$$\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\, n_i}\right| = \left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota\, a_1} \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota\, a_2}\right|,$$

so that

$$\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota\, a_1} \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota\, a_2}\right| = \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota}\right| - \log\left|\prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{\iota\, n_i}\right|.$$

Hence, for $l = 1, 2$,

$$\begin{aligned}
a_l &= \overline{r}_{l1} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\, a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1\, a_2}\right| + \overline{r}_{l2} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2\, a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2\, a_2}\right| \\
&= \overline{r}_{l1}\left(\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| - \log\left|\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{\iota_1\, n_i}\right|\right) + \\
&\quad + \overline{r}_{l2}\left(\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| - \log\left|\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{\iota_2\, n_i}\right|\right) \\
&= \overline{r}_{l1} \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| + \overline{r}_{l2} \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| - n_1\beta_{\gamma l1} - \cdots - n_\nu \beta_{\gamma l\nu},
\end{aligned}$$

where

$$\beta_{\gamma lk} = \left(\overline{r}_{l1} \log\left|\left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}}\right)^{\iota_1}\right| + \overline{r}_{l2} \log\left|\left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}}\right)^{\iota_2}\right|\right)$$

for $k = 1, \ldots, \nu$. Recall that $\mathbf{n} = A^{-1}(\mathbf{u} - \mathbf{r})$ and suppose $A^{-1} = (\overline{a}_{nm})$. We have

$$\mathbf{n} = A^{-1}(\mathbf{u} - \mathbf{r}) = \begin{pmatrix} \sum_{k=1}^{\nu} \overline{a}_{1k}(u_k - r_k) \\ \vdots \\ \sum_{k=1}^{\nu} \overline{a}_{\nu k}(u_k - r_k) \end{pmatrix}.$$

Now,

$$\begin{aligned} a_l &= \overline{r}_{l1} \log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_2} \right| - n_1 \beta_{\gamma l1} - \cdots - n_\nu \beta_{\gamma l\nu} \\ &= \overline{r}_{l1} \log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_2} \right| - \sum_{k=1}^{\nu} (u_k - r_k) \alpha_{\gamma lk}, \end{aligned}$$

where

$$\alpha_{\gamma lk} = \overline{a}_{1k} \beta_{\gamma l1} + \cdots + \overline{a}_{\nu k} \beta_{\gamma l\nu}$$

and

$$\beta_{\gamma lk} = \left(\overline{r}_{l1} \log \left| \left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}} \right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}} \right)^{\iota_2} \right| \right)$$

for $k = 1, \ldots, \nu$.

Since $\frac{\delta_2}{\lambda}$ is a quotient of elements which are conjugate to one another, by taking the norm on L of $\frac{\delta_2}{\lambda}$, we obtain $N\left(\frac{\delta_2}{\lambda}\right) = 1$. On the other hand, by definition, we have

$$1 = N\left(\frac{\delta_2}{\lambda}\right) = \prod_{\sigma : L \to \mathbb{C}} \sigma\left(\frac{\delta_2}{\lambda}\right).$$

Taking absolute values and logarithms,

$$0 = \sum_{\sigma : L \to \mathbb{C}} \log \left| \sigma\left(\frac{\delta_2}{\lambda}\right) \right|$$

so that

$$-\log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota} \right| = -\log \left| \iota\left(\frac{\delta_2}{\lambda}\right) \right| = \sum_{\substack{\sigma : L \to \mathbb{C} \\ \sigma \neq \iota}} \log \left| \sigma\left(\frac{\delta_2}{\lambda}\right) \right|.$$

Therefore,

$$\begin{aligned}|a_l| &= \left|\overline{r}_{l1}\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| + \overline{r}_{l2}\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| - \sum_{k=1}^{\nu}(u_k - r_k)\alpha_{\gamma lk}\right| \\ &\leq |\overline{r}_{l1}|\left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right| + |\overline{r}_{l2}|\left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right| + \sum_{k=1}^{\nu}|u_k - r_k||\alpha_{\gamma lk}|.\end{aligned}$$

Suppose $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| \geq 0$ and $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| \geq 0$. Then,

$$\begin{aligned}|a_l| &\leq |\overline{r}_{l1}|\left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right| + |\overline{r}_{l2}|\left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right| + \sum_{k=1}^{\nu}|u_k - r_k||\alpha_{\gamma lk}| \\ &= |\overline{r}_{l1}|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| + |\overline{r}_{l2}|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| + \sum_{k=1}^{\nu}|u_k - r_k||\alpha_{\gamma lk}| \\ &\leq \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}|\log\max\left\{\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|, 1\right\} + \\ &\qquad + \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}\log\max\left\{\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|, 1\right\} + \sum_{k=1}^{\nu}|u_k - r_k||\alpha_{\gamma lk}| \\ &\leq \sum_{w:L\to\mathbb{C}}\max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}|\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu}|u_k - r_k||\alpha_{\gamma lk}|.\end{aligned}$$

Alternatively, suppose that both $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| < 0$ and $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| < 0$. In this case,

$$
\begin{aligned}
|a_l| &\le |\overline{r}_{l1}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right| + |\overline{r}_{l2}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma l k}| \\
&= |\overline{r}_{l1}| \sum_{\substack{\sigma : L \to \mathbb{C} \\ \sigma \neq \iota_1}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right| + |\overline{r}_{l2}| \left(-\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right) + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma l k}| \\
&\le \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} \sum_{\substack{\sigma : L \to \mathbb{C} \\ \sigma \neq \iota_1}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right| + \\
&\qquad + \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} \left(-\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right) + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma l k}| \\
&\le \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} \sum_{\substack{w : L \to \mathbb{C} \\ \sigma \neq \iota_1, \iota_2}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma l k}| \\
&\le \sum_{w:L\to\mathbb{C}} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} |\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma l k}|.
\end{aligned}
$$

Lastly, if, without loss of generality, we have $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| < 0$ and $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| \geq 0$, then

$$
\begin{aligned}
|a_l| &\le |\overline{r}_{l1}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right| + |\overline{r}_{l2}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma l k}| \\
&= |\overline{r}_{l1}| \sum_{\substack{\sigma : L \to \mathbb{C} \\ \sigma \neq \iota_1}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right| + |\overline{r}_{l2}| \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma l k}| \\
&\le \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} \sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + |\overline{r}_{l2}| \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma l k}| \\
&= \sum_{w:L\to\mathbb{C}} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} |\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + |\overline{r}_{l1}| \log\max\left\{\left|\iota_1\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&\qquad + |\overline{r}_{l2}| \log\max\left\{\left|\iota_2\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma l k}|.
\end{aligned}
$$

In all three cases, it follows that

$$|a_l| \leq \sum_{w:L\to\mathbb{C}} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} |\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + |\overline{r}_{l1}| \log\max\left\{\left|\iota_1\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\ + |\overline{r}_{l2}| \log\max\left\{\left|\iota_2\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}|$$

where

$$\alpha_{\gamma lk} = \overline{a}_{1k}\beta_{\gamma l1} + \cdots + \overline{a}_{\nu k}\beta_{\gamma l\nu}$$

and

$$\beta_{\gamma lk} = \left(\overline{r}_{l1} \log\left|\left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}}\right)^{\iota_1}\right| + \overline{r}_{l2} \log\left|\left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}}\right)^{\iota_2}\right|\right)$$

for $k = 1, \ldots, \nu$.

Hence for $l = 1, 2$, we write

$$|a_l| \leq \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon l\sigma} \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} w_{\gamma lk} \log(p_k)|u_k - r_k|, \tag{6.8}$$

where

$$w_{\varepsilon l\sigma} = \begin{cases} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}[L:\mathbb{Q}] & \text{for } \sigma \notin I \\ \left(\max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} + |\overline{r}_{li}|\right)[L:\mathbb{Q}] & \text{for } \sigma = \iota_i \in I \end{cases} \tag{6.9}$$

and

$$w_{\gamma lk} = |\alpha_{\gamma lk}| \frac{[K:\mathbb{Q}]}{\log(p_k)}. \tag{6.10}$$

To summarize, we have proven the following lemma.

Lemma 6.4.3. *For any solution* $(x, y, a_1, \ldots, a_r, n_1, \ldots, n_\nu)$ *of* (6.2)*, for* $l = 1, 2$

$$|a_l| \leq \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon l\sigma} \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} w_{\gamma lk} \log(p_k)|u_k - r_k|.$$

6.4.1 The Archimedean ellipsoid: the real case

Let $\tau : L \to \mathbb{R} \subset \mathbb{C}$ be an embedding and let $l_\tau \geq c_\tau$ and $c > 0$ be given real numbers for $c_\tau = \log^+(2|\tau(\delta_2)|) = \log\max\{2|\tau(\delta_2)|, 1\}$. We define

$$\alpha_0 = [c \log|\tau(\delta_1)|] \quad \text{and} \quad \alpha_{\varepsilon 1} = \left[c \log \left| \tau\left(\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}} \right) \right| \right], \ \alpha_{\varepsilon 2} = \left[c \log \left| \tau\left(\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}} \right) \right| \right]. \tag{6.11}$$

For $i = 1, \ldots, \nu$, define

$$\alpha_{\gamma i} = \left[c \log \left| \tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}} \right) \right| \right]. \tag{6.12}$$

Here, $[\,\cdot\,]$ denotes the nearest integer function.

Let

$$w_\sigma = (w_{\varepsilon 1\sigma} + w_{\varepsilon 2\sigma}), \qquad w_k = (w_{\gamma 1k} + w_{\gamma 2k}) + \frac{[K:\mathbb{Q}]}{\log(p_k)} \sum_{i=1}^{\nu} |\overline{a}_{ik}| \tag{6.13}$$

for $\sigma : L \to \mathbb{C}$ and $k = 1, \ldots, \nu$. Here $w_{\varepsilon 1\sigma}, w_{\varepsilon 3\sigma}$ and $w_{\gamma 1k}, w_{\gamma 3k}$ are the coefficients (6.9) and (6.10), respectively. Let $\kappa_\tau = 3/2$ and

$$h_\tau\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[L:K]} \log\max\left\{ \left| \tau\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\},$$

the local height at τ in the decomposition of $h\left(\frac{\delta_2}{\lambda}\right)$.

Lemma 6.4.4. *Suppose* $(x, y, n_1, \ldots, n_\nu, a_1, \ldots, a_r)$ *is a solution of* (6.2). *If* $h_\tau\left(\frac{\delta_2}{\lambda}\right) > c_\tau$, *then*

$$\begin{aligned} &\left| \alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i} \right| \\ &\leq \frac{1}{2} \left(\frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} w_l \log(p_l) |u_l - r_l| + \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma: L \to \mathbb{C}} w_\sigma \log\max\left\{ \left| \sigma\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} \right) + \\ &\qquad + \left(\frac{1}{2} + c\kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)} \right). \end{aligned}$$

Proof. Let

$$\begin{aligned}\alpha &= \alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i} \\ &= [c \log |\tau(\delta_1)|] + \sum_{i=1}^{r} a_i \left[c \log \left| \tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right) \right| \right] + \sum_{i=1}^{\nu} n_i \left[c \log \left| \tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right) \right| \right]\end{aligned}$$

and

$$\Lambda_\tau = \log \left| \tau\left(\delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right) \right| = \log\left(\tau\left(\delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right)\right)$$

where the above equality follows from

$$\tau\left(\delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right) > 0.$$

Indeed, by assumption,

$$h_\tau\left(\frac{\delta_2}{\lambda}\right) > c_\tau = \log \max\{2|\tau(\delta_2)|, 1\},$$

so that

$$\begin{aligned}\exp\left(h_\tau\left(\frac{\delta_2}{\lambda}\right)\right) &> \exp(c_\tau) \\ \exp\left(\log \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right) &> \exp\left(\log \max\{2|\tau(\delta_2)|, 1\}\right) \\ \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} &> \max\{2|\tau(\delta_2)|, 1\}.\end{aligned}$$

From this last inequality, we must have that

$$\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = \left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|.$$

In this case,

$$\max\{2|\tau(\delta_2)|, 1\} < \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = \left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|.$$

It follows that

$$2|\tau(\delta_2)| \leq \max\{2|\tau(\delta_2)|, 1\} < \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = \left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|$$

and therefore

$$2|\tau(\delta_2)| < \left|\tau\left(\frac{\delta_2}{\lambda}\right)\right| = \frac{|\tau(\delta_2)|}{|\tau(\lambda)|} \implies |\tau(\lambda)| < \frac{1}{2}.$$

Recall that $\delta_1\tilde{y} - \delta_2\tilde{x} = 1$. This is equation (6.6) defined earlier. In particular, observe that $\lambda = \delta_2\tilde{x}$, so that applying τ, we obtain

$$\tau(\lambda) = \tau(\delta_2\tilde{x}) = \tau(\delta_1\tilde{y}) - 1.$$

Thus

$$|\tau(\lambda)| < \frac{1}{2} \implies \tau(\delta_1\tilde{y}) = \tau(\lambda) + 1 > 0.$$

This proves that

$$\tau(\delta_1\tilde{y}) = \tau\left(\delta_1 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right) > 0.$$

Having established this, we write,

$$\Lambda_\tau = \log\left|\tau\left(\delta_1 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right)\right| = \log\left(\tau\left(\delta_1 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right)\right)$$

or equivalently,

$$\Lambda_\tau = \log\left(\tau\left(\delta_1\right)\right) + \sum_{i=1}^{r} a_i \log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right) + \sum_{i=1}^{\nu} n_i \log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right).$$

By the triangle inequality,

$$|\alpha| \leq |\alpha - c\Lambda_\tau| + c|\Lambda_\tau|,$$

where

$$\begin{aligned}
|\alpha - c\Lambda_\tau| = &\left| [c\log(\tau(\delta_1))] + \sum_{i=1}^{r} a_i \left[c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right] + \sum_{i=1}^{\nu} n_i \left[c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right] + \right. \\
&\left. -c\log\left(\tau\left(\delta_1 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right)\right)\right| \\
&\leq |[c\log(\tau(\delta_1))] - c\log(\tau(\delta_1))| + \sum_{i=1}^{r} |a_i| \left| \left[c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right] - c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right| \\
&+ \sum_{i=1}^{\nu} |n_i| \left| \left[c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right] - c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right|.
\end{aligned}$$

Since $[\,\cdot\,]$ denotes the nearest integer function, it is clear that $|[\,c\,] - c| \leq 1/2$ for any integer c,

$$\begin{aligned}
|\alpha - c\Lambda_\tau| &\leq \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{r}|a_i| + \frac{1}{2}\sum_{i=1}^{\nu}|n_i| \\
&\leq \frac{1}{2}\left(1 + \sum_{i=1}^{r}|a_i| + |u_1 - r_1|\sum_{i=1}^{\nu}|\overline{a}_{i1}| + \cdots + |u_\nu - r_\nu|\sum_{i=1}^{\nu}|\overline{a}_{i\nu}|\right).
\end{aligned}$$

By Lemma 6.4.3,

$$|a_l| \leq \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon l\sigma}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} w_{\gamma lk}\log(p_k)|u_k - r_k|$$

for $l=1,2$. Applying this result to $|\alpha - c\Lambda_\tau|$, we obtain

$$
\begin{aligned}
|\alpha - c\Lambda_\tau| \leq \frac{1}{2} + \frac{1}{2}|u_1 - r_1| \sum_{i=1}^{\nu} |\overline{a}_{i1}| + \cdots + \frac{1}{2}|u_\nu - r_\nu| \sum_{i=1}^{\nu} |\overline{a}_{i\nu}| + \\
+ \frac{1}{2}\left(\frac{1}{[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon_1\sigma} \log\max\left\{ \left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} w_{\gamma_1 k} \log(p_k)|u_k - r_k| \right) + \\
+ \frac{1}{2}\left(\frac{1}{[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon_2\sigma} \log\max\left\{ \left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} w_{\gamma_2 k} \log(p_k)|u_k - r_k| \right) \\
= \frac{1}{2} + \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} \frac{(w_{\varepsilon_1\sigma} + w_{\varepsilon_2\sigma})}{2} \log\max\left\{ \left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
+ |u_1 - r_1| \left(\frac{(w_{\gamma_1 1} + w_{\gamma_2 1})}{2[K:\mathbb{Q}]} \log(p_1) + \frac{1}{2}\sum_{i=1}^{\nu} |\overline{a}_{i1}| \right) + \cdots \\
+ |u_\nu - r_\nu| \left(\frac{(w_{\gamma_1 \nu} + w_{\gamma_2 \nu})}{2[K:\mathbb{Q}]} \log(p_\nu) + \frac{1}{2}\sum_{i=1}^{\nu} |\overline{a}_{i\nu}| \right).
\end{aligned}
$$

Altogether, we have

$$
\begin{aligned}
|\alpha - c\Lambda_\tau| \leq \frac{1}{2} + \frac{1}{2[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} (w_{\varepsilon_1\sigma} + w_{\varepsilon_2\sigma}) \log\max\left\{ \left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
+ \frac{1}{2[K:\mathbb{Q}]} \sum_{k=1}^{\nu} \log(p_k)|u_k - r_k| \left((w_{\gamma_1 k} + w_{\gamma_2 k}) + \frac{[K:\mathbb{Q}]}{\log(p_k)} \sum_{i=1}^{\nu} |\overline{a}_{ik}| \right).
\end{aligned}
$$

Finally, using the notation of (6.13), this inequality reduces to

$$
|\alpha - c\Lambda_\tau| \leq \frac{1}{2} + \frac{1}{2[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} w_\sigma \log\max\left\{ \left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{2[K:\mathbb{Q}]} \sum_{l=1}^{\nu} w_l \log(p_l)|u_l - r_l|.
$$

Now the following upper bound for $|\Lambda_\tau|$ implies the statement. On using power series definition of exponential function, we obtain

$$
\Lambda_\tau(1 + \sum_{n\geq 2}(\Lambda_\tau)^{n-1}/n!) = \Lambda_\tau + \sum_{n\geq 2}(\Lambda_\tau)^n/n! = e^{\Lambda_\tau} - 1 = \tau(\lambda).
$$

If $\Lambda_\tau \geq 0$ then $1 + \sum_{n\geq 2}(\Lambda_\tau)^{n-1}/n! > 1$ which implies that $|\Lambda_\tau| \leq |\tau(\lambda)|$.

Suppose now that $\Lambda_\tau < 0$. Our assumption $h_\tau(z) \geq \log^+(2|\lambda_0|)$ means that $|\tau(\lambda)| \leq 1/2$ and thus $|\Lambda_\tau| = -\log(\tau(\lambda)+1) \leq -\log(1/2) = \log 2$. Therefore, the absolute value of $\sum_{n\geq 2}(\Lambda_\tau)^{n-1}/n!$ is at most

$$\sum_{n\geq 2}|\Lambda_\tau|^{n-1}/n! = \sum_{n\geq 1}|\Lambda_\tau|^n/(n+1)! \leq \tfrac{1}{2}\sum_{n\geq 1}|\Lambda_\tau|^n/n! \leq \tfrac{1}{2}e^{\log 2} - 1/2 = 1/2.$$

More precisely, for any even $N \geq 2$, we obtain

$$|\sum_{n\geq 2}(\Lambda_\tau)^{n-1}/n!| = |\sum_{n\geq 1}(\Lambda_\tau)^n/(n+1)!| \leq |\sum_{N\geq n\geq 1}(\Lambda_\tau)^n/(n+1)!| + \tfrac{1}{N+2}|\sum_{n>N}(\Lambda_\tau)^n/n!|$$

$$\leq |\sum_{N\geq n\geq 1}(\Lambda_\tau)^n/(n+1)!| + \tfrac{1}{N+2}e^{|\Lambda_\tau|} \leq |\sum_{N\geq n\geq 1}(\Lambda_\tau)^n/(n+1)!| + \tfrac{2}{N+2} := k_N.$$

We now give an upper bound for k_N. Since $\Lambda_\tau < 0$, we obtain

$$\sum_{n\geq 2}(\Lambda_\tau)^{n-1}/n! = \sum_{N\geq n\geq 1}(\Lambda_\tau)^n/(n+1)! = \sum_{N\geq n\geq 2,\, 2|n}\tfrac{|\Lambda_\tau|^n}{(n+1)!} - \tfrac{|\Lambda_\tau|^{n-1}}{n!}$$

$$= \sum_{N\geq n\geq 2,\, 2|n}\tfrac{|\Lambda_\tau|^{n-1}}{n!}(\tfrac{|\Lambda_\tau|}{n+1} - 1) = \tfrac{|\Lambda_\tau|}{2}(\tfrac{|\Lambda_\tau|}{3} - 1) + \sum_{N\geq n\geq 4,\, 2|n}\tfrac{|\Lambda_\tau|^{n-1}}{n!}(\tfrac{|\Lambda_\tau|}{n+1} - 1)$$

$$\geq \tfrac{\log 2}{2}(\tfrac{\log 2}{4} - 1) + \sum_{N\geq n\geq 4,\, 2|n}\tfrac{(\log 2)^{n-1}}{n!}(\tfrac{3/4(\log 2)}{n+1} - 1) := -k_N.$$

The last inequality follows by distinguishing two cases whether $|\Lambda_\tau| \leq 3/4 \cdot \log 2$ or not; note that $\ln(2)/2 \cdot (\ln(2)/4 - 1)/(-\ln(2)\cdot 3/8) \geq 1$. Now, on using that $-k_N$ is negative, it follows that $|1+\sum_{n\geq 2}(\Lambda_\tau)^{n-1}/n!| \geq 1 - |\sum_{n\geq 2}(\Lambda_\tau)^{n-1}/n!| \geq 1 - k_N$ and thus

$$|\Lambda_\tau| \leq \kappa_\tau|\tau(x)|, \quad \kappa_\tau = \tfrac{1}{1-k_N}|\tau(\lambda_0)|, \quad c_\tau = \log^+(2|\lambda_0|).$$

The constant κ_τ depends on N which can be taken arbitrarily as long as $N \geq 2$ is even. Further, the value k_N can be slightly improved when one finds the maximum of the functions $x^{n-1}(\frac{x}{n+1} - 1)$ on the interval $[0, \log 2]$ for each even $n \geq 2$. This is our reason for taking $\kappa_\tau = \frac{3}{2}$. Currently this is not the optimal choice of κ_τ, but it suffices for our present case.

Finally, we now have

$$\left|\alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i}\right|$$
$$\leq \frac{1}{2}\left(\frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l \log(p_l)|u_l - r_l|\right) +$$
$$+ \left(\frac{1}{2} + c\kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)}\right).$$

□

To summarize the results of this section, let $\mathbf{m} = (n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{r+\nu}$ be any solution of (6.2) with corresponding vector $\mathbf{n} = (n_1, \ldots, n_\nu)$. Take $\mathbf{l}, \mathbf{h} \in \mathbb{R}^{\nu+m}$ such that $\mathbf{0} \leq \mathbf{l} \leq \mathbf{h}$ and suppose $h_v(z) \leq h_v$ for all $v \in S^*$. By Lemma 6.4.1, we deduce

$$\log(2)^2 q_f(\mathbf{n}) \leq \sum_{k=1}^{\nu} \log(p_k)^2 |u_k - r_k|^2 \leq \sum_{k=1}^{\nu} h_k^2 =: b. \tag{6.14}$$

For $l = 1, 2$, Lemma 6.4.3 gives us

$$|a_l|^2 \leq \left(\frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} w_{\gamma lk}\log(p_k)|u_k - r_k| + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon l\sigma}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right)^2 \tag{6.15}$$

$$\leq \left(\frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} w_{\gamma lk} h_k + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon l\sigma} h_\sigma\right)^2 =: b_{\varepsilon_l}. \tag{6.16}$$

Finally, suppose in addition that

$$h_\tau\left(\frac{\delta_2}{\lambda}\right) \geq l_\tau > c_\tau.$$

Then by Lemma 6.4.4, we obtain

$$\begin{aligned}
&\left|\alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i}\right| \\
&\leq \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l \log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right) + \\
&\qquad + \left(\frac{1}{2} + c\kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)}\right) \\
&\leq \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l h_l + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma h_\sigma\right) + \frac{1}{2} + c\kappa_\tau e^{-l_\tau},
\end{aligned}$$

and we set

$$b_{\varepsilon_l^*} := \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l h_l + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma h_\sigma\right) + \frac{1}{2} + c\kappa_\tau e^{-l_\tau}. \tag{6.17}$$

It is of particular importance to note that the assumptions $h_\tau(z) \geq l_\tau$ and $h_v(z) \leq h_v$ for all $v \in S^*$ are not arbitrary. Indeed, for the vectors $\mathbf{l}, \mathbf{h}$, these conditions imply precisely that $(\tilde{x}, \tilde{y}) \in \Sigma_\tau(\mathbf{l}, \mathbf{h})$, where $(\tilde{x}, \tilde{y})$ are solutions to (6.2) corresponding to $\mathbf{m}$.

We are finally in position to define the ellipsoid corresponding to $\Sigma_\tau(\mathbf{l}, \mathbf{h})$. Fix any $\varepsilon_l^* \in \{\varepsilon_1, \dots, \varepsilon_r\}$. For each ε_l in $\{\varepsilon_1, \dots, \varepsilon_r\}$ such that $\varepsilon_l \neq \varepsilon_l^*$, we associate the bound b_{ε_l}. For ε_l, we associate the value $b_{\varepsilon_l^*}$.

Let

$$\mathbf{x} = (x_1, \dots, x_\nu, x_{\varepsilon_1}, \dots, x_{\varepsilon_r}) \in \mathbb{R}^{\nu+r}.$$

Then we define the ellipsoid $\mathcal{E}_\tau \subseteq \mathbb{R}^{r+\nu}$ by

$$\mathcal{E}_\tau = \{q_\tau(\mathbf{x}) \leq (1+r)(bb_{\varepsilon_1}\cdots b_{\varepsilon_r});\ \mathbf{x} \in \mathbb{R}^{r+\nu}\} \tag{6.18}$$

where

$$q_\tau(\mathbf{x}) = (b_{\varepsilon_1}\cdots b_{\varepsilon_r})\left(q_f(x_1, \dots, x_\nu) + \sum_{i=1}^{r} \frac{b}{b_{\varepsilon_i}} x_{\varepsilon_i}^2\right)$$

and

$$q_f(\mathbf{y}) = (A\mathbf{y})^{\mathrm{T}} D^2 A\mathbf{y}.$$

We associate to this ellipsoid a matrix. More precisely, we let $M = M_\tau$ be the matrix defining the ellipsoid $\mathcal{E}_\tau$. Explicitly, this is the matrix

$$M = \sqrt{b_{\varepsilon_1} \cdots b_{\varepsilon_r}} \begin{pmatrix} DA & 0 & \dots & 0 & 0 \\ 0 & \sqrt{\frac{b}{b_{\varepsilon 1}}} & \dots & 0 & 0 \\ 0 & 0 & \sqrt{\frac{b}{b_{\varepsilon 2}}} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \sqrt{\frac{b}{b_{\varepsilon^*}}} \end{pmatrix}.$$

Note that we never need to compute M, but rather $M^T M$ so that we only ever work with integral matrices. In this case,

$$\begin{aligned} M^T M = b_{\varepsilon_1} \cdots b_{\varepsilon_r} & \begin{pmatrix} A^T D^2 A & 0 & \dots & 0 & 0 \\ 0 & \frac{b}{b_{\varepsilon 1}} & \dots & 0 & 0 \\ 0 & 0 & \frac{b}{b_{\varepsilon 2}} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \frac{b}{b_{\varepsilon^*}} \end{pmatrix} \\ = & \begin{pmatrix} (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) A^T D^2 A & 0 & \dots & 0 & 0 \\ 0 & b b_{\varepsilon_2} \cdots b_{\varepsilon_r} & \dots & 0 & 0 \\ 0 & 0 & b b_{\varepsilon_1} b_{\varepsilon_3} \cdots b_{\varepsilon_r} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-1}} \end{pmatrix}. \end{aligned}$$

6.4.2 The non-Archimedean ellipsoid

We now restrict our attention to those $p_v \in \{p_1, \dots, p_\nu\}$ and define the corresponding ellipsoid. As before, let $\mathbf{m} = (n_1, \dots, n_\nu, a_1, \dots, a_r) \in \mathbb{R}^{r+\nu}$ be any solution of (6.2) with corresponding vector $\mathbf{n} = (n_1, \dots, n_\nu)$. Take $\mathbf{l}, \mathbf{h} \in \mathbb{R}^{\nu+m}$

such that $\mathbf{0} \le \mathbf{l} \le \mathbf{h}$ and suppose $h_v(z) \le h_v$ for all $v \in S^*$.

Now, Lemma 6.4.1 and Lemma 6.4.3 still hold here. In particular, we let b, b_{ε_l} be defined as in (6.14) and (6.15), respectively, where $l = 1, \dots, r$. We do not distinguish any ε_l^*. Instead, we will see later that the condition $h_v(z) \ge l_v$ corresponding to the set $\Sigma_v(\mathbf{l}, \mathbf{h})$ will be used elsewhere.

We define the ellipsoid $\mathcal{E}_v \subseteq \mathbb{R}^{\nu+r}$ by

$$\mathcal{E}_v = \{q_l(\mathbf{x}) \le (1+r)(bb_{\varepsilon_1} \cdots b_{\varepsilon_r});\ \mathbf{x} \in \mathbb{R}^{r+\nu}\}, \tag{6.19}$$

where

$$q_v(\mathbf{x}) = (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) \left(q_f(x_1, \dots, x_\nu) + \sum_{i=1}^{r} \frac{b}{b_{\varepsilon_i}} x_{\varepsilon_i}^2 \right)$$

and

$$q_f(\mathbf{y}) = (A\mathbf{y})^{\mathrm{T}} D^2 A\mathbf{y}.$$

Similar to the Archimedean case, we let $M = M_v$ be the matrix defining the ellipsoid $\mathcal{E}_v$. Explicitly, this is the matrix

$$M = \sqrt{b_{\varepsilon_1} \cdots b_{\varepsilon_r}} \begin{pmatrix} DA & 0 & \dots & 0 & 0 \\ 0 & \sqrt{\frac{b}{b_{\varepsilon 1}}} & \dots & 0 & 0 \\ 0 & 0 & \sqrt{\frac{b}{b_{\varepsilon 2}}} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \sqrt{\frac{b}{b_{\varepsilon}}} \end{pmatrix}.$$

As before, we never need to compute M, but rather $M^T M$ so that we only ever work with integral matrices. In this case,

$$M^T M = b_{\varepsilon_1} \cdots b_{\varepsilon_r} \begin{pmatrix} A^T D^2 A & 0 & \dots & 0 & 0 \\ 0 & \frac{b}{b_{\varepsilon 1}} & \dots & 0 & 0 \\ 0 & 0 & \frac{b}{b_{\varepsilon 2}} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \frac{b}{b_\varepsilon} \end{pmatrix}$$

$$= \begin{pmatrix} (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) A^T D^2 A & 0 & \dots & 0 & 0 \\ 0 & b b_{\varepsilon_2} \cdots b_{\varepsilon_r} & \dots & 0 & 0 \\ 0 & 0 & b b_{\varepsilon_1} b_{\varepsilon_3} \cdots b_{\varepsilon_r} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-1}} \end{pmatrix}.$$

6.5 The Archimedean sieve: the real case

Let $\tau : L \to \mathbb{C}$ be an embedding. We take $\mathbf{l}, \mathbf{h} \in \mathbb{R}^{m+\nu}$ with $\mathbf{0} \leq \mathbf{l} \leq \mathbf{h}$ and $l_\tau \geq \log 2$. Let c be a constant the size of e^{l_τ} and let $\alpha_0, \alpha_{\varepsilon 1}, \dots, \alpha_{\varepsilon r}, \alpha_{\gamma 1}, \dots, \alpha_{\gamma \nu}$ be defined as in (6.11) and (6.12).

Define the $(\nu + r) \times (\nu + r)$-dimensional matrix A_τ as

$$A_\tau = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 1 & 0 \\ \alpha_{\gamma 1} & \dots & \alpha_{\gamma \nu} & \alpha_{\varepsilon 1} & \dots & \alpha_{\varepsilon r} \end{pmatrix}$$

and consider the lattice defined by its columns. Let $\mathbf{w} = (0, \dots, 0, \alpha_0)$ be a vector of length $(\nu + r)$. We now consider the translated lattice Γ_τ defined by $A_\tau \mathbf{x} + \mathbf{w}$, where $\mathbf{x}$ is an arbitrary coordinate vector.

Let $\mathcal{E}_\tau = \mathcal{E}_\tau(h, l_\tau)$ be the ellipsoid constructed in (6.18). Let $\mathbf{m} = (n_1, \dots, n_\nu, a_1, \dots, a_r) \in \mathbb{R}^{r+\nu}$

be any solution of (6.2). We say that $\mathbf{m}$ is determined by some $\mathbf{y} \in \Gamma_\tau$ if

$$\mathbf{y} = (y_1, \ldots, y_{r+\nu}) = \left(n_1, \ldots, n_\nu, a_1, \ldots, a_{r-1}, \alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i} \right)$$

where the missing element a_l corresponds to ε_l^*.

Lemma 6.5.1. *Let* $\mathbf{m} = (n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{r+\nu}$ *be any solution of* (6.2) *which lies in* $\Sigma_\tau(l, h)$. *Then* $\mathbf{m}$ *is determined by some* $\mathbf{y} \in \Gamma_\tau \cap \mathcal{E}_\tau$.

Proof. Let

$$\mathbf{y} = \left(n_1, \ldots, n_\nu, a_1, \ldots, a_{r-1}, \alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i} \right).$$

Then $\mathbf{y} \in \Gamma_\tau$ and (6.17) implies that $y_{\varepsilon_l^*}^2 \leq b_{\varepsilon_l^*}$. Further (6.14) gives that $q_f((y_1, \ldots, y_\nu)) \leq b$, and (6.15) provides that $y_{\varepsilon_l}^2 \leq b_{\varepsilon_l}$ for $l = 1, \ldots, r$ with $\varepsilon_l \neq \varepsilon_l^*$. It follows that

$$q_\tau(\mathbf{y}) = (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) \left(q_f(y_1, \ldots, y_\nu) + \sum_{i=1}^{r} \frac{b}{b_{\varepsilon_i}} y_{\varepsilon_i}^2 \right) \leq (1 + r)(b b_{\varepsilon_1} \cdots b_{\varepsilon_r}).$$

This proves that $\mathbf{y} \in \mathcal{E}_\tau$ and hence the statement follows. $\square$

We now explicitly determine $\Gamma_\tau \cap \mathcal{E}_\tau$. Suppose that $\mathbf{y} \in \Gamma_\tau \cap \mathcal{E}_\tau$. Let $M = M_\tau$ be the matrix defining the ellipsoid $\mathcal{E}_\tau$. Since $\mathbf{y} \in \Gamma_\tau \cap \mathcal{E}_\tau$, there exists $\mathbf{x} \in \mathbb{R}^{r+\nu}$ such that $\mathbf{y} = A_\tau \mathbf{x} + \mathbf{w}$ and $\mathbf{y}^t M^t M \mathbf{y} \leq (1 + r)(b b_{\varepsilon_1} \cdots b_{\varepsilon_r})$. We thus have

$$(A_\tau \mathbf{x} + \mathbf{w})^t M^t M (A_\tau \mathbf{x} + \mathbf{w}) \leq (1 + r)(b b_{\varepsilon_1} \cdots b_{\varepsilon_r}).$$

As A_τ is clearly invertible, with matrix inverse

$$A_\tau^{-1} = \begin{pmatrix} 1 & 0 & \ldots & \ldots & 0 & 0 \\ 0 & 1 & \ldots & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & \ldots & 1 & 0 \\ -\frac{\alpha_{\gamma 1}}{\alpha_{\varepsilon r}} & \ldots & -\frac{\alpha_{\gamma \nu}}{\alpha_{\varepsilon r}} & -\frac{\alpha_{\varepsilon 1}}{\alpha_{\varepsilon r}} & \ldots & \frac{1}{\alpha_{\varepsilon r}} \end{pmatrix},$$

we can find a vector $\mathbf{c}$ such that $A_\tau \mathbf{c} = -\mathbf{w}$. Indeed, this vector is $\mathbf{c} = A_\tau^{-1}(-\mathbf{w})$, where

$$\mathbf{c} = A_\tau^{-1}\mathbf{w} = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 1 & 0 \\ -\frac{\alpha_{\gamma 1}}{\alpha_{\varepsilon r}} & \dots & -\frac{\alpha_{\gamma\nu}}{\alpha_{\varepsilon r}} & -\frac{\alpha_{\varepsilon 1}}{\alpha_{\varepsilon r}} & \dots & \frac{1}{\alpha_{\varepsilon r}} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ -\alpha_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ -\frac{\alpha_0}{\alpha_{\varepsilon r}} \end{pmatrix}.$$

Now,

$$\begin{aligned} (1+r)(bb_{\varepsilon_1} \cdots b_{\varepsilon_r}) &\geq (A_\tau \mathbf{x} + \mathbf{w})^t M^t M (A_\tau \mathbf{x} + \mathbf{w}) \\ &= (A_\tau(\mathbf{x} - \mathbf{c}))^T M^T M (A_\tau(\mathbf{x} - \mathbf{c})) \\ &= (\mathbf{x} - \mathbf{c})^T (M A_\tau)^T M A_\tau (\mathbf{x} - \mathbf{c}) \\ &= (\mathbf{x} - \mathbf{c})^T B^T B (\mathbf{x} - \mathbf{c}) \end{aligned}$$

where $B = MA_\tau$. That is, we are left to solve

$$(\mathbf{x} - \mathbf{c})^T B^T B (\mathbf{x} - \mathbf{c}) \leq (1+r)(bb_{\varepsilon_1} \cdots b_{\varepsilon_r}).$$

Now, finding all vectors satisfying this inequality amounts to computing all solutions to (6.2) contained in $\Sigma_\tau(\mathbf{l}, \mathbf{h})$. The set of vectors $\mathbf{x}$ can be found using the Fincke-Pohst algorithm outlined in Section 3.6.2.

6.6 The non-Archimedean Sieve

Let $v \in \{1, \dots, \nu\}$. We take vectors $\mathbf{l}, \mathbf{h} \in \mathbb{R}^{\nu+r}$ with $\mathbf{0} \leq \mathbf{l} \leq \mathbf{h}$ and

$$\frac{l_v}{\log(p)} \geq \max\left(\frac{1}{p-1}, \mathrm{ord}_{p_v}(\delta_1)\right) - \mathrm{ord}_{p_v}(\delta_2)$$

and then consider the translated lattice $\Gamma_v \subseteq \mathbb{Z}^{\nu+r}$ defined below. We say that $\mathbf{m} = (n_1, \dots, n_\nu, a_1, \dots, a_r) \in \mathbb{R}^{r+\nu}$ is determined by some $\mathbf{y} \in \Gamma_v$ if the entries of $\mathbf{y}$ are a (fixed) permutation of the entries of $\mathbf{m}$. Let $\mathcal{E}_v$ be the ellipsoid constructed in (6.19).

Lemma 6.6.1. *Any* $(\tilde{x}, \tilde{y}) \in \Sigma_v(l, h)$ *is determined by some* $\mathbf{y} \in \Gamma_v \cap \mathcal{E}_v$.

In the remainder of this section, we prove this lemma.

We begin by applying the results of Section 3.5. In particular, we consider the form

$$\Lambda_v = \sum_{i=1}^{1+\nu+r} b_i \alpha_i$$

where

$$b_1 = 1, \quad b_{1+i} = n_i \text{ for } i \in \{1, \ldots, \nu\},$$

$$b_{1+\nu+i} = a_i \text{ for } i \in \{1, \ldots, r\},$$

and

$$\alpha_1 = \log_{p_l} \delta_1, \quad \alpha_{1+i} = \log_{p_l} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(l)}} \right) \text{ for } i \in \{1, \ldots, \nu\},$$

$$\alpha_{1+\nu+i} = \log_{p_l} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(l)}} \right) \text{ for } i \in \{1, \ldots, r\}.$$

We apply Lemma 3.5.2 by which $\sum_{j=1}^{\nu} n_j a_{vj}$ can be computed directly if $\mathrm{ord}_{p_v}(\delta_1) \neq 0$. In doing so, we assume for the remainder of this chapter that $\mathrm{ord}_{p_v}(\delta_1) = 0$. Furthermore, we apply Lemma 4.5.4 to obtain a small bound on $\sum_{j=1}^{\nu} n_j a_{vj}$ when $\mathrm{ord}_{p_v}(\alpha_1) < \min_{2 \leq i \leq 1+\nu+r} \mathrm{ord}_{p_v}(\alpha_i)$. Again, in doing so, we assume

$$\mathrm{ord}_{p_v}(\alpha_1) \geq \min_{2 \leq i \leq 1+\nu+r} \mathrm{ord}_{p_v}(\alpha_i)$$

for the remainder of this chapter.

We now set some notation and give some preliminaries for the p_l-adic reduction procedures. Let I be the set of all indices $i' \in \{2, \ldots, 1+\nu+r\}$ for which

$$\mathrm{ord}_{p_v}(\alpha_{i'}) = \min_{2 \leq i \leq 1+\nu+r} \mathrm{ord}_{p_v}(\alpha_i).$$

Following [48], we are always in the case where there exists an index $i' \in I$ such that $\alpha_i/\alpha_{i'} \in \mathbb{Q}_{p_l}$ for $i = 1, \ldots, 1 + \nu + r$. Thus, let $\hat{i}$ denote this index. We define

$$\beta_i = -\frac{\alpha_i}{\alpha_{\hat{i}}} \quad i = 1, \ldots, 1 + \nu + r,$$

and

$$\Lambda'_v = \frac{1}{\alpha_{\hat{i}}}\Lambda_v = \sum_{i=1}^{1+\nu+r} b_i(-\beta_i).$$

Now, we have $\beta_i \in \mathbb{Z}_{p_v}$ for $i = 1, \ldots, 1 + \nu + r$.

Lemma 6.6.2. *Suppose* $\mathrm{ord}_{p_v}(\delta_1) = 0$ *and*

$$\sum_{i=1}^{v} n_i a_{li} > \frac{1}{p_v - 1} - \mathrm{ord}_{p_v}(\delta_2).$$

Then

$$\mathrm{ord}_{p_v}(\Lambda'_v) = \sum_{i=1}^{v} n_i a_{li} + \mathrm{ord}_{p_l}(\delta_2) - \mathrm{ord}_{p_l}(\alpha_{\hat{i}}).$$

Proof. Immediate from Lemma 3.5.3 and Lemma 3.5.4. □

We now describe the p_v-adic reduction procedure. Recall that l_v is a constant such that

$$\frac{l_v}{\log(p)} \geq \max\left(\frac{1}{p_v - 1}, \mathrm{ord}_{p_v}(\delta_1)\right) - \mathrm{ord}_{p_v}(\delta_2).$$

Now, let μ be the largest element of $\mathbb{Z}_{\geq 0}$ at most

$$\mu \leq \frac{l_v}{\log(p)} - \mathrm{ord}_{p_l}(\alpha_{\hat{i}}) + \mathrm{ord}_{p_l}(\delta_2).$$

For each $x \in \mathbb{Z}_{p_l}$, let $x^{\{\mu\}}$ denote the unique rational integer in $[0, p_l^{\mu} - 1]$ such that $\mathrm{ord}_{p_l}(x - x^{\mu}) \geq \mu$ (ie. $x \equiv x^{\{\mu\}} \pmod{p_l^{\mu}}$).

Let Γ_v be the $(\nu + r)$-dimensional translated lattice determined by $A_v\mathbf{x} + \mathbf{w}$, where A_v is the diagonal matrix having $\hat{i}^{\text{th}}$ row

$$\left(\beta_2^{\{\mu\}}, \cdots, \beta_{\hat{i}-1}^{\{\mu\}}, p_l^{\mu}, \beta_{\hat{i}+1}^{\{\mu\}}, \cdots, \beta_{1+\nu+r}^{\{\mu\}}\right) \in \mathbb{Z}^{\nu+r}.$$

Here, p_l^μ is the $(\hat{i}, \hat{i})$ entry of A_v. That is,

$$A_v = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & 0 & & \\ & & 1 & & & & \\ \beta_2^{\{\mu\}} & \cdots & \beta_{\hat{i}-1}^{\{\mu\}} & p_l^\mu & \beta_{\hat{i}+1}^{\{\mu\}} & \cdots & \beta_{1+\nu+r}^{\{\mu\}} \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

Additionally, $\mathbf{w}$ is the vector whose only non-zero entry is the $\hat{i}^{\text{th}}$ element, $\beta_1^{\{\mu\}}$,

$$\mathbf{w} = (0, \dots 0, \beta_1^{\{\mu\}}, 0, \dots, 0)^T \in \mathbb{Z}^{\nu+r}.$$

Of course, we must compute the β_i to p_l-adic precision at least μ in order to avoid errors here. Let $\mathbf{y} = (n_1, \dots, n_\nu, a_1, \dots, a_r) \in \mathbb{R}^{\nu+r}$ denote a solution to (6.2).

Lemma 6.6.3. *Suppose* $\operatorname{ord}_{p_v}(\delta_1) = 0$ *and*

$$\sum_{i=1}^{\nu} n_i a_{vi} > \frac{1}{p_v - 1} - \operatorname{ord}_{p_v}(\delta_2).$$

Then the following equivalence holds:

$$\sum_{i=1}^{\nu} n_i a_{vi} \geq \mu - \operatorname{ord}_{p_v}(\delta_2) + \operatorname{ord}_{p_v}(\alpha_{\hat{i}}) \quad \textit{if and only if} \quad \operatorname{ord}_{p_v}(\Lambda_v') \geq \mu$$

$$\textit{if and only if} \quad \mathbf{y} \in \Gamma_v.$$

Proof. By Lemma 6.6.2, the assumption means that

$$\operatorname{ord}_{p_v}(\Lambda_v') = \sum_{i=1}^{\nu} n_i a_{vi} + \operatorname{ord}_{p_v}(\delta_2) - \operatorname{ord}_{p_v}(\alpha_{\hat{i}}).$$

Now, suppose
$$\sum_{i=1}^{\nu} n_i a_{vi} \geq \mu - \mathrm{ord}_{p_v}(\delta_2) + \mathrm{ord}_{p_v}(\alpha_{\hat{i}}).$$
We thus have
$$\begin{aligned}\mathrm{ord}_{p_v}(\Lambda'_v) &= \sum_{i=1}^{\nu} n_i a_{vi} + \mathrm{ord}_{p_v}(\delta_2) - \mathrm{ord}_{p_v}(\alpha_{\hat{i}})\\ &\geq \mu - \mathrm{ord}_{p_v}(\delta_2) + \mathrm{ord}_{p_v}(\alpha_{\hat{i}}) + \mathrm{ord}_{p_v}(\delta_2) - \mathrm{ord}_{p_v}(\alpha_{\hat{i}})\\ &= \mu.\end{aligned}$$

Conversely, suppose $\mathrm{ord}_{p_v}(\Lambda'_v) \geq \mu$. Then
$$\mu \leq \mathrm{ord}_{p_v}(\Lambda'_v) = \sum_{i=1}^{\nu} n_i a_{vi} + \mathrm{ord}_{p_v}(\delta_2) - \mathrm{ord}_{p_v}(\alpha_{\hat{i}}).$$
That is,
$$\sum_{i=1}^{\nu} n_i a_{vi} \geq \mu - \mathrm{ord}_{p_v}(\delta_2) + \mathrm{ord}_{p_v}(\alpha_{\hat{i}}).$$
Hence, it follows that $\displaystyle\sum_{i=1}^{\nu} n_i a_{vi} \geq \mu - \mathrm{ord}_{p_v}(\delta_2) + \mathrm{ord}_{p_v}(\alpha_{\hat{i}})$ if and only if $\mathrm{ord}_{p_v}(\Lambda'_v) \geq \mu$.

Now, suppose $\mathbf{y} = (n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{\nu+r}$ is a solution to (6.2). Suppose further that $\displaystyle\sum_{i=1}^{\nu} n_i a_{vi} \geq \mu - \mathrm{ord}_{p_v}(\delta_2) + \mathrm{ord}_{p_v}(\alpha_{\hat{i}})$ so that $\mathrm{ord}_{p_v}(\Lambda'_v) \geq \mu$. Let
$$\lambda = \frac{1}{p_v^{\mu}} \sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})$$
and consider the $(\nu + r)$-dimensional vector
$$\mathbf{x} = (n_1, \ldots, n_{\hat{i}-1}, \lambda, n_{\hat{i}+1}, \ldots, n_\nu, a_1, \ldots, a_r).$$
We claim $\mathbf{x} \in \mathbb{Z}^{\nu+r}$. That is, $\lambda \in \mathbb{Z}$, meaning that $\sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})$ is divisible

by p_v^μ, or equivalently,

$$\mathrm{ord}_{p_v}\left(\sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})\right) \geq \mu.$$

Indeed, since

$$\mathrm{ord}_{p_v}\left(\beta_i^{\{\mu\}} - \beta_i\right) \geq \mu \quad \text{for } i = 1, \ldots, 1+\nu+r,$$

by definition, it follows that $\beta_i^{\{\mu\}}$ and β_i share the first $\mu - 1$ terms and thus $\mathrm{ord}_{p_v}(\beta_i) = \mathrm{ord}_{p_v}(\beta_i^{\{\mu\}})$. Now, to compute this order, we only need to concern ourselves with the first non-zero term in the series expansion of $\sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})$. Since $\beta_i^{\{\mu\}}$ and β_i share the first $\mu - 1$ terms, it follows that showing

$$\mathrm{ord}_{p_v}\left(\sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})\right) \geq \mu$$

is equivalent to showing that

$$\mathrm{ord}_{p_l}(\Lambda_l') \geq \mu.$$

Of course, this latter inequality is true by assumption. Thus $\lambda \in \mathbb{Z}$.

Then, computing $A_v\mathbf{x} + \mathbf{w}$ yields

$$A_v\mathbf{x} + \mathbf{w} = \begin{pmatrix} b_2 \\ \vdots \\ b_{\hat{i}-1} \\ b_2\beta_2^{\{\mu\}} + \cdots + b_{\hat{i}-1}\beta_{\hat{i}-1}^{\{\mu\}} + \lambda p_l^\mu + b_{\hat{i}+1}\beta_{\hat{i}+1}^{\{\mu\}} + \cdots + b_{\nu+r+1}\beta_{1+\nu+r}^{\{\mu\}} + \beta_1^{\{\mu\}} \\ b_{\hat{i}+1} \\ \vdots \\ b_{\nu+r+1} \end{pmatrix}$$

Now,

$$\lambda p_v^{\mu} = p_v^{\mu} \frac{1}{p_v^{\mu}} \sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}}) = \sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}}),$$

hence

$$\begin{aligned}
&b_2\beta_2^{\{\mu\}} + \cdots + b_{\hat{i}-1}\beta_{\hat{i}-1}^{\{\mu\}} + b_{\hat{i}+1}\beta_{\hat{i}+1}^{\{\mu\}} + \cdots + b_{\nu+r+1}\beta_{1+\nu+r}^{\{\mu\}} + \lambda p_l^{\mu} + \beta_1^{\{\mu\}} \\
&= b_{\hat{i}}(-\beta_{\hat{i}}^{\{\mu\}}) \\
&= b_{\hat{i}}
\end{aligned}$$

where the last equality follows from the fact that

$$-\beta_i = \frac{\alpha_{\hat{i}}}{\alpha_{\hat{i}}} = 1.$$

Thus,

$$A_v\mathbf{x} + \mathbf{w} = \begin{pmatrix} b_2 \\ \vdots \\ b_{\hat{i}-1} \\ b_{\hat{i}} \\ b_{\hat{i}+1} \\ \vdots \\ b_{\nu+r+1} \end{pmatrix} = \begin{pmatrix} n_1 \\ \vdots \\ n_\nu \\ a_1 \\ \vdots \\ a_r \end{pmatrix} = \mathbf{y}.$$

and $\mathbf{y} \in \Gamma_v$.

$\square$

Define

$$c_{p_v} = \log p_v \left(\max\left(\tfrac{1}{p_v-1}, \mathrm{ord}_{p_v}(\delta_1)\right) - \mathrm{ord}_{p_v}(\delta_2)\right).$$

Corollary 6.6.4. *Assume that $h_{p_v}(z) > \max(0, c_{p_v})$. Then the following equivalence holds:*

$$h_{p_v}(z) \geq \log p_v\left(\mu - \mathrm{ord}_{p_v}(\delta_2) + \mathrm{ord}_{p_v}(\alpha_{\hat{i}})\right) \quad \textit{if and only if} \quad \mathbf{y} \in \Gamma_v.$$

Proof. Recall from Proposition 6.1.3 that

$$h_{p_v}(z) = \begin{cases} \log(p_v)|u_v - r_v| \\ 0 \end{cases}.$$

Since $h_{p_v}(z) > 0$, it follows that $h_{p_v}(z) = \log(p_v)|u_v - r_v|$. Hence the assumption becomes

$$\log(p_v)|u_v - r_v| = h_{p_v}(z) > \log p_v \left(\max\left(\tfrac{1}{p_v - 1}, \mathrm{ord}_{p_v}(\delta_1) \right) - \mathrm{ord}_{p_v}(\delta_2) \right),$$

or equivalently,

$$\sum_{j=1}^{\nu} n_j a_{vj} > \left(\max\left(\tfrac{1}{p_v - 1}, \mathrm{ord}_{p_v}(\delta_1) \right) - \mathrm{ord}_{p_v}(\delta_2) \right).$$

Moreover, the conclusion is equivalent to

$$\log(p_v)|u_v - r_v| \geq \log p_v \left(\mu - \mathrm{ord}_{p_v}(\delta_2) + \mathrm{ord}_{p_v}(\alpha_{\hat{i}}) \right) \quad \text{if and only if} \quad \mathbf{y} \in \Gamma_v,$$

or,

$$\sum_{j=1}^{\nu} n_j a_{vj} \geq \left(\mu - \mathrm{ord}_{p_v}(\delta_2) + \mathrm{ord}_{p_v}(\alpha_{\hat{i}}) \right) \quad \text{if and only if} \quad \mathbf{y} \in \Gamma_v,$$

which is the previous lemma.

$\square$

We now prove Lemma 6.6.1.

Proof of Lemma 6.6.1. If $(n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{r+\nu}$ with corresponding $\tilde{x}, \tilde{y} \in \Sigma_v(\mathbf{l}, \mathbf{h})$, then, by definition, it corresponds to a solution $(\tilde{x}, \tilde{y}) \in \Sigma_v(\mathbf{l}, \mathbf{h})$. Hence $h_v(z) > l_v$, where l_v is a constant such that

$$\frac{l_v}{\log(p_v)} \geq \max\left(\frac{1}{p_v - 1}, \mathrm{ord}_{p_v}(\delta_1) \right) - \mathrm{ord}_{p_v}(\delta_2).$$

That is,

$$h_v(z) > l_v \geq \log(p_v)\left(\max\left(\frac{1}{p_v - 1}, \operatorname{ord}_{p_v}(\delta_1)\right) - \operatorname{ord}_{p_v}(\delta_2)\right) = c_p.$$

Now, recall that $\mathbf{l} \geq \mathbf{0}$ so that $l_v \geq 0$. It thus follows that

$$h_v(z) > l_v \geq \begin{cases} 0 \\ c_p \end{cases} \implies h_v(z) > \max(0, c_p).$$

In other words, the conditions of Corollary 6.6.4 are satisfied.

Now, recall that μ is the largest element of $\mathbb{Z}_{\geq 0}$ at most

$$\mu \leq \frac{l_v}{\log(p_v)} - \operatorname{ord}_{p_v}(\alpha_{\hat{i}}) + \operatorname{ord}_{p_v}(\delta_2).$$

That is

$$\frac{l_v}{\log(p_v)} \geq \mu + \operatorname{ord}_{p_v}(\alpha_{\hat{i}}) - \operatorname{ord}_{p_v}(\delta_2)$$

so that

$$h_v(z) > l_v \geq \log(p_v)\left(\mu + \operatorname{ord}_{p_l}(\alpha_{\hat{i}}) - \operatorname{ord}_{p_v}(\delta_2)\right).$$

Now, by Corollary 6.6.4, we must have $\mathbf{y} \in \Gamma_v$. This shows that $(\tilde{x}, \tilde{y})$ is determined by $\mathbf{y} = \mathbf{m}' \in \Gamma_v$, which proves Lemma 6.6.1. $\square$

Finally, suppose that $\mathbf{y} \in \Gamma_v \cap \mathcal{E}_v$. Let $M = M_v$ be the matrix defining the ellipsoid $\mathcal{E}_v$. That is

$$M = \sqrt{b_{\varepsilon_1} \cdots b_{\varepsilon_r}} \begin{pmatrix} DA & 0 & \dots & 0 & 0 \\ 0 & \sqrt{\frac{b}{b_{\varepsilon 1}}} & \dots & 0 & 0 \\ 0 & 0 & \sqrt{\frac{b}{b_{\varepsilon 2}}} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \sqrt{\frac{b}{b_{\varepsilon}}} \end{pmatrix}.$$

Recall that $A_v\mathbf{x} + \mathbf{w}$ defines the lattice Γ_v. In particular, since $\mathbf{y} \in \Gamma_v \cap \mathcal{E}_v$, there exists $\mathbf{x} \in \mathbb{R}^{r+\nu}$ such that $\mathbf{y} = A_v\mathbf{x} + \mathbf{w}$ and $\mathbf{y}^T M^T M\mathbf{y} \leq (1+r)(bb_{\varepsilon_1} \cdots b_{\varepsilon_r})$. We thus have

$$(A_v\mathbf{x} + \mathbf{w})^T M^T M(A_v\mathbf{x} + \mathbf{w}) \leq (1+r)(bb_{\varepsilon_1} \cdots b_{\varepsilon_r}).$$

As A_v is clearly invertible, with matrix inverse

$$A_v^{-1} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & 0 & & \\ & & 1 & & & & \\ -\frac{\beta_2^{\{\mu\}}}{p_l^\mu} & \cdots & -\frac{\beta_{\hat{i}-1}^{\{\mu\}}}{p_l^\mu} & \frac{1}{p_l^\mu} & -\frac{\beta_{\hat{i}+1}^{\{\mu\}}}{p_l^\mu} & \cdots & -\frac{\beta_{1+\nu+r}^{\{\mu\}}}{p_l^\mu} \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix},$$

we can find a vector $\mathbf{c}$ such that $A_v\mathbf{c} = -\mathbf{w}$. Indeed, this vector is $\mathbf{c} = A_v^{-1}(-\mathbf{w})$, where

$$\mathbf{c} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -\frac{\beta_1^{\{\mu\}}}{p^{\{\mu\}}} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Now,

$$\begin{aligned} (1+r)(bb_{\varepsilon_1} \cdots b_{\varepsilon_r}) &\geq (A_v\mathbf{x} + \mathbf{w})^T M^T M(A_v\mathbf{x} + \mathbf{w}) \\ &= (A_v\mathbf{x} - A_v\mathbf{c})^T M^T M(A_v\mathbf{x} - A_v\mathbf{c}) \\ &= (\mathbf{x} - \mathbf{c})^T (MA_v)^T MA_v(\mathbf{x} - \mathbf{c}) \\ &= (\mathbf{x} - \mathbf{c})^T B^T B(\mathbf{x} - \mathbf{c}) \end{aligned}$$

where $B = MA_v$. That is, we are left to solve

$$(\mathbf{x} - \mathbf{c})^T B^T B(\mathbf{x} - \mathbf{c}) \leq (1 + r)(bb_{\varepsilon_1} \cdots b_{\varepsilon_r}).$$

As in Section 6.5 finding all vectors satisfying this inequality amounts to computing all solutions to (6.2) contained in $\Sigma_v(\mathbf{l}, \mathbf{h})$. The set of vectors $\mathbf{x}$ can be found using the Fincke-Pohst algorithm outlined in Section 3.6.2.

Bibliography

[1] M. K. Agrawal, J. H. Coates, D. C. Hunt and A. J. van der Poorten, *Elliptic curves of conductor* 11, Math. Comp. 35 (1980), 991–1002. → pages 4, 114

[2] S. Akhtari and M. Bhargava, *A positive proportion of locally soluble Thue equations are globally insoluble*, preprint. → page 179

[3] R. Balasubramanian and T. N. Shorey, On the equation $a(x^m-1)/(x-1) = b(y^n-1)/(y-1)$, *Math. Scand.* 46 (1980), 177–182. → pages 12, 13

[4] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika. *12* (1966), 204-216. → page 4

[5] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Math. Proc. Camb. Phil. Soc.*. 65 (1969), 439–444. → pages 13, 61

[6] M. Bauer and M. A. Bennett, Applications of the hypergeometric method to the Generalized Ramanujan-Nagell equation, *The Ramanujan J.* 6 (2002), 209–270. → pages 68, 71

[7] K. Belabas, *A fast algorithm to compute cubic fields,* Math. Comp. 66 (1997), 1213–1237. → page 136

[8] K. Belabas and H. Cohen, *Binary cubic forms and cubic number fields*, Organic Mathematics (Burnaby, BC, 1995), 175–204. CMS Conf. Proc., 20 Amer. Math. Soc. 1997. → pages 136, 186, 187

[9] M. A. Bennett and A. Ghadermarzi, *Mordell's equation : a classical approach*, L.M.S. J. Comput. Math. 18 (2015), 633–646. → page 137

[10] M. A. Bennett and A. Rechnitzer, *Computing elliptic curves over $\mathbb{Q}$: bad reduction at one prime*, CAIMS 2015 proceedings.

[11] W. E. H. Berwick and G. B. Mathews, *On the reduction of arithmetical binary cubic forms which have a negative determinant*, Proc. London Math. Soc. (2) 10 (1911), 43–53. → page 137

[12] F. Beukers, On the generalized Ramanujan-Nagell equation I, Acta Arith. XXXVIII (1981), 389–410. → pages 63, 67

[13] F. Beukers, On the generalized Ramanujan-Nagell equation, II, Acta Arith. XXXIX (1981), 113–123. → pages 63, 67

[14] B. J. Birch and W. Kuyk (Eds.), *Modular Functions of One Variable IV*, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975. → page 114

[15] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.

[16] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, 1966. → page 18

[17] W. Bosma, J. Cannon and C. Playoust, The Magma Algebra System I: The User Language, *J. Symb. Comp.* **24** (1997), 235–265. (See also http://magma.maths.usyd.edu.au/magma/) → pages 5, 86, 126, 168, 170

[18] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the Modularity of Elliptic Curves over $\mathbb{Q}$: Wild 3-adic Exercises*, J. Amer. Math. Soc. 14 (2001), 843–939. → pages 114, 156

[19] A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. 23 (1990), 375–382. → pages 174, 175

[20] A. Brumer and J. H. Silverman, *The number of elliptic curves over $\mathbb{Q}$ with conductor N*, Manuscripta Math. 91 (1996), 95–102. → page 179

[21] Y. Bugeaud and K. Győry, Bounds for the solutions of Thue-Mahler equations and norm form equations, *Acta Arithmetica* 74.3 (1996), 273–292. → pages 95, 96

[22] Y. Bugeaud and T.N. Shorey, On the diophantine equation $\frac{x^m-1}{x-1} = \frac{y^n-1}{y-1}$, *Pacific J. Math.* 207 (2002), 61–75. → pages 5, 12, 13, 14, 63

[23] J. W. S. Cassels, *Local fields*, Cambridge University Press, 1986. → page 18

[24] G. V. Chudnovsky, On the method of Thue-Siegel, *Ann. of Math.* (2) 117 (1983), 325–382. → page 69

[25] J. Coates, *An effective p-adic analogue of a theorem of Thue. III. The diophantine equation $y^2 = x^3 + k$*, Acta Arith. 16 (1969/1970), 425–435. → pages 4, 113, 114

[26] F. Coghlan, *Elliptic Curves with Conductor $2^m 3^n$*, Ph.D. thesis, Manchester, England, 1967. → page 114

[27] J. H. E. Cohn, *A course in computational algebraic number theory*, Springer Verlag, 1995. → page 55

[28] J. H. E. Cohn, *Number theory volume I: tools and diophantine equations*, Springer Science + Business Media, LLC, 2007. → page 23

[29] J. E. Cremona, *Elliptic curve tables*, http://johncremona.github.io/ecdata/ → pages 114, 156

[30] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. Available online at http://homepages.warwick.ac.uk/staff/J.E.Cremona/book/fulltext/index.html → pages 114, 172

[31] J. E. Cremona, *Reduction of binary cubic and quartic forms,* LMS J. Comput. Math. 4 (1999), 64–94. → pages 136, 139

[32] J. E. Cremona, *mwrank and related programs for elliptic curves over $\mathbb{Q}$*, 1990–2017, http://www.warwick.ac.uk/staff/J.E.Cremona/mwrank/index.html → page 180

[33] J. E. Cremona and M. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. 16 (2007), 303–312. → pages 116, 124

[34] H. Davenport, *The reduction of a binary cubic form. I.*, J. London Math. Soc. 20 (1945), 14–22. → page 136

[35] H. Davenport, *The reduction of a binary cubic form. II.*, J. London Math. Soc. 20 (1945), 139–147. → page 136

[36] H. Davenport, *On the class-number of binary cubic forms. I.*, J. London Math. Soc. 26 (1951), 183–192; ibid, 27 (1952), 512. → page 136

[37] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II.*, Proc. Roy. Soc. London Ser. A. 322 (1971), 405–420. → page 136

[38] H. Davenport, D. J. Lewis and A. Schinzel, Equations of the form $f(x) = g(y)$, *Quart. J. Math. Oxford set (2)* 12 (1961), 304–312. → pages 4, 5, 12

[39] B. Edixhoven, A. de Groot and J. Top, *Elliptic curves over the rationals with bad reduction at only one prime*, Math. Comp. 54 (1990), 413–419. → pages 158, 177

[40] N. D. Elkies, *How many elliptic curves can have the same prime conductor?*, http://math.harvard.edu/~elkies/condp_banff.pdf → page 180

[41] N. D. Elkies, *Rational points near curves and small nonzero* $|x^3 - y^2|$ *via lattice reduction*, Lecture Notes in Computer Science 1838 (proceedings of ANTS-4, 2000; W.Bosma, ed.), 33–63. → page 182

[42] N. D. Elkies and M. Watkins, *Elliptic curves of large rank and small conductor*, Algorithmic number theory, 42–56, Lecture Notes in Comput. Sci., 3076, Springer, Berlin, 2004. → page 181

[43] U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Mathematics of Computation **44** (1985), no. 170, 463-471. → pages 55, 57

[44] A. Gherga, R. von Känel, B. Matschke, S. Siksek, Efficient resolution of Thue-Mahler equations, Manuscript in preparation (2018). → pages 14, 30, 35, 62, 90, 192, 205

[45] R. Goormaghtigh, *L'Intermédiaire des Mathématiciens* 24 (1917), 88. → pages 3, 11

[46] T. Hadano, *On the conductor of an elliptic curve with a rational point of order* 2, Nagoya Math. J. 53 (1974), 199–210. → page 159

[47] B. Haible, *CLN, a class library for numbers*, available from http://www.ginac.de/CLN/ → page 168

[48] K. Hambrook, Implementation of a Thue-Mahler solver, M.Sc. thesis, University of British Columbia, 2011. → pages 5, 30, 126, 224

[49] H. Hasse, *Arithmetische Theorie der kubischen Zahlköper auf klassenkörpertheoretischer Grundlage*, Math. Z. 31 (1930), 565–582. → page 160

[50] H. Hasse, *Number theory*, Springer-Verlag, 1980. → pages 18, 23

[51] B. He, A remark on the Diophantine equation $(x^3-1)/(x-1) = (y^n-1)/(y-1)$, *Glasnik Mat.* 44 (2009), 1–6. → page 14

[52] B. He and A. Togbé, On the number of solutions of Goormaghtigh equation for given x and y, *Indag. Mathem.* 19 (2008), 65–72. → pages 5, 13

[53] C. Hermite, *Note sur la réduction des formes homogènes à coefficients entiers et à deux indéterminées*, J. Reine Angew. Math. 36 (1848), 357–364. → page 136

[54] C. Hermite, *Sur la réduction des formes cubiques à deux indéterminées*, C. R. Acad. Sci. Paris 48 (1859), 351–357. → page 136

[55] G. Julia, *Étude sur les formes binaires non quadratiques à indéterminées réelles, ou complexes, ou à indéterminées conjuguées*, Mem. Acad. Sci. l'Inst. France 55 (1917), 1–293. → page 137

[56] R. von Kanel and B. Matschke, *Solving S-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture*, preprint, arXiv:1605.06079. → pages 152, 154, 155, 199

[57] C. Karanicoloff, Sur une équation diophantienne considérée par Goormaghtigh, *Ann. Polonici Math.* XIV (1963), 69–76. → pages 62, 73

[58] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer-Verlag,1977. → page 18

[59] A. Koutsianas, *Computing all elliptic curves over an arbitrary number field with prescribed primes of bad reduction*, Experiment. Math., http://www.tandfonline.com/doi/full/10.1080/10586458.2017.1325791 → page 152

[60] M. Le, On the Diophantine equation $(x^3-1)/(x-1) = (y^n-1)/(y-1)$, *Trans. Amer. Math. Soc.* 351 (1999), 1063–1074. → pages 5, 13

[61] M. Le, Exceptional solutions to the exponential Diophantine equation $(x^3-1)/(x-1) = (y^n-1)/(y-1)$, *J. Reine Angew. Math.* 543 (2002), 187–192. → pages 5, 13

[62] M. Le, On Goormaghtigh's equation $(x^3-1)/(x-1) = (y^n-1)/(y-1)$, *Acta Math. Sinica (Chin. Ser.)* 45 (2002), 505–508. → pages 5, 13

[63] A.K. Lenstra, H.W. Lenstra Jr., and L. Lovasz, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), 515-534. → pages 53, 54

[64] Liouville, J. *Sur des classes très étendues de quantités dont la valuer n^e est ni algebrique, ni même réductible á des irrationnelles algebriques*, C.R. Acad. Sci. Paris **18** (1844), 883-885, 910-911. → page 2

[65] W. Ljunggren, Noen Setninger om ubestemte likninger av formen $(x^n - 1)/(x - 1) = y^q$, *Norsk. Mat. Tidsskr.* 25 (1943), 17–20. → page 12

[66] The LMFDB Collaboration, The L-functions and Modular Forms Database, http://www.lmfdb.org → page 143

[67] K. Mahler, *Zur Approximation algebraischer Zahlen, I: Ueber den grössten Primteiler binärer Formen*, Math. Ann. 107 (1933), 691–730. → pages 4, 113

[68] K. Mahler, *An application of Jensen's formula to polynomials*, Mathematika 7 (1960), 98–100. → page 184

[69] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. 11 (1964), 257–262. → pages 188, 189

[70] L. Bernardin et al, Maple Programming Guide, Maplesoft, 2017, Waterloo ON, Canada. → page 168

[71] D. A. Markus, *Number Fields*, Springer-Verlag, 1977. → page 16

[72] J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math 400 (1989), 173–184. → page 156

[73] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.* 572 (2004), 167–195. → page 12

[74] G. L. Miller, *Riemann's hypothesis and tests for primality* in Proceedings of seventh annual ACM symposium on Theory of computing, 234–239 (1975). → page 168

[75] L. J. Mordell, *The diophantine equation $y^2 - k = x^3$*, Proc. London. Math. Soc. (2) 13 (1913), 60–80. → page 121

[76] L. J. Mordell, *Indeterminate equations of the third and fourth degree*, Quart. J. of Pure and Applied Math. 45 (1914), 170–186.

[77] L. J. Mordell, *Diophantine Equations,* Academic Press, London, 1969. → page 121

[78] T. Nagell, Note sur l'équation indéterminée $(x^n - 1)/(x - 1) = y^q$, *Norsk. Mat. Tidsskr.* 2 (1920), 75–78. → page 12

[79] T. Nagell, *Introduction to Number Theory*, New York, 1951. → page 166

[80] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 3rd ed., Springer-Verlag, 2004. → page 18

[81] Y. V. Nesterenko and T. N. Shorey, On an equation of Goormaghtigh, *Acta Arith.* 83 (1998), 381–389. → pages 5, 12, 63, 64, 66

[82] O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten II*, Math. Nach. 56 (1973), 269–280. → page 114

[83] J. Neukirch *Algebraic Number Theory*, Springer-Verlag, 1999. → page 16

[84] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3, J. Number Theory 44 (1993), 119–152. → page 116

[85] The PARI Group, Bordeaux. PARI/GP version `2.7.1`, 2014. available at `http://pari.math.u-bordeaux.fr/`. → pages 126, 170

[86] J. Park, B. Poonen, J. Voight and M. Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, preprint, arXiv:1602.01431. → page 179

[87] A. Pethő, *On the resolution of Thue inequalities*, J. Symbolic Computation 4 (1987), 103–109. → page 171

[88] A. Pethő, *On the representation of* 1 *by binary cubic forms of positive discriminant*, Number Theory, Ulm 1987 (Springer LNM 1380), 185–196. → pages 171, 185

[89] M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory 12 (1980) 128–138. → page 168

[90] R. Ratat, *L'Intermédiaire des Mathématiciens* 23 (1916), 150. → page 11

[91] G. Robin, Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. *Acta Arith.* XLII (1983), 367–389. → page 110

[92] K. Rubin and A. Silverberg, *Mod* 2 *representations of elliptic curves*, Proc. Amer. Math. Soc. 129 (2001), 53–57. → page 121

[93] The Sage Developers, SageMath, the Sage Mathematics Software System (Version 8.1), http://www.sagemath.org, 2018. → page 168

[94] B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. 10 (1975), 367–378. → pages 114, 160

[95] I. R. Shafarevich, *Algebraic number theory*, Proc. Internat. Congr. Mathematicians, Stockholm, Inst. Mittag-Leffler, Djursholm (1962), 163–176. → page 113

[96] D. Shanks, *Five number-theoretic algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics, (1973), 51–70. → page 162

[97] T. N. Shorey, An equation of Goormaghtigh and Diophantine approximations, Current Trends in Number Theory, edited by S.D.Adhikari, S.A.Katre and B.Ramakrishnan, Hindustan Book Agency, New Delhi (2002), 185–197. → pages 5, 13

[98] T. N. Shorey and R. Tijdeman, New applications of diophantine approximation to diophantine equations, *Math. Scand.* 39 (1976), 5–18. → page 12

[99] Siegel, C. L., *Uber einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Acad. Wiss. Phys.-Mat. Kl.**1**, (1929), 41-69. → page 3

[100] A. K. Silvester, B. K. Spearman and K. S. Williams, *Cyclic cubic fields of given conductor and given index*, Canad. Math. Bull. Vol. 49 (2006) 472–480. → page 164

[101] N.P. Smart, *The algorithmic resolution of diophantine equations*, Chapman and Hall, Cambridge University Press, 1998. → pages 23, 54

[102] J. P. Sorenson and J. Webster, *Strong Pseudoprimes to Twelve Prime Bases*, Math. Comp. 86 (2017), 985–1003. → page 168

[103] V. G. Sprindzuk, *Classical Diophantine Equations*, Springer-Verlag, Berlin, 1993. → pages 2, 3, 121

[104] V. G. Sprindzuk, A.I. Vinogradov, *The representation of numbers by binary forms (Russian)*, Matematicheskie Zametki **3** (1968), 369-376. → page 4

[105] W. Stein and M. Watkins, *A database of elliptic curves – first report*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Compute. Sci., vol. 2369, Springer, Berlin, 2002, pp. 267–275. → page 174

[106] N. M. Stephens, The Birch Swinnerton-Dyer Conjecture for Selmer curves of positive rank, *Ph.D. Thesis*, Manchester, 1965. → page 114

[107] O. Tange, *GNU Parallel - The Command-Line Power Tool*, ;login: The USENIX Magazine, (2011), 42–47. → page 140

[108] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135 (1909), 284–305. → pages 2, 3, 113

[109] R. Tijdeman, On the equation of Catalan, *Acta Arith.* 29 (1976), 197–209. → page 12

[110] N. Tzanakis and B. M. M. de Weger, *On the practical solutions of the Thue equation*, J. Number Theory 31 (1989), 99–132. → pages 4, 170

[111] N. Tzanakis and B. M. M. de Weger, *Solving a specific Thue-Mahler equation*, Math. Comp. 57 (1991) 799–815. → pages 4, 126

[112] N. Tzanakis and B. M. M. de Weger, How to explicitly solve a Thue-Mahler equation, *Compositio Math*. 84 (1992), 223–288. → pages 4, 30, 34, 35, 46, 47, 48, 49, 90, 95, 97, 100, 101, 126, 192

[113] M. Watkins, S. Donnelly, N. D. Elkies, T. Fisher, A. Granville and N. F. Rogers, *Ranks of quadratic twists of elliptic curves*, Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013, 63–98, Publ. Math. Besançon Algèbre Théorie Nr., 2014/2, Presses Univ. Franche-Comté, Besançon, 2015. → page 179

[114] B. M. M. de Weger, Algorithms for diophantine equations, CWI-Tract No. 65, Centre for Mathematics and Computer Science, Amsterdam, 1989. → pages 4, 54, 138

[115] B. M. M. de Weger, *The weighted sum of two S-units being a square*, Indag. Mathem. 1 (1990), 243–262. → page 138

[116] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. 141 (1995), 443–551. → page 114

[117] P. Yuan, On the Diophantine equation $ax^2 + by^2 = ck^n$, *Indag. Mathem.* 16 (2) (2005), 301–320. → page 112

[118] P. Yuan, On the diophantine equation $\frac{x^3-1}{x-1} = \frac{y^n-1}{y-1}$, *J. Number Theory* 112 (2005), 20–25. → page 14