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

by

Adela Gherga

B.Sc. Mathematics, McMaster University, 2006

M.Sc. Mathematics, McMaster University, 2010

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

This document provides brief instructions for using the `ubcdiss` class to write a UBC-conformant dissertation in LaTeX. This document is itself written using the `ubcdiss` class and is intended to serve as an example of writing a dissertation in LaTeX. This document has embedded Unique Resource Locators (URLS) and is intended to be viewed using a computer-based Portable Document Format (PDF) reader.

Note: Abstracts should generally try to avoid using acronyms.

Note: at University of British Columbia (UBC), both the Graduate and Postdoctoral Studies (GPS) Ph.D. defence programme and the Library's online submission system restricts abstracts to 350 words.

Lay Summary

The lay or public summary explains the key goals and contributions of the research/ scholarly work in terms that can be understood by the general public. It must not exceed 150 words in length.

Preface

At UBC, a preface may be required. Be sure to check the GPS guidelines as they may have specific content to be included.

Contents

List of Tables

List of Figures

Glossary

This glossary uses the handy `acroynym` package to automatically maintain the glossary. It uses the package's `printonlyused` option to include only those acronyms explicitly referenced in the LaTeX source.

GPS Graduate and Postdoctoral Studies

PDF Portable Document Format

URL Unique Resource Locator, used to describe a means for obtaining some resource on the world wide web

Acknowledgments

Thank those people who helped you.

Don’t forget your parents or loved ones.

You may wish to acknowledge your funding sources.

Chapter 1

Introduction

i mean, the beginning is the part you're not comfortable writing, right? the longer it went on, the better it flowed. at that point you're quoting and weaving results you know well, referencing the little mental web you have woven. it seems cohesive, but also i don't understand it. the beginning bit seems thrown together like Mike told you to include bits about DEs and so you begrudgingly injected something ?? like the very very beginning bit anyway, i'll e-mail you back the tex file and the pdf. i know you're not asking for this advice but it's coming from ozgur and yaniv and they are very smart and i trust them lots:

1. be very careful about whether you're using colloquial language, and how it might be interpreted. e.g. be careful not to insult people's work, and try to not to flip flop on how hand wavey you are being. I think I have a couple of notes in the file pertaining to each of these points
2. when citing work, either use the author names every time or don't. don't mix and match unless appropriate. why would you deny some the respect of appearing in your work, but not others?
3. if you're going to write notes to yourself in your thesis/papers, you must have a way of ensuring that you'll see them later before you send it off. caps lock is not sufficient and yaniv and ozgur can provide examples if you need. I included a little command for you so that you can just Cmd+F (or C-s ??) for all appearances of in the .tex file if you use it. Has the added advantage of making PDF text blue so that everyone reading too knows that it doesn't belong.

also my disclaimer for edits: 1. for some reason my brain is tired today; 2. I don't know the culture of your field nor some of the very elementary things you're presenting 3. Because of 1, I tried to communicate what I wanted to say using the best language I could, but may not have always succeeded at clarity/intent/approachability ?? So basically, remember that it's possible that my edits deserve to be treated with a grain of salt. ??

This start feels outside the realm of where you're going — it seems at once abrupt and off-topic. It would be nice to have an introductory sentence or two to get the reader on track before discussing the "required background" material. 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. why the history lesson? maybe you could use this as one way of motivating/introducing DEs: "look at these things. look how long they've been studied. here's why, and here are the ways people study them. . . . or something. . .

remove separate paragraph if it's the same thought — f is a DE right? If so, then these next lines are providing additional information to what was given above, not starting a new thread. 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 ~~or not~~ (1.1) has any solutions ~~at all~~ (too colloquial imo). Indeed, one of the most famous theorems in mathematics, Fermat's Last Theorem, proven by Wiles in 1995, 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 (there are so many commas in this sentence. You can remove at least 2 of 7 by splicing and/or rearranging). 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 $n \geq 3$ (feels like you really jump into the language here. you spelled out what a DE was, but now assume the reader knows the definition of an integral binary form. Personally, I knew the former but the latter reads like domain-specific jargon to me) and a is a fixed nonzero rational integer. In 1909, Thue [REF] proved that this equation has only finitely many solutions. This result followed from a sharpening of Liouville's inequality, 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 ([REF]) 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

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

what is the limit $\lambda \to \infty$ with respect to? 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 $\alpha^{(i)}$. 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 (descriptive? explicit? tight? tractable?) inequality (1.4) is known. The sharpening of the Liouville inequality however, especially in effective form, proved to be very difficult. REF? also "very difficult" seems a subjective qualification; is that okay for your audience?

In [REF:THUE], 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 $\lambda(q) = c_3 q^{\frac{1}{2}n-1-\varepsilon}$ this function does not match the one appearing above in displaymath. is that supposed to be the case? might have something to do with the $<$ not matching the $>$ in (1.4)? it is not clear to me, but hopefully it will be to typical reader, where $c_3 > 0$ depends on α and ε, thereby confirming that all Thue equations have only finitely many solutions. 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 ~~actually~~ find the solutions to (1.2). I feel like I would dance more carefully around calling someone's proof ineffective.

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 to his theorem on the finitude of the number of integral points on an algebraic curve of genus greater than zero [REF?]. However, as Siegel's result relies on Thue's rational approximation to algebraic numbers, it too is ineffective in the above sense.

Shortly following Thue's result, Goormaghtigh 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 ([REF]) 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 [REF] 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 $S = \{p_1, \ldots, p_v\}$ denotes a fixed set of prime numbers, $x, y, z_i \geq 0$, $i = 1, \ldots, v$ 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 each time I read this, I believe more strongly that a different word should be used to describe their work. ineffective seems like an attack, and a broad stroke that misses the precise critique you're looking to discuss.

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 [REF], based on his theory of bounds for linear forms in the logarithms of alge-

braic numbers. Generalizing Baker's ground-breaking result to the p-adic case, Sprindžuk and Vinogradov [CITE] and Coates [CITE] 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 [CITE], whose ideas were inspired in part by the method of Agrawal, Coates, Hunt, and van der Poorten [CITE] 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 as a MAGMA package [REF?].

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 ([REF]) were able to replace Siegel's result by an effective argument due to Runge. This result was improved by Nesterenko and Shorey ([REF]) and Bugeaud and Shorey ([REF]) using Baker's theory of linear forms in logarithms. In either case, in order to deduce effectively computable bounds (I like this use of effectively) 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 ([REF]) 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 ([REF]) 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, [**?**], [**?**], [**?**] and [**?**]. An excellent overview of results on this problem can be found in the survey of Shorey [**?**].

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 equation* (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*

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

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 $2^a 3^b$ 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

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

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 4. Samir's sieve - this may not be done in time as we only just received Samir's writeup and explanation as pertaining to Thue-Mahler equations.

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 [**?**] and Goormaghtigh [**?**] 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*

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

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

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

and Nagell-Ljunggren

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

In a certain sense, however, equation (4.1) appears to be rather harder to treat than (4.2) or (4.3). Techniques from Diophantine approximation (specifically, bounds for linear forms in complex and p-adic logarithms) have been applied by Tijdeman [**?**] to show that equation (4.2) has at most finitely many solutions in the four variables x, y, m and n (a result subsequently sharpened by Mihăilescu [**?**] via

a different method to solve (4.2) completely). Similarly, Shorey and Tijdeman [**?**] showed that equation (4.3) 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 [**?**] and Ljunggren [**?**]). In the case of equation (4.1), 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 [**?**] 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 [**?**]) or from bounds upon linear forms in logarithms (see e.g. Nesterenko and Shorey [**?**], and Bugeaud and Shorey [**?**]), 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 [**?**] shows that equation (4.1) has at most finitely many solutions if we fix only the set of prime divisors of x and y, while Bugeaud and Shorey [**?**] prove an analogous finiteness result, under the additional assumption of (4.4), provided the quotient $(m-1)/(n-1)$ is bounded above. Additional results on special cases of equation (4.1) are available in, for example, [**?**], [**?**], [**?**] and [**?**]. An excellent overview of results on this problem can be found in the survey of Shorey [**?**].

In this paper, we prove that, in fact, under assumption (4.4), equation (4.1) 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 (4.1), satisfying (4.4), 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 (4.5), in conjunction with, for example, work of Baker [**?**]. The constants present in our upper bound (4.5) 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 (4.1), subject to condition (4.4), for small fixed values of n.

Theorem 1.1.4. *If there is a solution in integers x, y and m to equation (4.1), with $n \in \{3, 4, 5\}$ and satisfying (4.4), then*

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

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 [**?**]. 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 [**?**] (see also He [**?**]). The techniques employed in both [**?**] and [**?**], 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 (4.1) in earlier work of Bugeaud and Shorey [**?**]. 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 (4.1). 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 (4.1), 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

Add some better intro: maybe see masters thesis
In this section we recall some basic results from algebraic number theory that we use throughout the remaining chapters. We refer to Marcus and Neukirch for full details. Establish notation. The background for the material presented in this chapter is taken primarily from Marcus and Neukirch, and the material presented in Section 2.2 can be found in [5]

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

fix intro: In this section we give a concise exposition of p-adic valuations. Everything in this document is based off of "Elementary and analytic theory of algebraic numbers" by W. Narkiewicz. Throughout this thesis, 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 $\mathrm{ord}_{\mathfrak{p}}((\alpha)\mathcal{O}_K)$. 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 $\mathrm{ord}_{\mathfrak{p}}$, 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

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

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

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

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:

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

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

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

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

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

where $k = \mathrm{ord}_p(x)$ and the p-adic digits u_i are in $\{0, \ldots, p-1\}$ with $u_k \neq 0$. If $\mathrm{ord}_p(x) \geq 0$ 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 $\mathrm{ord}_p(x) = 0$. 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

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

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

2.3 p-adic logarithms

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

1. $\log_p(xy) = \log_p(x) + \log_p(y)$ whenever $\mathrm{ord}_p(x-1) > 0$ and $\mathrm{ord}_p(y-1) > 0$.
2. $\log_p(z^k) = k \log(p)$ whenever $\mathrm{ord}_p(z-1) > 0$ and $k \in \mathbb{Z}$.
3. $\mathrm{ord}_p(\log_p(z)) = \mathrm{ord}_p(z-1)$ whenever $\mathrm{ord}_p(z-1) > 1/(p-1)$.

Proofs of the first and last property can be found in [Ha] (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

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

proofs and what e,f are?

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 $\log_p$ references here.

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 $\text{char}(K) \neq 2, 3$. 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 $a_1a_4 - a_2a_3 = \pm 1$. 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 $B_1U = B_2$. 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

introduction

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 $i = 1, \ldots, v$.

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 Tzanakis, de Weger, Hambrook, 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

$$N_{K/\mathbb{Q}}(x - y\theta) = cp_1^{z_1} \dots p_v^{z_v}. \tag{3.4}$$

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, de Weger ref and Hambrook here and instead apply the following results of cite new paper

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. *[Siksek] 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*

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

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

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

Lemma 3.3.2. *[Siksek] 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*

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

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

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

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

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

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

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

By assumption,

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

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

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

and

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

(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

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

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 $i = 1, 2, 3, \ldots$. 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 $\mathrm{ord}_{\mathfrak{p}}(u_i - \theta) \geq t_i \cdot e(\mathfrak{p}|p)$ 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 $p \in \{p_1, \ldots, p_v\}$ and let $\mathcal{L}_p$, $\mathcal{M}_p$ be as given by Algorithm 3.3.3. Let $(x, y, z_1, \ldots, z_v)$ 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

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

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 $\mathrm{ord}_{\mathfrak{q}}(1 - u_i\theta) \geq t_i \cdot e(\mathfrak{q}|p)$ and thus $1 - \alpha\theta = 0$ in $K_{\mathfrak{q}}$. But as $p \mid u_0$, we have $\mathrm{ord}_p(\alpha) \geq 1$, and so $\mathrm{ord}_{\mathfrak{q}}(\theta) < 0$. 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 $\mathrm{ord}_{\mathfrak{q}}(x) = 0$ and $\mathrm{ord}_{\mathfrak{q}}(x - y\theta) = \mathrm{ord}_{\mathfrak{q}}(1 - (y/x)\theta)$ 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, deWeger and used in Hambrook 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. In particular, we outline some examples in the following table.

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.

- After the above two refinements, we reduced the redundancy in the sets M_p and L_p similar to Kyle Hambrook's redundancy removal.

Add test examples, restructure subsection, table format?

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

- for $i \in \{1, \ldots, \nu\}$, $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_K$ arising from Algorithm 3.3.3 and Algorithm 3.3.6 applied to $p \in \{p_1, \ldots, p_v\}$, such that $(\mathfrak{b}, \mathfrak{p}_i) \in M_p$ for some ideal $\mathfrak{b}$;

- for $i \in \{\nu + 1, \ldots, v\}$, 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 $\mathfrak{p}_1, \ldots, \mathfrak{p}_\nu$, 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 $i_0, j, k \in \{1, \ldots, n\}$ (should this be ν?) 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 $(x, y, z_1, \ldots, z_v)$ has been reduced to solving finitely many equations of the form (3.11) for the variables $(x, y, n_1, \ldots, n_\nu, a_1, \ldots, a_r)$.

3.4.4 Computational remarks and comparisons

In Section 3.4.1, we follow closely the method of Tzanakis, de Weger 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 $i = 1, \ldots, \nu$. 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 $\mathbf{r} = (r_1, \ldots, r_\nu)$ 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. table with numbers

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. table with numbers

However, when generating the vectors $\mathbf{r} = (r_1, \ldots, r_\nu)$ 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. This in itself may present its own problems can't remember why though.

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. table. 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 formatting of 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 $p \in \{p_1, \ldots, p_\nu\}$ and study the p-adic valuations of the numbers appearing in (3.11). In particular, for $l \in \{1, \ldots, \nu\}$, 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 $p_l \in \{p_1, \ldots, p_\nu\}$ 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 tzanakis [**?**] tells us that $\frac{\varepsilon_1^{(i_0)}}{\varepsilon_1^{(j)}}, \ldots, \frac{\varepsilon_r^{(i_0)}}{\varepsilon_r^{(j)}}$ and $\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}, \ldots, \frac{\varepsilon_r^{(k)}}{\varepsilon_r^{(j)}}$ 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 $\mathbf{a_i} = (a_{1i}, \ldots, a_{\nu i})$ 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 [**?**] ref.

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 [**?**] 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,

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

□

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

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

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 δ_1, $\frac{\gamma_1^{(k)}}{\gamma_1^{(j)}},\dots,\frac{\gamma_\nu^{(k)}}{\gamma_\nu^{(j)}}$, and $\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}},\dots,\frac{\varepsilon_r^{(k)}}{\varepsilon_r^{(j)}}$. Since finite p_l-adic fields are complete, $\alpha_i \in L$ for $i = 1,\dots,1+\nu+r$ 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 $i = 1,\dots,1+\nu+r$ 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 $h = 1,\dots,s$.

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

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

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

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

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

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

we have

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

for every $h \in \{1, \ldots, s\}$. □

Lemma 3.5.4. *If*

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

then

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

Proof. Immediate from Lemma 2.3.2. □

Lemma 3.5.5.

(i) If $\operatorname{ord}_{p_l}(\alpha_1) < \min\limits_{2\le i\le 1+\nu+r} \operatorname{ord}_{p_l}(\alpha_i)$*, 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 $h \in \{1, \dots, s\}$*, if* $\operatorname{ord}_{p_l}(\alpha_{1h}) < \min\limits_{2\le i\le 1+\nu+r} \operatorname{ord}_{p_l}(\alpha_{ih})$*, 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

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

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

$$\sum_{i=1}^{\nu} n_i a_{li} \ge \min_{2\le i\le 1+\nu+r} \operatorname{ord}_{p_l}(\alpha_i) - \operatorname{ord}_{p_l}(\delta_2).$$

Observe that

$$\begin{aligned} \operatorname{ord}_{p_l}(\alpha_1) &= \operatorname{ord}_{p_l}\left(\Lambda_l - \sum_{i=2}^{1+\nu+r} b_i \alpha_i \right) \\ &\ge \min\left\{ \operatorname{ord}_{p_l}(\Lambda_l), \min_{2\le i\le 1+\nu+r} \operatorname{ord}_{p_l}(b_i \alpha_i) \right\}. \end{aligned}$$

Therefore, it suffices to show that

$$\operatorname{ord}_{p_l}(\Lambda_l) \ge \min_{2\le i\le 1+\nu+r} \operatorname{ord}_{p_l}(b_i \alpha_i).$$

By Lemma 2.3.2, the first inequality implies $\mathrm{ord}_{p_l}(\Lambda_l) = \sum_{i=1}^{\nu} n_i a_{li} + \mathrm{ord}_{p_l}(\delta_2)$, from which the result follows.

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

□

3.6 Lattice-Based Reduction

references for this are the two books living in the $x + y = z$ folder on the desktop

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 **??** 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. These are algorithms which have many important applications in a variety of mathematical fields, including factorization of polynomials, public-key cryptography, and the disproof of the Mertens Conjecture references from de Weger.

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 $\mathbb{R}^n$,

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

is this too much notation? should I stick to jsut using Φ?

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 (ref: LLL). 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 typeset for Magma, including de Weger's exact integer version. (ref).

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*

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

refs of where this lemma can be found - Cohen, for 1; see Hambrook p49 bottom of Lemma 18.1 Note that the assumption in Lemma 4.5.8 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 (ref: p49 of Hambrook). A version of this algorithm with some improvements due to Stehlé is implemented in Magma format. 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 Fincke-Pohst paper that if we label the columns of R by $\mathbf{r}_i$ and the rows of R^{-1} by $\mathbf{r}'_i$, then

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

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 (text). Unfortunately, this implementation does not support *translated* lattices, a variant of the Fincke-Pohst algorithm which we will need in **??**. 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 (format) 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 (format) 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. table of large numbers of short vectors found?

Chapter 4

Goormaghtigh Equations

introduction

More than a century ago, Ratat [**?**] and Goormaghtigh [**?**] 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*

$$\frac{x^m-1}{x-1} = \frac{y^n-1}{y-1}, \quad y > x > 1, \ m > n > 2. \tag{4.1}$$

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

$$x^m - y^n = 1, \quad x, y, m, n > 1, \tag{4.2}$$

and Nagell-Ljunggren

$$\frac{x^m-1}{x-1} = y^n, \quad x, y, n > 1, \ m > 2. \tag{4.3}$$

In a certain sense, however, equation (4.1) appears to be rather harder to treat than (4.2) or (4.3). Techniques from Diophantine approximation (specifically, bounds for linear forms in complex and p-adic logarithms) have been applied by Tijdeman [**?**] to show that equation (4.2) has at most finitely many solutions in the four variables x, y, m and n (a result subsequently sharpened by Mihăilescu [**?**] via a different method to solve (4.2) completely). Similarly, Shorey and Tijdeman [**?**] showed that equation (4.3) 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 [**?**] and Ljunggren [**?**]). In the case of equation (4.1), 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 [**?**] 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 [**?**]) or from bounds upon linear forms in logarithms (see e.g. Nesterenko and Shorey [**?**], and Bugeaud and Shorey [**?**]), we require constraints upon m and n, that either $m = n + 1$, or that

$$\gcd(m - 1, n - 1) = d > 1. \tag{4.4}$$

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 [**?**] shows that equation (4.1) has at most finitely many solutions if we fix only the set of prime divisors of x and y, while Bugeaud and Shorey [**?**] prove an analogous finiteness result, under the additional assumption of (4.4), provided the quotient $(m - 1)/(n - 1)$ is bounded above. Additional results on special cases of equation (4.1) are available in, for example, [**?**], [**?**], [**?**] and [**?**]. An excellent overview of results on this problem can be found in the survey of Shorey [**?**].

In this paper, we prove that, in fact, under assumption (4.4), equation (4.1) 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 (4.1),*

satisfying (4.4), then

$$x < (3d)^{4n/d} \leq 36^n. \tag{4.5}$$

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 (4.5), in conjunction with, for example, work of Baker [**?**]. The constants present in our upper bound (4.5) 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 (4.1), subject to condition (4.4), for small fixed values of n.

Theorem 4.0.2. *If there is a solution in integers x, y and m to equation (4.1), with $n \in \{3, 4, 5\}$ and satisfying (4.4), 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 [**?**]. 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 [**?**] (see also He [**?**]). The techniques employed in both [**?**] and [**?**], 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 (4.1) in earlier work of Bugeaud and Shorey [**?**]. 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 (4.1). 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 (4.1), 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.

4.1 Rational approximations

In what follows, we will always assume that x, y, m and n are integers satisfying (4.1) with (4.4), and write

$$m - 1 = dm_0 \quad \text{and} \quad n - 1 = dn_0. \tag{4.6}$$

We note, for future use, that an appeal to Théorème II of Karanicoloff [**?**] (which, in our notation, states that the only solution to (4.1) with $n_0 = 1$ and $m_0 = 2$ in (4.6) 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, [**?**] and [**?**], is the observation that the existence of a solution to (4.1) with (4.4) implies a number of unusually good rational approximations to certain irrational algebraic numbers. One such approximation arises from rewriting (4.1) as

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

whereby

$$\left| \sqrt[d]{\frac{y(x-1)}{x(y-1)}} - \frac{x^{m_0}}{y^{n_0}} \right| < \frac{1}{y^{dn_0}}. \tag{4.7}$$

The latter inequality was used, in conjunction with lower bounds for linear forms in logarithms (in [**?**]) and with machinery based upon Padé approximation to binomial functions (in [**?**]), to derive a number of strong restrictions upon x, y and d satisfying equation (4.1).

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 (4.7). 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 [**?**], [**?**].

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

$$x^{m_0} < y^{n_0} < \left(\frac{x}{x-1}\right)^{1/d} x^{m_0} \leq \sqrt{40/39}\,x^{m_0} < 1.013\,x^{m_0}. \tag{4.8}$$

We will rewrite (4.1) 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 [**?**], $A_k(d)$ 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 [**?**]).

We thus have

$$x^{dm_0} - \frac{(x-1)}{x} \left(\sum_{k=0}^{n_0} A_k(d) y^{n_0-k} \right)^d = \frac{1}{x} + \frac{x-1}{x} \sum_{j=0}^{(d-1)n_0-1} B_j(d) y^j \quad (4.9)$$

and so

$$0 < x^{dm_0} - \frac{(x-1)}{x} \left(\sum_{k=0}^{n_0} A_k(d) y^{n_0-k} \right)^d < \frac{(dn_0+1)(d+1)}{2(n_0+1)d^2} \frac{y}{y-1} y^{(d-1)n_0-1}. \quad (4.10)$$

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

$$0 < x^{dm_0} - \frac{(x-1)}{x} \left(\sum_{k=0}^{n_0} A_k(d) y^{n_0-k} \right)^d < 0.769\, y^{(d-1)n_0-1}. \quad (4.11)$$

Applying the Mean Value Theorem,

$$0 < x^{m_0} - \sqrt[d]{\frac{x-1}{x}} \sum_{k=0}^{n_0} A_k(d) y^{n_0-k} < 0.769 \frac{y^{(d-1)n_0-1}}{dY^{d-1}}, \quad (4.12)$$

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 (4.12) and the fact that $d \geq 2$ and $x \geq 40$,

$$0 < x^{m_0} - \sqrt[d]{\frac{x-1}{x}} \sum_{k=0}^{n_0} A_k(d) y^{n_0-k} < \frac{0.779}{dy}. \tag{4.13}$$

Let us define

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

where by $\text{ord}_p(z)$ 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

$$C(k,d) < \left(d \prod_{p|d} p^{1/(p-1)} \right)^k. \tag{4.14}$$

Further (see displayed equation (18) of Nesterenko and Shorey [**?**]), and critically for our purposes, $C(k,d)A_k(d)$ is an integer. Multiplying equation (4.9) by $C(n_0,d)$ and setting

$$P = C(n_0,d)\, x^{m_0} \quad \text{and} \quad Q = C(n_0,d) \sum_{k=0}^{n_0} A_k(d) y^{n_0-k}, \tag{4.15}$$

then P and Q are integers and, defining

$$\epsilon = P - \sqrt[d]{\frac{x-1}{x}} Q, \tag{4.16}$$

we thus have, from (4.13), that the following result holds.

Proposition 4.1.1. *Suppose that (x,y,m,n) is a solution in integers to equation*

(4.1), with (4.4) and $x \geq 40$. If we define ϵ via (4.16), then

$$0 < \epsilon < \frac{0.779\, C(n_0, d)}{dy}. \tag{4.17}$$

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 [**?**], [**?**].

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

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

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

$$P_{m_1,m_2}(z) = \sum_{k=0}^{m_1}\binom{m_2+1/d}{k}\binom{m_1+m_2-k}{m_2}z^k \tag{4.18}$$

and

$$Q_{m_1,m_2}(z) = \sum_{k=0}^{m_2}\binom{m_1-1/d}{k}\binom{m_1+m_2-k}{m_1}z^k. \tag{4.19}$$

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

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

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

$$Q_1 = x^{m_2} C(m_2, d) Q_{m_1,m_2}(-1/x), \tag{4.21}$$

it follows, from Lemma 3.1 of Chudnovsky [**?**], that C_0, P_1 and Q_1 are integers. Further, from (4.20),

$$|\delta| = \frac{\sin(\pi/d)\, C(m_2, d)}{\pi\, x^{m_1+1}} \int_0^1 \frac{v^{m_2+1/d}(1-v)^{m_1-1/d} dv}{(1-(1-v)/x)^{m_2+1}}. \tag{4.22}$$

Recall that P and Q are defined as in (4.15). Here and henceforth, we will assume that

$$m_2 - m_1 = m_0. \tag{4.23}$$

We have

Lemma 4.2.1. *If m_1 and m_2 are nonnegative integers satisfying (4.23), then it follows that $PQ_1 \neq C_0 P_1 Q$.*

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

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

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

and

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

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

$$\text{ord}_p\left(\frac{C_0 P_1 Q}{P Q_1}\right) = (m_0 - n_0)\,\text{ord}_p(d) + \text{ord}_p\left(\frac{m_2!}{m_1! n_0!}\right) > 0$$

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 $PQ_1 - C_0P_1Q$ is a nonzero integer multiple of $C(n_0, d)\,x^{m_0}$, so that, from the definitions of ϵ and δ,

$$|\epsilon Q_1 - \delta Q| = |PQ_1 - C_0P_1Q| \geq C(n_0, d)\,x^{m_0}. \tag{4.24}$$

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 (4.8),

$$Q < 1.039\,C(n_0, d)\,x^{m_0}. \tag{4.25}$$

Combining (4.8), (4.17), (4.24) and (4.25), we thus have

Proposition 4.2.2. *Suppose that (x, y, m, n) is a solution in integers to equation (4.1), with (4.4) and $x \geq 40$. If m_0, n_0 and d are defined as in (4.6), and m_1 and m_2 are nonnegative integers satisfying (4.23), then for Q_1 and $|\delta|$ as given in (4.21) and (4.22), we may conclude that*

$$|Q_1| > 1.28\,d\,(1 - 1.039|\delta|)\,x^{m_0+m_0/n_0}. \tag{4.26}$$

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 (4.22). Then

$$|Q_1| < \sqrt[d]{\frac{x}{x-1}} \left(\frac{(\alpha+1)^2}{\alpha} \left(e\left(\alpha+1\right)\right)^{m_1} x^{m_2} C(m_2,d) + |\delta| \right). \tag{4.27}$$

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

$$r(\alpha,u) = \frac{1}{2u}\left((\alpha+1) - (\alpha-1)u - \sqrt{((\alpha+1)-(\alpha-1)u)^2 - 4u} \right), \tag{4.28}$$

and

$$M(\alpha,x) = \frac{(1-r(\alpha,1/x)/x)^\alpha}{(1-r(\alpha,1/x))^\alpha r(\alpha,1/x)}. \tag{4.29}$$

Via the Mean Value Theorem,

$$\frac{1}{\alpha+1} < r(\alpha,1/x) < \frac{x}{(x-1)(\alpha+1)} \tag{4.30}$$

and so, from calculus,

$$M(\alpha,x) < \left(\frac{(x-1)\,(\alpha+1)-1}{(x-1)(\alpha+1)-x} \right)^\alpha \cdot (\alpha+1) < e\,(\alpha+1) \tag{4.31}$$

and

$$M(\alpha,x) > \left(1 + \frac{x-1}{x\alpha}\right)^\alpha \left(\frac{x-1}{x}\right)\ (\alpha+1). \tag{4.32}$$

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

$$|C_0 P_1| \leq \frac{(1-r(\alpha,1/x)/x)^{1/d}}{r(\alpha,1/x)(1-r(\alpha,1/x))}\, M(\alpha,x)^{m_1} x^{m_2} C(m_2,d),$$

whereby inequalities (4.30) and (4.31) imply that

$$|C_0 P_1| < \frac{(\alpha+1)^2}{\alpha} \left(e\,(\alpha+1)\right)^{m_1} x^{m_2}\, C(m_2, d).$$

Since $C_0 P_1 = \sqrt[d]{\frac{x-1}{x}}\, Q_1 + \delta$, we conclude as desired. □

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

$$x^{m_2} \left|Q_{m_1,m_2}(-1/x)\right| = \left| \sum_{k=0}^{m_2} \binom{m_1 - 1/d}{k} \binom{m_1 + m_2 - k}{m_1} (-1)^k x^{m_2-k} \right|. \tag{4.33}$$

Defining

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

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

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

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

$$0 < f(k+1)/f(k) < \frac{(m_1 - k)(m_2 - k)}{(k+1)(m_1 + m_2 - k)} \leq \frac{m_1 m_2}{m_1 + m_2}. \tag{4.34}$$

If instead $k \geq m_1$,

$$\frac{(m_1 - k - 1)(m_2 - k)}{(k+1)(m_1 + m_2 - k)} < f(k+1)/f(k) < 0. \tag{4.35}$$

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

$$m_1 = \left[\frac{m_0}{2n_0}\right] \quad \text{and} \quad m_2 = m_0 + \left[\frac{m_0}{2n_0}\right], \tag{4.36}$$

for m_0, n_0 and d as given in (4.6). 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 (4.22) 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 [**?**], 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 (4.22),

$$|\delta| < \frac{\sin(\pi/d)\, C(m_2,d)}{\pi\, x^{m_1+1}} \leq \frac{C(m_2,d)}{\pi\, x^{m_1+1}}. \tag{4.37}$$

From (4.36), $m_1 + 1 > \frac{m_0}{2n_0}$ 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,

$$|Q_1| > 1.25\, d\, x^{m_0+m_0/n_0}. \tag{4.38}$$

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 (4.38) 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 (4.38), $d \geq 2$ 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

$$9d^2 < (1 + m_0/m_1)^{1/m_0}\, C(m_0 + m_1, d)^{1/m_0}\, (e\,(2 + m_0/m_1))^{m_1/m_0}. \quad (4.39)$$

If $d = 2$, Proposition 4.1.2 yields

$$36 < (1 + m_0/m_1)^{1/m_0}\, 4^{1+m_1/m_0}\, (e\,(2 + m_0/m_1))^{m_1/m_0}, \quad (4.40)$$

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

If $d \geq 3$, (4.39) 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

$$2.744 < \frac{9\sqrt{d}}{2\sqrt{2}(\log d)^{3/2}} < (1 + m_0/m_1)^{1/m_0}\, (e\,(2 + m_0/m_1))^{m_1/m_0}. \quad (4.41)$$

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 (4.41), 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 (4.14) and (4.39),

$$9d^2 < (1 + m_0/m_1)^{1/m_0} \left(d \prod_{p|d} p^{1/(p-1)} \right)^{1+m_1/m_0} (e\,(2 + m_0/m_1))^{m_1/m_0}. \quad (4.42)$$

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 (4.42) 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, (4.38) 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 (4.38), 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. $n = 3,\ d = 2,\ n_0 = 1,\ 2 \le x \le 46655,$
2. $n = 4,\ d = 3,\ n_0 = 1,\ 2 \le x \le 122826,$
3. $n = 5,\ d = 2,\ n_0 = 2,\ 2 \le x \le 60466175,$
4. $n = 5,\ d = 4,\ n_0 = 1,\ 2 \le x \le 248831.$

Initially, we will suppose that $x \ge 40$ and, in all cases, that m_1 and m_2 are nonnegative integers satisfying (4.23). 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 (4.22) 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 (4.22), it thus follows that

$$|\delta| < \frac{\sin(\pi/d)\, C(m_2, d)}{\pi\, x^{m_1+1}}\, M(\alpha, x)^{1/d-m_1}. \tag{4.43}$$

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

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 (4.43) 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 (4.32), 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 (4.31),

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

We may therefore apply Proposition 4.2.2 to conclude that

$$|Q_1| > 2.477\, x^{2m_0}. \tag{4.44}$$

From (4.27), 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

$$x < \left(2.75 \cdot 14.951^{m_1}\, 4^{m_0+m_1}\right)^{\frac{1}{m_0-m_1}}. \tag{4.45}$$

We may check that $m_0 > 3.4 m_1$ (so that $\alpha > 4.4$) whenever $m_0 \geq 96$ and hence, since the right hand side of (4.45) 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 (4.44) 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 (4.1). If $m_0 = 4$ (so that $m = 9$) and $40 \leq x \leq 108$, there are, similarly, no solutions to (4.1) 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 (4.43) 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 (4.32), $x \geq 85$ 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

$$|Q_1| > 3.808\, x^{2m_0} \tag{4.46}$$

while (4.27), 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

$$x < \left(1.707 \cdot 14.217^{m_1} \, (3\sqrt{3})^{m_0+m_1}\right)^{\frac{1}{m_0-m_1}}. \tag{4.47}$$

We may check that $m_0 \geq 3.14m_1$, 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, (4.46) 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 (4.1). 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 (4.1).

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 (4.43) 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 (4.32), 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 (4.31),

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

We may therefore apply Proposition 4.2.2 to conclude that

$$|Q_1| > 2.552\, x^{\frac{3}{2} m_0}. \tag{4.48}$$

On the other hand, from (4.27), 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 $m_0 > 5.809 m_1$ (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 $m_0 \leq 331$,

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

and hence Proposition 4.2.4, (4.48) 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 (4.1).

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 (4.43) 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 (4.32), 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 (4.31),

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

We may therefore apply Proposition 4.2.2 to conclude that

$$|Q_1| > 5.109\, x^{2m_0}. \tag{4.49}$$

On the other hand, from (4.27), 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 $m_0 \geq 2.87 m_1$ (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, (4.49) 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 (4.1) (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 (4.1) with $2 \leq x \leq 39$. In this case, (4.1) becomes

$$y^2 + y + 1 = \frac{x^m - 1}{x - 1}, \tag{4.50}$$

whereby

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

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

$$Y^2 = X^3 - k, \tag{4.51}$$

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 (4.51) for the values of k arising from $2 \leq x \leq 39$ and $0 \leq \delta \leq 2$ rather quickly using Magma's *IntegralPoints* routine (see [**?**]). 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

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

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 (4.50), 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 (4.1) 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 (4.1) 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 (4.1) with $n = 4$.

4.5 Small values of x for $n = 5$

In case $n = 5$, solving equation (4.1) 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 (4.1) as

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

so that

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

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

$$Y^2 = (x^2 - x)\left(y^4 + y^3 + y^2 + y\right) + x^2; \tag{4.52}$$

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 (4.52) 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 (4.52) 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 formatIntegralQuarticPoints 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 (4.1) as

$$F_x(y, 1) = x^m, \tag{4.53}$$

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 (4.53) 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 (4.53) becomes

$$F_x(y, 1) = p_1^{Z_1} \dots p_v^{Z_v} \tag{4.54}$$

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.

(use algorhtms of Ch 3, but we point out the important differences)

4.5.1 First steps and small bounds

Following arguments of Chapter 3 for solving Thue-Mahler equations, put $S = \{p_1, \ldots, p_v\}$. 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 (4.54) 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

$$g(t) = (x-1)^3 F\left(\frac{t}{x-1}\right) = t^4 + (x-1)t^3 + (x-1)^2t^2 + (x-1)^3t + x(x-1)^3.$$

Note that $g(t)$ is irreducible in $\mathbb{Z}[t]$. Writing $K = \mathbb{Q}(\theta)$ with $g(\theta) = 0$, it follows that (4.54) is equivalent to

$$N_{K/\mathbb{Q}}((x-1)y - \theta) = (x-1)^3 p_1^{Z_1} \ldots p_v^{Z_v}. \tag{4.55}$$

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 (4.55) leads to finitely many ideal equations of the form

$$((x-1)y - \theta)\mathcal{O}_K = \mathfrak{a} \prod_{j=1}^{m_1} \mathfrak{p}_{1j}^{z_{1j}} \cdots \prod_{j=1}^{m_v} \mathfrak{p}_{vj}^{z_{vj}} \tag{4.56}$$

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

$$((x-1)y - \theta)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{u_1} \cdots \mathfrak{p}_v^{u_v} \tag{4.57}$$

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 [**?**] tzanakis de weger and [**?**]chapter 3, 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 Mathematica (format and cite) 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 (4.57) 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

$$(x-1)y - \theta = \alpha\zeta\varepsilon_1^{a_1}\gamma_1^{n_1}\cdots\gamma_v^{n_v} \tag{4.58}$$

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

$$(x-1)^3 \cdot p_1^{t_1+r_1}\cdots p_v^{t_v+r_v}, \tag{4.59}$$

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 (4.54) is now reduced to the problem of solving finitely many equations of the form (4.59) 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

$$\lambda = \delta_1 \left(\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}\right)^{a_1} \prod_{i=1}^{v} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i} - 1 = \delta_2 \left(\frac{\varepsilon_1^{(i_0)}}{\varepsilon_1^{(j)}}\right)^{a_1} \prod_{i=1}^{v} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i}, \quad (4.60)$$

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

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

and

$$b_{v+2} = a_1.$$

Put

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

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 $i = 1, \dots, v$), and $\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(l)}}$. Since finite p-adic fields are complete, $\alpha_i \in L$ for $i = 1, \dots, v+2$ 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 $i = 1, \dots, v+2$ write

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

Then

$$\Lambda_l = \sum_{h=1}^{s} \Lambda_{lh} \phi^{h-1}, \tag{4.61}$$

with

$$\Lambda_{lh} = \sum_{i=1}^{v+2} b_i \alpha_{ih}$$

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

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*

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

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 $\operatorname{ord}_{p_l}(\alpha_1) < \min\limits_{2 \le i \le v+2} \operatorname{ord}_{p_l}(\alpha_i)$*, 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 $h \in \{1, \ldots, s\}$*, if* $\operatorname{ord}_{p_l}(\alpha_{1h}) < \min\limits_{2 \le i \le v+2} \operatorname{ord}_{p_l}(\alpha_{ih})$*, 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

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

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 $l \in \{1, \ldots, v\}$ 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 [**?**], 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, (4.60). 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 [**?**] requires the computation of the absolute logarithmic height of each algebraic number in the product of (4.60). 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 [**?**] 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 [**?**], we now describe this bound.

Arguing as in [**?**], 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, [**?**] 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 [**?**] $R_T \leq R_K h_K (4\log^* P)^{4v}$. 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 [**?**], namely

$$R_K < \frac{|\text{Disc}(K)|^{1/2}(\log|\text{Disc}(K)|)^3}{3! h_K}.$$

Now we have all of the components necessary to explicitly compute an upper bound on C_8, denoted C_9 in [**?**], 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 (4.59), 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 [**?**] but differs substantially in order to accommodate our new S-unit equation, which, unlike in [**?**], 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

$$C_{13} = \sum_{j=1}^{v} \max_{1\le i\le 4} |\log|\gamma_j^{(i)}||$$

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

$$C_{14} = \min\left(|\log|\varepsilon_1^{(1)}||, |\log|\varepsilon_1^{(2)}||\right) = |\log|\varepsilon_1^{(k)}||.$$

By (4.55),

$$|\beta^{(k)}| \cdot \prod_{i\ne k} |\beta^{(i)}| = (x-1)^3 \cdot p_1^{Z_1} \cdots p_v^{Z_v},$$

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 [**?**], we reduce the above bound considerably by applying the LLL-algorithm to approximation lattices associated to the linear forms in logarithms obtained from (4.60).

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 **??** (need title) 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 [**?**], our

brute force search simply checks for solutions of (4.53) 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 **??** name, 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

$$\mathrm{ord}_{p_l}(\alpha_{\hat{i}h}) = \min_{2 \le i \le v+2}(\alpha_{ih}),$$

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*

$$\sum_{i=1}^{v} n_i a_{li} > \frac{1}{p_l - 1} - \mathrm{ord}_{p_l}(\delta_2).$$

In the special case, we have

$$\mathrm{ord}_{p_l}(\Lambda'_l) = \sum_{i=1}^{v} n_i a_{li} + d_l$$

with

$$d_l = \mathrm{ord}_{p_l}(\delta_2) - \mathrm{ord}_{p_l}(\alpha_{\hat{i}}).$$

In the general case we have

$$\mathrm{ord}_{p_l}(\Lambda'_l) \ge \sum_{i=1}^{v} n_i a_{li} + d_l$$

with

$$d_l = \mathrm{ord}_{p_l}(\delta_2) - \frac{1}{2}\,\mathrm{ord}_{p_l}(\mathit{Disc}(G(t))) - \mathrm{ord}_{p_l}(\alpha_{\hat{i}h}).$$

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 4.5.7,

$$\mathrm{ord}_{p_l}\left(\sum_{i=1}^{v+2} b_i(-\beta_i) \right) = \mathrm{ord}_{p_l}(\Lambda_l') \geq \sum_{i=1}^{v} n_i a_{li} + d_l \geq \mu.$$

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 (4.14), 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 $d \leq d_0 = 10^5$.

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

$$\sum_{p|d} \frac{\log p}{p-1} \leq \sum_{p \leq p_{\omega(d)}} \frac{\log p}{p-1}, \tag{4.62}$$

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 [**?**] 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

$$\sum_{p<x}\frac{\log p}{p} < \log x - 1.33258 + \frac{1}{2\log x}, \tag{4.63}$$

for all $x \geq 319$. Also, if $j \geq 2$,

$$\int_k^\infty \frac{\log u}{u^j}du = \frac{(j-1)\log(k)+1}{(j-1)^2 k^{j-1}}. \tag{4.64}$$

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

$$\sum_{p<x}\frac{\log p}{p^j} < \sum_{p<10^6}\frac{\log p}{p^j} + \frac{(j-1)\log(10^6)+1}{(j-1)^2 10^{6(j-1)}}. \tag{4.65}$$

By explicit computation, from (4.65), we find that

$$\sum_{j=2}^{10}\sum_{p<x}\frac{\log p}{p^j} < 0.755, \tag{4.66}$$

while, from (4.64),

$$\sum_{j\geq 11}\sum_{p<x}\frac{\log p}{p^j} < \sum_{j\geq 11}\frac{(j-1)\log(2)+1}{(j-1)^2 2^{j-1}} < \sum_{j\geq 11}\frac{1}{(j-1)2^{j-1}}. \tag{4.67}$$

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 (4.63), 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

$$\sum_{p|d}\frac{\log p}{p-1} < \log\log d.$$

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 (4.1), subject to condition (4.4), 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 (4.1), 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 (4.4). This result was obtained earlier as Corollary 4.1 of Yuan [**?**], though the statement there overlooks the solutions $(x, y, m, n) = (-2, 6, 7, 3), (2, -6, 5, 3)$ and $(2, -91, 13, 3)$.

Appendix A

Supporting Materials

This would be any supporting material not central to the dissertation. For example:

- additional details of methodology and/or data;
- diagrams of specialized equipment developed.;
- copies of questionnaires and survey instruments.