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 $f(x_1, \dots, x_n)$ be a polynomial with integer coefficients. We wish to study the set of solutions $(x_1, \dots, x_n) \in \mathbb{Z}^n$ to the equation

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

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 algebraic 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*

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

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

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

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

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

In the 1950's and 1960's, Taniyama and Weil asked whether all elliptic curves over $\mathbb{Q}$ of a given conductor N are related to modular functions. While this conjecture is now known as the Modularity Theorem, until its proof in 2001 [**?**], attempts to verify it sparked a large effort to tabulate all elliptic curves over $\mathbb{Q}$ of given conductor N. In 1966, Ogg ([**?**], [**?**]) determined all elliptic curves defined over $\mathbb{Q}$ with conductor of the form 2^a. Coghlan, in his dissertation [**?**], studied the curves of conductor $2^a 3^b$ 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 $p_1, \dots, p_v$. 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 $p_1, \dots, p_v$ 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

Chapter 2

Preliminaries

1. algebraic number theory background [edited once] Section 2.1.
2. p-adics valuations [edited once] Section 2.2
3. p-adic logs [edited once] Section 2.3
4. Weil height [edited once] Section 2.4
5. Elliptic curves [DONE - rough]

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. The number of classes 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 $N_{K/\mathbb{Q}}(\mathfrak{a}) = \#\left(\mathcal{O}_K/\mathfrak{a}\right)$. 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 $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$ 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 $\operatorname{ord}_{\mathfrak{p}}(\alpha)$ for $\operatorname{ord}_{\mathfrak{p}}((\alpha)\mathcal{O}_K)$. Every prime ideal defines a discrete non-Archimedean valuation on K via

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

and we have

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

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

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

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

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

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

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

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

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

E can be written as

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

Associated to this curve are the quantities

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

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

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

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

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

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

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

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

2.6 Cubic forms

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

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

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

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

for all x, y, where $a_1a_4 - a_2a_3 = \pm 1$. 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

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

Chapter 3

Algorithms for Thue-Mahler Equations

1. First Steps Section 3.1
2. rel number field Section 3.2
3. Lattices **??**
4. Setup with Lemmata from Samir
5. LLL [DONE - roughly]
6. Fincke-Pohst with changes from Benjamin [DONE- roughly]
7. linear forms in logs

3.1 First steps

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

$$F(X,Y) = c_0X^n + c_1X^{n-1}Y + \cdots + c_{n-1}XY^{n-1} + c_nY^n$$

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

$$F(X, Y) = cp_1^{Z_1} \cdots p_v^{Z_v} \tag{3.1}$$

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

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

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

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

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

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

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 $i \in \{1, \ldots, v\}$.

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 $(x, y, z_1, \dots, z_v)$ 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 $u \in \{0, 1, 2, \dots, p^t - 1\}$. If $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_K$ lying over p, then*

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

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 (a) 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 (b) Let

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

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

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

and

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

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

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

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

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

(iii) Else

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

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

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

and return to Step (b). 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 $\operatorname{ord}_{\mathfrak{p}}(u_i - \theta) \geq t_i \cdot e(\mathfrak{p}|p)$ infinitely often. However, the sequence $\{u_i\}_{i=1}^{\infty}$ converges to some $\alpha \in \mathbb{Z}_p$ so that $\alpha = \theta$ in $\mathcal{O}_{\mathfrak{p}}$. 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

$$t_0 = 1, \qquad \mathcal{U}_0 = \{w \ : \ w \in \{0, 1, \ldots, p-1\}\}.$$

These are 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 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 (i) or (ii). Write $u = u_i$ and $t = t_i$ for $x/y \equiv u \pmod{p^t}$. By Lemma 3.3.1, we have $\mathfrak{b}_u \mid (x - y\theta)\mathcal{O}_K$. Moreover, by that lemma and the definition of $\mathcal{P}_u$, if $\mathfrak{q} \notin \mathcal{P}_u$ 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 $\mathcal{L}_p$. By the above remarks, we know that (3.6) is satisfied, proving the lemma in this case.

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 $g(t)$ satisfying $\alpha \equiv u \pmod{p^t}$. The algorithm adds $(\mathfrak{b}_u, \mathfrak{p})$ to the set $\mathcal{M}_p$, and by the above, $(x - y\theta)\mathcal{O}_K/\mathfrak{b}_u$ is an integral ideal, not divisible by any prime $\mathfrak{q} \mid p$, $\mathfrak{q} \neq \mathfrak{p}$. Thus there is some positive $v_p \geq 0$ such that (**??**) is satisfied, proving the lemma in this case. □

Algorithm 3.3.6. To compute L_p and M_p.

Step (a) 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 **??**.

Step (b) Let

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

Step (c) Let

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

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

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

and

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

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

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

(iii) Else

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

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

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

and return to Step (c). 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 $t_i = t_0 + i$.

Then there is an infinite sequence $\{u_i\}$ such that $u_{i+1} \equiv u_i \pmod{t_i}$ and so that $\mathcal{P}_{u_i} \neq \emptyset$. Moreover, $p \mid u_0$. Let α be the limit of $\{u_i\}$ in $\mathbb{Z}_p$. By the pigeon-hole principle there is some $\mathfrak{q} \mid p$ appearing in infinitely many $\mathcal{P}_{u_i}$, and so $\mathrm{ord}_{\mathfrak{q}}(1 - u_i\theta) \geq t_i \cdot e(\mathfrak{q}/p)$. 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 does terminate. $\square$

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

- *either there is some $\mathfrak{b} \in \mathcal{L}_p$ such that* (**??**) *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* (**??**) *is satisfied.*

Proof. Now let (x, y) be a solution to (**??**). In view of Lemma **??** we may suppose $p \mid y$. Then $\mathrm{ord}_{\mathfrak{q}}(x - y\theta) = \mathrm{ord}_{\mathfrak{q}}(1 - y/x\theta)$. The rest of the proof is similar to the proof of Lemma **??**. $\square$

3.3.1 Refinements

- If some $\mathfrak{b}$ is contained L_p, and some $(\mathfrak{b}', \mathfrak{p})$ is contained 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 and the conclusion to Lemma 3.3.8 continues to hold.
- If some $(\mathfrak{b}, \mathfrak{p})$, $(\mathfrak{b}', \mathfrak{p})$ are contained 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 and the conclusion to Lemma 3.3.8 continues to hold.
- After the above two refinements, we reduced the redundancy in the sets M_p and L_p similar to Kyle Hambrook's redundancy removal.

3.4 Factorization of the Thue-Mahler Equation

Let

$$g(t) = g_{i1}(t) \cdots g_{im}(t)$$

be the decomposition of $g(t)$ into irreducible polynomials $g_{ij}(t) \in \mathbb{Q}_{p_i}[t]$. The prime ideals in K dividing p_i are in one-to-one correspondence with $g_{i1}(t), \ldots, g_{im}(t)$, and in particular, $\deg(g_{ij}(t)) = e_{ij} f_{ij}$.

After applying Algorithm **??** and Algorithm 3.3.6, we are reduced to solving finitely many 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

- $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_K$ arising from Algorithm **??** and Algorithm 3.3.6 applied to $p_i \in \{p_1, \ldots, p_v\}$, such that $(\mathfrak{b}_\mathfrak{i}, \mathfrak{p}_i) \in M_{p_i}$ for some ideal $\mathfrak{b}_i$.
- $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ of norm $|c| \cdot p_1^{t_1} \cdots p_v^{t_v}$ such that $u_i + t_i = z_i$. Note that if $M_{p_i} = \emptyset$ for some i (necessarily $i \in \{\nu + 1, \ldots, v\}$) we take $u_i = 0$.

For each choice of $\mathfrak{a}$ and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_\nu$, we reduce this equation to a number of so-called "S-unit equations". In the worst case scenario, the method in Tzanakis-de Weger reduces this to h^v such equations, where h is the class number of K. The method of Siksek, described below, gives only $m/2$ S-unit equations, where m is the number of roots of unity in K (typically this means only one S-unit equation).

Let

$$\phi : \mathbb{Z}^v \to \mathrm{Cl}(K), \qquad (n_1, \ldots, n_\nu) \mapsto [\mathfrak{p}_1]^{n_1} \cdots [\mathfrak{p}_\nu]^{n_\nu}.$$

We can compute the image and kernel of this map in `Magma`. Note that if (3.8) has a solution $\mathbf{u} = (u_1, \ldots, u_\nu)$ then, by (3.8),

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

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, and compute a preimage $\mathbf{r} = (r_1, \ldots, r_\nu)$ using `Magma`. Then $\mathbf{u} - \mathbf{r}$ 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 and let

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

where the $n_i \in \mathbb{Z}$. Here, we adopt the notation

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

and we let A be the matrix with columns $\mathbf{a}_1, \ldots, \mathbf{a}_\nu$. Hence the $(i,j)^{\text{th}}$ entry of A is a_{ij}, the i^{th} entry of the vector $\mathbf{a}_j$. Then $\mathbf{u} = A\mathbf{n} + \mathbf{r}$ 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

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

Then we can rewrite (3.8) as

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

Now

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

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

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

for some $\alpha \in K^*$. We note that some of the r_i might be negative so we don't expect α to be an algebraic integer in general. This can be problematic later in the algorithm when we compute the embedding of α into our p-adic fields. In those instances, the precision on our $\theta^{(i)}$ may not be high enough, and as a result, α may be mapped to 0. Increasing the precision is not ideal at this point, as it would require us to recompute a fair amount of data and so is computationally inefficient. Instead, we force the r_i to be positive by adding sufficiently many multiples of the class number. (Having already computed the class group, computing the class number is not costly.)

Now,

$$[\mathfrak{c}_j] = [\tilde{\mathfrak{p}}^{\mathbf{a}_j}] = \phi(\mathbf{a}_j) = [1]$$

as the $\mathbf{a}_j$ are a basis for the kernel of ϕ. Thus for all $j \in \{1, \ldots, \nu\}$, there are $\gamma_j \in K^*$ such that $\mathfrak{c}_j = \gamma_j \mathcal{O}_K$.

Thus we have rewritten (3.8) as

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

for unknown integers $(n_1, \ldots, n_\nu)$. Note that the number of cases has not increased. If $[\mathbf{a}]^{-1}$ is not in the image of ϕ then we have a contradiction. If $[\mathbf{a}]^{-1}$ is in the image of ϕ then we obtain one corresponding equation (3.9).

3.4.1 Refinements

In most cases, the method described above is far more efficient than that of Tzanakis-de Weger, however, computing the class group may still be a costly computation. For some values of x, it may happen that computing the class group will take longer than directly checking each potential ideal equation. This case arises when. In such cases, we proceed as follows.

For $i = 1, \ldots, \nu$ let h_i be the smallest positive integer for which $\mathfrak{p}_i^{h_i}$ is principal and let s_i be a positive integer satisfying $0 \leq s_i < h_i$. 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 diagonal matrix with h_i along the diagonal. For every possible combination of the s_i, we set $\mathbf{r} = (s_1, \ldots, s_\nu)$. 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 $\mathbf{n} = (n_1, \ldots, n_\nu)$.

Using the above notation, we write

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

Thus, we can write (3.8) as

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

Now, by definition of h_j, there exist $\gamma_j \in K^*$ such that

$$[\mathfrak{c}_j] = [\tilde{\mathfrak{p}}^{\mathbf{a}_j}] = \mathfrak{p}_j^{h_j} = \gamma_j \mathcal{O}_K.$$

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

Now, for each choice of $\mathbf{r}$, if $\mathbf{u}$ is a solution, we must necessarily have

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

Hence, we iterate through every possible $\mathbf{r}$, and store those cases for which this occurs.

At this point, regardless of which method was used to compute A and $\mathbf{r}$, we note that the ideal generated by α has norm

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

Now the n_i are related to the z_i via

$$z_i = u_i + t_i = \sum_{j=1}^{\nu} n_j a_{ij} + r_i + t_i.$$

Hence

$$Z_i = z_i - \mathrm{ord}_p(u) - \mathrm{ord}_p(a) = \sum_{j=1}^{\nu} n_j a_{ij} + r_i + t_i - \mathrm{ord}_p(u) - \mathrm{ord}_p(a)$$

Here, we note that $u_i = r_i = 0$ for all $i \in \{\nu + 1, \ldots, v\}$.

Fix a complete set of fundamental units of $\mathcal{O}_K : \varepsilon_1, \ldots, \varepsilon_r$. 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

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

with unknowns $a_i \in \mathbb{Z}$, $n_i \in \mathbb{Z}_{\geq 0}$, 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. Since K is a degree 3 extension of $\mathbb{Q}$, we either have 3 real embeddings of K into $\mathbb{C}$ (hence $s = 3$, $t = 0$ and $r = s + t - 1 = 3 + 0 - 1 = 2$), or there is one real embedding of K into $\mathbb{C}$ and a pair of complex conjugate embeddings of K into $\mathbb{C}$ (hence $s = 1$, $t = 1$, and $r = s + t - 1 = 1 + 1 - 1 = 1$). That is, we have either

$$x - y\theta = \alpha\zeta\varepsilon_1^{a_1} \cdot \gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu} \quad \text{or} \quad x - y\theta = \alpha\zeta\varepsilon_1^{a_1}\varepsilon_2^{a_2} \cdot \gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu} \tag{3.11}$$

To summarize, our original problem of solving (**??**) has been reduced to the problem of solving finitely many equations of the form (3.11) for the variables

$$x, y, a_1, n_1, \ldots, n_\nu \quad \text{or} \quad x, y, a_1, a_2, n_1, \ldots, n_\nu.$$

From here, we deduce a so-called S-unit equation. In doing so, we eliminate the variables x, y and set ourselves up to bound the exponents $a_1, n_1, \ldots, n_\nu$, respectively $a_1, a_2, n_1, \ldots, n_\nu$. We note here that generating the class group can be a timely computation. However, if we follow the method of Tzanakis-de Weger, we may be left with h^ν S-unit equations, all of which we would need to apply the principal ideal test to. That is to say, computing the class group is a faster operation than the alternative provided by Tzanakis-de Weger.

3.5 The S-Unit Equation

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 $\theta^{(1)}, \theta^{(2)}, \theta^{(3)}$. Let $i_0, j, k \in \{1, 2, 3\}$ 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

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

applying these embeddings to $\beta = x - y\theta$ yields

$$\lambda = \delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i} - 1 = \delta_2 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i}, \tag{3.12}$$

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 and $r = 1$ or $r = 2$.

Note that δ_1 and δ_2 are constants, in the sense that they do not rely on

$$x, y, a_1, \ldots, a_r, n_1, \ldots, n_\nu.$$

3.5.1 Lattices: LLL and the Fincke-Pohst algorithm

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

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

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

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

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

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 $a \in \mathbb{R}$.

In particular, given a basis we can define a specific bilinear form on our lattice Γ as part of its structure. In the case of integral lattices, we have $\Phi : \Gamma \times \Gamma \to \mathbb{Z}$. This form describes a kind of distance between elements $\mathbf{x}$ and $\mathbf{y}$ of the lattice defined by $\Phi(\mathbf{x}, \mathbf{y})$.

A *quadratic form* is a homogeneous polynomial of degree 2. A form Q is called positive definite if $Q(\mathbf{x})$ is strictly positive for any nonzero $\mathbf{x}$. A lattice is called *positive definite* if its quadratic form is positive definite.

A bilinear form has an associated quadratic form $Q : \Gamma \to \mathbb{Z}$ which is simply defined by $Q(\mathbf{x}) = \Phi(\mathbf{x}, \mathbf{x})$. The bilinear forms (and their associated quadratic forms) that we will be using come from the usual inner product on vectors in $\mathbb{R}^n$, also known as the dot product $\mathbf{u} \cdot \mathbf{v}$ for $\mathbf{u}, \mathbf{v} \in \Gamma$, and multiplication with the basis matrix for coordinate vectors. That is, if $\mathbf{u} = B\mathbf{x}$ and $\mathbf{v} = B\mathbf{y}$ for a basis B, we have $\Phi(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T B^T B\mathbf{y}$.

If $\mathbf{v} = B\mathbf{x}$, the *norm* of the vector $\mathbf{v} \in \Gamma$ is defined by the quadratic form. We will be using the inner product $\mathbf{v} \cdot \mathbf{v}$. The norm of the coordinate vector $\mathbf{x}$ is then

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

Notice that this is also $\mathbf{x}^T A\mathbf{x}$ where $B^T B = A$. Here, A is an example of the Gram matrix of Γ. The *Gram matrix* of a lattice with basis B with respect to a bilinear form Φ is defined to be the matrix A with entries $a_{ij} = \Phi(\mathbf{b}_i, \mathbf{b}_j)$.

The bilinear form on L can be written with respect to either embedded or coordinate vectors. Using another basis to express the lattice elements is possible, and sometimes preferable. But 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.

If A and B are invertible $n \times n$ real matrices, then the lattice generated by the columns of A is equal to the lattice generated by the columns of B if and only if there is a unimodular matrix U such that $AU = B$.

LLL Intro-ish: taken from Cohen p103 Among al1 the Z bases of a lattice L, some are better than others. The ones whose elements are the shortest (for the corresponding norm associated to the quadratic form q) are called reduced. Since the bases al1 have the same determinant, to be reduced implies also that a basis is not too far from being orthogonal. The notion of reduced basis is quite old, and in fact in some sense one can even define an optimal notion of reduced basis. The problem with this is that no really satisfactory algorithm is known to find such a basis in a reasonable time, except in dimension 2 (Algorithm 1.3.14), and quite recently in dimension 3 from the work of B. Valle [Val]. A real breakthrough came in 1982when A. K. Lenstra, H. W. Lenstra and L. Lovkz succeeded in giving a new notion of reduction (what is now called 2.6 Lattice Reduction Algorithms 85 LLL-reduction) and simultaneously a reduction algorithm which is determin- istic and polynomial time (see [LLL]).This has proved invaluable.

Let Γ be a lattice with $\mathbf{c}_1, \ldots, \mathbf{c}_n$. Define the vectors $\mathbf{c}_i^*$ for $i = 1, \ldots, n$ and real numbers μ_{ij} ($1 \leq j < i \leq n$) inductively by

$$\mathbf{c}_i^* = \mathbf{c}_i - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{c}_j^*, \quad \mu_{ij} = \frac{\langle \mathbf{c}_i, \mathbf{c}_j^* \rangle}{\langle \mathbf{c}_j, \mathbf{c}_j^* \rangle}$$

(This is just the Gram-Scmidt process). The basis $_1, \ldots, _n$ is called *LLL-reduced* it

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

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

These properties implies 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). The LLL algorithm takes as input an arbitrary basis for a lattice and outputs an LLL-reduced basis for the lattice. The algorithm is typically modified to additionally output a unimodular matrix U such that $B = AU$, where A is the matrix whose column-vectors are the input basis and B is the matrix whose column-vectors are the LLL-reduced output basis. Several versions of this algorirhm are implemented in MAGMA, including de Weger's exact integer version. (ref).

For Γ an n-dimensional lattice and $\mathbf{y}$ a vector in $\mathbb{R}^n$, we define

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

The most important property of an LLL-reduced basis for us is the following lemma.

Lemma 3.5.1. *lemma 18.1*

refs of where this lemma can be found - Cohen, for 1 Note that the assumption in lemma cite is equivalent to $\mathbf{y} \notin \Gamma$.

Cohen: We see that the vector bl in a reduced basis is, in a very precise sense, not too far from being the shortest non-zero vector of L. In fact, it often is the shortest, and when it is not, one can, most of the time, work with bl instead of the actual shortest vector. As has already been mentioned, what makes al1these notions and theorems so valuable is that there is a very simple and efficient algorithm to find a reduced basis in a lattice. We now describe this algorithm in its simplest form.

Fincke-Pohst

We show how to modify the Fincke-Pohst algorithm to output short vectors in a translated lattice. That is, we compute the set of vectors x such that

$$(x-c)^t B^t B(x-c) \leq C$$

where c is some vector over $\mathbb{Q}$ which represents the translation of our lattice.

We begin with the usual Fincke-Pohst method for

$$x^t B^t B x \leq C.$$

We call a vector $\mathbf{v}$ *small* if its norm $\Phi(\mathbf{v}, \mathbf{v})$ is less than a constant C. This clearly depends on the basis which is given, and can vary depending on the choice of basis. If a particular basis is not specified, it is assumed to be the matrix B which defines the Gram matrix $A = B^t B$. This is equivalent to solving the inequality $\Phi(\mathbf{y}, \mathbf{y}) \leq C$ where $\Phi(\mathbf{y}, \mathbf{y}) = \mathbf{y}^t \mathbf{y}$ denotes the norm of the vector computed with respect to the lattice. Let B denote the matrix whose columns are the basis vectors of the lattice $\mathcal{L}$. As an element of the lattice, $\mathbf{y} = B\mathbf{x}$ for some coordinate vector $\mathbf{x} \in \mathbb{Z}^n$. So our inequality becomes

$$\Phi(\mathbf{y}, \mathbf{y}) = \mathbf{y}^t \mathbf{y} = \mathbf{x}^t B^t B \mathbf{x} \leq C.$$

We consider the quadratic form $Q(\mathbf{x}) = \mathbf{x}^t B^t B \mathbf{x}$ and solve $Q(\mathbf{x}) \leq C$.

Quadratic Completion

To solve our inequality, it helps to first rearrange the terms of our quadratic form. This reformulation is called the quadratic completion or quadratic complementation. Here we assume the lattice is positive definite. That is, every nonzero element has a positive norm. With this, we can find the Cholesky decomposition $A = LL^t$, where L is a lower triangular matrix. Equivalently, we can express this as $A = R^t R$, where R is an upper triangular matrix. Since Fincke-Pohst uses upper triangular matrices, this is what we will use. The formulas below will reflect this. We now express Q as:

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

Our coefficients q_{ij} are defined from R and stored in a matrix for convenience.

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

Since R is upper triangular, the matrix $Q = [q_{ij}]$ will be as well.

To obtain the upper triangular matrix R from our matrix A, we compute the diagonal and non-diagonal entries as follows:

$$r_{ii} = \sqrt{a_{ii} - \sum_{k=1}^{i-1} r_{ki}^2}$$

$$r_{ij} = \frac{1}{r_{ii}} \left(a_{ij} - \sum_{k=1}^{j-1} r_{ki} r_{kj} \right) .$$

Using these, we can reformulate the construction of the coefficients of Q to use values from A. We will soon see how it is possible to do away with using the

Cholesky decomposition entirely.

$$q_{ii} = a_{ii} - \sum_{k=1}^{i-1} r_{ki}^2$$

$$q_{ij} = \frac{1}{r_{ii}^2}\left(a_{ij} - \sum_{k=1}^{j-1} r_{ki}r_{kj}\right).$$

By putting this construction in terms of the coefficients of Q only, we arrive at the following

$$q_{ii} = a_{ii} - \sum_{k=1}^{i-1} q_{ki}^2 q_{kk}$$

$$q_{ij} = \frac{1}{q_{ii}}\left(a_{ij} - \sum_{k=1}^{j-1} q_{ki}q_{kj}q_{kk}\right).$$

We can then calculate these coefficients, starting with q_{11} and calculating q_{1j} for $1 \leq j \leq m$. Then we continue by calculating q_{22} and q_{2j} for $2 \leq j \leq m$. We proceed by first always calculating the diagonal entry q_{ii} and then q_{ij} for $i \leq j \leq m$ until we reach q_{mm}. In practice, this is how we compute the coefficients for our form. However, it is equally possible to first compute the Cholesky Decomposition using available methods, and then computing the entries of Q from this. In fact, we do exactly this, by first computing the Cholesky decomposition.

The usual Fincke-Pohst way to bound x_i

Since the sum $Q(x)$ is less than C, the individual term $q_{mm}x_m^2$ must also be less than C.

$$\begin{aligned}\sum_{i=1}^{m} q_{ii}\left(x_i + \sum_{j=i+1}^{m} q_{ij}x_j\right)^2 &\leq C \\ q_{mm}x_m^2 &\leq C \\ x_m^2 &\leq \frac{C}{q_{mm}}.\end{aligned}$$

In fact, x_m is bounded above by $\sqrt{C/q_{mm}}$ and below by $-\sqrt{C/q_{mm}}$.

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.

$$\begin{aligned}
q_{mm}x_m^2 &\leq C \\
q_{m-1,m-1}\left(x_{m-1} + q_{m-1,m}x_m\right)^2 &\leq C - q_{mm}x_m^2 \\
q_{m-2,m-2}\left(x_{m-2} + \sum_{j=m-1}^{m} q_{m-2,j}x_j\right)^2 &\leq C - q_{mm}x_m^2 - q_{m-1,m-1}\left(x_{m-1} + q_{m-1,m}x_m\right)^2
\end{aligned}$$

Let

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

so that we can rewrite $Q(\mathbf{x})$ as

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

In general,

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

Let T_k denote the bound on the right-hand side. That is

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

so that $T_m = C$, $T_{m-1} = C - q_{mm}x_m^2$ and

$$T_{m-2} = C - q_{mm}x_m^2 - q_{m-1,m-1}\left(x_{m-1} + q_{m-1,m}x_m\right)^2.$$

We set T_m as C and find each subsequent T_k by subtracting the next term from the outer summand:

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

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

Now, we have an upper bound for each summand.

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

Using this, we can estimate upper and lower bounds for each x_k in the coordinate vector $\mathbf{x}$. We start by computing the last entries of $\mathbf{x}$ and their bounds first. Assuming that the last several entries of $\mathbf{x}$ have been assigned, upper and lower bounds on x_k can be determined. Now that we have established a bound on a term in the outer sum, we can determine bounds on the specific entry x_k. Take the above equation, and solve for x_k. Take the above equation and solve for x_k:

$$\begin{aligned}(x_k + U_k)^2 &\le T_k/q_{kk}\\ x_k + U_k &\le \sqrt{T_k/q_{kk}}\\ x_k &\le \sqrt{T_k/q_{kk}} - U_k.\end{aligned}$$

Similarly, we have a lower bound:

$$x_k \ge -\sqrt{T_k/q_{kk}} - U_k.$$

Since x_k must be an integer, we can restrict our bounds further. Let $t_k = \sqrt{T_k/q_{kk}}$.

$$UB_k = \lfloor t_k - U_k \rfloor$$

$$LB_k = \lceil -t_k - U_k \rceil$$

Here UB_k is the upper bound on x_k and LB_k is the lower bound on x_k.

$$LB_x \le x_k \le UB_k.$$

To enumerate all of the vectors $\mathbf{x}$ such that $Q(\mathbf{x}) \le C$, begin with the last entry

x_m (letting all other $x_j = 0$). Determine the upper and lower bounds UB_m and LB_m by first calculating $t_m = \sqrt{T_m/q_{mm}}$. We define $U_m = 0$, and by definition remember that $T_m = C$.

For each entry x_i, starting with x_m and going down to x_1, we initialize the value to be $x_i = LB_i$. After the value is initialized, we begin to increment the values of all the entries, adding 1 to each entry until we either reach the last index (in which case we have found a solution) or we exceed the upper bound on a particular entry (we will need to readjust the previously assigned entries). If at any time the lower bound exceeds the upper bound for a given entry, it will become immediately apparent when the value for that entry is initialized. We must then backtrack to our previous entries (that is, entries with a higher index). If we reach x1 without exceeding the upper bounds for any entry, then we have found a complete vector $\mathbf{x}$ which satisfies $Q(\mathbf{x}) \leq C$.

We will know we have found all the short vectors when we reach the zero vector. This is because we start by assigning each value x_i its lower bound, which is calculated with respect to the values $x_{i+1}, \ldots, x_n$. We increase x_i incrementally, until it exceeds the corresponding calculated upper bound. When this happens we revisit x_{i+1}, increasing its value. Since x_{i+1} was originally assigned its own lower bound, it starts off as a negative integer and increases steadily until it reaches 0. Likewise, the other values will start off negative at each iteration and slowly increase in value. It is only when all entries are 0 that the algorithm terminates. When we add each vector, we also add the vector with entries $-x_i$ for each i. In this we capture all the small vectors without having to check positive values for x_n.

Before beginning the search, first find the coefficients of the quadratic form expressed as above. Initialize T_k, U_k, UB_k and x_k to be 0 for all k. Begin with $i = m$ and $T_i = C$ as the value bounding our vectors.

It is noted in the Fincke-Pohst paper that if we label the columns of R by $\mathbf{r}_i$ (from the Cholesky decomposition $\mathbf{x}^t R^t R \mathbf{x}$) and the rows of R^{-1} by $\mathbf{r}'_i$, then we see that

$$x_i^2 = \left(\mathbf{r}_i'^t \left(\sum_{k=1}^{m} x_k \mathbf{r}_k \right) \right)^2 \leq \mathbf{r}_i'^t \mathbf{r}_i (\mathbf{x}^t R^t R \mathbf{x}) \leq \|\mathbf{r}'_i\|^2 C.$$

So it may behoove us to reduce the rows of R^{-1} in order to reduce our search space. Furthermore, it helps to put the smallest basis vectors first, so reordering the columns may also be beneficial.

Express this reduction with a unimodular matrix V^{-1} so that $R_1^{-1} = V^{-1}R^{-1}$. Then reorder the columns of R_1 with a permutation matrix P. Since $R_1 = RV$, we then have that $R_2 = (RV)P$.

Then $R_2^{-1} = P^{-1}V^{-1}R^{-1}$. If we find a solution to the inequality $\mathbf{y}^t R_2^t R_2 \mathbf{y} \leq C$, we can recover a solution to our original inequality by $\mathbf{x} = VP\mathbf{y}$. Since $R_2^{-1} = P^{-1}V^{-1}R^{-1}$, we know that $R_2 = RVP$.

$$\begin{aligned} \mathbf{y}^t R_2^t R_2 \mathbf{y} &\leq C \\ \mathbf{y}^t (P^t V^t R^t)(RVP)\mathbf{y} &\leq C \\ (\mathbf{y}^t P^t V^t) R^t R (VP\mathbf{y}) &\leq C \\ (VP\mathbf{y})^t R^t R (VP\mathbf{y}) &\leq C \\ \mathbf{x}^t R^t R \mathbf{x} &\leq C. \end{aligned}$$

This improves the search time by giving us a nicer quadratic form to work with. Once we find solutions to the inequality given by $Q_2(\mathbf{y}) = \mathbf{y}^t R_2^t R_2 \mathbf{y} \leq C$, it is a simple matter of translating them into solutions of our original inequality.

3.5.2 Translated Lattices

We now explain how to apply Fincke-Pohst to the case

$$(x-c)^t B^t B (x-c) \leq C.$$

In place of the usual reduction listed above, we use MAGMA's built-in LLLGram function on the symmetric positive-definite matrix $A = B^t B$. Here, since A is symmetric and positive-definite, it can be written as $A = R^t R$ for some upper triangular matrix R (via Cholesky Decomposition).The function LLLGram, with input A, computes a matrix G which is the Gram matrix corresponding to a LLL-reduced form of the matrix R. This function returns three values:

- A LLL-reduced Gram matrix G of the Gram matrix A;
- A unimodular matrix U in the matrix ring over $\mathbb{Z}$ whose degree is the number of rows of A such that $G = U^t AU$ (technically it returns $G = UAU^t$, but we change this here to simplify our computations later);
- The rank of A (which equals the dimension of the lattice generated by R).

Thus

$$(U^{-1})^t GU^{-1} = A$$

and we have

$$\begin{aligned}(x-c)^t B^t B(x-c) &\leq C \\ (x-c)^t A(x-c) &\leq C \\ (x-c)^t (U^{-1})^t GU^{-1}(x-c) &\leq C \\ \left(U^{-1}(x-c)\right)^t G \left(U^{-1}(x-c)\right) &\leq C \\ (y-d)^t G\,(y-d) &\leq C\end{aligned}$$

where

$$y = U^{-1}x \quad \text{and} \quad d = U^{-1}c.$$

Now, we are in position to enumerate the short vectors y satisfying

$$(y-d)^t G\,(y-d) \leq C.$$

We retrieve our solutions x via $x = Uy$.

As before, we generate the matrix Q such that

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

Since the sum $Q(x)$ is less than C, the individual term $q_{mm}(y_m - d_m)^2$ must also be less than C.

$$\sum_{i=1}^{m} q_{ii} \left(y_i - d_i + \sum_{j=i+1}^{m} q_{ij}(y_j - d_j) \right)^2 \leq C$$
$$q_{mm}(y_m - d_m)^2 \leq C.$$

Here, in place of the usual method of bounding $y_m - d_m$ by $\sqrt{C/q_{mm}}$ and $-\sqrt{C/q_{mm}}$, we instead let y_m vary between $-\lfloor(-d_m)\rfloor$ and $-\lceil(-d_m)\rceil$. In this way, we simply need to verify that, for these choices of y_m, the equivalence

$$q_{mm}(y_m - d_m)^2 \leq C$$

is satisfied. If it is, we store this value of y_m, otherwise we let $y_m = y_m + 1$. This illustrates the first step in establishing bounds on a specific entry y_i. Adding more terms from the outer sum to this sequence, a pattern emerges.

Let

$$U_i = -d_i + \sum_{j=i+1}^{m} q_{ij}(y_j - d_j)$$

so that we can rewrite $Q(\mathbf{x})$ as

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

In general,

$$q_{kk}(y_k + U_k)^2 \leq C - \sum_{i=k+1}^{m} q_{ii}(y_i + U_i)^2.$$

Let T_k denote the bound on the right-hand side. That is

$$T_k = C - \sum_{i=k+1}^{m} q_{ii}(y_i + U_i)^2,$$

so that $T_m = C$, $T_{m-1} = C - q_{mm}(y_m - d_m)^2$ and

$$T_{m-2} = C - q_{mm}(y_m - d_m)^2 - q_{m-1,m-1}\left(y_{m-1} - d_{m-1} + q_{m-1,m}(y_m - d_m)\right)^2.$$

We set T_m as C and find each subsequent T_k by subtracting the next term from the outer summand:

$$T_k = C - \sum_{i=k+1}^{m} q_{ii}(y_i + U_i)^2,$$

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

Now, we have an upper bound for each summand.

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

Using this, we can estimate upper and lower bounds for each y_k in the coordinate vector $\mathbf{y}$. We start by computing the last entries of $\mathbf{y}$ and their bounds first. Assuming that the last several entries of $\mathbf{y}$ have been assigned, upper and lower bounds on y_k can be determined. Now that we have established a bound on a term in the outer sum, we can determine bounds on the specific entry y_k. The following diagram illustrates the scenario. In the usual Fincke-Pohst algorithm, we take the above equation and solve for y_k:

$$\begin{aligned}(y_k + U_k)^2 &\leq T_k/q_{kk}\\ y_k + U_k &\leq \sqrt{T_k/q_{kk}}\\ y_k &\leq \sqrt{T_k/q_{kk}} - U_k.\end{aligned}$$

Similarly, we have a lower bound:

$$y_k \geq -\sqrt{T_k/q_{kk}} - U_k.$$

Since x_k must be an integer, we can restrict our bounds further. Let $t_k = \sqrt{T_k/q_{kk}}$.

$$UB_k = \lfloor t_k - U_k \rfloor$$

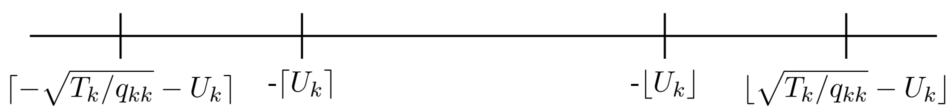
$$LB_k = \lceil -t_k - U_k \rceil$$

Here UB_k is the upper bound on y_k and LB_k is the lower bound on y_k.

$$LB_k \leq y_k \leq UB_k.$$

3.5.3 Refinements

We note here that computing LB_k and UB_k is highly inefficient as it often requires high precision to accurately compute $\sqrt{T_k/q_{kk}}$. Instead, we adopt the following bounds, as per Matshke's algorithm. To help justify this process, we refer to the following diagram



As stated above,

$$\lceil -\sqrt{T_k/q_{kk}} - U_k \rceil = LB_k \leq y_k \leq UB_k = \lfloor \sqrt{T_k/q_{kk}} - U_k \rfloor.$$

In our old implementation for non-translated lattices, we set each $y_k = LB_k$ and increased each term until we reached the zero (centre) vector. Here since the centre vector is non-zero, we instead set each $y_k = -\lceil U_k \rceil$ and increase each y_k successively until $y_k > \lfloor \sqrt{T_k/q_{kk}} - U_k \rfloor$. This is equivalent to the above computation and generates only half of the vectors, assuming symmetry. This symmetry can only be applied if the centre vector is defined over $\mathbb{Z}$, otherwise we must compute all vectors. To do (we can also break symmetry and compute all vectors in the $\mathbb{Z}$ case), we also set $y_k = \lceil U_k \rceil - 1$ and successively decrease this term until $y_k < \lceil -\sqrt{T_k/q_{kk}} - U_k \rceil$.

Of course, in this refinement, we want to avoid computing $\sqrt{T_k/q_{kk}}$, and so instead of verifying whether $y_k > \lfloor \sqrt{T_k/q_{kk}} - U_k \rfloor$ or $y_k < \lceil -\sqrt{T_k/q_{kk}} - U_k \rceil$, we compute $q_{kk}(y_k + U_k)^2$ in each case and verify whether

$$q_{kk}(y_k + U_k)^2 \leq C - \sum_{i=k+1}^{m} q_{ii}(y_i + U_i)^2$$

holds. In the first round, if this does not hold and if $y_k < -\lfloor U_k \rfloor$, we continue to iterate $y_k = y_k + 1$, otherwise we simply iterate $y_k = y_k + 1$. Once this equivalence does not hold and $y_k \geq -\lfloor U_k \rfloor$, we stop this loop. We then reset $y_k = \lceil U_k \rceil - 1$ and search in the other direction, by successively subtracting 1 if

$$q_{kk}(y_k + U_k)^2 \leq C - \sum_{i=k+1}^{m} q_{ii}(y_i + U_i)^2$$

holds. We stop searching in this direction only once this equivalence does not hold.

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.