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

Thesis Drafty McDraft

July 4, 2019

1 Abstract

To Do

- citations
- everything else
- check preamble
- separate introduction into subsections [lit review, new results]

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. ??

2 Introduction

This start feels outside the realm of where you're going — it seems at once abrupt and off-topic. It would be nice to have an introductory sentence or two to get the reader on track before discussing the "required background" material. A Diophantine equation is a polynomial equation in several variables defined over the integers. The term *Diophantine* refers to the Greek mathematician Diophantus of Alexandria, who studied such equations in the 3rd century A.D. why the history lesson? maybe you could use this as one way of motivating/introducing DEs: "look at these things. look how long they've been studied. here's why, and here are the ways people study them. . . . or something. . .

remove separate paragraph if it's the same thought — f is a DE right? If so, then these next lines are providing additional information to what was given above, not starting a new thread. Let $f(x_1, \ldots, x_n)$ be a polynomial with integer coefficients. We wish to study the set of solutions $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ to the equation

$$f(x_1, \ldots, x_n) = 0. \tag{1}$$

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) 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) 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*,

$$f(x, y) = a, \tag{2}$$

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

$$\left|\alpha - \frac{p}{q}\right| > \frac{c_1}{q^n}, \tag{3}$$

where $c_1 > 0$ is a value depending explicitly on α. The finitude of the number of solutions to (2) follows directly from a sharpening of (3) of the type

$$\left|\alpha - \frac{p}{q}\right| > \frac{\lambda(q)}{q^n}, \quad \lambda(q) \to \infty. \tag{4}$$

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 (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 (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 (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 (2) provided that an effective (descriptive? explicit? tight? tractable?) inequality (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 (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 (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 (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

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1} \tag{5}$$

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 (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 (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*,

$$f(x, y) = a p_1^{z_1} \cdots p_v^{z_v}, \quad (x, y) = 1, \tag{6}$$

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 (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

$$\gcd(m-1, n-1) > 1, \tag{7}$$

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 (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 (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 (7), provided the quotient $(m-1)/(n-1)$ is bounded above. Additional results on special cases of equation (5) are available in, for example, [**?**], [**?**], [**?**] and [**?**]. An excellent overview of results on this problem can be found in the survey of Shorey [**?**].

2.1 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 (7), equation (5) has at most finitely many solutions which may be found effectively, even if we fix only a single exponent.

Theorem 2.1 (BeGhKr)**.** *If there is a solution in integers x, y, n and m to equation* (5)*, satisfying* (7)*, then*

$$x < (3d)^{4n/d} \leq 36^n. \tag{8}$$

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 (8), in conjunction with, for example, work of Baker ([REF]). The constants present in our upper bound (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 (5), subject to condition (7), for small fixed values of n.

Theorem 2.2 (BeGhKr)**.** *If there is a solution in integers x, y and m to equation* (5)*, with $n \in \{3, 4, 5\}$ and satisfying* (7)*, then*

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

In the case $n = 5$ of Theorem (2.2) “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

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

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

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

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

$$\mu_0 y - \lambda_0 x = 1 \tag{9}$$

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, (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 (9) via a finite number of principalization tests. The method of [TdW] reduces (6) to $(m/2)h^v$ S-unit equations, where m is the number of roots of unity of K, h is the class number, and v is the number of rational primes $p_1, \ldots, p_v$. The method of Siksek that we employ gives only $m/2$ S-unit equations. The principle computational work here consists of computing an integral basis, a system of fundamental units, and a splitting field of K, as well as computing the class group of K and the factorizations of the primes $p_1, \ldots, p_v$ into prime ideals in the ring of integers of K.

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

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

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

For a given (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 (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 (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 (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

3 Preliminaries

1. algebraic number theory background [DONE - roughly]
2. Setup with Lemmata from Samir
3. LLL [DONE - roughly]
4. Fincke-Pohst with changes from Benjamin [DONE- roughly]
5. linear forms in logs
6. Elliptic curves [DONE - rough]
7. p-adics [DONE - rough]

3.1 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 $n = [K : \mathbb{Q}]$. Each such field has 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. Denote the number of real embeddings by s and the number of conjugate complex embeddings by $2t$, where $n = s + 2t$. Dirichlet's Unit Theorem states 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, $\varepsilon_1, \dots, \varepsilon_r$ such that the group of units of K is given by

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

There are only finitely many roots of unity in K. 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 of σ of K. For algebraic integers, $N_{K/\mathbb{Q}} \in \mathbb{Z}$. 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. The number of classes is called the *class number* of $\mathcal{O}_K$, and it is denoted by h_K. For an ideal $\mathfrak{a}$, it is always true that $\mathfrak{a}^{h_K}$ is principal. The norm of the (integral) ideal $\mathfrak{a}$ is defined by $N_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. If $\mathfrak{a} = (\alpha)\mathcal{O}_K$ is a principal ideal, then $N_{K/\mathbb{Q}}(\mathfrak{a}) = \left|N_{K/\mathbb{Q}}(\alpha)\right|$.

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

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

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

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

add $n = ref$ theorem

3.2 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. NarkiewiczBy $\overline{\mathbb{Q}}_p$ we denote the algebraic closure of $\mathbb{Q}_p$, and by $\mathbb{C}_p$ the completion, with respect to the absolute value, of $\overline{\mathbb{Q}}_p$. add References

Let $g(t)$ be an irreducible polynomial in $\mathbb{Q}[t]$ of degree n and let $K = \mathbb{Q}(\theta)$, where $g(\theta) = 0$. A homomorphism of the multiplicative group of $f : K^* \to \mathbb{R}_{\geq 0}$ into the group of positive real numbers is called a *valuation* if it satisfies the condition

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

We extend this to all of K by putting $f(0) = 0$. If a valuation $f(x)$ satisfies

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

then it is called a *non-Archimedean valuation*. All remaining valuations are called *Archimedean*. A valuation of $v(x)$ of K is called *discrete* if the set of values of $\log v(x)$ is discrete. If v is a discrete valuation of a field K, then it is non-Archimedean.

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

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

Moreover, 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 $\mathbb{C}$.

We say that two valuations are *equivalent* if they define the same topology. Valuations defined by different prime ideals are non-equivalent, and 2 valuations defined by different embeddings of K into the complex field are equivalent iff those embeddings are complex conjugated. A *place* of a number field F is an equivalence class of absolute values on F.

The topology induced in K by a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we shall call the $\mathfrak{p}$-*adic topology*. In the ring $\mathbb{Q}$, the prime ideals are generated by the rational primes p, and the resulting topology in the field $\mathbb{Q}$ of rational numbers is called the p-*adic topology*. A place of a number field F is an equivalence class of absolute values on F.

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.

Let V be the set of all normalized valuations of an algebraic number field K. Then for every non-zero element $a \in K$ we have

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

There are one-to-one correspondences between each of the following four sets of objects:

1. the prime ideals in (the ring of integers of) K that divide p.
2. The irreducible polynomial factors of $g(t)$ in $\mathbb{Q}_p[t]$.
3. The classes of conjugate embeddings of K into the algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$.
4. The extensions of the p-adic valuation ord_p on $\mathbb{Q}$ to K.

In what follows, we will describe the important features of these correspondences. Note that two embeddings of K into $\overline{\mathbb{Q}_p}$ are called *conjugate* if they map θ to the roots of hte same irreducible polynomial in $\mathbb{Q}_p[t]$. Note also that what we call a p-adic valuation is sometimes called a p-adic order.

Let

$$(p)\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$$

change notation of the e_i be the decomposition of $(p)\mathcal{O}_K$ into prime ideals of $\mathcal{O}_K$, with inertial degree f_i for $\mathfrak{p}_i$ over p. Let $K_{\mathfrak{p}_i}$ denote the completion of K with respect to $\mathrm{ord}_{\mathfrak{p}_i}$. Let

$$g(t) = g_1(t) \cdots g_m(t)$$

be the decomposition of $g(t)$ into irreducible polynomials in $\mathbb{Q}_p[t]$. For each $i \in \{1, \ldots, m\}$, let $n_i = \deg g_i(t)$. The correspondence between $\mathfrak{p}_i$ and $g_i(t)$ is such that $n_i = e_i f_i$ and $K_{\mathfrak{p}_i} \simeq \mathbb{Q}_p(\theta_i)$, where $g_i(\theta_i) = 0$.

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 $K \hookrightarrow K_{\mathfrak{p}_i} \simeq \mathbb{Q}(\theta_i) \simeq \mathbb{Q}_p\left(\theta_i^{(j)}\right)$.

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

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

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

$$\operatorname{ord}_p(xy) = \operatorname{ord}_p(x) + \operatorname{ord}_p(y), \quad \operatorname{ord}_p(x + y) \geq \min\{\operatorname{ord}_p(x), \operatorname{ord}_p(y)\}$$

still hold when $x, y \in \mathbb{C}_p$. It is convenient to record here that an element $x \in \mathbb{C}_p$ having $\operatorname{ord}_p(x) = 0$ is called a p-adic *unit*.

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

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

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

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

and we have

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

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 normalized absolute values $|\ |_v$ and $\|\ \|_v$ on k which we now define. If $v|\infty$, then $\|\ \|_v$ restricted to $\mathbb{Q}$ is the usual Archimedean absolute value; if $v|p$ for a rational prime p, then $\|\ \|_v$ restricted to $\mathbb{Q}$ is the usual p-adic absolute value. We then set

$$|\ |_v = \|\ \|_v^{[k_v:\mathbb{Q}_v]/[k:\mathbb{Q}]}.$$

The *logarithmic Weil height* $h : \overline{\mathbb{Q}} \to [0, \infty)$ is now defined as follows. Given $\alpha \in \overline{\mathbb{Q}}$, select any number field k containing α, and let

$$h(\alpha) = \frac{1}{[k : \mathbb{Q}]} \sum_{v} \log^{+} |\alpha|_v,$$

the sum being taken over all places v of k. The height does not depend on the choice of k containing α. We note that if α is an algebraic unit, then $|\alpha|_v = 1$ for all finite places v, and therefore $h(\alpha)$ can be taken over the infinite places only. In particular, if $\alpha \in \mathbb{Q}$, then with $\alpha = p/q$ for $p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$, we have $h(\alpha) = \log \max\{|p|, |q|\}$ and if $\alpha \in \mathbb{Z}$ then $h(\alpha) = \log |\alpha|$. check this.

The p-adic logarithm Every non-zero $\alpha \in \mathbb{Q}_p$ has a p-adic expansion

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

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

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

For $\mathrm{ord}_p(\alpha) \geq k$ we also write $\alpha \equiv 0 \mod p^k$. The p-adic norm is defined by

$$|\alpha|_p = p^{-\mathrm{ord}_p(\alpha)}.$$

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 $\mathrm{ord}_p(z-1) > 1/(p-1)$.

where to find proofs?

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

Lemma 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.*

1. *There is a positive integer r such that $\mathrm{ord}_p(z^r - 1) > 0$.*
2. *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.*
3. *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?

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 $\mathrm{ord}_p(z^r - 1) > 0$, and 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 $\log_p$ refs.

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 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

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

3.3 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 3.3. *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

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

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.

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

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:

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

Similarly, we have a lower bound:

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

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 x_k and LB_k is the lower bound on x_k.

$$LB_x \leq x_k \leq UB_k.$$

To enumerate all of the vectors $\mathbf{x}$ such that $Q(\mathbf{x}) \leq C$, 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.

3.4 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 $G = U^t A U$ (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

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

and we have

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

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 $t_k = \sqrt{T_k/q_{kk}}$.

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

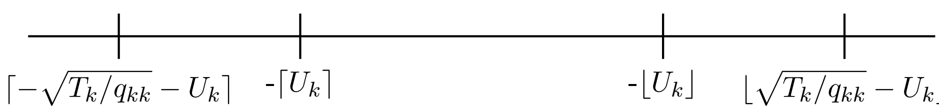
$$LB_k = \lceil -t_k - U_k \rceil$$

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 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.

3.6 Preliminaries: Elliptic Curves

Let K be a field. An *elliptic curve* E over K is a nonsingular curve of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{10}$$

with $a_i \in K$, having a specified base point, $\mathcal{O} \in E$. An equation of the form (10) is called a *Weierstrass equation*. For an elliptic curve E over K, this equation is unique up to a coordinate transformation of the form

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

with $r, s, t, u \in K, u \neq 0$. Writing

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

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

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

if $\text{char}(K) \neq 2, 3$, we can make several linear changes of variables so that, using these values, our elliptic curve has equation

$$E : y^2 = x^3 - 27c_4x - 54c_6. \tag{11}$$

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. Additionally, one may show that 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 $K = \mathbb{Q}$, we can choose the Weierstrass model (10) with the $a_i \in \mathbb{Z}$ and the p-order of Δ minimal for each prime p. Supposing (10) is such a global minimal model for an elliptic curve E over $\mathbb{Q}$, reducing the coefficients modulo a prime p, we obtain a (possibly singular) curve over $\mathbb{F}_p$, namely

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}, \tag{12}$$

with $\tilde{a_i} \in \mathbb{F}_p$. 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 bad reduction of E is measured by the *conductor* of E,

$$N = \prod_{p \text{ prime}} p^{f_p},$$

where $f_p \neq 0$ if $p \nmid \Delta$ (so $f_p = 0$ for all but finitely many primes p), while $f_p = 1$ if the singularity is a node, and $f_p \geq 2$ if the singularity is a cusp. The f_p, hence the conductor, are invariant under isogeny. Hence, roughly speaking, the conductor N is the product of primes at which E has bad reduction raised to small powers, while the discriminant Δ is a product of the same primes, but they may sometimes appear to large powers.

3.7 Preliminaries: 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, a cubic form $G_F(x, y)$ defined via

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

4 Goormaghtigh paper

5 Rational approximations

6 The Thue-Mahler Equation

Let $a \in \mathbb{Z}$ be nonzero, let $S = \{p_1, \ldots, p_v\}$ be a set of rational primes, and let $F \in \mathbb{Z}[X, Y]$ be irreducible and homogeneous of degree $n \geq 3$. We consider the classical Thue–Mahler equation

$$F(X,Y) = ap_1^{Z_1} \cdots p_v^{Z_v}, \quad (X,Y) \in \mathbb{Z}^2, \tag{13}$$

where

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

and $\gcd(X, Y) = 1$.

We would like to enumerate the set of solutions $\{X, Y, Z_1, \ldots, Z_v\}$ of (13), where $Z_i \geq 0$ for $i = 1, \ldots, v$. Solutions to this equation having $(X, Y) = 1$ and $n = 3$ correspond to elliptic curves with good reduction outside of $\{p_1, \ldots, p_v\}$. The algorithm of Tzanakis, de Weger generates solutions (X, Y) in the case

$$(X, Y) = 1, \quad (a, p_1, \ldots, p_v) = 1, \quad (Y, c_0) = 1.$$

To implement this algorithm for our specific application, we modify our Thue-Mahler equation so that we are reduced to the case where

$$(X, Y) = 1, \quad (a, p_1, \ldots, p_v) = 1, \quad c_0 = 1.$$

The solutions corresponding to these conditions are then converted back into solutions of the original Thue-Mahler equation. The remainder of this section outlines these modifications.

6.1 Reducing to $(a, p_1, \ldots, p_v) = 1$ and $c_0 = 1$

Our binary form F is irreducible by assumption and thus at least one of the coefficients c_0 and c_n is nonzero. Hence, we can always transform the given Thue–Mahler equation (13) to one with $c_0 \neq 0$ by interchanging x and y and by renaming the coefficients c_i appropriately. This shows that we always may and do assume that $c_0 \neq 0$ in order to solve (13).

Question 6.1. *Do we need to do this? If one of c_0 or c_n is 0, then F is reducible.*

Let $q_1, \ldots, q_w$ denote the distinct prime divisors of a such that $q_i \notin \{p_1, \ldots, p_v\}$ for $i = 1, \ldots, w$, and write

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

for some integers $b_i > 0$ where $(q_1, \ldots, q_w, p_1, \ldots, p_v) = 1$. Let $(X, Y, Z_1, \ldots, Z_v)$ denote a solution of the Thue-Mahler equation in question and let $Y = d\overline{Y}$, $c_0 = d\overline{c_0}$, where

$d = (c_0, Y)$. Then our equation becomes

$$\begin{aligned}
F(X,Y) &= c_0X^n + c_1X^{n-1}Y + \cdots + c_{n-1}XY^{n-1} + c_nY^n \\
&= d\overline{c_0}X^n + c_1X^{n-1}(d\overline{Y}) + \cdots + c_{n-1}X(d\overline{Y})^{n-1} + c_n(d\overline{Y})^n \\
&= d\left(\overline{c_0}X^n + c_1X^{n-1}\overline{Y} + \cdots + c_{n-1}Xd^{n-2}\overline{Y}^{n-1} + c_nd^{n-1}\overline{Y}^n\right) \\
&= ap_1^{Z_1}\dots p_v^{Z_v} \\
&= \prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(a)} \cdot p_1^{Z_1}\dots p_v^{Z_v} \\
&= \prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(a)+Z_i}.
\end{aligned}$$

Henct d divides $\prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(a)+Z_i}$. Hence

$$d = (c_0, Y) = \prod_{i=1}^{w} q_i^{s_i} \cdot \prod_{i=1}^{v} p_i^{t_i},$$

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

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

Let $\mathcal{D}$ be the set of all positive rational integers m dividing c_0 such that $\mathrm{ord}_p(m) \le \mathrm{ord}_p(a)$ for each rational prime $p \notin S$. In other words,

$$\mathcal{D} := \{m \in \mathbb{Z}_{>0} \ : \ m \mid c_0 \text{ and } \mathrm{ord}_p(m) \le \mathrm{ord}_p(a) \text{ for all } p \notin S\}.$$

In the above notation, $\mathcal{D}$ is the set of all such possible values $d = (c_0, Y)$. That is, given d such that

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

as above, then clearly $d \mid c_0$ by construction. In other words, since

$$\mathrm{ord}_{q_i}(d) = s_i \le \min\{\mathrm{ord}_{q_i}(a), \mathrm{ord}_{q_i}(c_0)\} \le \mathrm{ord}_{q_i}(c_0)$$

and

$$\mathrm{ord}_{p_i}(d) = t_i \le \min\{\mathrm{ord}_{p_i}(a) + Z_i, \mathrm{ord}_{p_i}(c_0)\} \le \mathrm{ord}_{p_i}(c_0),$$

for all $q_i \in \{q_1, \ldots, q_w\}$ and all $p_i \in S$, we have $d \mid c_0$.

In addition, for all $p \notin S$, the statement $\mathrm{ord}_p(d) \leq \mathrm{ord}_p(a)$ is nontrivial only for those primes for which $p \mid d$ or $p \mid a$. We observe that the set of primes $p \notin S$ such that $p \mid d$ is $\{q_1, \ldots, q_w\}$, which is precisely the set of primes $p \notin S$ such that $p \mid a$. Now,

$$\mathrm{ord}_{q_i}(d) = s_i \leq \min\{\mathrm{ord}_{q_i}(a), \mathrm{ord}_{q_i}(c_0)\} \leq \mathrm{ord}_{q_i}(a).$$

If $p \notin S$ and $p \notin \{q_1, \ldots, q_w\}$, then

$$0 = \mathrm{ord}_p(d) = \mathrm{ord}_p\left(\prod_{i=1}^{w} q_i^{s_i} \cdot \prod_{i=1}^{v} p_i^{t_i}\right) \leq \mathrm{ord}_p(a) = \mathrm{ord}_p\left(\prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(a)}\right) = 0.$$

Hence $d \mid c_0$ such that $\mathrm{ord}_p(d) \leq \mathrm{ord}_p(a)$ for all $p \notin S$, and so $d \in \mathcal{D}$.

Conversely, suppose $d \in \mathcal{D}$ so that $d \mid c_0$. Since

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

and $\mathrm{ord}_p(d) \leq \mathrm{ord}_p(a)$ for all $p \notin S$, then the right-hand side of

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

is non-zero only for the primes $\{q_1, \ldots, q_w\}$. That is,

$$\mathrm{ord}_p(d) = 0$$

for all $p \notin \{q_1, \ldots, q_w\}$ and for $i \in \{1, \ldots, w\}$

$$\mathrm{ord}_{q_i}(d) \leq \mathrm{ord}_{q_i}(a) = b_i.$$

In other words, the only prime factors appearing in d outside of S are those among $\{q_1, \ldots, q_w\}$. That is,

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

for some integers t_i, and s_i such that $s_i \leq \mathrm{ord}_{q_i}(a) = b_i$. Of course, since $d \mid c_0$, we must necessarily have

$$s_i \le \min\{\mathrm{ord}_{q_i}(a), \mathrm{ord}_{q_i}(c_0)\}.$$

Similarly, for t_i, as $d \mid c_0$, we must have

$$t_i \le \mathrm{ord}_{q_i}(c_0)\}.$$

It follows that these sets are identical.

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

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

Suppose (X, Y) is a solution of (13) with $(X, Y) = 1$ and $(c_0, Y) = d$. Then, multiplying by u yields

$$\begin{aligned}
uF(X,Y) &= \frac{c_0^{n-1}}{d^n} F(X,Y) \\
&= \frac{c_0^n}{d^n} X^n + \frac{c_0^{n-1}}{d^n} c_1 X^{n-1} Y + \cdots + \frac{c_0^{n-1}}{d^n} c_{n-1} X Y^{n-1} + \frac{c_0^{n-1}}{d^n} c_n Y^n \\
&= ua \prod_{i=1}^{v} p_i^{Z_i} \\
&= \frac{c_0^{n-1}}{d^n} \prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(a)} \prod_{i=1}^{v} p_i^{Z_i} \\
&= \left(\frac{c_0}{d}\right)^{n-1} \frac{\prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(a)} \prod_{i=1}^{v} p_i^{Z_i}}{d}.
\end{aligned}$$

From above, we know that

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

with

$$s_i \le \min\{\mathrm{ord}_{q_i}(a), \mathrm{ord}_{q_i}(c_0)\} \quad \text{and} \quad t_i \le \mathrm{ord}_{q_i}(c_0)\}.$$

Hence

$$\frac{\prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(a)} \prod_{i=1}^{v} p_i^{Z_i}}{d} = \frac{\prod_{i=1}^{w} q_i^{b_i} \cdot \prod_{i=1}^{v} p_i^{\mathrm{ord}_{p_i}(a)} \prod_{i=1}^{v} p_i^{Z_i}}{\prod_{i=1}^{w} q_i^{s_i} \cdot \prod_{i=1}^{v} p_i^{t_i}}.$$

Indeed $d \mid a\prod_{i=1}^{v} p_i^{z_i}$. Of course, $d \mid c_0$ by definition so that the above equation is an integer equation. Now

$$\begin{aligned}
uF(X,Y) &= ua\prod_{i=1}^{v} p_i^{Z_i} \\
&= \left(\prod_{p\notin S} p^{\mathrm{ord}_p(u)} \prod_{p\in S} p^{\mathrm{ord}_p(u)}\right) \cdot \left(\prod_{p\notin S} p^{\mathrm{ord}_p(a)} \prod_{p\in S} p^{\mathrm{ord}_p(a)}\right) \cdot \prod_{i=1}^{v} p_i^{Z_i} \\
&= \prod_{p\notin S} p^{\mathrm{ord}_p(u)+\mathrm{ord}_p(a)} \prod_{p\in S} p^{Z_i+\mathrm{ord}_p(u)+\mathrm{ord}_p(a)} \\
&= \prod_{p\notin S} p^{\mathrm{ord}_p(ua)} \prod_{p\in S} p^{Z_i+\mathrm{ord}_p(ua)},
\end{aligned}$$

and it follows that

$$uF(X,Y) = c\prod_{p\in S} p^{Z_i+\mathrm{ord}_p(ua)}.$$

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

Now, suppose that $(X, Y, Z_1, \ldots, Z_v)$ is a solution of (13) and let $d = \gcd(c_0, Y)$. That is, $d \in \mathcal{D}$. Let

$$x = \tfrac{c_0 X}{d}, \quad y = \tfrac{Y}{d} \quad \text{and} \quad z_i = \mathrm{ord}_p(u) + \mathrm{ord}_p(a) + Z_i$$

for all $i \in \{1, \ldots, v\}$, and let

$$C_i = c_i c_0^{i-1} \quad \text{for } i = 1, \ldots, n.$$

By definition of d, we note that $x, y \in \mathbb{Z}$.

Under this definition,

$$X = \frac{dx}{c_0}, \quad Y = dy,$$

and

$$\begin{aligned}
uF(X,Y) &= \frac{c_0^n}{d^n}X^n + \frac{c_0^{n-1}}{d^n}c_1X^{n-1}Y + \cdots + \frac{c_0^{n-1}}{d^n}c_{n-1}XY^{n-1} + \frac{c_0^{n-1}}{d^n}c_nY^n \\
&= \frac{c_0^n}{d^n}\left(\frac{dx}{c_0}\right)^n + \frac{c_0^{n-1}}{d^n}c_1\left(\frac{dx}{c_0}\right)^{n-1}(dy) + \cdots + \frac{c_0^{n-1}}{d^n}c_{n-1}\left(\frac{dx}{c_0}\right)(dy)^{n-1} + \frac{c_0^{n-1}}{d^n}c_n(dy)^n \\
&= x^n + c_1x^{n-1}y + \cdots + c_0^{n-2}c_{n-1}xy^{n-1} + c_0^{n-1}c_ny^n \\
&= x^n + C_1x^{n-1}y + \cdots + C_{n-1}xy^{n-1} + C_ny^n \\
&= c\prod_{p\in S} p^{\mathrm{ord}_p(u)+\mathrm{ord}_p(a)+Z_i} \\
&= c\prod_{p\in S} p^{z_i}.
\end{aligned}$$

Let $f(x,y) = uF(X,Y)$ so that

$$f(x,y) = x^n + C_1x^{n-1}y + \cdots + C_{n-1}xy^{n-1} + C_ny^n = cp_1^{z_1}\cdots p_v^{z_v}. \tag{14}$$

Since there are only finitely many choices for $d = \gcd(c_0, Y)$, it follows that there are only finitely many choices for $\{c, u, d\}$. Then, solving (13) is equivalent to solving the finitely many equations (14) for each choice of c, u, 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

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

We note that for any choice of c, u, d, the left-hand side of (14) is the same. Thus, to solve (14), we need only to enumerate over every possible c. Now, if $\mathcal{C}$ denotes the set of all $\{c, u, d\}$ and $d_1, d_2 \in \mathcal{D}$, we may have $\{c, u_1, d_1\}, \{c, u_2, d_2\} \in \mathcal{C}$. That is, d_1, d_2 may share the same value of c, reiterating that we need only solve (14) for each distinct c.

7 The Relevant Algebraic Number Field

Now, for each c, we solve

$$f(x,y) = x^n + C_1x^{n-1}y + \cdots + C_{n-1}xy^{n-1} + C_ny^n = cp_1^{z_1}\cdots p_v^{z_v}.$$

Here,

$$\gcd(x, y) = 1 \quad \text{and} \quad \gcd(c, p_1, \dots, p_v) = 1.$$

In our case, $n = 3$ and so

$$f(x, y) = x^3 + C_1x^2y + C_2xy^2 + C_3y^3 = cp_1^{z_1} \cdots p_v^{z_v}.$$

Following the Thue-Mahler solver algorithm, put

$$g(t) = F(t, 1) = t^3 + C_1t^2 + C_2t + C_3$$

and note that $g(t)$ is irreducible in $\mathbb{Z}[t]$. Let $K = \mathbb{Q}(\theta)$ with $g(\theta) = 0$. Then (14) is equivalent to solving finitely many equations of the form

$$N_{K/\mathbb{Q}}(x - y\theta) = cp_1^{z_1} \dots p_v^{z_v} \tag{15}$$

for each distinct value of c.

8 Decomposition of Primes

Let p_i be any rational prime and let

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

be the factorization of p_i into prime ideals in the ring of integers $\mathcal{O}_K$ of K. Let f_{ij} be the residue degree of $\mathfrak{p}_{ij}$ over p_i. We have $\deg(g_i(t)) = e_{ij}f_{ij}$.

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 $g_{i1}(t), \dots, g_{im}(t)$, and in particular, $\deg(g_{ij}(t)) = e_{ij}f_{ij}$.

Then, since $N(\mathfrak{p}_{ij}) = p_i^{f_{ij}}$, (15) leads to finitely many ideal equations of the form

$$(x - y\theta)\mathcal{O}_K = \mathfrak{a} \prod_{j=1}^{m_1} \mathfrak{p}_{1j}^{z_{1j}} \cdots \prod_{j=1}^{m_v} \mathfrak{p}_{vj}^{z_{vj}} \tag{16}$$

where $\mathfrak{a}$ is an ideal of norm $|c|$ (for each choice of c) and the z_{ij} are unknown integers related to z_i by $\sum_{j=1}^{m_i} f_{ij} z_{ij} = z_i$. Thus

$$Z_i = z_i - \mathrm{ord}_p\, u - \mathrm{ord}_p(a) = \sum_{j=1}^{m_i} f_{ij} z_{ij} - \mathrm{ord}_p\, u - \mathrm{ord}_p(a).$$

Our first task is to cut down the number of variables appearing in (16). We will do this by showing that only a few prime ideals can divide $(x - y\theta)\mathcal{O}_K$ to a large power.

9 An Alternative to 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 here and instead apply the following results of Siksek.

Let $p \in \{p_1, \ldots, p_v\}$. We will produce two finite lists L_p and M_p. The list L_p consists of certain ideals $\mathfrak{b}$ supported at the prime ideals above p. The list M_p consists of certain pairs $(\mathfrak{b}, \mathfrak{p})$ where $\mathfrak{b}$ is supported at the prime ideals above p, and $\mathfrak{p} \mid p$ is a prime ideal satisfying $e(\mathfrak{p}/p) = f(\mathfrak{p}/p) = 1$. We want the lists to satisfy the following property. If (x, y) is a solution to (14) then

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

$$\mathfrak{b} \mid (x - y\theta)\mathcal{O}_K, \qquad (x - y\theta)\mathcal{O}_K/\mathfrak{b} \text{ is coprime to } (p)\mathcal{O}_K; \tag{17}$$

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

$$(\mathfrak{b} \cdot \mathfrak{p}^{v_p}) \mid (x - y\theta)\mathcal{O}_K, \qquad (x - y\theta)\mathcal{O}_K/(\mathfrak{b} \cdot \mathfrak{p}^{v_p}) \text{ is coprime to } (p)\mathcal{O}_K. \tag{18}$$

To generate the lists M_p, L_p we consider two 'affine patches': $p \nmid y$ and $p \mid y$. As motivation for the method we first state and prove two lemmas.

Lemma 9.1. *[Siksek] Let (x, y) be a solution of (14) with $p \nmid y$, let t be a positive integer, and suppose $x/y \equiv u \pmod{p^t}$, where $u \in \{0, 1, 2, \ldots, p^t - 1\}$. If $\mathfrak{q} \mid p$, then*

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

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

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

Lemma 9.2. *[Siksek] Let (x, y) be a solution of (14) with $p \mid y$ (and thus $p \nmid x$), let t be a positive integer, and suppose $y/x \equiv u \pmod{p^t}$, where $u \in \{0, 1, 2, \ldots, p^t - 1\}$. If $\mathfrak{q} \mid p$, then*

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

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

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

Proof of Lemmas 9.1 and 9.2. Suppose $p \nmid y$. Thus $\mathfrak{q} \nmid y$ and hence $\operatorname{ord}_{\mathfrak{q}}(x - y\theta) = \operatorname{ord}_{\mathfrak{q}}(x/y - \theta)$. Since

$$x/y - \theta = u - \theta + x/y - u,$$

we have

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

But

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

by assumption, completing the proof of Lemma 9.1. The proof of Lemma 9.2 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 9.3. 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
$$\mathcal{P}_u = \{\mathfrak{q} \mid p \;:\; \mathrm{ord}_{\mathfrak{q}}(u-\theta) \geq t \cdot e(\mathfrak{q}/p)\},$$

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

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

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 9.4. *Algorithm 9.3 terminates.*

Proof. Suppose otherwise. Write $t_0 = 1$ and $t_i = t_0 + i$ for $i = 1, 2, 3, \dots$. Then there is an infinite sequence of congruence classes $u_i \pmod{p^{t_i}}$ such that $u_{i+1} \equiv u_i \pmod{p^{t_i}}$, and such that the u_i fail the hypotheses of both (i) and (ii). In particular, $\mathcal{P}_{u_i}$ is non-empty. By the pigeon-hole principle, some $\mathfrak{p}$ appears in infinitely many of the $\mathcal{P}_{u_i}$. Thus $\mathrm{ord}_{\mathfrak{p}}(u_i - \theta) \geq t_i \cdot e(\mathfrak{p}/p)$ infinitely often. However, the sequence $\{u_i\}$ converges to some $\alpha \in \mathbb{Z}_p$. Thus $\alpha = \theta$ 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 particular, $\mathfrak{p}$ corresponds to the factor $(t-\alpha)$ in the p-adic factorisation of $g(t)$. There can be at most one such $\mathfrak{p}$, and so $\mathcal{P}_{u_i} = \{\mathfrak{p}\}$. In particular, the hypotheses of (ii) are satisfied and we have a contradiction. $\square$

Lemma 9.5. *Let $p \in \{p_1, \ldots, p_v\}$ and let $\mathcal{L}_p$, $\mathcal{M}_p$ be as given by Algorithm 9.3. Let (x, y) be a solution to (14). Then*

- *either there is some $\mathfrak{b} \in \mathcal{L}_p$ such that (17) 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 (18) 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. In particular, there is some i such that $x/y \equiv u_i \pmod{p^{t_i}}$ where $u_i \in \mathcal{U}_i$, but there is no element in $\mathcal{U}_{i+1}$ congruent to x/y modulo $p^{t_{i+1}}$. Thus u_i must satisfy the hypotheses of either (i) or (ii). Write $u = u_i$ and $t = t_i$ so that $x/y \equiv u \pmod{p^t}$. By Lemma 9.1, 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 $\mathcal{L}_p$, and by the above we know that (17) 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 (18) is satisfied, proving the lemma in this case. □

Algorithm 9.6. 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 9.3.

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

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

(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 9.7. *Algorithm 9.6 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. ☐

Lemma 9.8. *Let $p \in \{p_1, \ldots, p_v\}$ and let L_p, M_p be as given by Algorithm 9.6. Let (x, y) be a solution to (14). Then*

- *either there is some $\mathfrak{b} \in \mathcal{L}_p$ such that (17) 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 (18) is satisfied.*

Proof. Now let (x, y) be a solution to (14). In view of Lemma 9.5 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 9.5. ☐

9.1 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 9.8 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 9.8 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.

10 Factorization of the Thue-Mahler Equation

After applying Algorithm 9.3 and Algorithm 9.6, we are reduced to solving finitely many equations of the form

$$(x - y\theta)\mathcal{O}_K = \mathfrak{a}\mathfrak{p}_1^{u_1} \cdots \mathfrak{p}_\nu^{u_\nu} \tag{19}$$

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 9.3 and Algorithm 9.6 applied to $p_i \in \{p_1, \ldots, p_v\}$, such that $(\mathfrak{b}_\mathrm{i}, \mathfrak{p}_i) \in M_{p_i}$ 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 (19) has a solution $\mathbf{u} = (u_1, \ldots, u_\nu)$ then, by (19),

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

In particular, if $[\mathfrak{a}]^{-1}$ does not belong to the image of ϕ then (19) 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 (19) 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 (19) as

$$(x - y\theta)\mathcal{O}_K = \alpha \cdot \gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu} \mathcal{O}_K \tag{20}$$

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 (20).

10.1 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 (19) 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 (19) as

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

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

$$x - y\theta = \alpha\zeta\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}\gamma_1^{n_1}\cdots\gamma_\nu^{n_\nu} \tag{21}$$

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

$$x - y\theta = \alpha\zeta\varepsilon_1^{a_1}\cdot\gamma_1^{n_1}\cdots\gamma_\nu^{n_\nu} \quad \text{or} \quad x - y\theta = \alpha\zeta\varepsilon_1^{a_1}\varepsilon_2^{a_2}\cdot\gamma_1^{n_1}\cdots\gamma_\nu^{n_\nu} \tag{22}$$

To summarize, our original problem of solving (13) has been reduced to the problem of solving finitely many equations of the form (22) 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.

11 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

$$\lambda = \delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}} \right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}} \right)^{n_i} - 1 = \delta_2 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}} \right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}} \right)^{n_i}, \tag{23}$$

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

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

12 Specializing to Degree 3

We are interested in solving a Thue-Mahler equation of degree 3. That is,

$$F(X,Y) = c_0X^3 + c_1X^2Y + c_2XY^2 + c_3Y^3 = ap_1^{Z_1} \cdots p_v^{Z_v}.$$

Making the relevant changes as in the setup above (ie. reducing to a monic polynomial having solutions $(x, y) = 1$) and putting $g(t) = F(t, 1)$ yields

$$g(t) = t^3 + C_1t^2 + C_2t + C_3,$$

an irreducible polynomial in $\mathbb{Z}[t]$. Then, setting $K = \mathbb{Q}(\theta)$ with $g(\theta) = 0$ yields a field K of degree 3 over $\mathbb{Q}$. Hence, the splitting field of K is divisible by 3. Since the Galois group is a subgroup of S_3, there are only two possibilities, namely A_3 or S_3. Recall that the discriminant of $g(t)$ is defined as

$$D = C_1^2C_2^2 - 4C_2^3 - 4C_1^3C_3 - 27C_3^2 + 18C_1C_2C_3.$$

The Galois group of $g(t)$ is A_3 if and only if D is a square. Explicitly, if D is the square of an element of $\mathbb{Q}$, then the splitting field of the irreducible cubic $g(t)$ is obtained by adjoining any single root of $g(t)$ to K. The resulting field is Galois over $\mathbb{Q}$ of degree 3 with cyclic group of order 3 as Galois group. In particular, K is the Galois group of $g(t)$. In this case,

$$g(t) = (t - \theta_1)(t - \theta_2)(t - \theta_3)$$

in K, where $\theta_1, \theta_2, \theta_3 \in K$ and, without loss of generality, $\theta_1 = \theta$.

If D is not the square of an element of $\mathbb{Q}$, then the splitting field of $g(t)$ is of degree 6 over $\mathbb{Q}$, hence is the field $K\left(\theta, \sqrt{D}\right)$ for any one of the roots θ of $g(t)$. This extension is Galois over $\mathbb{Q}$ with Galois group S_3. In this case,

$$g(t) = (t - \theta)\tilde{g}(t)$$

in $K = \mathbb{Q}(\theta)$, where $\tilde{g}(t) \in K[t]$ is an irreducible degree 2 polynomial. The Galois group is generated by σ, which takes θ to one of the other roots of $g(t)$ and fixes $\sqrt{D}$, and τ, which takes $\sqrt{D}$ to $-\sqrt{D}$ and fixes θ. In particular, if $L = K(\theta, \sqrt{D})$,

$$\mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id_L}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\},$$

where

$$\mathrm{id_L} : \begin{cases} \theta_1 \mapsto \theta_1 \\ \theta_2 \mapsto \theta_2 \\ \theta_3 \mapsto \theta_3 \\ \sqrt{D} \mapsto \sqrt{D} \end{cases}, \sigma : \begin{cases} \theta_1 \mapsto \theta_2 \\ \theta_2 \mapsto \theta_3 \\ \theta_3 \mapsto \theta_1 \\ \sqrt{D} \mapsto \sqrt{D} \end{cases}, \sigma^2 : \begin{cases} \theta_1 \mapsto \theta_3 \\ \theta_2 \mapsto \theta_1 \\ \theta_3 \mapsto \theta_2 \\ \sqrt{D} \mapsto \sqrt{D} \end{cases},$$

$$\tau : \begin{cases} \theta_1 \mapsto \theta_1 \\ \theta_2 \mapsto \theta_3 \\ \theta_3 \mapsto \theta_2 \\ \sqrt{D} \mapsto -\sqrt{D} \end{cases}, \tau\sigma : \begin{cases} \theta_1 \mapsto \theta_3 \\ \theta_2 \mapsto \theta_2 \\ \theta_3 \mapsto \theta_1 \\ \sqrt{D} \mapsto -\sqrt{D} \end{cases}, \tau\sigma^2 : \begin{cases} \theta_1 \mapsto \theta_2 \\ \theta_2 \mapsto \theta_1 \\ \theta_3 \mapsto \theta_3 \\ \sqrt{D} \mapsto -\sqrt{D} \end{cases}.$$

We note of course, that since $\sqrt{D} = (\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3)$, in order to map $\sqrt{D}$ to $-\sqrt{D}$, two of $\theta_1, \theta_2, \theta_3$ must be interchanged.

Let $p \in S$ and choose $\mathfrak{P} \in L$ over p. Let $L_{\mathfrak{P}}$ denote the completion of L at $\mathfrak{P}$. There are 3 possibilities for the factorization of $g(t) \in \mathbb{Q}_p[t]$:

1. $g(t) = g_1(t)$, where $\deg g_1(t) = 3$. That is $g(t)$ is irreducible in $\mathbb{Q}_p[t]$. It follows that

$$(p)\mathcal{O}_K = \mathfrak{p}_1^{e_1}$$

so that there is only 1 prime ideal lying above p. Since $3 = \deg g_1(t) = e_1 d_1$, it follows that either $e_1 = 1$ and $d_1 = 3$ or $e_1 = 3$ and $d_1 = 1$, so that we have the following 2 subcases:

(a) $g(t) = g_1(t) \in \mathbb{Q}_p[t]$ is irreducible of degree 3 and

$$(p)\mathcal{O}_K = \mathfrak{p}_1 \quad \text{with } e_1 = 1, d_1 = 3.$$

In this case $\theta^{(1)}, \theta^{(2)}, \theta^{(3)} = \theta_1^{(1)}, \theta_1^{(2)}, \theta_1^{(3)} \in \overline{\mathbb{Q}}_p \backslash \mathbb{Q}_p$.

Further, there is only one prime ideal, $\mathfrak{p}_1$ over p, so all roots $\theta_1^{(1)}, \theta_1^{(2)}, \theta_1^{(3)}$ of $g(t)$ over $L_{\mathfrak{P}}$ are associated to it.

(b) $g(t) = g_1(t) \in \mathbb{Q}_p[t]$ is irreducible of degree 3 and

$$(p)\mathcal{O}_K = \mathfrak{p}_1^3 \quad \text{with } e_1 = 3, d_1 = 1.$$

In this case $\theta^{(1)}, \theta^{(2)}, \theta^{(3)} = \theta_1^{(1)}, \theta_1^{(2)}, \theta_1^{(3)} \in \overline{\mathbb{Q}}_p$.

2. $g(t) = g_1(t)g_2(t)$ where (without loss of generality) $\deg g_1(t) = 1$ and $\deg g_2(t) = 2$. It follows that

$$(p)\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}$$

so that there are 2 prime ideal lying above p. Since $1 = \deg g_1(t) = e_1 d_1$ and $2 = \deg g_2(t) = e_2 d_2$, it follows that $e_1 = d_1 = 1$ and either $e_2 = 1$ and $d_2 = 2$ or $e_2 = 2$ and $d_2 = 1$, so that we have the following 2 subcases:

(a) $g(t) = g_1(t)g_2(t) \in \mathbb{Q}_p[t]$ where $\deg g_1(t) = 1$ and $\deg g_2(t) = 2$ and

$$(p)\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \quad \text{with } e_1 = 1, d_1 = 1 \text{ and } e_2 = 1, d_2 = 2.$$

In this case $\theta^{(1)}, \theta^{(2)}, \theta^{(3)} = \theta_1^{(1)}, \theta_2^{(1)}, \theta_2^{(2)} \in \overline{\mathbb{Q}}_p$, where $\theta_1^{(1)} \in \mathbb{Q}_p$.

(b) $g(t) = g_1(t)g_2(t) \in \mathbb{Q}_p[t]$ where $\deg g_1(t) = 1$ and $\deg g_2(t) = 2$ and

$$(p)\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2 \quad \text{with } e_1 = 1, d_1 = 1 \text{ and } e_2 = 2, d_2 = 1.$$

In this case $\theta^{(1)}, \theta^{(2)}, \theta^{(3)} = \theta_1^{(1)}, \theta_2^{(1)}, \theta_2^{(2)} \in \overline{\mathbb{Q}}_p$, where $\theta_1^{(1)} \in \mathbb{Q}_p$.

3. $g(t) = g_1(t)g_2(t)g_3(t)$ where $\deg g_1(t) = \deg g_2(t) = \deg g_3(t) = 1$. It follows that

$$(p)\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$$

so that there are 3 prime ideal lying above p. Since $1 = \deg g_i(t) = e_i d_i$ for $i = 1, 2, 3$, it follows that that $e_i = d_i = 1$ for $i = 1, 2, 3$ so that we have the following case:

(a) $g(t) = g_1(t)g_2(t)g_3(t) \in \mathbb{Q}_p[t]$ where $\deg g_1(t) = \deg g_2(t) = \deg g_3(t) = 1$ and

$$(p)\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \quad \text{ with } e_i = d_i = 1 \text{ for } i = 1, 2, 3.$$

In this case $\theta^{(1)}, \theta^{(2)}, \theta^{(3)} = \theta_1^{(1)}, \theta_2^{(1)}, \theta_3^{(1)} \in \mathbb{Q}_p$.

13 Initial Heights

The sieves involving logarithms are of local nature. To obtain a global sieve, we work with the global logarithmic Weil height

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

Similar as the Néron-Tate height on $E(\overline{\mathbb{Q}})$, the height h on $\mathbb{G}_m(\overline{\mathbb{Q}})$ is invariant under conjugation and it admits a decomposition into local heights which can be related to complex and p-adic logarithms. We now begin to construct the sieve.

Let $\mathbf{n} = (n_1, \ldots, n_\nu, a_1, \ldots, a_r)$ be a solution to (23), let

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

and consider the Weil height of $\frac{\delta_2}{\lambda}$,

$$\frac{\delta_2}{\lambda} = \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(j)}}{\varepsilon_i^{(i_0)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{n_i}.$$

Given the global Weil height of δ_2/λ, or all the local heights of δ_2/λ, we will construct several ellipsoids ‘containing’ $\mathbf{n}$ such that the volume of the ellipsoids are as small as possible. We begin by computing the height of δ_2/λ.

13.1 Decomposition of the Weil height.

Lemma 13.1. *Let $\mathfrak{P}$ be a finite place of L and let $\mathfrak{P}^{(i_0)} = \sigma_{i_0}(\mathfrak{P})$ and $\mathfrak{P}^{(j)} = \sigma_j(\mathfrak{P})$ lying over $\mathfrak{p}^{(i_0)}$, $\mathfrak{p}^{(j)}$ respectively, where $\sigma_{i_0} : L \to L$, $\theta \mapsto \theta^{(i_0)}$ and $\sigma_j : L \to L$, $\theta \mapsto \theta^{(j)}$ are two automorphisms of L such that (i_0, j, k) form a subgroup of S_3 of order 3. For $i = 1, \ldots, \nu$,*

$$\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)\mathcal{O}_L = \left(\prod_{\mathfrak{P}|\mathfrak{p}_1} \frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_1^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_1^{(i_0)})}}\right)^{a_{1i}} \cdots \left(\prod_{\mathfrak{P}|\mathfrak{p}_\nu} \frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_\nu^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_\nu^{(i_0)})}}\right)^{a_{\nu i}}$$

where $\mathfrak{P}^{(j)} \neq \mathfrak{P}^{(i_0)}$ for all $\mathfrak{P}$ lying above $\mathfrak{p}$ in K.

Proof. Since

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

for $i = 1, \ldots, \nu$, where

$$\mathfrak{p}_i\mathcal{O}_L = \prod_{\mathfrak{P}|\mathfrak{p}_i} \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p}_i)},$$

it holds that

$$(\gamma_i)\mathcal{O}_L = \left(\prod_{\mathfrak{P}|\mathfrak{p}_1} \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p}_1)}\right)^{a_{1i}} \cdots \left(\prod_{\mathfrak{P}|\mathfrak{p}_\nu} \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p}_\nu)}\right)^{a_{\nu i}}.$$

Let $\mathfrak{P}^{(i_0)}, \mathfrak{P}^{(j)}$ denote the ideal $\mathfrak{P}$ under the automorphisms of L

$$\sigma_{i_0} : L \to L, \quad \theta \mapsto \theta^{(i_0)} \quad \text{and} \quad \sigma_j : L \to L, \quad \theta \mapsto \theta^{(j)},$$

respectively. That is, $\mathfrak{P}^{(i_0)} = \sigma_{i_0}(\mathfrak{P})$ and $\mathfrak{P}^{(j)} = \sigma_j(\mathfrak{P})$. Then

$$\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)\mathcal{O}_L = \left(\prod_{\mathfrak{P}|\mathfrak{p}_1} \frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_1^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_1^{(i_0)})}}\right)^{a_{1i}} \cdots \left(\prod_{\mathfrak{P}|\mathfrak{p}_\nu} \frac{\mathfrak{P}^{(j)\ e(\mathfrak{P}^{(j)}|\mathfrak{p}_\nu^{(j)})}}{\mathfrak{P}^{(i_0)\ e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_\nu^{(i_0)})}}\right)^{a_{\nu i}}.$$

Now, to show that $\mathfrak{P}^{(j)} \neq \mathfrak{P}^{(i_0)}$ for all $\mathfrak{P}$ lying above $\mathfrak{p}$ in K, we consider the decomposition group of $\mathfrak{P}$,

$$D(\mathfrak{P}|p) = \{\sigma \in G \ : \ \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Let L_D denote the field under L fixed by $D(\mathfrak{P}|p)$. By Galois theory, we have the following tower of fields

$$\begin{tikzcd} L \arrow[d, dash, "r"'] \\ L_D \arrow[d, dash, "f(\mathfrak{P}|p)"'] \\ L_E \arrow[d, dash, "e(\mathfrak{P}|p)"'] \\ \mathbb{Q} \end{tikzcd}$$

where $[L : \mathbb{Q}] = 6$. From this tower of fields, we may determine the decomposition group. Let $p \in S$. For any $\mathfrak{p}$ lying over p, we note that L/K is a Galois extension of degree 2. Hence there are 3 possibilities for the decomposition of $\mathfrak{p}$ in L. Namely

i. $r = 2$ and $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$. Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$.

ii. $e(\mathfrak{P}|\mathfrak{p}) = 2$ and $r = f(\mathfrak{P}|\mathfrak{p}) = 1$. Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^2$.

iii. $f(\mathfrak{P}|\mathfrak{p}) = 2$ and $r = e(\mathfrak{P}|\mathfrak{p}) = 1$. Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1$.

For $p \in S$, there are 5 possibilities for the decomposition of p in K. In particular,

1. $(p)\mathcal{O}_K = \mathfrak{p}_1$ with $e(\mathfrak{p}_1|p) = 1, f(\mathfrak{p}_1|p) = 3$. By the PIRL, it follows that this prime ideal is bounded and therefore does not appear unbounded in (19).

2. $(p)\mathcal{O}_K = \mathfrak{p}_1^3$ with $e(\mathfrak{p}_1|p) = 3, f(\mathfrak{p}_1|p) = 1$. By the PIRL, it follows that this prime ideal is bounded and therefore does not appear unbounded in (19).

3. $(p)\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $e(\mathfrak{p}_1|p) = f(\mathfrak{p}_1|p) = 1$ and $e(\mathfrak{p}_2|p) = 1, f(\mathfrak{p}_2|p) = 2$.

   Looking at the possibilities for the factorization of $\mathfrak{p}_2$ in L, we observe

   i. Since

   $$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_2)e(\mathfrak{p}|p) = 1 \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}_2)f(\mathfrak{p}|p) = 2,$$

   it follows from $6 = r \cdot e(\mathfrak{P}|p) \cdot f(\mathfrak{P}|p)$ that $r = 3$. Hence

   $$(p)\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3 \implies |D(\mathfrak{P}_i|p)| = 2.$$

   ii. Since

   $$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_2)e(\mathfrak{p}|p) = 2 \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}_2)f(\mathfrak{p}|p) = 2,$$

it follows from $6 = r \cdot e(\mathfrak{P}|p) \cdot f(\mathfrak{P}|p) = r \cdot 4$ that such a case is not possible.

iii. Since

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_2)e(\mathfrak{p}|p) = 1 \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}_2)f(\mathfrak{p}|p) = 4,$$

it follows from $6 = r \cdot e(\mathfrak{P}|p) \cdot f(\mathfrak{P}|p) = r \cdot 4$ that such a case is not possible.

Now, since

$$e(\mathfrak{P}|p) = 1 \quad \text{and} \quad f(\mathfrak{P}|p) = 2$$

is the only possible case, we have that $|D(\mathfrak{P}_i|p)| = 2$ for $i = 1, 2, 3$.

4. $(p)\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2$ with $e(\mathfrak{p}_1|p) = f(\mathfrak{p}_1|p) = 1$ and $e(\mathfrak{p}_2|p) = 2, f(\mathfrak{p}_2|p) = 1$.

Looking at the possibilities for the factorization of $\mathfrak{p}_2$ in L, we observe

i. Since

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_2)e(\mathfrak{p}|p) = 2 \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}_2)f(\mathfrak{p}|p) = 1,$$

it follows from $6 = r \cdot e(\mathfrak{P}|p) \cdot f(\mathfrak{P}|p)$ that $r = 3$. Hence

$$(p)\mathcal{O}_L = \mathfrak{P}_1^2\mathfrak{P}_2^2\mathfrak{P}_3^2 \implies |D(\mathfrak{P}_i|p)| = 2.$$

ii. Since

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_2)e(\mathfrak{p}|p) = 4 \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}_2)f(\mathfrak{p}|p) = 1,$$

it follows from $6 = r \cdot e(\mathfrak{P}|p) \cdot f(\mathfrak{P}|p) = r \cdot 4$ that such a case is not possible.

iii. Since

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_2)e(\mathfrak{p}|p) = 2 \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}_2)f(\mathfrak{p}|p) = 2,$$

it follows from $6 = r \cdot e(\mathfrak{P}|p) \cdot f(\mathfrak{P}|p) = r \cdot 4$ that such a case is not possible.

Now, since

$$e(\mathfrak{P}|p) = 2 \quad \text{and} \quad f(\mathfrak{P}|p) = 1$$

is the only possible case, we have that $|D(\mathfrak{P}_i|p)| = 2$ for $i = 1, 2, 3$.

5. $(p)\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ with $e(\mathfrak{p}_i|p) = f(\mathfrak{p}_i|p) = 1$ for $i = 1, 2, 3$.

Looking at the possibilities for the factorization of $\mathfrak{p}_i$ in L, we observe

i. Since

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_i)e(\mathfrak{p}|p) = 1 \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}_i)f(\mathfrak{p}|p) = 1,$$

it follows from $6 = r \cdot e(\mathfrak{P}|p) \cdot f(\mathfrak{P}|p)$ that $r = 6$. Hence

$$(p)\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4\mathfrak{P}_5\mathfrak{P}_6 \implies |D(\mathfrak{P}_i|p)| = 1.$$

In this case, the only automorphism σ on L such that $\sigma(\mathfrak{P}) = \mathfrak{P}$ is the identity map, hence there can be no cancellation in this case.

ii. Since

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_i)e(\mathfrak{p}|p) = 2 \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}_i)f(\mathfrak{p}|p) = 1,$$

it follows from $6 = r \cdot e(\mathfrak{P}|p) \cdot f(\mathfrak{P}|p)$ that $r = 3$. Hence

$$(p)\mathcal{O}_L = \mathfrak{P}_1^2\mathfrak{P}_2^2\mathfrak{P}_3^2 \implies |D(\mathfrak{P}_i|p)| = 2.$$

iii. Since

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_2)e(\mathfrak{p}|p) = 1 \quad \text{and} \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}_2)f(\mathfrak{p}|p) = 2,$$

it follows from $6 = r \cdot e(\mathfrak{P}|p) \cdot f(\mathfrak{P}|p)$ that $r = 3$. Hence

$$(p)\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3 \implies |D(\mathfrak{P}_i|p)| = 2.$$

From the above list, we observe that we are left to determine whether $D(\mathfrak{P}_i|p)$ having cardinality 2 can result in $\mathfrak{P}^{(i_0)} = \mathfrak{P}^{(j)}$. We recall that the generating automorphisms of S_3 either permute θ or send $\sqrt{D}$ to $-\sqrt{D}$. If we fix $\theta = \theta_1$, then, in sending θ_1 to θ_1, then we either select an element of S_3 that has order 1 (the identity map) or order 2 (τ). To send θ_1 to θ_2, our choices are either an order 3 element (σ) or an order 2 element, $\tau\sigma^2$. Lastly, to send θ_1 to θ_3, we choose either between an order 3 element, σ^2, or an order 2 element, $\tau\sigma$. The choice of the automorphisms themselves do not matter so long as θ is permuted. In other words, we choose (i_0, j, k) so that it forms an order 3 subgroup of S_3. Since only a cardinality 2 subgroup can map a prime ideal $\mathfrak{P}$ to itself, it follows that this choice of

(i_0, j, k) cannot coincide with $D(\mathfrak{P}|p)$ and therefore cannot lead to $\mathfrak{P}^{(i_0)} = \mathfrak{P}^{(j)}$. $\square$

For the remainder of this paper, we assume that (i_0, j, k) are automorphisms of L selected as in Lemma 13.1.

Lemma 13.2. *Let $\mathfrak{P}$ be a finite place of L and let $\mathfrak{P}^{(i_0)} = \sigma_{i_0}(\mathfrak{P})$ and $\mathfrak{P}^{(j)} = \sigma_j(\mathfrak{P})$, where $\sigma_{i_0} : L \to L$, $\theta \mapsto \theta^{(i_0)}$ and $\sigma_j : L \to L$, $\theta \mapsto \theta^{(j)}$ are two automorphisms of L. For*

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

we have

$$\operatorname{ord}_{\mathfrak{P}} \left(\frac{\delta_2}{\lambda} \right) = \begin{cases} (u_l - r_l) e(\mathfrak{P}^{(j)} | \mathfrak{p}_l^{(j)}) & \text{if } \mathfrak{P}^{(j)} \mid p_l,\ p_l \in \{p_1, \ldots, p_\nu\} \\ (r_l - u_l) e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_l^{(i_0)}) & \text{if } \mathfrak{P}^{(i_0)} \mid p_l,\ p_l \in \{p_1, \ldots, p_\nu\} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Lemma 13.1, we have

$$\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}} \right) \mathcal{O}_L = \left(\prod_{\mathfrak{P} | \mathfrak{p}_1} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_1^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_1^{(i_0)})} \right)^{a_{1i}} \cdots \left(\prod_{\mathfrak{P} | \mathfrak{p}_\nu} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_\nu^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_\nu^{(i_0)})} \right)^{a_{\nu i}}.$$

Hence

$$\begin{aligned}
\left(\frac{\delta_2}{\lambda} \right) \mathcal{O}_L &= \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{n_1} \cdots \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{n_\nu} \mathcal{O}_L \\
&= \left(\prod_{\mathfrak{P} | \mathfrak{p}_1} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_1^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_1^{(i_0)})} \right)^{n_1 a_{11}} \cdots \left(\prod_{\mathfrak{P} | \mathfrak{p}_\nu} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_\nu^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_\nu^{(i_0)})} \right)^{n_1 a_{\nu 1}} \cdots \\
&\quad \cdots \left(\prod_{\mathfrak{P} | \mathfrak{p}_1} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_1^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_1^{(i_0)})} \right)^{n_\nu a_{1\nu}} \cdots \left(\prod_{\mathfrak{P} | \mathfrak{p}_\nu} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_\nu^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_\nu^{(i_0)})} \right)^{n_\nu a_{\nu\nu}} \\
&= \left(\prod_{\mathfrak{P} | \mathfrak{p}_1} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_1^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_1^{(i_0)})} \right)^{\sum_{i=1}^{\nu} n_i a_{1i}} \cdots \left(\prod_{\mathfrak{P} | \mathfrak{p}_\nu} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_\nu^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_\nu^{(i_0)})} \right)^{\sum_{i=1}^{\nu} n_i a_{\nu i}} \\
&= \left(\prod_{\mathfrak{P} | \mathfrak{p}_1} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_1^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_1^{(i_0)})} \right)^{u_1 - r_1} \cdots \left(\prod_{\mathfrak{P} | \mathfrak{p}_\nu} \frac{\mathfrak{P}^{(j)}\ e(\mathfrak{P}^{(j)} | \mathfrak{p}_\nu^{(j)})}{\mathfrak{P}^{(i_0)}\ e(\mathfrak{P}^{(i_0)} | \mathfrak{p}_\nu^{(i_0)})} \right)^{u_\nu - r_\nu}
\end{aligned}$$

and so

$$\operatorname{ord}_{\mathfrak{P}}\left(\frac{\delta_2}{\lambda}\right) = \begin{cases} (u_l - r_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}) & \text{if } \mathfrak{P}^{(j)} \mid p_l,\ p_l \in \{p_1, \ldots, p_\nu\} \\ (r_l - u_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)}) & \text{if } \mathfrak{P}^{(i_0)} \mid p_l,\ p_l \in \{p_1, \ldots, p_\nu\} \\ 0 & \text{otherwise.} \end{cases}$$

$\square$

Let $\log^+(\cdot)$ denote the real valued function $\max(\log(\cdot), 0)$ on $\mathbb{R}_{\geq 0}$.

Proposition 13.3. *The height $h\left(\frac{\delta_2}{\lambda}\right)$ admits a decomposition*

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu}\log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}$$

Further, if $\deg g(t) = 3$ then

$$\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = \begin{cases} 2\max_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} & \text{if } \sqrt{\Delta}\notin\mathbb{Q} \\ \max_{w:L\to\mathbb{C}}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} & \text{if } \sqrt{\Delta}\in\mathbb{Q} \end{cases}$$

when one can choose $(i_0), (j), (k) : L \to \mathbb{C}$ such that $\mathfrak{p}_p^{(j)} \neq \mathfrak{p}_p^{(i_0)}$ for all $p \in S$.

Proof of Proposition 13.3. Since $\frac{\delta_2}{\lambda} \in L$, the definition of the absolute logarithmic Weil height gives

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[L:\mathbb{Q}]}\sum_{w\in M_L}\log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\}$$

where $||z||_w$ are the usual norms and M_L is a set of inequivalent absolute values on L.

In particular, if $w : L \to \mathbb{C}$ is an infinite place, we obtain

$$\log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} = \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}.$$

Now, for $z = \frac{\delta_2}{\lambda}$ and $w = \mathfrak{P}$ a finite place, we have

$$\log\max\{\|z\|_w, 1\} = \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{\operatorname{ord}_{\mathfrak{P}}(z)}}\right), 0\right\}.$$

By Lemma 13.2,

$$\operatorname{ord}_{\mathfrak{P}}\left(\frac{\delta_2}{\lambda}\right) = \begin{cases} (u_l - r_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}) & \text{if } \mathfrak{P}^{(j)} \mid p_l,\ p_l \in \{p_1, \ldots, p_\nu\} \\ (r_l - u_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)}) & \text{if } \mathfrak{P}^{(i_0)} \mid p_l,\ p_l \in \{p_1, \ldots, p_\nu\} \\ 0 & \text{otherwise.} \end{cases}$$

That is, for $\mathfrak{P}^{(j)} \mid p_l$ where $p_l \in \{p_1, \ldots, p_\nu\}$, we have

$$\begin{aligned} \log\max\{||z||_w, 1\} &= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{\operatorname{ord}_{\mathfrak{P}}(z)}}\right), 0\right\} \\ &= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{(u_l-r_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)})}}\right), 0\right\} \\ &= \max\left\{\log\left(\frac{1}{p_l^{(u_l-r_l)f(\mathfrak{P}^{(j)}|p_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)})}}\right), 0\right\} \\ &= \max\left\{-(u_l - r_l)f(\mathfrak{P}^{(j)} \mid p_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)})\log(p_l), 0\right\}. \end{aligned}$$

For $p_l \in \{p_1, \ldots, p_\nu\}$, there is 1 unique prime ideal $\mathfrak{p}_1$ in the ideal equation (19) lying above p_l in K. Hence, each $\mathfrak{P}$ lying over p_l must also lie over $\mathfrak{p}_l$. Now,

$$\begin{aligned} \sum_{\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}} \log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} &= \sum_{\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}} \max\left\{-(u_l - r_l)f(\mathfrak{P}^{(j)} \mid p_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)})\log(p_l), 0\right\} \\ &= \max\left\{(r_l - u_l)\log(p_l), 0\right\} \sum_{\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}} f(\mathfrak{P}^{(j)} \mid p_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}) \\ &= \max\left\{(r_l - u_l)\log(p_l), 0\right\} \sum_{\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}} f(\mathfrak{P}^{(j)} \mid \mathfrak{p}_l^{(j)})f(\mathfrak{p}_l^{(j)} \mid p_l)e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}) \\ &= \max\left\{(r_l - u_l)\log(p_l), 0\right\} f(\mathfrak{p}_l^{(j)} \mid p_l) \sum_{\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}} f(\mathfrak{P}^{(j)} \mid \mathfrak{p}_l^{(j)})e(\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}) \\ &= \max\left\{(r_l - u_l)\log(p_l), 0\right\} f(\mathfrak{p}_l^{(j)} \mid p_l)[L : \mathbb{Q}(\theta^{(j)})] \\ &= \max\left\{(r_l - u_l)\log(p_l), 0\right\} f(\mathfrak{p}_l^{(j)} \mid p_l)[L : K]. \end{aligned}$$

where the last inequality follows from $K = \mathbb{Q}(\theta) \cong \mathbb{Q}(\theta^{(j)})$

Similarly, for $\mathfrak{P}^{(i_0)} \mid p_l$ where $p_l \in \{p_1, \ldots, p_\nu\}$, we have

$$\begin{aligned}
\log\max\{\|z\|_w, 1\} &= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{\operatorname{ord}_{\mathfrak{P}}(z)}}\right), 0\right\} \\
&= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{(r_l-u_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)})}}\right), 0\right\} \\
&= \max\left\{\log\left(\frac{1}{p_l^{(r_l-u_l)f(\mathfrak{P}^{(i_0)}|p_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)})}}\right), 0\right\} \\
&= \max\left\{-(r_l-u_l)f(\mathfrak{P}^{(i_0)} \mid p_l)e(\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)})\log(p_l), 0\right\},
\end{aligned}$$

and so

$$\sum_{\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)}} \log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} = \max\left\{(u_l - r_l)\log(p_l), 0\right\} f(\mathfrak{p}_l^{(i_0)} \mid p_l)[L:K].$$

Lastly, if $w = \mathfrak{P}$ such that $\mathfrak{P} \neq \mathfrak{P}^{(i_0)}, \mathfrak{P}^{(j)}$, we have

$$\begin{aligned}
\log\max\{\|z\|_w, 1\} &= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{\operatorname{ord}_{\mathfrak{P}}(z)}}\right), 0\right\} \\
&= \max\left\{\log\left(\frac{1}{N(\mathfrak{P})^{0}}\right), 0\right\} \\
&= 0.
\end{aligned}$$

Now, we have

$$\begin{aligned}
h\left(\frac{\delta_2}{\lambda}\right) &= \frac{1}{[L:\mathbb{Q}]}\sum_{w\in M_L}\log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} \\
&= \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[L:\mathbb{Q}]}\sum_{\mathfrak{P}\in\mathcal{O}_L \text{ finite}}\log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_{\mathfrak{P}}, 1\right\},
\end{aligned}$$

where

$$
\begin{aligned}
&\sum_{\mathfrak{P}\in\mathcal{O}_L \text{ finite}} \log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} \\
&= \sum_{l=1}^{\nu}\left(\sum_{\mathfrak{P}^{(j)}|\mathfrak{p}_l^{(j)}} \log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} + \sum_{\mathfrak{P}^{(i_0)}|\mathfrak{p}_l^{(i_0)}} \log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\}\right) \\
&= \sum_{l=1}^{\nu}\Big(\max\{(r_l-u_l)\log(p_l),0\}\, f(\mathfrak{p}_l^{(j)} \mid p_l)[L:K] + \max\{(u_l-r_l)\log(p_l),0\}\, f(\mathfrak{p}_l^{(i_0)} \mid p_l)[L:K]\Big) \\
&= [L:K]\sum_{l=1}^{\nu}\log(p_l)\left(\max\{-(u_l-r_l),0\}+\max\{(u_l-r_l),0\}\right) \\
&= [L:K]\sum_{l=1}^{\nu}\log(p_l)\max\{-(u_l-r_l),(u_l-r_l)\} \\
&= [L:K]\sum_{l=1}^{\nu}\log(p_l)|u_l-r_l|.
\end{aligned}
$$

Here, we recall that $K=\mathbb{Q}(\theta)\cong\mathbb{Q}(\theta^{(i_0)})\cong\mathbb{Q}(\theta^{(j)})$ and therefore

$$f(\mathfrak{p}_l^{(i_0)} \mid p_l) = f(\mathfrak{p}_l^{(j)} \mid p_l) = f(\mathfrak{p}_l \mid p_l) = 1.$$

Altogether, we have

$$
\begin{aligned}
h\left(\frac{\delta_2}{\lambda}\right) &= \frac{1}{[L:\mathbb{Q}]}\sum_{w\in M_L}\log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_w, 1\right\} \\
&= \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[L:\mathbb{Q}]}\sum_{\mathfrak{P}\in\mathcal{O}_L \text{ finite}}\log\max\left\{\left\|\frac{\delta_2}{\lambda}\right\|_{\mathfrak{P}}, 1\right\} \\
&= \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu}\log(p_l)|u_l-r_l| \\
&= \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\log\left(p_1^{|u_1-r_1|}\cdots p_\nu^{|u_\nu-r_\nu|}\right)
\end{aligned}
$$

To prove the last statement, we first assume that $\sqrt{\Delta}\in\mathbb{Q}$. Then $L=\mathbb{Q}(\theta,\sqrt{\Delta})=\mathbb{Q}(\theta)=K$ and the Galois group of $L/\mathbb{Q}$ is the alternating group A_3. Hence the Galois group is generated by σ, which takes θ to one of the other roots of $g(t)$. In particular,

$$\mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id_L}, \sigma, \sigma^2\},$$

where

$$\mathrm{id_L} : \begin{cases} \theta_1 \mapsto \theta_1 \\ \theta_2 \mapsto \theta_2 \\ \theta_3 \mapsto \theta_3 \\ \sqrt{D} \mapsto \sqrt{D} \end{cases}, \sigma : \begin{cases} \theta_1 \mapsto \theta_2 \\ \theta_2 \mapsto \theta_3 \\ \theta_3 \mapsto \theta_1 \\ \sqrt{D} \mapsto \sqrt{D} \end{cases}, \sigma^2 : \begin{cases} \theta_1 \mapsto \theta_3 \\ \theta_2 \mapsto \theta_1 \\ \theta_3 \mapsto \theta_2 \\ \sqrt{D} \mapsto \sqrt{D} \end{cases},$$

Writing $j = 1, i_0 = 2$ and $k = 3$, the orbit of

$$\frac{\delta_2}{\lambda} = \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(1)}}{\varepsilon_i^{(2)}} \right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(1)}}{\gamma_i^{(2)}} \right)^{n_i} \in L$$

is

$$\left\{ \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(1)}}{\varepsilon_i^{(2)}} \right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(1)}}{\gamma_i^{(2)}} \right)^{n_i}, \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(2)}}{\varepsilon_i^{(3)}} \right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(2)}}{\gamma_i^{(3)}} \right)^{n_i}, \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(3)}}{\varepsilon_i^{(1)}} \right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(3)}}{\gamma_i^{(1)}} \right)^{n_i} \right\}.$$

We choose $a, b, c \in \{1, 2, 3\}$ such that

$$\left| \prod_{i=1}^{r} \left(\varepsilon_i^{(a)} \right)^{a_i} \prod_{i=1}^{\nu} \left(\gamma_i^{(a)} \right)^{n_i} \right| \geq \left| \prod_{i=1}^{r} \left(\varepsilon_i^{(b)} \right)^{a_i} \prod_{i=1}^{\nu} \left(\gamma_i^{(b)} \right)^{n_i} \right| \geq \left| \prod_{i=1}^{r} \left(\varepsilon_i^{(c)} \right)^{a_i} \prod_{i=1}^{\nu} \left(\gamma_i^{(c)} \right)^{n_i} \right|.$$

Then we obtain

$$\begin{aligned}
\sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\} &= \log\max\left\{\left|\mathrm{id}_L\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\} + \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\} \\
&\quad + \log\max\left\{\left|\sigma^2\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\} \\
&= \log\max\left\{\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(a)}}{\varepsilon_i^{(b)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(a)}}{\gamma_i^{(b)}}\right)^{n_i}\right|,1\right\} \\
&\quad + \log\max\left\{\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(b)}}{\varepsilon_i^{(c)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(b)}}{\gamma_i^{(c)}}\right)^{n_i}\right|,1\right\} \\
&\quad + \log\max\left\{\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(c)}}{\varepsilon_i^{(a)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(c)}}{\gamma_i^{(a)}}\right)^{n_i}\right|,1\right\} \\
&= \log\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(a)}}{\varepsilon_i^{(b)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(a)}}{\gamma_i^{(b)}}\right)^{n_i}\right| \\
&\quad + \log\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(b)}}{\varepsilon_i^{(c)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(b)}}{\gamma_i^{(c)}}\right)^{n_i}\right| \\
&= \log\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(a)}}{\varepsilon_i^{(c)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(a)}}{\gamma_i^{(c)}}\right)^{n_i}\right|.
\end{aligned}$$

Hence it follows that

$$\sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\} = \max_{w:L\to\mathbb{C}}\sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\}.$$

It remains to consider the case when $\sqrt{\Delta}\notin\mathbb{Q}$. Then the Galois group of $L/\mathbb{Q}$ is the symmetric group S_3. We now write $j=1, i_0=2$, and $k=3$, the orbit of

$$\frac{\delta_2}{\lambda} = \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(1)}}{\varepsilon_i^{(2)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(1)}}{\gamma_i^{(2)}}\right)^{n_i} \in L$$

is

$$\begin{aligned}
&\left\{\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(1)}}{\varepsilon_i^{(2)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(1)}}{\gamma_i^{(2)}}\right)^{n_i}, \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(2)}}{\varepsilon_i^{(3)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(2)}}{\gamma_i^{(3)}}\right)^{n_i}, \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(3)}}{\varepsilon_i^{(1)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(3)}}{\gamma_i^{(1)}}\right)^{n_i}\right. \\
&\quad\left.\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(3)}}{\varepsilon_i^{(2)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(3)}}{\gamma_i^{(2)}}\right)^{n_i}, \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(1)}}{\varepsilon_i^{(3)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(1)}}{\gamma_i^{(3)}}\right)^{n_i}, \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(2)}}{\varepsilon_i^{(1)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(2)}}{\gamma_i^{(1)}}\right)^{n_i}\right\}.
\end{aligned}$$

We choose $a, b, c \in \{1,2,3\}$ such that

$$\left|\prod_{i=1}^{r}\left(\varepsilon_i^{(a)}\right)^{a_i}\prod_{i=1}^{\nu}\left(\gamma_i^{(a)}\right)^{n_i}\right| \geq \left|\prod_{i=1}^{r}\left(\varepsilon_i^{(b)}\right)^{a_i}\prod_{i=1}^{\nu}\left(\gamma_i^{(b)}\right)^{n_i}\right| \geq \left|\prod_{i=1}^{r}\left(\varepsilon_i^{(c)}\right)^{a_i}\prod_{i=1}^{\nu}\left(\gamma_i^{(c)}\right)^{n_i}\right|.$$

Then we obtain

$$\begin{aligned}
\sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} &= \log\max\left\{\left|\mathrm{id}_L\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} \\
&\quad + \log\max\left\{\left|\sigma^2\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \log\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} \\
&\quad + \log\max\left\{\left|\tau\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \log\max\left\{\left|\tau\sigma^2\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} \\
&= \log\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(a)}}{\varepsilon_i^{(b)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(a)}}{\gamma_i^{(b)}}\right)^{n_i}\right| \\
&\quad + \log\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(b)}}{\varepsilon_i^{(c)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(b)}}{\gamma_i^{(c)}}\right)^{n_i}\right| \\
&\quad + \log\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(a)}}{\varepsilon_i^{(c)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(a)}}{\gamma_i^{(c)}}\right)^{n_i}\right| \\
&= 2\log\left|\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(a)}}{\varepsilon_i^{(c)}}\right)^{a_i}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(a)}}{\gamma_i^{(c)}}\right)^{n_i}\right|.
\end{aligned}$$

Hence it follows that

$$\sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = 2\max_{w:L\to\mathbb{C}} \sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}.$$

□

13.2 Initial height bounds

Recall that we seek solutions to

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

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 $r = 2$.

In Rafael's notation, let

$$y = \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}, \quad x = \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i}$$

so that our equation is
$$\delta_1 y - 1 = \delta_2 x.$$

Equivalently, letting $\mu_0 = \delta_1$ and $\lambda_0 = \delta_2$, we arrive at

$$\mu_0 y - \lambda_0 x = 1,$$

just as in Rafael's notation.

Returning to our notation, we see that

$$\begin{aligned}\lambda &= \delta_2 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i} \\ &= \delta_2 x \\ &= \lambda_0 x.\end{aligned}$$

Hence, let $z := \frac{1}{x} = \frac{\delta_2}{\lambda}$.

Now, let Σ denote the set of pairs (x, y) satisfying the equation

$$\mu_0 y - \lambda_0 x = 1.$$

That is, let Σ denote the set of tuples $(n_1, \ldots, n_\nu, a_1, \ldots, a_r)$ giving x, y which satisfy

$$\mu_0 y - \lambda_0 x = 1.$$

Let $l, h \in \mathbb{R}^{S^*}$ with $0 \leq l \leq h$. Then we define $\Sigma(l, h)$ as the set of all $(x, y) \in \Sigma$ such that

$\left(h_v\left(\frac{\delta_2}{\lambda}\right)\right) \leq h$ and such that $\left(h_v\left(\frac{\delta_2}{\lambda}\right)\right) \nleq l$,

$$\Sigma(l,h) = \{(x,y) \in \Sigma \mid (h_v(z)) \leq h \text{ and } (h_v(z)) \nleq l\}.$$

Since we are comparing vectors, we note that $(h_v(z)) \nleq l$ does not necessarily mean that $l < (h_v(z))$. Instead, this means that not *all* coordinates $h_v(z)$ satisfy $h_v(z) \leq l_v$, and hence there is at least one coordinate for which $h_v(z) > l_v$.

Here we write $\Sigma(h) = \Sigma(l,h)$ if $l = 0$.

$$\Sigma(h) = \Sigma(0,h) = \{(x,y) \in \Sigma \mid (h_v(z)) \leq h \text{ and } (h_v(z)) \nleq 0\},$$

so that at least one coordinate satisfies $h_v(z) > 0$.

Further, for each $w \in S^*$, we denote by $\Sigma_w(l,h)$ the set of all $(x,y) \in \Sigma(h)$ such that $h_w(z) > l_w$.

$$\begin{aligned}\Sigma_w(l,h) &= \{(x,y) \in \Sigma(h) \mid h_w(z) > l_w\}\\ &= \{(x,y) \in \Sigma \mid (h_v(z)) \leq h \text{ and } (h_v(z)) \nleq 0 \text{ and } h_w(z) > l_w\}.\end{aligned}$$

Recall that

$$f(X,Y) = X^3 + C_1X^2Y + C_2XY^2 + C_3Y^3 = cp_1^{z_1} \cdots p_v^{z_v}.$$

and $\gcd(X,Y) = 1$ and $S = \{p_1, \ldots, p_v\}$. Let

$$N_S = \prod_{p \in S} p.$$

To measure an integer m and the finite set S, we take

$$\begin{aligned}m_S &= 1728 N_S^2 \prod_{p \notin S} p^{\min(2,\operatorname{ord}_p(m))}\\ &= 1728 \prod_{p \in S} p^2 \prod_{\substack{p \notin S\\ p \mid m}} p^{\min(2,\operatorname{ord}_p(m))}.\end{aligned}$$

Recall further that the Weil height of an integer $n \in \mathbb{Z}\backslash 0$ is given by

$$h(n) = \log |n|.$$

Now, denote by $h(f-c)$ the maximum logarithmic Weil heights of the coefficients of the polynomial $f-c$,

$$\begin{aligned}
h(f-a) &= h(x^3 + C_1x^2y + C_2xy^2 + C_3y^3 - c) \\
&= \max(h(1), h(C_1), h(C_2), h(C_3), h(-c)) \\
&= \max(\log|1|, \log|C_1|, \log|C_2|, \log|C_3|, \log|c|) \\
&= \max(0, \log|C_1|, \log|C_2|, \log|C_3|, \log|c|) \\
&= \max(\log|C_1|, \log|C_2|, \log|C_3|, \log|c|),
\end{aligned}$$

where we recall that $C_i \in \mathbb{N}$. Put $m = 432\Delta c^2$ with Δ the discriminant of F. Now, let

$$\Omega = 2m_S \log(m_S) + 172h(f-c).$$

By Rafael and Benjamin's paper,

$$\max(h(X), h(Y)) \leq \Omega.$$

We recall that

$$\beta = X - Y\theta = \alpha\zeta\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \cdot \gamma_1^{n_1} \cdots \gamma_\nu^{n_\nu}$$

and we define

$$\Omega' = 2h(\alpha) + 4\Omega + 2h(\theta) + 2\log(2).$$

For $z \in K$, we recall

$$h(z) = \frac{1}{[K:\mathbb{Q}]} \sum_{w \in M_K} \log\max\{\|z\|_w, 1\}$$

where $||z||_w$ are the usual norms and M_K is a set of inequivalent absolute values on K. Now,

$$(\alpha)\mathcal{O}_K = \mathfrak{p}_1^{A_1} \cdots \mathfrak{p}_n^{A_n} \quad \text{and} \quad (\theta)\mathcal{O}_K = \mathfrak{p}_1^{B_1} \cdots \mathfrak{p}_m^{B_m}.$$

For $w = \mathfrak{p}$ a finite place, we have

$$\log\max\{\|z\|_w, 1\} = \max\left\{\log\left(\frac{1}{N(\mathfrak{p}_i)^{\mathrm{ord}_{\mathfrak{p}_i}(\alpha)}}\right), 0\right\} = \max\left\{\log\left(\frac{1}{p^{fA_i}}\right), 0\right\} = 0$$

and

$$\log\max\{\|z\|_w, 1\} = \max\left\{\log\left(\frac{1}{N(\mathfrak{p}_i)^{\mathrm{ord}_{\mathfrak{p}_i}(\theta)}}\right), 0\right\} = \max\left\{\log\left(\frac{1}{p^{fB_i}}\right), 0\right\} = 0.$$

It follows that

$$h(\alpha) = \frac{1}{[K:\mathbb{Q}]}\sum_{w\in M_K}\log\max\left\{\|\alpha\|_w, 1\right\} = \frac{1}{[K:\mathbb{Q}]}\sum_{\sigma:K\to\mathbb{C}}\log\max\left\{|\sigma(\alpha)|, 1\right\}$$

and

$$h(\theta) = \frac{1}{[K:\mathbb{Q}]}\sum_{w\in M_K}\log\max\left\{\|\theta\|_w, 1\right\} = \frac{1}{[K:\mathbb{Q}]}\sum_{\sigma:K\to\mathbb{C}}\log\max\left\{|\sigma(\theta)|, 1\right\}.$$

Now,

$$\begin{aligned}\Omega' &= 2h(\alpha) + 4\Omega + 2h(\theta) + 2\log(2)\\ &= \frac{2}{[K:\mathbb{Q}]}\sum_{\sigma:K\to\mathbb{C}}\log\max\left\{|\sigma(\alpha)|, 1\right\} + 4\Omega + \frac{2}{[K:\mathbb{Q}]}\sum_{\sigma:K\to\mathbb{C}}\log\max\left\{|\sigma(\theta)|, 1\right\} + 2\log(2)\end{aligned}$$

Lemma 13.4. *Let* $\mathbf{m} = (n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{r+\nu}$ *be any solution of* (22). *If* $\mathbf{h} \in \mathbb{R}^{\nu+r}$ *with* $\mathbf{h} = (\Omega')$, *then* $\mathbf{m} \in \Sigma(h)$, *where*

$$\Sigma(h) = \Sigma(0, h) = \{(x, y) \in \Sigma \mid (h_v(z)) \leq h \text{ and } (h_v(z)) \not\leq 0\},$$

That is, all solutions $(x, y) \in \Sigma$ satisfy $\mathbf{m} \in \Sigma(h)$ if $\mathbf{h} = (\Omega')$.

Proof. Let $(x, y) \in \Sigma$. Then (x, y) satisfy $\mu_0 y - \lambda_0 x = 1$. We must show that the resulting value of $z := \frac{1}{x} = \frac{\delta_2}{\lambda}$ arising from this choice of x, y satisfies

$$0 < \left(h_v\left(\frac{\delta_2}{\lambda}\right)\right) \leq h.$$

Now, via Rafael and Benjamin, for a solution X, Y of $f(X, Y) = cp_1^{z_1}\cdots p_v^{z_v}$, we have

$$\max(h(X), h(Y)) \leq \Omega.$$

We use the following height properties

1. For a non-zero rational number a/b where $\gcd(a,b)=1$,

$$h(a/b) = \max\{\log|a|, \log|b|\}$$

2. For $\alpha \in \overline{\mathbb{Q}}$, $n \in \mathbb{N}$, we have

$$h(n\alpha) = nh(\alpha).$$

3. For $\alpha, \beta \in \overline{\mathbb{Q}}$, we have

$$h(\alpha+\beta) \le h(\alpha) + h(\beta) + \log 2.$$

4. For $\alpha, \beta \in \overline{\mathbb{Q}}$, we have

$$h(\alpha\beta) \le h(\alpha) + h(\beta).$$

5. For $\alpha \in \overline{\mathbb{Q}}$, we have

$$h(1/\alpha) = h(\alpha).$$

Now, applying these properties to $\beta = X - \theta Y$, we obtain

$$\begin{aligned} h(\beta) &= h(X - \theta Y) \\ &\le h(X) + h(-\theta Y) + \log 2 \\ &\le h(X) + h(-\theta) + h(Y) + \log 2 \\ &= h(X) + h(\theta) + h(Y) + \log 2 \\ &\le 2\Omega + h(\theta) + \log 2. \end{aligned}$$

Now, $h(\beta) = h(\beta^{(i)})$, hence

$$h(\beta^{(i)}) \le 2\Omega + h(\theta) + \log 2.$$

Further, we have

$$
\begin{aligned}
\delta_2 x &= \delta_2 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}} \right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}} \right)^{n_i} \\
&= \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\alpha^{(i_0)}\zeta^{(i_0)}}{\alpha^{(j)}\zeta^{(j)}} \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}} \right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}} \right)^{n_i} \\
&= \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}}.
\end{aligned}
$$

This means that

$$
\begin{aligned}
x &= \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}} \cdot \frac{1}{\delta_2} \\
&= \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}} \cdot \frac{1}{\frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\alpha^{(i_0)}\zeta^{(i_0)}}{\alpha^{(j)}\zeta^{(j)}}} \\
&= \frac{\theta^{(j)} - \theta^{(k)}}{\theta^{(k)} - \theta^{(i_0)}} \cdot \frac{\beta^{(i_0)}}{\beta^{(j)}} \cdot \frac{\theta^{(k)} - \theta^{(i_0)}}{\theta^{(j)} - \theta^{(k)}} \cdot \frac{\alpha^{(j)}\zeta^{(j)}}{\alpha^{(i_0)}\zeta^{(i_0)}} \\
&= \frac{\beta^{(i_0)}}{\beta^{(j)}} \cdot \frac{\alpha^{(j)}\zeta^{(j)}}{\alpha^{(i_0)}\zeta^{(i_0)}}.
\end{aligned}
$$

Hence,

$$
\begin{aligned}
h(x) &= h\left(\frac{\beta^{(i_0)}}{\beta^{(j)}} \cdot \frac{\alpha^{(j)}\zeta^{(j)}}{\alpha^{(i_0)}\zeta^{(i_0)}} \right) \\
&= h(\beta^{(i_0)}) + h\left(\frac{1}{\beta^{(j)}}\right) + h(\alpha^{(j)}) + h\left(\frac{1}{\alpha^{(i_0)}}\right) + h(\zeta^{(j)}) + h\left(\frac{1}{\zeta^{(i_0)}}\right) \\
&= 2h(\beta) + 2h(\alpha) + 2h(\zeta) \\
&\leq 2(2\Omega + h(\theta) + \log 2) + 2h(\alpha) + 2h(\zeta) \\
&= 4\Omega + 2h(\theta) + 2\log 2 + 2h(\alpha) + 2h(\zeta).
\end{aligned}
$$

Now,

$$\begin{aligned}
h(\zeta) &= \frac{1}{[K:\mathbb{Q}]} \sum_{w \in M_K} \log \max \{\|\zeta\|_w, 1\} \\
&= \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma: K \to \mathbb{C}} \log \max \{|\sigma(\zeta)|, 1\} \\
&= \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma: K \to \mathbb{C}} \log \max \{1, 1\} \\
&= 0.
\end{aligned}$$

Therefore,

$$h(x) \leq 4\Omega + 2h(\theta) + 2\log 2 + 2h(\alpha) = \Omega'$$

and hence

$$h(z) = h\left(\frac{\delta_2}{\lambda}\right) = h(1/x) = h(x) \leq \Omega'.$$

Together with $h_v\left(\frac{\delta_2}{\lambda}\right) \leq h\left(\frac{\delta_2}{\lambda}\right)$ implies

$$h_v\left(\frac{\delta_2}{\lambda}\right) \leq \Omega'$$

for each $v \in S^*$. Similarly, by definition, we have $h_v\left(\frac{\delta_2}{\lambda}\right) \geq 0$. That is, $(x, y) \in \Sigma(h)$ as required. □

13.3 Coverings of Σ

From the previous section, we see that all solutions $(x, y) \in \Sigma$ satisfy $\mathbf{m} \in \Sigma(h)$ if $\mathbf{h} = (\Omega')$.

Now, let $l, h \in \mathbb{R}^{\nu+r}$ with $0 \leq l \leq h$. With the definitions of the previous section, we have that

Lemma 13.5. *It holds that* $\Sigma(h) = \Sigma(l, h) \cup \Sigma(l)$ *and* $\Sigma(l, h) = \cup_{v \in S^*} \Sigma_v(l, h)$.

Proof. Recall that

$$\Sigma(l, h) = \{(x, y) \in \Sigma \mid (h_v(z)) \leq h \text{ and } (h_v(z)) \nleq l\},$$

$$\Sigma(h) = \Sigma(0, h) = \{(x, y) \in \Sigma \mid (h_v(z)) \leq h \text{ and } (h_v(z)) \nleq 0\},$$

and for each $w \in S^*$

$$\Sigma_w(l, h) = \{(x, y) \in \Sigma \mid (h_v(z)) \leq h \text{ and } (h_v(z)) \nleq 0 \text{ and } h_w(z) > l_w\}.$$

Suppose $(x, y) \in \Sigma(h)$. By definition this means, $(h_v(z)) \leq h$ and that $h_v(z) > 0$ for at least one coordinate. Since $0 \leq l \leq h$, it follows that either $(h_v(z)) \leq l$ or $(h_v(z)) \nleq l$. That is, either all coordinates satisfy $h_v(z) \leq l_v$, or there is at least one coordinate for which $h_v(z) > l_v$, meaning that either $(x, y) \in \Sigma(l)$ or $(x, y) \in \Sigma(l, h)$. Hence $(x, y) \in \Sigma(l, h) \cup \Sigma(l)$. That is, $\Sigma(h) \subseteq \Sigma(l, h) \cup \Sigma(l)$.

Conversely, we suppose that $(x, y) \in \Sigma(l, h) \cup \Sigma(l)$. It follows that either $(h_v(z)) \leq h$ and $(h_v(z)) \nleq l$ or $(h_v(z)) \leq l$ and $(h_v(z)) \nleq 0$. In either case, this means that $(h_v(z)) \leq h$ and $(h_v(z)) \nleq 0$. Hence $(x, y) \in \Sigma(h)$. Thus $\Sigma(h) \supseteq \Sigma(l, h) \cup \Sigma(l)$. Together with the previous paragraph, this yields $\Sigma(h) = \Sigma(l, h) \cup \Sigma(l)$.

To prove the second point, let $(x, y) \in \Sigma(l, h)$. Then there exists $w \in S^*$ with $h_w(z) > l_w$ and thus (x, y) lies in $\Sigma_w(l, h)$. Hence $\Sigma(l, h) \subseteq \cup_{v \in S^*} \Sigma_v(l, h)$. Lastly, since each set $\Sigma_v(l, h)$ is contained in $\Sigma(l, h)$ it follows that $\Sigma(l, h) = \cup_{v \in S^*} \Sigma_v(l, h)$. □

Suppose now we are given an initial bound h_0 with $\Sigma = \Sigma(h_0)$ and pairs $(l_n, h_n) \in \mathbb{R}^{\nu+r} \times \mathbb{R}^{\nu+r}$ with $0 \leq l_n \leq h_n$ and $h_{n+1} = l_n$ for $n = 0, \ldots, N$. Then we can cover Σ:

$$\Sigma = \Sigma(l_N) \cup \left(\cup_{n=0}^{N} \cup_{v \in S^*} \Sigma_v(l_n, h_n)\right).$$

Indeed this follows directly by applying the above lemma N times. In the subsequent sections, we shall show that one can efficiently enumerate each set $\Sigma_v(l_n, h_n)$ by finding all points in the intersection $\Gamma_v \cap \mathcal{E}_v$ of a lattice Γ_v with an ellipsoid $\mathcal{E}_v$.

If $h_0 = (b, \ldots, b)$ for b the initial height bound, then Lemma 13.5 gives

$$\Sigma = \Sigma(h_0), \quad \Sigma(h) = \Sigma(l, h) \cup \Sigma(l) \quad \text{and} \quad \Sigma(l, h) = \cup_{v \in S^*} \Sigma_v(l, h).$$

Thus, after choosing a good sequence of lower and upper bounds (i.e. $l, h \in R^{S^*}$ with $0 \leq l \leq h$) covering the whole space $0 \leq h_0$, we are reduced to compute $\Sigma_v(l, h)$.

13.3.1 Refined coverings

13.4 Controlling the exponents in terms of the Weil Height

We now work with the norm $\|\cdot\|_\infty$. However, below we shall give much more precise estimates (which are essentially optimal) to make the volumes of the involved ellipsoids as small as possible.

13.4.1 Bounding $\{n_1, \ldots, n_\nu\}$

Lemma 13.6. *For any solution* $(x, y, a_1, \ldots, a_r, n_1, \ldots, n_\nu)$ *of* (22)*, we have*

$$\|\mathbf{n}\|_\infty \leq \|A^{-1}\|_\infty \frac{h\left(\frac{\delta_2}{\lambda}\right)}{\log(2)}.$$

Proof. Recall that $\mathbf{n} = (n_1, \ldots, n_\nu)^{\mathrm{T}}$ and

$$A\mathbf{n} = \mathbf{u} - \mathbf{r}.$$

Now, taking the $\|\cdot\|_\infty$ norm of both sides yields

$$\mathbf{n} = A^{-1}(\mathbf{u} - \mathbf{r}) \implies \|\mathbf{n}\|_\infty = \|A^{-1}(\mathbf{u} - \mathbf{r})\|_\infty \leq \|A^{-1}\|_\infty \|\mathbf{u} - \mathbf{r}\|_\infty.$$

Here,

$$\|\mathbf{u} - \mathbf{r}\|_\infty = \max_{1 \leq l \leq \nu} |u_l - r_l|.$$

Now, since

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[L : \mathbb{Q}]} \sum_{w : L \to \mathbb{C}} \log \max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K : \mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l)|u_l - r_l|,$$

it follows that

$$0 \leq |u_l - r_l| \log(p_l) \leq h\left(\frac{\delta_2}{\lambda}\right)$$

for each $l \in \{1, \ldots, \nu\}$. In other words,

$$|u_l - r_l| \leq \frac{h\left(\frac{\delta_2}{\lambda}\right)}{\log(p_l)}$$

and so

$$\max_{1\le l\le \nu} |u_l - r_l| \le \max_{1\le l\le \nu}\left(\frac{h\left(\frac{\delta_2}{\lambda}\right)}{\log(p_l)}\right) = \frac{h\left(\frac{\delta_2}{\lambda}\right)}{\log(2)}.$$

Altogether this gives

$$\|\mathbf{n}\|_\infty \le \|A^{-1}\|_\infty \|\mathbf{u}-\mathbf{r}\|_\infty \le \|A^{-1}\|_\infty \frac{h\left(\frac{\delta_2}{\lambda}\right)}{\log(2)}.$$

□

13.4.2 Bounding $\{a_1, \ldots, a_r\}$

We next consider the quadratic form $q_f = A^T D^2 A$ on $\mathbb{Z}^\nu$ and where D^2 is a $\nu \times \nu$ diagonal matrix with diagonal entries $\lfloor \frac{\log(p_i)^2}{\log(2)^2} \rfloor$ for $p_i \in S$. We note that $\lfloor (\log(2))^2 \rfloor = 0$, so if the diagonal entries of D were set to $\lfloor \log(p_i)^2$ and $2 \in S$, our matrix D would not be invertible. In this case, when generating the lattice and ellipsoid, this will yield a matrix which is not positive-definite, meaning that we will not be able to apply Fincke-Pohst. With this in mind, the quadratic form q_f is positive definite since A is invertible.

Lemma 13.7. *For any solution $(x, y, n_1, \ldots, n_\nu, a_1, \ldots, a_r)$ of (22), we have*

$$\frac{\log(2)^2}{[K:\mathbb{Q}]} q_f(\mathbf{n}) = \frac{\log(2)^2}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \left\lfloor \frac{\log(p_l)^2}{\log(2)^2} \right\rfloor |u_l - r_l|^2 < \left(h\left(\frac{\delta_2}{\lambda}\right)\right)^2.$$

Proof. Recall that $\mathbf{n} = (n_1, \ldots, n_\nu)^{\mathrm{T}}$ and

$$A\mathbf{n} = \mathbf{u} - \mathbf{r}.$$

Assume first that $2 \notin S$. Now

$$\begin{aligned}
q_f(\mathbf{n}) &= (A\mathbf{n})^{\mathrm{T}} D^2 A\mathbf{n} \\
&= \mathbf{n}^{\mathrm{T}} A^{\mathrm{T}} D^2 A\mathbf{n} \\
&= (\mathbf{u}-\mathbf{r})^{\mathrm{T}} D^2 (\mathbf{u}-\mathbf{r}) \\
&= \begin{pmatrix} u_1 - r_1 & \dots & u_\nu - r_\nu \end{pmatrix} \begin{pmatrix} \lfloor \frac{\log(p_1)^2}{\log(2)^2} \rfloor & 0 & \dots & 0 \\ 0 & \lfloor \frac{\log(p_2)^2}{\log(2)^2} \rfloor & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lfloor \frac{\log(p_\nu)^2}{\log(2)^2} \rfloor \end{pmatrix} \begin{pmatrix} u_1 - r_1 \\ \vdots \\ u_\nu - r_\nu \end{pmatrix} \\
&= \left\lfloor \frac{\log(p_1)^2}{\log(2)^2} \right\rfloor (u_1 - r_1)^2 + \dots + \left\lfloor \frac{\log(p_\nu)^2}{\log(2)^2} \right\rfloor (u_\nu - r_\nu)^2 \\
&= \sum_{l=1}^{\nu} \left\lfloor \frac{\log(p_l)^2}{\log(2)^2} \right\rfloor |u_l - r_l|^2.
\end{aligned}$$

Hence it follows that

$$q_f(\mathbf{n}) = \sum_{l=1}^{\nu} \left\lfloor \frac{\log(p_l)^2}{\log(2)^2} \right\rfloor |u_l - r_l|^2.$$

Now, recall that

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]} \sum_{w:L \to \mathbb{C}} \log\max\left\{ \left| w\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\}.$$

It follows that

$$\begin{aligned}
\frac{\log(2)^2}{[K:\mathbb{Q}]} q_f(\mathbf{n}) &= \frac{\log(2)^2}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \left\lfloor \frac{\log(p_l)^2}{\log(2)^2} \right\rfloor |u_l - r_l|^2 \\
&\le \frac{\log(2)^2}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \frac{\log(p_l)^2}{\log(2)^2} |u_l - r_l|^2 \\
&= \frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l)^2 |u_l - r_l|^2
\end{aligned}$$

since all terms are positive.

If $2 \in S$, we have

$$
\begin{aligned}
q_f(\mathbf{n}) &= (A\mathbf{n})^{\mathrm{T}} D^2 A\mathbf{n} \\
&= \mathbf{n}^{\mathrm{T}} A^{\mathrm{T}} D^2 A\mathbf{n} \\
&= (\mathbf{u}-\mathbf{r})^{\mathrm{T}} D^2 (\mathbf{u}-\mathbf{r}) \\
&= \begin{pmatrix} u_1 - r_1 & \dots & u_\nu - r_\nu \end{pmatrix}
\begin{pmatrix}
\lfloor \frac{\log(2)^2}{\log(2)^2} \rfloor & 0 & \dots & 0 \\
0 & \lfloor \frac{\log(p_2)^2}{\log(2)^2} \rfloor & \dots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \dots & \lfloor \frac{\log(p_\nu)^2}{\log(2)^2} \rfloor
\end{pmatrix}
\begin{pmatrix} u_1 - r_1 \\ \vdots \\ u_\nu - r_\nu \end{pmatrix} \\
&= \begin{pmatrix} u_1 - r_1 & \dots & u_\nu - r_\nu \end{pmatrix}
\begin{pmatrix}
1 & 0 & \dots & 0 \\
0 & \lfloor \frac{\log(p_2)^2}{\log(2)^2} \rfloor & \dots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \dots & \lfloor \frac{\log(p_\nu)^2}{\log(2)^2} \rfloor
\end{pmatrix}
\begin{pmatrix} u_1 - r_1 \\ \vdots \\ u_\nu - r_\nu \end{pmatrix} \\
&= (u_1 - r_1)^2 + \left\lfloor \frac{\log(p_2)^2}{\log(2)^2} \right\rfloor (u_2 - r_2)^2 + \dots + \left\lfloor \frac{\log(p_\nu)^2}{\log(2)^2} \right\rfloor (u_\nu - r_\nu)^2 \\
&= |u_1 - r_1|^2 + \sum_{l=2}^{\nu} \left\lfloor \frac{\log(p_l)^2}{\log(2)^2} \right\rfloor |u_l - r_l|^2.
\end{aligned}
$$

Hence it follows that

$$
q_f(\mathbf{n}) = |u_1 - r_1|^2 + \sum_{l=2}^{\nu} \left\lfloor \frac{\log(p_l)^2}{\log(2)^2} \right\rfloor |u_l - r_l|^2.
$$

Now, recall that

$$
h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]} \sum_{w:L\to\mathbb{C}} \log\max\left\{ \left| w\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\}.
$$

It follows that

$$\begin{aligned}
\frac{\log(2)^2}{[K:\mathbb{Q}]} q_f(\mathbf{n}) &= \frac{\log(2)^2}{[K:\mathbb{Q}]}\left(|u_1-r_1|^2+\sum_{l=2}^{\nu}\left\lfloor\frac{\log(p_l)^2}{\log(2)^2}\right\rfloor|u_l-r_l|^2\right)\\
&\leq \frac{\log(2)^2}{[K:\mathbb{Q}]}\left(|u_1-r_1|^2+\sum_{l=2}^{\nu}\frac{\log(p_l)^2}{\log(2)^2}|u_l-r_l|^2\right)\\
&= \frac{1}{[K:\mathbb{Q}]}\left(\log(2)^2|u_1-r_1|^2+\sum_{l=2}^{\nu}\log(p_l)^2|u_l-r_l|^2\right)\\
&= \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu}\log(p_l)^2|u_l-r_l|^2
\end{aligned}$$

since all terms are positive. □

Now,

$$\frac{\log(2)^2}{[K:\mathbb{Q}]} q_f(\mathbf{n}) = \frac{\log(2)^2}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu}\left\lfloor\frac{\log(p_l)^2}{\log(2)^2}\right\rfloor|u_l-r_l|^2.$$

Take $\mathbf{h}\in\mathbb{R}^{r+\nu}$ such that $\mathbf{h}\geq\mathbf{0}$. Let $\mathbf{m}=(n_1,\dots,n_\nu,a_1,\dots,a_r)\in\mathbb{R}^{r+\nu}$ be any solution of (22). Denote by $h_v\left(\frac{\delta_2}{\lambda}\right)$ the v^{th} entry of the solution vector

$$\left(\log(p_1)|u_1-r_1|,\dots,\log(p_\nu)|u_\nu-r_\nu|,\log\max\left\{\left|w_1\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\},\dots,\log\max\left\{\left|w_n\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\}\right)$$

and suppose $h_v(z)\leq h_v$ for all $v\in\{1,\dots,r+\nu\}$. Then we deduce

$$\log(2)^2 q_f(\mathbf{n}) = \log(2)^2\sum_{k=1}^{\nu}\left\lfloor\frac{\log(p_k)^2}{\log(2)^2}\right\rfloor|u_k-r_k|^2 \leq \sum_{k=1}^{\nu}\log(p_k)^2|u_k-r_k|^2 \leq \sum_{k=1}^{\nu}h_k^2.$$

Recall that for the degree 3 Thue-Mahler equation, either $r=1$ or $r=2$. Choose a set I of embeddings $L\to\mathbb{C}$ of cardinality r. For $r=1$, this is simply

$$R=\left(\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right|\right).$$

Clearly, as long as we choose ι_1 such that $\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right|\neq 0$, that is $\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right|\neq 1$, this matrix is invertible, with inverse matrix

$$R^{-1} = \left(\frac{1}{\log \left| \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}} \right)^{\iota_1} \right|} \right).$$

When $r = 2$, we let I be the set of embeddings $L \to \mathbb{C}$ of cardinality 2 such that for any $\alpha \in K$, it holds that $I\alpha^{(i_0)} \cup I\alpha^{(j)} = \mathrm{Gal}(L/\mathbb{Q})\alpha$. Such a set I exists. Then we consider the 2×2 matrix

$$R = \begin{pmatrix} \log \left| \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}} \right)^{\iota_1} \right| & \log \left| \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}} \right)^{\iota_1} \right| \\ \log \left| \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}} \right)^{\iota_2} \right| & \log \left| \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}} \right)^{\iota_2} \right| \end{pmatrix}.$$

Here, we let I be the set of embeddings $L \to \mathbb{C}$ of cardinality 2 such that for any $\alpha \in K$, it holds that $I\alpha^{(i_0)} \cup I\alpha^{(j)} = \mathrm{Gal}(L/\mathbb{Q})\alpha$. Such a set I exists.

Lemma 13.8. *When $r = 2$, the matrix R has an inverse*

$$R^{-1} = \begin{pmatrix} \overline{r}_{11} & \overline{r}_{12} \\ \overline{r}_{21} & \overline{r}_{22} \end{pmatrix}.$$

Proof. See Rafael's proof. $\square$

Bounding $\{a_1, \ldots, a_r\}$ when $r = 1$.

Suppose first that $r = 1$. Now, for any solution $(x, y, a_1, n_1, \ldots, n_\nu)$ of (22), set

$$\vec{\varepsilon} = \begin{pmatrix} a_1 \end{pmatrix}.$$

Now,

$$\begin{aligned} R\vec{\varepsilon} &= \left(\log \left| \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}} \right)^{\iota_1} \right| \right) \begin{pmatrix} a_1 \end{pmatrix} \\ &= \left(a_1 \log \left| \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}} \right)^{\iota_1} \right| \right) \\ &= \left(\log \left| \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}} \right)^{\iota_1} \right|^{a_1} \right) \\ &= \left(\log \left| \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}} \right)^{\iota_1 \ a_1} \right| \right). \end{aligned}$$

Since R is invertible, we find

$$\vec{\varepsilon} = \left(a_1\right) = R^{-1}\left(\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1}\right|\right)$$
$$= \left(\frac{1}{\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right|}\right)\left(\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1}\right|\right)$$
$$= \left(\overline{r}_{11}\right)\left(\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1}\right|\right)$$
$$= \left(\overline{r}_{11}\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1}\right|\right).$$

It follows that

$$a_1 = \overline{r}_{11}\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1}\right|.$$

Now, to estimate $|a_1|$, we begin to estimate the sum on the right hand side. For this, we consider

$$\frac{\delta_2}{\lambda} = \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{a_1}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{n_i}.$$

For any embedding $\iota : L \to \mathbb{C}$, we have

$$\left(\frac{\delta_2}{\lambda}\right)^{\iota}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\ n_i} = \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota\ a_1}.$$

Taking absolute values, we obtain

$$\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\ n_i}\right| = \left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota\ a_1}\right|,$$

so that

$$\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota\ a_1}\right| = \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota}\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\ n_i}\right|$$
$$= \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota}\right| + \log\left|\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\ n_i}\right|$$
$$= \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota}\right| - \log\left|\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{\iota\ n_i}\right|.$$

Hence,

$$
\begin{aligned}
a_1 &= \overline{r}_{11} \log \left| \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}} \right)^{\iota_1 \ a_1} \right| \\
&= \overline{r}_{11} \left(\log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| - \log \left| \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}} \right)^{\iota_1 \ n_i} \right| \right) \\
&= \overline{r}_{11} \left(\log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| - n_1 \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| - \cdots - n_\nu \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right| \right).
\end{aligned}
$$

Recall that

$$A\mathbf{n} = \mathbf{u} - \mathbf{r}$$

so

$$\mathbf{n} = A^{-1}(\mathbf{u} - \mathbf{r}).$$

If

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1\nu} \\ a_{21} & a_{22} & \dots & a_{2\nu} \\ \vdots & \vdots & \ddots & \vdots \\ a_{\nu 1} & a_{\nu 2} & \dots & a_{\nu\nu} \end{pmatrix},$$

then

$$A^{-1} = \begin{pmatrix} \overline{a}_{11} & \overline{a}_{12} & \dots & \overline{a}_{1\nu} \\ \overline{a}_{21} & \overline{a}_{22} & \dots & \overline{a}_{2\nu} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{a}_{\nu 1} & \overline{a}_{\nu 2} & \dots & \overline{a}_{\nu\nu} \end{pmatrix},$$

and

$$\begin{pmatrix} n_1 \\ \vdots \\ n_\nu \end{pmatrix} = \mathbf{n} = A^{-1}(\mathbf{u} - \mathbf{r})$$

$$= \begin{pmatrix} \overline{a}_{11} & \overline{a}_{12} & \dots & \overline{a}_{1\nu} \\ \overline{a}_{21} & \overline{a}_{22} & \dots & \overline{a}_{2\nu} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{a}_{\nu 1} & \overline{a}_{\nu 2} & \dots & \overline{a}_{\nu\nu} \end{pmatrix} \begin{pmatrix} u_1 - r_1 \\ \vdots \\ u_\nu - r_\nu \end{pmatrix}$$

$$= \begin{pmatrix} \overline{a}_{11}(u_1 - r_1) + \cdots + \overline{a}_{1\nu}(u_\nu - r_\nu) \\ \vdots \\ \overline{a}_{\nu 1}(u_1 - r_1) + \cdots + \overline{a}_{\nu\nu}(u_\nu - r_\nu) \end{pmatrix}$$

$$= \begin{pmatrix} \sum_{k=1}^{\nu} \overline{a}_{1k}(u_k - r_k) \\ \vdots \\ \sum_{k=1}^{\nu} \overline{a}_{\nu k}(u_k - r_k) \end{pmatrix}$$

Now,

$$\begin{aligned}
a_1 &= \overline{r}_{11} \left(\log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| - n_1 \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| - \cdots - n_\nu \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right| \right) \\
&= \overline{r}_{11} \left(\log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| - (\overline{a}_{11}(u_1 - r_1) + \cdots + \overline{a}_{1\nu}(u_\nu - r_\nu)) \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| - \cdots \right. \\
&\qquad \left. \cdots - (\overline{a}_{\nu 1}(u_1 - r_1) + \cdots + \overline{a}_{\nu\nu}(u_\nu - r_\nu)) \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right| \right) \\
&= \overline{r}_{11} \left[\log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| - (u_1 - r_1) \left(\overline{a}_{11} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| + \cdots + \overline{a}_{\nu 1} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right| \right) - \cdots \right. \\
&\qquad \left. \cdots - (u_\nu - r_\nu) \left(\overline{a}_{1\nu} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| + \cdots + \overline{a}_{\nu\nu} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right| \right) \right] \\
&= \overline{r}_{11} \left[\log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| - (u_1 - r_1)\alpha_{\gamma 1} - \cdots - (u_\nu - r_\nu)\alpha_{\gamma\nu} \right] \\
&= \overline{r}_{11} \left(\log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| - \sum_{k=1}^{\nu} (u_k - r_k)\alpha_{\gamma k} \right)
\end{aligned}$$

where

$$\alpha_{\gamma k} = \overline{a}_{1k} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| + \cdots + \overline{a}_{\nu k} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right|.$$

Taking absolute values, this yields

$$\begin{aligned} |a_1| &= \left| \overline{r}_{11} \left(\log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| - \sum_{k=1}^{\nu} (u_k - r_k) \alpha_{\gamma k} \right) \right| \\ &\leq |\overline{r}_{11}| \left| \log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| \right| + \left| - \sum_{k=1}^{\nu} (u_k - r_k) \alpha_{\gamma k} \overline{r}_{11} \right| \\ &\leq |\overline{r}_{11}| \left| \log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| \right| + \sum_{k=1}^{\nu} |u_k - r_k| |\alpha_{\gamma k} \overline{r}_{11}|. \end{aligned}$$

Now, if $\log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| \geq 0$ we obtain

$$\begin{aligned} |a_1| &\leq |\overline{r}_{11}| \left| \log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| \right| + \sum_{k=1}^{\nu} |u_k - r_k| |\alpha_{\gamma k} \overline{r}_{11}| \\ &\leq |\overline{r}_{11}| \log \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right| + \sum_{k=1}^{\nu} |u_k - r_k| |\alpha_{\gamma k} \overline{r}_{11}| \\ &\leq |\overline{r}_{11}| \log \max \left\{ \left| \left(\frac{\delta_2}{\lambda} \right)^{\iota_1} \right|, 1 \right\} + \sum_{k=1}^{\nu} |u_k - r_k| |\alpha_{\gamma k} \overline{r}_{11}| \\ &\leq \sum_{\sigma : L \to \mathbb{C}} |\overline{r}_{11}| \log \max \left\{ \left| \sigma \left(\frac{\delta_2}{\lambda} \right) \right|, 1 \right\} + \sum_{k=1}^{\nu} |\alpha_{\gamma k} \overline{r}_{11}| |u_k - r_k|. \end{aligned}$$

Recall that $\frac{\delta_2}{\lambda}$ is a quotient of elements which are conjugate to one another. In other words, taking the norm on L of $\frac{\delta_2}{\lambda}$, we obtain $N\left(\frac{\delta_2}{\lambda}\right) = 1$. On the other hand, by definition, we have

$$1 = N\left(\frac{\delta_2}{\lambda}\right) = \prod_{\sigma : L \to \mathbb{C}} \sigma\left(\frac{\delta_2}{\lambda}\right).$$

Taking absolute values and logarithms,

$$0 = \sum_{\sigma : L \to \mathbb{C}} \log \left| \sigma \left(\frac{\delta_2}{\lambda} \right) \right|$$

so that

$$-\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| = -\log\left|\iota_1\left(\frac{\delta_2}{\lambda}\right)\right| = \sum_{\substack{\sigma\,:\,L\to\mathbb{C}\\ \sigma\neq\iota_1}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|.$$

Hence if $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| < 0$ we obtain

$$\begin{aligned}
|a_1| &\leq |\overline{r}_{11}|\left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right| + \sum_{k=1}^{\nu}|u_k - r_k||\alpha_{\gamma k}\overline{r}_{11}| \\
&\leq |\overline{r}_{11}|\left(-\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right) + \sum_{k=1}^{\nu}|u_k - r_k||\alpha_{\gamma k}\overline{r}_{11}| \\
&= |\overline{r}_{11}|\left(\sum_{\substack{\sigma\,:\,L\to\mathbb{C}\\ \sigma\neq\iota_1}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|\right) + \sum_{k=1}^{\nu}|u_k - r_k||\alpha_{\gamma k}\overline{r}_{11}| \\
&\leq |\overline{r}_{11}|\sum_{\substack{\sigma\,:\,L\to\mathbb{C}\\ \sigma\neq\iota_1}} \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu}|u_k - r_k||\alpha_{\gamma k}\overline{r}_{11}| \\
&\leq \sum_{\sigma:L\to\mathbb{C}} |\overline{r}_{11}|\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu}|\alpha_{\gamma k}\overline{r}_{11}||u_k - r_k|.
\end{aligned}$$

In both cases, it follows that

$$|a_1| \leq \sum_{\sigma:L\to\mathbb{C}} |\overline{r}_{11}|\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu}|\alpha_{\gamma k}\overline{r}_{11}||u_k - r_k|$$

for

$$\alpha_{\gamma k} = \overline{a}_{1k}\log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_1}\right| + \cdots + \overline{a}_{\nu k}\log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_1}\right|$$

Recall that

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu}\log(p_k)|u_k - r_k|.$$

Hence

$$
\begin{aligned}
|a_1| &\leq \sum_{\sigma:L\to\mathbb{C}} |\overline{r}_{11}| \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu} |\alpha_{\gamma k}\overline{r}_{11}||u_k - r_k| \\
&= \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} |\overline{r}_{11}|[L:\mathbb{Q}] \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&\quad + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} |\alpha_{\gamma k}\overline{r}_{11}| \frac{[K:\mathbb{Q}]}{\log(p_k)} \log(p_k)|u_k - r_k| \\
&= \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon\sigma} \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} w_{\gamma k} \log(p_k)|u_k - r_k|
\end{aligned}
$$

where

$$
w_{\varepsilon\sigma} = |\overline{r}_{11}|[L:\mathbb{Q}] \quad \text{and} \quad w_{\gamma k} = |\alpha_{\gamma k}\overline{r}_{11}| \frac{[K:\mathbb{Q}]}{\log(p_l)}
$$

and

$$
\alpha_{\gamma k} = \overline{a}_{1k} \log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_1}\right| + \cdots + \overline{a}_{\nu k} \log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_1}\right|
$$

for $k = 1, \ldots, \nu$. That is,

$$
\begin{aligned}
|a_1| &\leq \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon\sigma} \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} w_{\gamma k} \log(p_k)|u_k - r_k| \\
&\leq \max\{w_{\varepsilon\sigma}, w_{\gamma 1}, \ldots, w_{\gamma\nu}\} h\left(\frac{\delta_2}{\lambda}\right)
\end{aligned}
$$

Bounding $\{a_1, \ldots, a_r\}$ when $r = 2$.

Now, suppose $r = 2$. For any solution $(x, y, n_1, \ldots, n_\nu, a_1, a_2)$ of (22), set

$$
\vec{\varepsilon} = \begin{pmatrix} a_1 & a_2 \end{pmatrix}^{\mathrm{T}}.
$$

Now,

$$\begin{aligned}
R\vec{\varepsilon} &= \begin{pmatrix} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right| & \log\left|\left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1}\right| \\ \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2}\right| & \log\left|\left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2}\right| \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \\
&= \begin{pmatrix} a_1 \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right| + a_2 \log\left|\left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1}\right| \\ a_1 \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2}\right| + a_2 \log\left|\left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2}\right| \end{pmatrix} \\
&= \begin{pmatrix} \log\left(\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1}\right|^{a_1} \cdot \left|\left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1}\right|^{a_2}\right) \\ \log\left(\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2}\right|^{a_1} \cdot \left|\left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2}\right|^{a_2}\right) \end{pmatrix} \\
&= \begin{pmatrix} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1 a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1 a_2}\right| \\ \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2 a_2} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2 a_2}\right| \end{pmatrix}.
\end{aligned}$$

Now, since R is invertible with $R^{-1} = (\overline{r}_{nm})$, we find

$$\begin{aligned}
\vec{\varepsilon} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} &= R^{-1} \begin{pmatrix} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1 a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1 a_2}\right| \\ \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2 a_2} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2 a_2}\right| \end{pmatrix} \\
&= \begin{pmatrix} \overline{r}_{11} & \overline{r}_{12} \\ \overline{r}_{21} & \overline{r}_{22} \end{pmatrix} \begin{pmatrix} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1 a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1 a_2}\right| \\ \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2 a_2} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2 a_2}\right| \end{pmatrix} \\
&= \begin{pmatrix} \overline{r}_{11} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1 a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1 a_2}\right| + \overline{r}_{12} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2 a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2 a_2}\right| \\ \overline{r}_{21} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1 a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1 a_2}\right| + \overline{r}_{22} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2 a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2 a_2}\right| \end{pmatrix}.
\end{aligned}$$

and so we have

$$a_l = \overline{r}_{l1} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1 a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1 a_2}\right| + \overline{r}_{l2} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2 a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2 a_2}\right|$$

for $l = 1, 2$.

Now, to estimate $|a_l|$, we begin to estimate the sum on the right hand side. For this, we consider

$$\frac{\delta_2}{\lambda} = \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{a_1} \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{a_2} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{n_i}.$$

For any embedding $\iota : L \to \mathbb{C}$, we have

$$\left(\frac{\delta_2}{\lambda}\right)^{\iota} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\ n_i} = \left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota\ a_1} \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota\ a_2}.$$

Taking absolute values, we obtain

$$\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\ n_i}\right| = \left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota\ a_1} \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota\ a_2}\right|,$$

so that

$$\begin{aligned}
\log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota\ a_1} \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota\ a_2}\right| &= \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\ n_i}\right| \\
&= \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota}\right| + \log\left|\prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{\iota\ n_i}\right| \\
&= \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota}\right| - \log\left|\prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{\iota\ n_i}\right|.
\end{aligned}$$

Hence, for $l = 1, 2$,

$$\begin{aligned}
a_l &= \overline{r}_{l1} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_1\ a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_1\ a_2}\right| + \overline{r}_{l2} \log\left|\left(\frac{\varepsilon_1^{(j)}}{\varepsilon_1^{(i_0)}}\right)^{\iota_2\ a_1} \cdot \left(\frac{\varepsilon_2^{(j)}}{\varepsilon_2^{(i_0)}}\right)^{\iota_2\ a_2}\right| \\
&= \overline{r}_{l1} \left(\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| - \log\left|\prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{\iota_1\ n_i}\right|\right) + \\
&\quad + \overline{r}_{l2} \left(\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| - \log\left|\prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(j)}}{\gamma_i^{(i_0)}}\right)^{\iota_2\ n_i}\right|\right) \\
&= \overline{r}_{l1} \left(\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| - n_1 \log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_1}\right| - \cdots - n_\nu \log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_1}\right|\right) + \\
&\quad + \overline{r}_{l2} \left(\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| - n_1 \log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_2}\right| - \cdots - n_\nu \log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_2}\right|\right).
\end{aligned}$$

Now, for $l = 1, 2$,

$$\begin{aligned}
a_l &= \overline{r}_{l1}\left(\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| - n_1 \log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_1}\right| - \cdots - n_\nu \log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_1}\right|\right) + \\
&\quad + \overline{r}_{l2}\left(\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| - n_1 \log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_2}\right| - \cdots - n_\nu \log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_2}\right|\right) \\
&= \overline{r}_{l1}\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| + \overline{r}_{l2}\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| + \\
&\quad - n_1\left(\overline{r}_{l1}\log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_1}\right| + \overline{r}_{l2}\log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_2}\right|\right) - \cdots \\
&\quad \cdots - n_\nu\left(\overline{r}_{l1}\log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_1}\right| + \overline{r}_{l2}\log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_2}\right|\right) \\
&= \overline{r}_{l1}\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| + \overline{r}_{l2}\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| - n_1\beta_{\gamma l1} - \cdots - n_\nu\beta_{\gamma l\nu},
\end{aligned}$$

where

$$\beta_{\gamma lk} = \left(\overline{r}_{l1}\log\left|\left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}}\right)^{\iota_1}\right| + \overline{r}_{l2}\log\left|\left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}}\right)^{\iota_2}\right|\right)$$

for $k = 1, \ldots, \nu$. Recall that

$$A\mathbf{n} = \mathbf{u} - \mathbf{r}$$

so

$$\mathbf{n} = A^{-1}(\mathbf{u} - \mathbf{r}).$$

If

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1\nu} \\ a_{21} & a_{22} & \ldots & a_{2\nu} \\ \vdots & \vdots & \ddots & \vdots \\ a_{\nu1} & a_{\nu2} & \ldots & a_{\nu\nu} \end{pmatrix},$$

then

$$A^{-1} = \begin{pmatrix} \overline{a}_{11} & \overline{a}_{12} & \ldots & \overline{a}_{1\nu} \\ \overline{a}_{21} & \overline{a}_{22} & \ldots & \overline{a}_{2\nu} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{a}_{\nu1} & \overline{a}_{\nu2} & \ldots & \overline{a}_{\nu\nu} \end{pmatrix},$$

and

$$\begin{pmatrix} n_1 \\ \vdots \\ n_\nu \end{pmatrix} = \mathbf{n} = A^{-1}(\mathbf{u} - \mathbf{r})$$

$$= \begin{pmatrix} \overline{a}_{11} & \overline{a}_{12} & \dots & \overline{a}_{1\nu} \\ \overline{a}_{21} & \overline{a}_{22} & \dots & \overline{a}_{2\nu} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{a}_{\nu 1} & \overline{a}_{\nu 2} & \dots & \overline{a}_{\nu\nu} \end{pmatrix} \begin{pmatrix} u_1 - r_1 \\ \vdots \\ u_\nu - r_\nu \end{pmatrix}$$

$$= \begin{pmatrix} \overline{a}_{11}(u_1 - r_1) + \dots + \overline{a}_{1\nu}(u_\nu - r_\nu) \\ \vdots \\ \overline{a}_{\nu 1}(u_1 - r_1) + \dots + \overline{a}_{\nu\nu}(u_\nu - r_\nu) \end{pmatrix}$$

$$= \begin{pmatrix} \sum_{k=1}^{\nu} \overline{a}_{1k}(u_k - r_k) \\ \vdots \\ \sum_{k=1}^{\nu} \overline{a}_{\nu k}(u_k - r_k) \end{pmatrix}$$

Now,

$$\begin{aligned} a_l &= \overline{r}_{l1} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_2} \right| - n_1 \beta_{\gamma l1} - \dots - n_\nu \beta_{\gamma l\nu} \\ &= \overline{r}_{l1} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_2} \right| - \left(\overline{a}_{11}(u_1 - r_1) + \dots + \overline{a}_{1\nu}(u_\nu - r_\nu)\right) \beta_{\gamma l1} - \cdots \\ &\qquad \cdots - (\overline{a}_{\nu 1}(u_1 - r_1) + \dots + \overline{a}_{\nu\nu}(u_\nu - r_\nu))\beta_{\gamma l\nu} \\ &= \overline{r}_{l1} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_2} \right| - (u_1 - r_1)(\overline{a}_{11}\beta_{\gamma l1} + \dots + \overline{a}_{\nu 1}\beta_{\gamma l\nu}) - \cdots \\ &\qquad \cdots - (u_\nu - r_\nu)\left(\overline{a}_{1\nu}\beta_{\gamma l1} + \dots + \overline{a}_{\nu\nu}\beta_{\gamma l\nu}\right) \\ &= \overline{r}_{l1} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_2} \right| - (u_1 - r_1)\alpha_{\gamma l1} - \dots - (u_\nu - r_\nu)\alpha_{\gamma l\nu} \\ &= \overline{r}_{l1} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_2} \right| - \sum_{k=1}^{\nu} (u_k - r_k)\alpha_{\gamma lk} \end{aligned}$$

where

$$\alpha_{\gamma lk} = \overline{a}_{1k}\beta_{\gamma l1} + \dots + \overline{a}_{\nu k}\beta_{\gamma l\nu}$$

and

$$\beta_{\gamma lk} = \left(\overline{r}_{l1} \log \left| \left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}} \right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}} \right)^{\iota_2} \right| \right)$$

for $k = 1, \ldots, \nu$.

Further, recall that $\frac{\delta_2}{\lambda}$ is a quotient of elements which are conjugate to one another. In other words, taking the norm on L of $\frac{\delta_2}{\lambda}$, we obtain $N\left(\frac{\delta_2}{\lambda}\right) = 1$. On the other hand, by definition, we have

$$1 = N\left(\frac{\delta_2}{\lambda}\right) = \prod_{\sigma : L \to \mathbb{C}} \sigma\left(\frac{\delta_2}{\lambda}\right).$$

Taking absolute values and logarithms,

$$0 = \sum_{\sigma : L \to \mathbb{C}} \log \left| \sigma\left(\frac{\delta_2}{\lambda}\right) \right|$$

so that

$$-\log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota} \right| = -\log \left| \iota\left(\frac{\delta_2}{\lambda}\right) \right| = \sum_{\substack{\sigma : L \to \mathbb{C} \\ \sigma \neq \iota}} \log \left| \sigma\left(\frac{\delta_2}{\lambda}\right) \right|.$$

Taking absolute values, this yields

$$\begin{aligned}
|a_l| &= \left| \overline{r}_{l1} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_2} \right| - \sum_{k=1}^{\nu} (u_k - r_k) \alpha_{\gamma lk} \right| \\
&\leq |\overline{r}_{l1}| \left| \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_1} \right| \right| + |\overline{r}_{l2}| \left| \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_2} \right| \right| + \left| - \sum_{k=1}^{\nu} (u_k - r_k) \alpha_{\gamma lk} \right| \\
&\leq |\overline{r}_{l1}| \left| \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_1} \right| \right| + |\overline{r}_{l2}| \left| \log \left| \left(\frac{\delta_2}{\lambda}\right)^{\iota_2} \right| \right| + \sum_{k=1}^{\nu} |u_k - r_k| |\alpha_{\gamma lk}|
\end{aligned}$$

where

$$\alpha_{\gamma lk} = \overline{a}_{1k} \beta_{\gamma l1} + \cdots + \overline{a}_{\nu k} \beta_{\gamma l\nu}$$

and

$$\beta_{\gamma lk} = \left(\overline{r}_{l1} \log \left| \left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}} \right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}} \right)^{\iota_2} \right| \right)$$

for $k = 1, \ldots, \nu$.

Suppose $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| \geq 0$ and $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| \geq 0$. Then, we obtain

$$\begin{aligned}
|a_l| &\leq |\overline{r}_{l1}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right| + |\overline{r}_{l2}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&= |\overline{r}_{l1}| \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| + |\overline{r}_{l2}| \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&\leq \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}| \log\max\left\{\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|, 1\right\} + \\
&\qquad + \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} \log\max\left\{\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|, 1\right\} + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&\leq \sum_{w:L\to\mathbb{C}} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}| \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}|.
\end{aligned}$$

Alternatively, suppose that both $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| < 0$ and $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| < 0$. Then

$$\begin{aligned}
|a_l| &\leq |\overline{r}_{l1}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right| + |\overline{r}_{l2}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&= |\overline{r}_{l1}| \left(-\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right) + |\overline{r}_{l2}| \left(-\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right) + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&= |\overline{r}_{l1}| \sum_{\substack{\sigma : L \to \mathbb{C} \\ \sigma \neq \iota_1}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right| + |\overline{r}_{l2}| \left(-\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right) + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&\leq \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} \sum_{\substack{\sigma : L \to \mathbb{C} \\ \sigma \neq \iota_1}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right| + \\
&\qquad + \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} \left(-\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right) + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&\leq \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} \sum_{\substack{w : L \to \mathbb{C} \\ \sigma \neq \iota_1, \iota_2}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&\leq \sum_{w:L\to\mathbb{C}} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}| \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}|.
\end{aligned}$$

Lastly, if, without loss of generality, we have $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right| < 0$ and $\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| \geq 0$, then

$$\begin{aligned}
|a_l| &\leq |\overline{r}_{l1}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right| + |\overline{r}_{l2}| \left|\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right|\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&= |\overline{r}_{l1}| \left(-\log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_1}\right|\right) + |\overline{r}_{l2}| \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&= |\overline{r}_{l1}| \sum_{\substack{\sigma\,:\,L\to\mathbb{C} \\ \sigma\neq\iota_1}} \log\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right| + |\overline{r}_{l2}| \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&\leq \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} \sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + |\overline{r}_{l2}| \log\left|\left(\frac{\delta_2}{\lambda}\right)^{\iota_2}\right| + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}| \\
&= \sum_{w:L\to\mathbb{C}} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}| \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + |\overline{r}_{l1}| \log\max\left\{\left|\iota_1\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&\qquad + |\overline{r}_{l2}| \log\max\left\{\left|\iota_2\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}|.
\end{aligned}$$

In all cases, it follows that we have

$$\begin{aligned}
|a_l| \leq \sum_{w:L\to\mathbb{C}} &\max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}| \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + |\overline{r}_{l1}| \log\max\left\{\left|\iota_1\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&+ |\overline{r}_{l2}| \log\max\left\{\left|\iota_2\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \sum_{k=1}^{\nu} |u_k - r_k||\alpha_{\gamma lk}|
\end{aligned}$$

where

$$\alpha_{\gamma lk} = \overline{a}_{1k}\beta_{\gamma l1} + \cdots + \overline{a}_{\nu k}\beta_{\gamma l\nu}$$

and

$$\beta_{\gamma lk} = \left(\overline{r}_{l1} \log\left|\left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}}\right)^{\iota_1}\right| + \overline{r}_{l2} \log\left|\left(\frac{\gamma_k^{(j)}}{\gamma_k^{(i_0)}}\right)^{\iota_2}\right|\right)$$

for $k = 1, \ldots, \nu$. That is, for $k = 1, \ldots, \nu$, we have

$$\begin{aligned}
\alpha_{\gamma lk} = \overline{a}_{1k} &\left(\overline{r}_{l1} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_2} \right| \right) + \cdots \\
&\cdots + \overline{a}_{\nu k} \left(\overline{r}_{l1} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_2} \right| \right) \\
&= \left(\overline{a}_{1k} \overline{r}_{l1} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| + \cdots + \overline{a}_{\nu k} \overline{r}_{l1} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right| \right) + \\
&\quad + \left(\overline{a}_{1k} \overline{r}_{l2} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_2} \right| + \cdots + \overline{a}_{\nu k} \overline{r}_{l2} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_2} \right| \right) \\
&= \overline{r}_{l1} \left(\overline{a}_{1k} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| + \cdots + \overline{a}_{\nu k} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right| \right) + \\
&\quad + \overline{r}_{l2} \left(\overline{a}_{1k} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_2} \right| + \cdots + \overline{a}_{\nu k} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_2} \right| \right).
\end{aligned}$$

Recall that

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[L:\mathbb{Q}]} \sum_{w: L \to \mathbb{C}} \log \max \left\{ \left| w\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} + \frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l) |u_l - r_l|.$$

Hence for $l = 1, 2$,

$$\begin{aligned}
|a_l| \leq &\sum_{w: L \to \mathbb{C}} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} | \log \max \left\{ \left| w\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} + |\overline{r}_{l1}| \log \max \left\{ \left| \iota_1\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} + \\
&\quad + |\overline{r}_{l2}| \log \max \left\{ \left| \iota_2\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} + \sum_{k=1}^{\nu} |u_k - r_k| |\alpha_{\gamma lk}| \\
&= \frac{1}{[L:\mathbb{Q}]} \sum_{w: L \to \mathbb{C}} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} [L:\mathbb{Q}] \log \max \left\{ \left| w\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} + \\
&\quad + \frac{[L:\mathbb{Q}]}{[L:\mathbb{Q}]} |\overline{r}_{l1}| \log \max \left\{ \left| \iota_1\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} + \frac{[L:\mathbb{Q}]}{[L:\mathbb{Q}]} |\overline{r}_{l2}| \log \max \left\{ \left| \iota_2\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} + \\
&\quad + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} \frac{[K:\mathbb{Q}]}{\log(p_k)} \log(p_k) |u_k - r_k| |\alpha_{\gamma lk}| \\
&= \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma: L \to \mathbb{C}} w_{\varepsilon l \sigma} \log \max \left\{ \left| \sigma\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} w_{\gamma lk} \log(p_k) |u_k - r_k|
\end{aligned}$$

where

$$w_{\varepsilon l\sigma} = \begin{cases} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}[L:\mathbb{Q}] & \text{for } \sigma \notin I \\ (\max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} + |\overline{r}_{li}|)\,[L:\mathbb{Q}] & \text{for } \sigma = \iota_i \in I \end{cases}$$

and

$$w_{\gamma lk} = |\alpha_{\gamma lk}| \frac{[K:\mathbb{Q}]}{\log(p_k)}$$

where

$$\begin{aligned} \alpha_{\gamma lk} = \overline{a}_{1k} &\left(\overline{r}_{l1} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}} \right)^{\iota_2} \right| \right) + \cdots \\ &\cdots + \overline{a}_{\nu k} \left(\overline{r}_{l1} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_1} \right| + \overline{r}_{l2} \log \left| \left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}} \right)^{\iota_2} \right| \right) \end{aligned}$$

for $k = 1, \ldots, \nu$.

That is,

$$\begin{aligned} |a_l| &\le \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma: L \to \mathbb{C}} w_{\varepsilon l\sigma} \log \max \left\{ \left| \sigma\left(\frac{\delta_2}{\lambda}\right) \right|, 1 \right\} + \frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} w_{\gamma lk} \log(p_k) |u_k - r_k| \\ &\le \max\{w_{\varepsilon l\sigma_1}, \ldots, w_{\varepsilon\sigma_?}, w_{\gamma 1}, \ldots, w_{\gamma\nu}\} h\left(\frac{\delta_2}{\lambda}\right). \end{aligned}$$

Together with the case $r = 1$, we have proven the following lemma

Lemma 13.9. *For any solution $(x, y, a_1, \ldots, a_r, n_1, \ldots, n_\nu)$ of (22), we have*

$$|a_l| \le \max\{w_{\varepsilon\sigma_1}, \ldots, w_{\varepsilon\sigma_?}, w_{\gamma 1}, \ldots, w_{\gamma\nu}\} h\left(\frac{\delta_2}{\lambda}\right)$$

where $l = 1, \ldots, r$, where $r = 1, 2$.

Remark 13.10. In Lemma 13.9, one can take $w_{\epsilon 1} = [L:K]\|r_\epsilon\|_\infty$ for $v \in I$ if $|I| = 1$ and the summand $\sum_{v:L\to\mathbb{C}} w_{\epsilon v} h_v(z)$ can be replaced by $3[L:K]\|r_\epsilon\|_\infty \max_{v:L\to\mathbb{C}} h_v(z)$ if $|I| = 2$.

Proof. In the case $|I| = 1$, we either have precisely one non-negative or precisely one negative. If precisely one non-negative then the claim follows, and if precisely one negative then we just get $\sum_{v|\infty} h_v(z)$ by above proof, which again proves the claim.

Consider now the case $|I| = 2$. The claim follows if both are non-negative. If both are negative then we just apply once $N(z) = 1$ (and product formula) and the claim follows again. Finally, if one is non-negative and one negative, then we compute that

$$2\sum_{v\in I\setminus I^-} h_v(z) + \sum_{v|\infty, v\notin I} h_v(z) \leq 3\max_{v|\infty} h_v(z).$$

This follows since there are at most 3 positive ones in total and if there are indeed 3 positive ones, then the middle one cancels out (see proof of above lemma). □

Question 13.11. *I should go through the above. But isn't it more accurate if we just compute the bound as is?*

Now,

$$|a_l|^2 \leq \left(\frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} w_{\gamma lk}\log(p_k)|u_k - r_k| + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon l\sigma}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right)^2. \tag{24}$$

Take $\mathbf{h}\in\mathbb{R}^{r+\nu}$ such that $\mathbf{h}\geq\mathbf{0}$. Let $\mathbf{m} = (n_1,\ldots,n_\nu,a_1,\ldots,a_r)\in\mathbb{R}^{r+\nu}$ be any solution of (22). Denote by $h_v\left(\frac{\delta_2}{\lambda}\right)$ the v^{th} entry of the vector

$$\left(\log(p_1)|u_1 - r_1|,\ldots,\log(p_\nu)|u_\nu - r_\nu|, \log\max\left\{\left|w_1\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\},\ldots,\log\max\left\{\left|w_n\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right)$$

and suppose $h_v(z)\leq h_v$ for all $v\in\{1,\ldots,r+\nu\}$. Then we deduce

$$|a_l|^2 \leq \left(\frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} w_{\gamma lk}h_k + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon l\sigma}h_\sigma\right)^2$$

13.5 Archimedean ellipsoid: real case, $r = 2$.

We first consider the case when all roots of f are real numbers. That is, there are 3 real embeddings, hence $s = 3, t = 0$ and therefore $r = s + t - 1 = 2$.

Let $\tau : L\to\mathbb{R}\subset\mathbb{C}$ be an embedding and let $l_\tau\geq c_\tau$ and $c > 0$ be given real numbers for $c_\tau = \log^+(2|\tau(\delta_2)|) = \log\max\{2|\tau(\delta_2)|, 1\}$. We define

$$\alpha_0 = [c\log|\tau(\delta_1)|] \quad\text{and}\quad \alpha_{\varepsilon 1} = \left[c\log\left|\tau\left(\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}\right)\right|\right],\ \ \alpha_{\varepsilon 2} = \left[c\log\left|\tau\left(\frac{\varepsilon_2^{(k)}}{\varepsilon_2^{(j)}}\right)\right|\right].$$

For $i = 1, \dots, \nu$, define

$$\alpha_{\gamma i} = \left[c \log \left| \tau \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}} \right) \right| \right].$$

Here, $[\,\cdot\,]$ denotes the nearest integer function. Recall that

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} \log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]} \sum_{w:L\to\mathbb{C}} \log\max\left\{ \left| w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}.$$

Let

$$h_\tau\left(\frac{\delta_2}{\lambda}\right) = \log\max\left\{ \left| \tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\},$$

the τ^{th} entry in the second summand of $h\left(\frac{\delta_2}{\lambda}\right)$ and $k_\tau = \frac{3}{2}$.

Lemma 13.12. *Suppose $(x, y, n_1, \dots, n_\nu, a_1, \dots, a_r)$ is a solution of (22). If $h_\tau\left(\frac{\delta_2}{\lambda}\right) > c_\tau$ and $\kappa_\tau = 3/2$, then*

$$\begin{aligned} &\left| \alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i} \right| \\ &\le \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]} \sum_{l=1}^{\nu} w_l \log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma:L\to\mathbb{C}} w_\sigma \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right) + \\ &\qquad + \left(\frac{1}{2} + c\kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)} \right). \end{aligned}$$

Proof. Let

$$\begin{aligned} \alpha &= \alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i} \\ &= [c \log|\tau(\delta_1)|] + \sum_{i=1}^{r} a_i \left[c\log\left|\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right|\right] + \sum_{i=1}^{\nu} n_i \left[c\log\left|\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right|\right] \end{aligned}$$

and

$$\Lambda_\tau = \log\left| \tau\left(\delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i} \right)\right| = \log\left(\tau\left(\delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i} \right)\right)$$

where the above equality follows from

$$\tau\left(\delta_1 \prod_{i=1}^{r} \left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu} \left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i} \right) > 0.$$

Indeed, by assumption, it holds that

$$h_\tau\left(\frac{\delta_2}{\lambda}\right) = \log\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} > c_\tau = \log\max\{2|\tau(\delta_2)|, 1\}$$

Thus

$$\begin{aligned}
\exp\left(h_\tau\left(\frac{\delta_2}{\lambda}\right)\right) &> \exp(c_\tau)\\
\exp\left(\log\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right) &> \exp\left(\log\max\{2|\tau(\delta_2)|, 1\}\right)\\
\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} &> \max\{2|\tau(\delta_2)|, 1\}
\end{aligned}$$

Now, we have

$$\max\{2|\tau(\delta_2)|, 1\} < \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}.$$

If

$$\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = 1,$$

then

$$\max\{2|\tau(\delta_2)|, 1\} < \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = 1.$$

If $\max\{2|\tau(\delta_2)|, 1\} = 1$, then

$$1 = \max\{2|\tau(\delta_2)|, 1\} < \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = 1,$$

which is impossible, so we must have that $2|\tau(\delta_2)| \geq 1$. In this case,

$$1 \leq 2|\tau(\delta_2)| = \max\{2|\tau(\delta_2)|, 1\} < \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = 1,$$

which again is impossible. It follows that we must have

$$\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = \left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|.$$

In this case,

$$\max\{2|\tau(\delta_2)|, 1\} < \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = \left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|.$$

It follows that

$$2|\tau(\delta_2)| \leq \max\{2|\tau(\delta_2)|, 1\} < \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} = \left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|$$

and therefore

$$2|\tau(\delta_2)| < \left|\tau\left(\frac{\delta_2}{\lambda}\right)\right| = \frac{|\tau(\delta_2)|}{|\tau(\lambda)|} \implies |\tau(\lambda)| < \frac{1}{2}.$$

Now, since

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

where

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

we have

$$\lambda = \mu - 1.$$

Applying τ, this is

$$\tau(\lambda) = \tau(\mu) - 1$$

and thus

$$|\tau(\lambda)| < \frac{1}{2} \implies \tau(\mu) = \tau(\lambda) + 1 > 0.$$

It follows that

$$\tau(\mu) = \tau\left(\delta_1 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right) > 0.$$

Now,

$$\Lambda_\tau = \log\left|\tau\left(\delta_1 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right)\right| = \log\left(\tau\left(\delta_1 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right)\right)$$

and thus

$$\begin{aligned}
\Lambda_\tau &= \log\left(\tau\left(\delta_1 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right)\right) \\
&= \log\left(\tau\left(\delta_1\right)\tau\left(\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i}\right)\tau\left(\prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right)\right) \\
&= \log\left(\tau\left(\delta_1\right)\prod_{i=1}^{r}\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i}\prod_{i=1}^{\nu}\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right) \\
&= \log\left(\tau\left(\delta_1\right)\right) + \log\left(\prod_{i=1}^{r}\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i}\right) + \log\left(\prod_{i=1}^{\nu}\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right) \\
&= \log\left(\tau\left(\delta_1\right)\right) + \sum_{i=1}^{r} a_i \log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right) + \sum_{i=1}^{\nu} n_i \log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)
\end{aligned}$$

We have

$$|\alpha| = |\alpha + c\Lambda_\tau - c\Lambda_\tau|$$

so that by the triangle inequality,

$$|\alpha| \leq |\alpha - c\Lambda_\tau| + c|\Lambda_\tau|.$$

Now,

$$\begin{aligned}
|\alpha - c\Lambda_\tau| &= \Bigg| [c\log(\tau(\delta_1))] + \sum_{i=1}^{r} a_i \left[c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right] + \sum_{i=1}^{\nu} n_i \left[c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right] + \\
&\qquad - c\log\left(\tau\left(\delta_1 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)^{n_i}\right)\right)\Bigg| \\
&= \Bigg| [c\log(\tau(\delta_1))] + \sum_{i=1}^{r} a_i \left[c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right] + \sum_{i=1}^{\nu} n_i \left[c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right] + \\
&\qquad - c\log\left(\tau\left(\delta_1\right)\right) - \sum_{i=1}^{r} a_i c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right) - \sum_{i=1}^{\nu} n_i c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\Bigg| \\
&= \Bigg| \{[c\log(\tau(\delta_1))] - c\log\left(\tau\left(\delta_1\right)\right)\} + \sum_{i=1}^{r} \left\{ a_i \left[c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right] - a_i c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right\} \\
&\qquad + \sum_{i=1}^{\nu} \left\{ n_i \left[c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right] - n_i c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right\}\Bigg| \\
&\le |[c\log(\tau(\delta_1))] - c\log\left(\tau\left(\delta_1\right)\right)| + \left|\sum_{i=1}^{r} \left\{ a_i \left[c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right] - a_i c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right\}\right| \\
&\qquad + \left|\sum_{i=1}^{\nu} \left\{ n_i \left[c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right] - n_i c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right\}\right| \\
&\le |[c\log(\tau(\delta_1))] - c\log\left(\tau\left(\delta_1\right)\right)| + \sum_{i=1}^{r} |a_i| \left|\left[c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right] - c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right| \\
&\qquad + \sum_{i=1}^{\nu} |n_i| \left|\left[c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right] - c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right|.
\end{aligned}$$

Now, since $[\ \cdot\ ]$ denotes the nearest integer function, it is clear that $|[\ c\ ] - c| \le 1/2$ for any integer c. Hence

$$\begin{aligned}
|\alpha - c\Lambda_\tau| &\leq |[c\log(\tau(\delta_1))] - c\log(\tau(\delta_1))| + \sum_{i=1}^{r} |a_i| \left| \left[c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right] - c\log\left(\tau\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)\right)\right| \\
&\quad + \sum_{i=1}^{\nu} |n_i| \left| \left[c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right] - c\log\left(\tau\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right)\right)\right| \\
&\leq \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{r}|a_i| + \frac{1}{2}\sum_{i=1}^{\nu}|n_i| \\
&= \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{r}|a_i| + \frac{1}{2}\sum_{i=1}^{\nu}\left|\sum_{k=1}^{\nu}\overline{a}_{ik}(u_k - r_k)\right| \\
&= \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{r}|a_i| + \frac{1}{2}\sum_{i=1}^{\nu}|\overline{a}_{i1}(u_1 - r_1) + \cdots + \overline{a}_{i\nu}(u_\nu - r_\nu)| \\
&= \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{r}|a_i| + \frac{1}{2}\,|(\overline{a}_{11}(u_1 - r_1) + \cdots + \overline{a}_{1\nu}(u_\nu - r_\nu)) + \cdots \\
&\quad \cdots + (\overline{a}_{\nu 1}(u_1 - r_1) + \cdots + \overline{a}_{\nu\nu}(u_\nu - r_\nu))| \\
&= \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{r}|a_i| + \frac{1}{2}\,|(u_1 - r_1)(\overline{a}_{11} + \cdots + \overline{a}_{\nu 1}) + \cdots + (u_\nu - r_\nu)(\overline{a}_{1\nu} + \cdots + \overline{a}_{\nu\nu})| \\
&\leq \frac{1}{2}\left(1 + \sum_{i=1}^{r}|a_i| + |u_1 - r_1||\overline{a}_{11} + \cdots + \overline{a}_{\nu 1}| + \cdots + |u_\nu - r_\nu||\overline{a}_{1\nu} + \cdots + \overline{a}_{\nu\nu}|\right) \\
&= \frac{1}{2}\left(1 + \sum_{i=1}^{r}|a_i| + |u_1 - r_1|\sum_{i=1}^{\nu}|\overline{a}_{i1}| + \cdots + |u_\nu - r_\nu|\sum_{i=1}^{\nu}|\overline{a}_{i\nu}|\right).
\end{aligned}$$

Recall that when $r = 2$, we have, for $l = 1, 2$

$$|a_l| \leq \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma: L\to\mathbb{C}} w_{\varepsilon l\sigma}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} w_{\gamma lk}\log(p_k)|u_k - r_k|$$

where

$$w_{\varepsilon l\sigma} = \begin{cases} \max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\}[L:\mathbb{Q}] & \text{for } \sigma \notin I \\ (\max\{|\overline{r}_{l1}|, |\overline{r}_{l2}|\} + |\overline{r}_{li}|)\,[L:\mathbb{Q}] & \text{for } \sigma = \iota_i \in I \end{cases}$$

and

$$w_{\gamma lk} = |\alpha_{\gamma lk}|\frac{[K:\mathbb{Q}]}{\log(p_k)}$$

where

$$\alpha_{\gamma lk} = \overline{a}_{1k}\left(\overline{r}_{l1}\log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_1}\right| + \overline{r}_{l2}\log\left|\left(\frac{\gamma_1^{(j)}}{\gamma_1^{(i_0)}}\right)^{\iota_2}\right|\right) + \cdots$$
$$\cdots + \overline{a}_{\nu k}\left(\overline{r}_{l1}\log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_1}\right| + \overline{r}_{l2}\log\left|\left(\frac{\gamma_\nu^{(j)}}{\gamma_\nu^{(i_0)}}\right)^{\iota_2}\right|\right)$$

for $k = 1, \ldots, \nu$.

Now,

$$
\begin{aligned}
|\alpha - c\Lambda_\tau| &\leq \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{r}|a_i| + \frac{1}{2}|u_1 - r_1|\sum_{i=1}^{\nu}|\overline{a}_{i1}| + \cdots + \frac{1}{2}|u_\nu - r_\nu|\sum_{i=1}^{\nu}|\overline{a}_{i\nu}| \\
&\leq \frac{1}{2} + \frac{1}{2}|u_1 - r_1|\sum_{i=1}^{\nu}|\overline{a}_{i1}| + \cdots + \frac{1}{2}|u_\nu - r_\nu|\sum_{i=1}^{\nu}|\overline{a}_{i\nu}| + \\
&\quad + \frac{1}{2}\left(\frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon_1\sigma}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} w_{\gamma_1 k}\log(p_k)|u_k - r_k|\right) + \\
&\quad + \frac{1}{2}\left(\frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon_2\sigma}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} w_{\gamma_2 k}\log(p_k)|u_k - r_k|\right) \\
&= \frac{1}{2} + \frac{1}{2}|u_1 - r_1|\sum_{i=1}^{\nu}|\overline{a}_{i1}| + \cdots + \frac{1}{2}|u_\nu - r_\nu|\sum_{i=1}^{\nu}|\overline{a}_{i\nu}| + \\
&\quad + \frac{1}{2}\left(\frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} (w_{\varepsilon_1\sigma} + w_{\varepsilon_2\sigma})\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right) + \\
&\quad + \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} (w_{\gamma_1 k} + w_{\gamma_2 k})\log(p_k)|u_k - r_k|\right) \\
&= \frac{1}{2} + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} \frac{(w_{\varepsilon_1\sigma} + w_{\varepsilon_2\sigma})}{2}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&\quad + \frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} \frac{(w_{\gamma_1 k} + w_{\gamma_2 k})}{2}\log(p_k)|u_k - r_k| \\
&\quad + \frac{1}{2}|u_1 - r_1|\sum_{i=1}^{\nu}|\overline{a}_{i1}| + \cdots + \frac{1}{2}|u_\nu - r_\nu|\sum_{i=1}^{\nu}|\overline{a}_{i\nu}| \\
&= \frac{1}{2} + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} \frac{(w_{\varepsilon_1\sigma} + w_{\varepsilon_2\sigma})}{2}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&\quad + \frac{1}{[K:\mathbb{Q}]}\left(\frac{(w_{\gamma_1 1} + w_{\gamma_2 1})}{2}\log(p_1)|u_1 - r_1| + \cdots + \frac{(w_{\gamma_1 \nu} + w_{\gamma_2 \nu})}{2}\log(p_\nu)|u_\nu - r_\nu|\right) \\
&\quad + \frac{1}{2}|u_1 - r_1|\sum_{i=1}^{\nu}|\overline{a}_{i1}| + \cdots + \frac{1}{2}|u_\nu - r_\nu|\sum_{i=1}^{\nu}|\overline{a}_{i\nu}| \\
&= \frac{1}{2} + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} \frac{(w_{\varepsilon_1\sigma} + w_{\varepsilon_2\sigma})}{2}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&\quad + |u_1 - r_1|\left(\frac{(w_{\gamma_1 1} + w_{\gamma_2 1})}{2[K:\mathbb{Q}]}\log(p_1) + \frac{1}{2}\sum_{i=1}^{\nu}|\overline{a}_{i1}|\right) + \cdots \\
&\quad + |u_\nu - r_\nu|\left(\frac{(w_{\gamma_1 \nu} + w_{\gamma_2 \nu})}{2[K:\mathbb{Q}]}\log(p_\nu) + \frac{1}{2}\sum_{i=1}^{\nu}|\overline{a}_{i\nu}|\right).
\end{aligned}
$$

Altogether, we have

$$
\begin{aligned}
|\alpha - c\Lambda_\tau| &= \frac{1}{2} + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} \frac{(w_{\varepsilon_1\sigma}+w_{\varepsilon_2\sigma})}{2}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&\quad + |u_1 - r_1|\left(\frac{(w_{\gamma_1 1}+w_{\gamma_2 1})}{2[K:\mathbb{Q}]}\log(p_1) + \frac{1}{2}\sum_{i=1}^{\nu}|\overline{a}_{i1}|\right) + \cdots \\
&\quad + |u_\nu - r_\nu|\left(\frac{(w_{\gamma_1 \nu}+w_{\gamma_2 \nu})}{2[K:\mathbb{Q}]}\log(p_\nu) + \frac{1}{2}\sum_{i=1}^{\nu}|\overline{a}_{i\nu}|\right) \\
&= \frac{1}{2} + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} \frac{(w_{\varepsilon_1\sigma}+w_{\varepsilon_2\sigma})}{2}\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&\quad + \sum_{k=1}^{\nu}|u_k - r_k|\left(\frac{(w_{\gamma_1 k}+w_{\gamma_2 k})}{2[K:\mathbb{Q}]}\log(p_k) + \frac{1}{2}\sum_{i=1}^{\nu}|\overline{a}_{ik}|\right) \\
&= \frac{1}{2} + \frac{1}{2[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} (w_{\varepsilon_1\sigma}+w_{\varepsilon_2\sigma})\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \\
&\quad + \frac{1}{2[K:\mathbb{Q}]}\sum_{k=1}^{\nu}\log(p_k)|u_k - r_k|\left((w_{\gamma_1 k}+w_{\gamma_2 k}) + \frac{[K:\mathbb{Q}]}{\log(p_k)}\sum_{i=1}^{\nu}|\overline{a}_{ik}|\right).
\end{aligned}
$$

Now, let

$$
w_\sigma = (w_{\varepsilon 1\sigma}+w_{\varepsilon 2\sigma}), \qquad w_k = (w_{\gamma 1k}+w_{\gamma 2k}) + \frac{[K:\mathbb{Q}]}{\log(p_k)}\sum_{i=1}^{\nu}|\overline{a}_{ik}|
$$

for $\sigma : L \to \mathbb{C}$ and $k = 1, \ldots, \nu$. That is,

$$
\begin{aligned}
|\alpha - c\Lambda_\tau| &\leq \frac{1}{2} + \frac{1}{2[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{2[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l\log(p_l)|u_l - r_l| \\
&\leq \frac{1}{2} + \frac{1}{2}\left(\frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma\log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l\log(p_l)|u_l - r_l|\right).
\end{aligned}
$$

We compare this to $h\left(\frac{\delta_2}{\lambda}\right)$, which we recall is given by

$$
h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu}\log(p_l)|u_l - r_l|.
$$

Now, we bound $c|\Lambda_\tau|$ to obtain a bound for $|\alpha|$. Via Rafael, we will see that this bound is

$$c|\Lambda_\tau| \leq c\kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)}.$$

Since

$$\tau(\lambda) = \tau\left(\delta_2 \prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i} \prod_{i=1}^{\nu}\left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right)^{n_i}\right) = \tau(\mu) - 1 = e^{\Lambda_\tau} - 1,$$

the power series definition of exponential function gives

$$\tau(\lambda) = e^{\Lambda_\tau} - 1 = \sum_{n=0}^{\infty}\frac{\Lambda_\tau^n}{n!} - 1 = \sum_{n=1}^{\infty}\frac{\Lambda_\tau^n}{n!} = \Lambda_\tau + \sum_{n=2}^{\infty}\frac{\Lambda_\tau^n}{n!} = \Lambda_\tau\left(1 + \sum_{n=2}^{\infty}\frac{\Lambda_\tau^{n-1}}{n!}\right).$$

If $\Lambda_\tau \geq 0$ then $1 + \sum_{n\geq 2}(\Lambda_\tau)^{n-1}/n! > 1$ which implies that

$$|\Lambda_\tau| \leq |\Lambda_\tau|\left|1 + \sum_{n\geq 2}\frac{(\Lambda_\tau)^{n-1}}{n!}\right| = |\tau(\lambda)|.$$

Suppose now that $\Lambda_\tau < 0$. Our assumption

$$h_\tau\left(\frac{\delta_2}{\lambda}\right) = \log\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} > c_\tau = \log\max\{2|\tau(\delta_2)|, 1\}$$

means that $|\tau(\lambda)| < 1/2$. That is,

$$-\frac{1}{2} < \tau(\lambda) < \frac{1}{2} \implies \frac{1}{2} < \tau(\lambda) + 1 < \frac{3}{2} \implies \log\left(\frac{1}{2}\right) < \log(\tau(\lambda)+1) < \log\left(\frac{3}{2}\right).$$

In particular,

$$-\log(1/2) > -\log(\tau(\lambda)+1).$$

Together with

$$\tau(\lambda) + 1 = \tau(\mu) \implies \log(\tau(\lambda)+1) = \log(\tau(\mu)) = \Lambda_\tau < 0,$$

this means that

$$|\Lambda_\tau| = -\log(\tau(\lambda)+1) \leq -\log(1/2) = \log 2.$$

Therefore

$$
\begin{aligned}
\left|\sum_{n\geq 2}\frac{(\Lambda_\tau)^{n-1}}{n!}\right| &\leq \sum_{n\geq 2}\frac{|\Lambda_\tau|^{n-1}}{n!} \\
&= \sum_{n\geq 1}\frac{|\Lambda_\tau|^{n}}{(n+1)!} \\
&= \frac{|\Lambda_\tau|}{1\cdot 2} + \frac{|\Lambda_\tau|^2}{1\cdot 2\cdot 3} + \frac{|\Lambda_\tau|^3}{1\cdot 2\cdot 3\cdot 4} + \frac{|\Lambda_\tau|^4}{1\cdot 2\cdot 3\cdot 4\cdot 5} + \cdots \\
&= \frac{1}{2}\left(\frac{|\Lambda_\tau|}{1} + \frac{|\Lambda_\tau|^2}{1\cdot 3} + \frac{|\Lambda_\tau|^3}{1\cdot 3\cdot 4} + \frac{|\Lambda_\tau|^4}{1\cdot 3\cdot 4\cdot 5} + \cdots\right) \\
&\leq \frac{1}{2}\left(\frac{|\Lambda_\tau|}{1} + \frac{|\Lambda_\tau|^2}{1\cdot 2} + \frac{|\Lambda_\tau|^3}{1\cdot 2\cdot 3} + \frac{|\Lambda_\tau|^4}{1\cdot 2\cdot 3\cdot 4} + \cdots\right) \\
&= \frac{1}{2}\left(\sum_{n\geq 1}\frac{|\Lambda_\tau|^n}{n!}\right) \\
&= \frac{1}{2}\left(\sum_{n\geq 0}\frac{|\Lambda_\tau|^n}{n!} - 1\right) \\
&= \frac{1}{2}(e^{|\Lambda_\tau|} - 1) \\
&\leq \frac{1}{2}(e^{\log 2} - 1) = \frac{1}{2}
\end{aligned}
$$

where the second inequality follows from the fact that $\frac{1}{1\cdot 3\cdot 4\cdots n} \leq \frac{1}{1\cdot 2\cdots(n-1)}$ since for $n \geq 3$,

$$2 \leq n \implies 1\cdot 2\cdot 3\cdots(n-1) < 1\cdot 3\cdot 4\cdots n.$$

More generally, applying the same idea as above for any even $N \geq 2$, we obtain

$$
\begin{aligned}
\left|\sum_{n\geq 2} \frac{(\Lambda_\tau)^{n-1}}{n!}\right| &= \left|\sum_{n\geq 1} \frac{\Lambda_\tau^n}{(n+1)!}\right| \\
&= \left|\frac{\Lambda_\tau}{1\cdot 2} + \frac{\Lambda_\tau^2}{1\cdot 2\cdot 3} + \frac{\Lambda_\tau^3}{1\cdot 2\cdot 3\cdot 4} + \frac{\Lambda_\tau^4}{1\cdot 2\cdot 3\cdot 4\cdot 5} + \cdots\right| \\
&= \left|\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!} + \frac{\Lambda_\tau^{N+1}}{1\cdots(N+2)} + \frac{\Lambda_\tau^{N+2}}{1\cdots(N+3)} + \frac{\Lambda_\tau^{N+3}}{1\cdots(N+4)} + \cdots\right| \\
&= \left|\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!} + \frac{1}{N+2}\left(\frac{\Lambda_\tau^{N+1}}{1\cdots(N+1)} + \frac{\Lambda_\tau^{N+2}}{1\cdots(N+1)\cdot(N+3)} + \cdots\right)\right| \\
&\leq \left|\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!}\right| + \frac{1}{N+2}\left|\sum_{n=N+1}^{\infty} \frac{\Lambda_\tau^n}{n!}\right| \\
&\leq \left|\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!}\right| + \frac{1}{N+2}\left(\sum_{n=N+1}^{\infty} \frac{|\Lambda_\tau|^n}{n!}\right) \\
&= \left|\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!}\right| + \frac{1}{N+2}\left(\sum_{n=0}^{\infty} \frac{|\Lambda_\tau|^n}{n!} - \sum_{n=0}^{N} \frac{|\Lambda_\tau|^n}{n!}\right) \\
&\leq \left|\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!}\right| + \frac{1}{N+2}\left(\sum_{n=0}^{\infty} \frac{|\Lambda_\tau|^n}{n!}\right) \\
&= \left|\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!}\right| + \frac{1}{N+2} e^{|\Lambda_\tau|} \\
&\leq \left|\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!}\right| + \frac{1}{N+2} e^{\log 2} \\
&= \left|\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!}\right| + \frac{2}{N+2} := k_N.
\end{aligned}
$$

We now give an upper bound for k_N. Since $\Lambda_\tau < 0$, we obtain

$$\begin{aligned}
\sum_{n=1}^{N} \frac{\Lambda_\tau^n}{(n+1)!} &= \frac{\Lambda_\tau}{2!} + \frac{\Lambda_\tau^2}{3!} + \frac{\Lambda_\tau^3}{4!} + \frac{\Lambda_\tau^4}{5!} + \cdots \\
&= \frac{|\Lambda_\tau|^2}{3!} - \frac{-\Lambda_\tau}{2!} + \frac{|\Lambda_\tau|^4}{5!} - \frac{-\Lambda_\tau^3}{4!} + \cdots \\
&= \frac{|\Lambda_\tau|^2}{3!} - \frac{|\Lambda_\tau|}{2!} + \frac{|\Lambda_\tau|^4}{5!} - \frac{|\Lambda_\tau|^3}{4!} + \cdots \\
&= \sum_{\substack{n=2\\ n|2}}^{N} \left(\frac{|\Lambda_\tau|^n}{(n+1)!} - \frac{|\Lambda_\tau|^{n-1}}{n!} \right) \\
&= \sum_{\substack{n=2\\ n|2}}^{N} \frac{|\Lambda_\tau|^{n-1}}{n!} \left(\frac{|\Lambda_\tau|}{n+1} - 1 \right) \\
&= \frac{|\Lambda_\tau|}{2} \left(\frac{|\Lambda_\tau|}{3} - 1 \right) + \sum_{\substack{n=4\\ n|2}}^{N} \frac{|\Lambda_\tau|^{n-1}}{n!} \left(\frac{|\Lambda_\tau|}{n+1} - 1 \right) \\
&\geq \frac{|\Lambda_\tau|}{2} \left(\frac{|\Lambda_\tau|}{4} - 1 \right) + \sum_{\substack{n=4\\ n|2}}^{N} \frac{|\Lambda_\tau|^{n-1}}{n!} \left(\frac{|\Lambda_\tau|}{n+1} - 1 \right)
\end{aligned}$$

$$\sum_{n\geq 2} (\Lambda_\tau)^{n-1}/n! = \sum_{N\geq n\geq 1} (\Lambda_\tau)^n/(n+1)! = \sum_{N\geq n\geq 2,\, 2|n} \tfrac{|\Lambda_\tau|^n}{(n+1)!} - \tfrac{|\Lambda_\tau|^{n-1}}{n!}$$

$$= \sum_{N\geq n\geq 2,\, 2|n} \tfrac{|\Lambda_\tau|^{n-1}}{n!}\left(\tfrac{|\Lambda_\tau|}{n+1} - 1\right) = \tfrac{|\Lambda_\tau|}{2}\left(\tfrac{|\Lambda_\tau|}{3} - 1\right) + \sum_{N\geq n\geq 4,\, 2|n} \tfrac{|\Lambda_\tau|^{n-1}}{n!}\left(\tfrac{|\Lambda_\tau|}{n+1} - 1\right)$$

$$\geq \tfrac{\log 2}{2}\left(\tfrac{\log 2}{4} - 1\right) + \sum_{N\geq n\geq 4,\, 2|n} \tfrac{(\log 2)^{n-1}}{n!}\left(\tfrac{3/4(\log 2)}{n+1} - 1\right) := -k_N.$$

The last inequality follows by distinguishing two cases whether $|\Lambda_\tau| \leq 3/4 \cdot \log 2$ or not; note that $ln(2)/2 * (ln(2)/4 - 1)/(-ln(2) * 3/8) \geq 1$. Now, on using that $-k_N$ is negative, it follows that $|1 + \sum_{n\geq 2} (\Lambda_\tau)^{n-1}/n!| \geq 1 - |\sum_{n\geq 2} (\Lambda_\tau)^{n-1}/n!| \geq 1 - k_N$ and thus

$$|\Lambda_\tau| \leq \kappa_\tau |\tau(x)|, \quad \kappa_\tau = \tfrac{1}{1-k_N} |\tau(\lambda_0)|, \quad c_\tau = \log^+(2|\lambda_0|).$$

DETAILS HERE NEED TO BE CLARIFIED, SO FOR NOW, WE WILL JUST TAKE

$k_N = 1/2$ That is,

$$\left|\sum_{n\geq 2} \frac{(\Lambda_\tau)^{n-1}}{n!}\right| \leq \frac{1}{2}$$

hence... ACTUALLY I DON'T UNDERSTAND THIS PROOF AT ALL, SO WE WILL TAKE $k_N = 1/2$, giving us

$$|\Lambda_\tau| \leq \kappa_\tau |\tau(x)|, \quad \kappa_\tau = \tfrac{1}{1-k_N}|\tau(\lambda_0)|, \quad c_\tau = \log^+(2|\lambda_0|),$$

hence

$$\kappa_\tau = \tfrac{1}{1-1/2}|\tau(\lambda_0)| = 2|\tau(\lambda_0)| \implies |\Lambda_\tau| \leq \kappa_\tau|\tau(x)| = 2|\tau(\lambda_0)||\tau(x)|.$$

Now,

$$\begin{aligned}
-h_\tau\left(\frac{\delta_2}{\lambda}\right) = -\log\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} \implies e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)} &= e^{-\log\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\}} \\
&= e^{\log\left(\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\}\right)^{-1}} \\
&= \left(\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right)^{-1} \\
&= \frac{1}{\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}} \\
&= \max\left\{\left|\tau\left(\frac{\lambda}{\delta_2}\right)\right|, 1\right\} \\
&= \max\left\{\left|\tau(x)\right|, 1\right\}.
\end{aligned}$$

In addition,

$$\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right| \leq \max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\} \implies \frac{1}{\max\left\{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}} \leq \frac{1}{\left|\tau\left(\frac{\delta_2}{\lambda}\right)\right|} = \left|\tau\left(\frac{\lambda}{\delta_2}\right)\right| = |\tau(x)|.$$

Therefore, all together, we have

$$|\Lambda_\tau| \leq \kappa_\tau|\tau(x)| \leq \kappa_\tau \max\{|\tau(x)|, 1\} = \kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)} \leq \kappa_\tau e^{-l_\tau}$$

NO THIS STILL DOESN'T MAKE SENSE. LET'S JUST GO WITH RAFAELS BOUND with $k_\tau = 2|\tau(\delta_2)|$

Altogether, we now have

$$
\begin{aligned}
&\left|\alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i}\right| \\
&\leq \frac{1}{2}\left(\frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\} + \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l \log(p_l)|u_l - r_l|\right) + \\
&\qquad + \left(\frac{1}{2} + c\kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)}\right).
\end{aligned}
$$

□

Recall that

$$
h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu}\log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}}\log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\}.
$$

Take $\mathbf{h} \in \mathbb{R}^{r+\nu}$ such that $\mathbf{h} \geq \mathbf{0}$. Let $\mathbf{m} = (n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{r+\nu}$ be any solution of (22) with

$$
h_\tau\left(\frac{\delta_2}{\lambda}\right) \geq l_\tau
$$

where we denote by $h_v\left(\frac{\delta_2}{\lambda}\right)$ the v^{th} entry of the vector

$$
\left(\log(p_1)|u_1 - r_1|, \ldots, \log(p_\nu)|u_\nu - r_\nu|, \max\left\{\left|\tau_1\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\}, \ldots, \log\max\left\{\left|\tau_n\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\}\right).
$$

Since

$$
h_\tau\left(\frac{\delta_2}{\lambda}\right) \geq l_\tau > c_\tau,
$$

the previous lemma holds. That is,

$$
\begin{aligned}
&\left|\alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i}\right| \\
&\leq \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l \log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|,1\right\}\right) + \\
&\qquad + \left(\frac{1}{2} + c\kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)}\right).
\end{aligned}
$$

Suppose $h_v\left(\frac{\delta_2}{\lambda}\right) \leq h_v$ for all $v \in \{1, \ldots, r+\nu\}$. Then, since

$$l_\tau \leq h_\tau\left(\frac{\delta_2}{\lambda}\right) \leq h_\tau \implies -h_\tau \leq -h_\tau\left(\frac{\delta_2}{\lambda}\right) \leq -l_\tau \implies e^{-h_\tau} \leq e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)} \leq e^{-l_\tau},$$

we deduce

$$\begin{aligned}
&\left|\alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i}\right| \\
&\leq \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l \log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma \log\max\left\{\left|\sigma\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}\right) + \\
&\qquad + \left(\frac{1}{2} + c\kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)}\right) \\
&\leq \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l h_l + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma h_\sigma\right) + \left(\frac{1}{2} + c\kappa_\tau e^{-h_\tau\left(\frac{\delta_2}{\lambda}\right)}\right) \\
&\leq \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l h_l + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma h_\sigma\right) + \frac{1}{2} + c\kappa_\tau e^{-l_\tau}
\end{aligned}$$

We finally can define the ellipsoid. Let

$$b = \frac{1}{\log(2)^2}\sum_{k=1}^{\nu} h_k^2$$

where

$$\log(2)^2 q_f(\mathbf{n}) = \log(2)^2 \sum_{k=1}^{\nu}\left\lfloor \frac{\log(p_k)^2}{\log(2)^2}\right\rfloor |u_k - r_k|^2 \leq \sum_{k=1}^{\nu}\log(p_k)^2|u_k - r_k|^2 \leq \sum_{k=1}^{\nu} h_k^2.$$

For each ε_l in $\{\varepsilon_1, \ldots, \varepsilon_r\}$ such that $\varepsilon_l \neq \varepsilon_l^*$, we define

$$|a_l|^2 \leq \left(\frac{1}{[K:\mathbb{Q}]}\sum_{k=1}^{\nu} w_{\gamma l k} h_k + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_{\varepsilon l \sigma} h_\sigma\right)^2 =: b_{\varepsilon_l}$$

Now, for ε_l in $\{\varepsilon_1, \ldots, \varepsilon_r\}$ such that $\varepsilon_l = \varepsilon_l^*$, we define

$$
\begin{aligned}
&\left|\alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i}\right|^2 \\
&\leq \left(\frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l h_l + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma:L\to\mathbb{C}} w_\sigma h_\sigma\right) + \frac{1}{2} + c\kappa_\tau e^{-l_\tau}\right)^2 =: b_{\varepsilon_l}.
\end{aligned}
$$

Let

$$\mathbf{x} = (x_1, \ldots, x_\nu, x_{\varepsilon_1}, \ldots, x_{\varepsilon_r}) \in \mathbb{R}^{\nu+r}.$$

Then we define the ellipsoid $\mathcal{E}_\tau \subseteq \mathbb{R}^{r+\nu}$ by

$$
\begin{aligned}
\mathcal{E}_\tau = \{q_\tau(\mathbf{x}) &\leq (1+r)(bb_{\varepsilon_1}\cdots b_{\varepsilon_r});\ \mathbf{x} \in \mathbb{R}^{r+\nu}\}, \qquad \text{where} \\
q_\tau(\mathbf{x}) &= (b_{\varepsilon_1}\cdots b_{\varepsilon_r})\left(q_f(x_1, \ldots, x_\nu) + \sum_{i=1}^{r} \frac{b}{b_{\varepsilon_i}} x_{\varepsilon_i}^2\right) \\
q_\tau(\mathbf{x}) &= \left((b_{\varepsilon_1}\cdots b_{\varepsilon_r})\cdot q_f(x_1, \ldots, x_\nu) + (b_{\varepsilon_1}\cdots b_{\varepsilon_r})\sum_{i=1}^{r} \frac{b}{b_{\varepsilon_i}} x_{\varepsilon_i}^2\right) \\
q_\tau(\mathbf{x}) &= \left((b_{\varepsilon_1}\cdots b_{\varepsilon_r})\cdot q_f(x_1, \ldots, x_\nu) + \sum_{i=1}^{r} b(b_{\varepsilon_1}\cdots b_{\varepsilon_{i-1}} b_{\varepsilon_{i+1}} b_{\varepsilon_r}) x_{\varepsilon_i}^2\right)
\end{aligned}
$$

where

$$q_f(\mathbf{y}) = (A\mathbf{y})^{\mathrm{T}} D^2 A\mathbf{y}.$$

Now, if

$$\mathbf{x} = (x_1, \ldots, x_\nu, x_{\varepsilon_1}, \ldots, x_{\varepsilon_r}) \in \mathbb{R}^{\nu+r}$$

is a solution, it follows that

$$
\begin{aligned}
q_\tau(\mathbf{x}) &= \left((b_{\varepsilon_1}\cdots b_{\varepsilon_r})\cdot q_f(x_1, \ldots, x_\nu) + \sum_{i=1}^{r} b(b_{\varepsilon_1}\cdots b_{\varepsilon_{i-1}} b_{\varepsilon_{i+1}} b_{\varepsilon_r}) x_{\varepsilon_i}^2\right) \\
&\leq (b_{\varepsilon_1}\cdots b_{\varepsilon_r})\cdot b + \sum_{i=1}^{r} b(b_{\varepsilon_1}\cdots b_{\varepsilon_{i-1}} b_{\varepsilon_{i+1}} b_{\varepsilon_r}) b_{\varepsilon_i} \\
&= (1+r)(bb_{\varepsilon_1}\cdots b_{\varepsilon_r}).
\end{aligned}
$$

13.6 Archimedean sieve: Real case, $r = 2$

Suppose that all roots of f are real so that $r = 2$. Let $\tau : L \to \mathbb{C}$ be an embedding. We take $l, h \in \mathbb{R}^{m+\nu}$ with $0 \le l \le h$ and $l_\tau \ge \log 2$. Then we consider the translated lattice $\Gamma_\tau \subset \mathbb{Z}^{r+\nu}$ defined by

$$\Gamma_\tau = \Phi_\tau(\mathbb{Z}^{r+\nu}) + w$$

where $w = (0, \ldots, 0, \alpha_0)^{\mathrm{T}}$ for c a constant of the size e^{l_τ} and where Φ_τ is a linear transformation which is the identity on $\mathbb{Z}^{u+r-1}$ and which sends

$$(0, \ldots, 0, 1) \mapsto (\alpha_{\gamma 1}, \ldots, \alpha_{\gamma\nu}, \alpha_{\varepsilon 1}, \ldots, \alpha_{\varepsilon r}).$$

That is,

$$\left(\left[c \log\left(\tau\left(\frac{\gamma_1^{(k)}}{\gamma_1^{(j)}}\right)\right)\right], \ldots, \left[c \log\left(\tau\left(\frac{\gamma_\nu^{(k)}}{\gamma_\nu^{(j)}}\right)\right)\right], \left[c \log\left(\tau\left(\frac{\varepsilon_1^{(k)}}{\varepsilon_1^{(j)}}\right)\right)\right], \ldots, \left[c \log\left(\tau\left(\frac{\varepsilon_r^{(k)}}{\varepsilon_r^{(j)}}\right)\right)\right]\right).$$

The matrix associated to this lattice is therefore

$$\Gamma_\tau = \begin{pmatrix} 1 & 0 & \ldots & \ldots & 0 & 0 \\ 0 & 1 & \ldots & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & \ldots & 1 & 0 \\ \alpha_{\gamma 1} & \ldots & \alpha_{\gamma\nu} & \alpha_{\varepsilon 1} & \ldots & \alpha_{\varepsilon r} \end{pmatrix}.$$

Let $\mathcal{E}_\tau = \mathcal{E}_\tau(h, l_\tau)$ be the ellipsoid constructed in (**??**). Let $\mathbf{m} = (n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{r+\nu}$ be any solution of (22). We say that $\mathbf{m}$ is determined by some $\mathbf{y} \in \Gamma_\tau$ if

$$\mathbf{y} = (y_1, \ldots, y_{r+\nu}) = \left(n_1, \ldots, n_\nu, a_1, \ldots, a_{r-1}, \alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i}\right)$$

where the missing element a_i corresponds to ε^*.

Lemma 13.13. *Let $\mathbf{m} = (n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{r+\nu}$ be any solution of (22) which lies in $\Sigma_\tau(l, h)$. Then $\mathbf{m}$ is determined by some $\gamma \in \Gamma_\tau \cap \mathcal{E}_\tau$.*

Suppose that $\gamma \in \Gamma_\tau \cap \mathcal{E}_\tau$. Let $M = M_\tau$ be the matrix defining the ellipsoid

$$\mathcal{E}_\tau : z^t M^t M z \le (1 + r)(b b_{\varepsilon_1} \cdots b_{\varepsilon_r}),$$

that is,

$$M = \sqrt{b_{\varepsilon_1}\cdots b_{\varepsilon_r}} \begin{pmatrix} DA & 0 & \dots & 0 & 0 \\ 0 & \sqrt{\frac{b}{b_{\varepsilon 1}}} & \dots & 0 & 0 \\ 0 & 0 & \sqrt{\frac{b}{b_{\varepsilon 2}}} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \sqrt{\frac{b}{b_{\varepsilon^*}}} \end{pmatrix}.$$

Note that we never need to compute M, but rather $M^T M$ so that we do not need to worry about precision. In this case,

$$\begin{aligned} M^T M &= b_{\varepsilon_1}\cdots b_{\varepsilon_r} \begin{pmatrix} A^T D^2 A & 0 & \dots & 0 & 0 \\ 0 & \frac{b}{b_{\varepsilon 1}} & \dots & 0 & 0 \\ 0 & 0 & \frac{b}{b_{\varepsilon 2}} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \frac{b}{b_{\varepsilon^*}} \end{pmatrix} \\ &= \begin{pmatrix} (b_{\varepsilon_1}\cdots b_{\varepsilon_r})A^T D^2 A & 0 & \dots & 0 & 0 \\ 0 & bb_{\varepsilon_2}\cdots b_{\varepsilon_r} & \dots & 0 & 0 \\ 0 & 0 & bb_{\varepsilon_1}b_{\varepsilon_3}\cdots b_{\varepsilon_r} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & bb_{\varepsilon_1}\cdots b_{\varepsilon_{r-1}} \end{pmatrix}. \end{aligned}$$

Since $\gamma \in \Gamma_\tau \cap \mathcal{E}_\tau$, there exists $x \in \mathbb{R}^{r+\nu}$ such that $\gamma = \Gamma_\tau x + w$ and $\gamma^t M^t M \gamma \leq (1+r)(bb_{\varepsilon_1}\cdots b_{\varepsilon_r})$. We thus have

$$(\Gamma_\tau x + w)^t M^t M (\Gamma_\tau x + w) \leq (1+r)(bb_{\varepsilon_1}\cdots b_{\varepsilon_r}).$$

As Γ_τ is clearly invertible, with matrix inverse

$$\Gamma_\tau^{-1} = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 1 & 0 \\ -\frac{\alpha_{\gamma 1}}{\alpha_{\varepsilon r}} & \dots & -\frac{\alpha_{\gamma \nu}}{\alpha_{\varepsilon r}} & -\frac{\alpha_{\varepsilon 1}}{\alpha_{\varepsilon r}} & \dots & \frac{1}{\alpha_{\varepsilon r}} \end{pmatrix},$$

we can find a vector c such that $\Gamma_\tau c = -w$. Indeed, this vector is $c = \Gamma_\tau^{-1}(-w)$, where

$$c = \Gamma_\tau^{-1} w = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 1 & 0 \\ -\frac{\alpha_{\gamma 1}}{\alpha_{\varepsilon r}} & \dots & -\frac{\alpha_{\gamma \nu}}{\alpha_{\varepsilon r}} & -\frac{\alpha_{\varepsilon 1}}{\alpha_{\varepsilon r}} & \dots & \frac{1}{\alpha_{\varepsilon r}} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ -\alpha_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ -\frac{\alpha_0}{\alpha_{\varepsilon r}} \end{pmatrix}.$$

Now,

$$\begin{aligned} (1+r)(bb_{\varepsilon_1}\cdots b_{\varepsilon_r}) &\geq (\Gamma_\tau x + w)^t M^t M(\Gamma_\tau x + w) \\ &= (\Gamma_\tau x - (-w))^t M^t M(\Gamma_\tau x - (-w)) \\ &= (\Gamma_\tau x - \Gamma_\tau c)^t M^t M(\Gamma_\tau x - \Gamma_\tau c) \\ &= (\Gamma_\tau (x - c))^t M^t M(\Gamma_\tau (x - c)) \\ &= (x-c)^t (M\Gamma_\tau)^t M\Gamma_\tau (x-c) \\ &= (x-c)^t B^t B(x-c) \end{aligned}$$

where $B = M\Gamma_\tau$. That is, we are left to solve

$$(x-c)B^t B(x-c) \leq (1+r)(bb_{\varepsilon_1}\cdots b_{\varepsilon_r}).$$

13.7 Archimedean Real Case Summary

If $(n_1, \dots, n_\nu, a_1, \dots, a_r) \in \mathbb{R}^{r+\nu}$ is a solution which lies in $\Sigma_\tau(l,h)$, then, by definition, it corresponds to a solution (x,y) satisfying

$$\Sigma_\tau(l,h) = \{(x,y) \in \Sigma \mid (h_v(z)) \leq h \text{ and } (h_v(z)) \nleq 0 \text{ and } h_\tau(z) > l_\tau\}.$$

Here, l_τ is defined as some constant such that

$$l_\tau > c_\tau.$$

By the computations above (see page 99), it follows that

$$\left|\alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i}\right| \leq \frac{1}{2}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} w_l h_l + \frac{1}{[L:\mathbb{Q}]}\sum_{\sigma: L\to\mathbb{C}} w_\sigma h_\sigma\right) + \frac{1}{2} + c\kappa_\tau e^{-l_\tau}.$$

Now, consider the vector

$$\gamma = (n_1, \dots, n_\nu, a_1, \dots, a_{r-1}, \alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i})$$

and the lattice defined by $\Gamma_\tau x + w$

$$\begin{pmatrix} 1 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 1 & 0 \\ \alpha_{\gamma 1} & \dots & \alpha_{\gamma \nu} & \alpha_{\varepsilon 1} & \dots & \alpha_{\varepsilon r} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{\nu+r-1} \\ x_{\nu+r} \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \alpha_0 \end{pmatrix}$$

for some vector $(x_1, \dots, x_{\nu+r}) \in \mathbb{Z}^{\nu+r}$. If $(x_1, \dots, x_{\nu+r}) = (n_1, \dots, n_\nu, a_1, \dots, a_r)$, then a quick computation shows that

$$\Gamma_\tau x + w = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{\nu+r-1} \\ \alpha_0 + \sum_{i=1}^{r} x_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} x_i \alpha_{\gamma i} \end{pmatrix} = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ a_{r-1} \\ \alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i} \end{pmatrix} = \gamma^T.$$

Hence, γ is in the lattice Γ.

Now, consider the ellipsoid $\mathcal{E}_\tau$. We claim that $\gamma \in \mathcal{E}_\tau$. Indeed, this means that

$$\gamma^t M^t M \gamma \leq (1+r)(b b_{\varepsilon_1} \cdots b_{\varepsilon_r}).$$

In particular

$$
\begin{aligned}
&\gamma^T M^T M \gamma \\
&= \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ a_{r-1} \\ \alpha_0 + \sum_{i=1}^r a_i \alpha_{\varepsilon i} + \sum_{i=1}^\nu n_i \alpha_{\gamma i} \end{pmatrix} \begin{pmatrix} (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) A^T D^2 A & 0 & \dots & 0 \\ 0 & b b_{\varepsilon_2} \cdots b_{\varepsilon_r} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-1}} \end{pmatrix} \gamma \\
&= \begin{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_\nu \end{pmatrix} (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) A^T D^2 A \\ a_1 b b_{\varepsilon_2} \cdots b_{\varepsilon_r} \\ \vdots \\ a_{r-1} b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-2}} b_{\varepsilon_r} \\ (\alpha_0 + \sum_{i=1}^r a_i \alpha_{\varepsilon i} + \sum_{i=1}^\nu n_i \alpha_{\gamma i})\, b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-1}} \end{pmatrix} \begin{pmatrix} n_1 & \dots & a_{r-1} & \alpha_0 + \sum_{i=1}^r a_i \alpha_{\varepsilon i} + \sum_{i=1}^\nu n_i \alpha_{\gamma i} \end{pmatrix} \\
&= \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_\nu \end{pmatrix} (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) A^T D^2 A \begin{pmatrix} n_1 & \dots & n_\nu \end{pmatrix} + a_1^2 b b_{\varepsilon_2} \cdots b_{\varepsilon_r} + \cdots + a_{r-1}^2 b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-2}} b_{\varepsilon_r} + \\
&\qquad + \left(\alpha_0 + \sum_{i=1}^r a_i \alpha_{\varepsilon i} + \sum_{i=1}^\nu n_i \alpha_{\gamma i} \right)^2 b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-1}}.
\end{aligned}
$$

Now, by definition, we have

$$\gamma^T M^T M \gamma = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_\nu \end{pmatrix} (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) A^T D^2 A \begin{pmatrix} n_1 & \dots & n_\nu \end{pmatrix} + a_1^2 b b_{\varepsilon_2} \cdots b_{\varepsilon_r} + \cdots + a_{r-1}^2 b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-2}} b_{\varepsilon_r} +$$

$$+ \left(\alpha_0 + \sum_{i=1}^{r} a_i \alpha_{\varepsilon i} + \sum_{i=1}^{\nu} n_i \alpha_{\gamma i} \right)^2 b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-1}}$$

$$\le (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) q_f(n_1 \dots n_\nu) + b_{\varepsilon_1} b b_{\varepsilon_2} \cdots b_{\varepsilon_r} + \cdots + b_{\varepsilon_{r-1}} b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-2}} b_{\varepsilon_r} + b_{\varepsilon_r} b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-2}} b_{\varepsilon_{r-1}}$$

$$\le (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) b + r(b b_{\varepsilon_1} \cdots b_{\varepsilon_r})$$

$$= (1 + r)(b b_{\varepsilon_1} \cdots b_{\varepsilon_r}).$$

Thus $\gamma \in \mathcal{E}_\tau$. Thus, if we assume that our solution lies in $\Sigma_\tau(l, h)$, it follows that $\gamma \in \Gamma \cap \mathcal{E}_\tau$. Now, by Rafael,

$$\Sigma = \Sigma(h_0), \quad \Sigma(h) = \Sigma(l, h) \cup \Sigma(l) \quad \text{and} \quad \Sigma(l, h) = \cup_{v \in S^*} \Sigma_v(l, h).$$

Thus, we collect all solutions from $\Sigma_\tau(l, h)$ and continue to generate all solutions at the other places.

MAYBE COULD USE MORE DETAIL HERE

14 Non-Archimedean Case

14.1 Non-Archimedean sieve

Note that in this section we might use v and l interchangeably. Eventually this will be fixed to be consistent...

Let $v \in \{1, \dots, \nu\}$. We take vectors $l, h \in \mathbb{R}^{\nu+r}$ with $0 \le l \le h$ and

$$\frac{l_v}{\log(p)} \ge \max\left(\frac{1}{p-1}, \operatorname{ord}_{p_v}(\delta_1) \right) - \operatorname{ord}_{p_v}(\delta_2)$$

and then consider the translated lattice $\Gamma_v \subseteq \mathbb{Z}^{\nu+r}$ defined below. We say that $(x, y) \in \Sigma$ with $\mathbf{m} = (n_1, \dots, n_\nu, a_1, \dots, a_r) \in \mathbb{R}^{r+\nu}$ is determined by some $\gamma \in \Gamma_v$ if the entries of

γ are a (fixed) permutation of the entries of $\mathbf{m}$. Let $\mathcal{E}_v$ be the ellipsoid constructed in (26).

Lemma 14.1. *And* $(x, y) \in \Sigma_v(l, h)$ *is determined by some* $\gamma \in \Gamma_v \cap \mathcal{E}_v$.

In the remainder of this section, we prove this lemma.

14.1.1 Computing $u_l - r_l = \sum_{i=1}^{\nu} n_i a_{li}$

Recall that $z \in \mathbb{C}_p$ having $\mathrm{ord}_p(z) = 0$ is called a p-adic unit.

Let $l \in \{1, \ldots, \nu\}$ and consider the prime $p = p_l$. For every $i \in \{1, \ldots, r\}$, part (ii) of the Corollary of Lemma 2 of Tzanakis-de Weger tells us that $\frac{\varepsilon_1^{(i_0)}}{\varepsilon_1^{(j)}}$ and $\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}$ (for $i = 1, \ldots, r$) are p_l-adic units.

From now on we make the following choice for the index i_0. Let $g_l(t)$ be the irreducible factor of $g(t)$ in $\mathbb{Q}_{p_l}[t]$ corresponding to the prime ideal $\mathfrak{p}_l$. Since $\mathfrak{p}_l$ has ramification index and residue degree equal to 1, $\deg(g_l[t]) = 1$. We choose $i_0 \in \{1, 2, 3\}$ so that $\theta^{(i_0)}$ is the root of $g_l(t)$. The indices of j, k are fixed, but arbitrary.

Lemma 14.2.

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

(ii) Let $i \in \{1, \ldots, \nu\}$. *Then* $\mathrm{ord}_{p_l}\left(\frac{\gamma_i^{(i_0)}}{\gamma_i^{(j)}}\right) = a_{li}$, *where* $\mathbf{a_i} = (a_{1i}, \ldots, a_{\nu i})$.

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

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

we have

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

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

$$\mathrm{ord}_{p_l}(\gamma_i^{(i_0)}) = \frac{1}{e_l} \mathrm{ord}_{\mathfrak{p}_l}(\gamma_i) = \mathrm{ord}_{\mathfrak{p}_l}(\mathfrak{p}_1^{a_{1i}} \cdots \mathfrak{p}_\nu^{a_{\nu i}}) = a_{li}.$$

□

We consider the form

$$\Lambda_{p_l} = \log_{p_l}(\delta_1) + \sum_{i=1}^{r} a_i \log_{p_l}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right) + \sum_{i=1}^{\nu} n_i \log_{p_l}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right).$$

To simplify our exposition, we introduce the following notation.

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

and

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

Put

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

and

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

Now,

$$\Lambda_{p_l} = \log_{p_l}(\delta_1) + \sum_{i=1}^{r} a_i \log_{p_l}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right) + \sum_{i=1}^{\nu} n_i \log_{p_l}\left(\frac{\gamma_i^{(k)}}{\gamma_i^{(j)}}\right) = \sum_{i=1}^{1+\nu+r} b_i \alpha_i.$$

The next lemma deals with a special case in which the n_l can be computed directly.

Lemma 14.3. *Let $l \in \{1, \ldots, \nu\}$. If $\mathrm{ord}_{p_l}(\delta_1) \neq 0$, then*

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

Proof. Apply the Corollary of Lemma 2 of Tzanakis-de Weger and Lemma 14.2 to both expressions of λ in (23). On the one hand, we obtain $\mathrm{ord}_{p_l}(\lambda) = \min\{\mathrm{ord}_{p_l}(\delta_1), 0\}$, and on the other hand, we obtain

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

□

That is,

$$\sum_{i=1}^{\nu} n_i a_{li} = \begin{cases} -\operatorname{ord}_{p_l}(\delta_2) & \text{if } \operatorname{ord}_{p_l}(\delta_1) > 0 \\ \operatorname{ord}_{p_l}(\delta_1) - \operatorname{ord}_{p_l}(\delta_2) = \operatorname{ord}_{p_l}(\delta_1/\delta_2) & \text{if } \operatorname{ord}_{p_l}(\delta_1) < 0 \end{cases}$$

From here, we will need to assume that $\operatorname{ord}_{p_l}(\delta_1) = 0$. We first recall the following result of the p_l-adic logarithm:

Lemma 14.4. *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*

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

then

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

NOT CLEAR TO ME IF THE BELOW IS AN EFFICIENT COMPUTATION TO MAKE, OR THAT IT HAPPENS OFTEN ENOUGH TO TEST.

For $l \in \{1, \ldots \nu\}$, we identify conditions in which n_l can be bounded by a small explicit constant.

Let L be a finite extension of $\mathbb{Q}_{p_l}$ containing δ_1, $\frac{\gamma_i^{(k)}}{\gamma_i^{(l)}}$ (for $i = 1, \ldots, \nu$), and $\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(l)}}$ (for $i = 1, \ldots, r$). Since finite p-adic fields are complete, $\alpha_i \in L$ for $i = 1, \ldots, 1 + \nu + r$ as well. Choose $\phi \in \overline{\mathbb{Q}_{p_l}}$ such that $L = \mathbb{Q}_{p_l}(\phi)$ and $\operatorname{ord}_{p_l}(\phi) > 0$. Let $G(t)$ be the minimal polynomial of ϕ over $\mathbb{Q}_{p_l}$ and let S be its degree. For $i = 1, \ldots, 1 + \nu + r$ write

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

Then

$$\Lambda_l = \sum_{h=1}^{S} \Lambda_{lh} \phi^{h-1}, \tag{25}$$

with

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

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

Lemma 14.5. *For every $h \in \{1, \ldots, S\}$, we have*

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

Proof. Taking the images of (25) under conjugation $\phi \mapsto \phi^{(h)}$ $(h = 1, \ldots, S)$ gives

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

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

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

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

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

we have

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

for every $h \in \{1, \ldots, S\}$. □

Remark. The above can made more precise using the γ_{jk}, possibly giving us a tighter subsequent bound on the n_l.

Lemma 14.6. *If* $\mathrm{ord}_{p_l}(\delta_1) = 0$ *and*

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

then

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

Proof. Immediate from Lemma 14.4. $\square$

Said another way, this means

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

Lemma 14.7. *Suppose* $\mathrm{ord}_{p_l}(\delta_1) = 0$.

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

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

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

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

where

$$\nu_l = \frac{1}{2} \mathrm{ord}_{p_l}(\mathit{Disc}(G(t)))$$

AGAIN, IT'S NOT CLEAR HOW EFFICIENT THIS COMPUTATION IS... WE SHALL SEE. PART (1) IS ACTUALLY NEEDED IN THE REST OF THE COMPUTATIONS, BUT PART (2) MIGHT BE THE INEFFICIENT PART OF THIS.

Proof.

(i) We prove the contrapositive. Suppose

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

and

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

Observe that

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

Therefore, it suffices to show that

$$\mathrm{ord}_{p_l}(\Lambda_l) \geq \min_{2\leq i\leq 1+\nu+r} \mathrm{ord}_{p_l}(b_i\alpha_i).$$

By Lemma 14.4, the first inequality implies $\mathrm{ord}_{p_l}(\Lambda_l) = \sum_{i=1}^{\nu} n_i a_{li} + \mathrm{ord}_{p_l}(\delta_2)$, from which the result follows.

(ii) We prove the contrapositive. Let $h \in \{1, \ldots, S\}$ and suppose

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

and

$$\sum_{i=1}^{\nu} n_i a_{li} \geq \nu_l + \min_{2\leq i\leq 1+\nu+r} \mathrm{ord}_{p_l}(\alpha_{ih}) - \mathrm{ord}_{p_l}(\delta_2).$$

Observe that

$$\begin{aligned}\mathrm{ord}_{p_l}(\alpha_{1h}) &= \mathrm{ord}_{p_l}\left(\Lambda_{lh} - \sum_{i=2}^{1+\nu+r} b_i\alpha_{ih}\right) \\ &\geq \min\left\{\mathrm{ord}_{p_l}(\Lambda_{lh}), \min_{2\leq i\leq 1+\nu+r} \mathrm{ord}_{p_l}(b_i\alpha_{ih})\right\}\end{aligned}$$

Therefore, it suffices to show that

$$\mathrm{ord}_{p_l}(\Lambda_{lh}) \geq \min_{2\leq i\leq 1+\nu+r} \mathrm{ord}_{p_l}(b_i\alpha_{ih}).$$

By Lemma 14.4, the first inequality implies $\mathrm{ord}_{p_l}(\Lambda_l) = \sum_{i=1}^{\nu} n_i a_{li} + \mathrm{ord}_{p_l}(\delta_2)$. Combining this with Lemma 14.5 yields

$$\mathrm{ord}_{p_l}(\Lambda_{lh}) \geq \sum_{i=1}^{\nu} n_i a_{li} + \mathrm{ord}_{p_l}(\delta_2) - \nu_l.$$

The results now follow from our second assumption.

□

We now set some notation and give some preliminaries for the p_l-adic reduction procedures. Consider a fixed index $l \in \{1,\ldots,v\}$. Following Lemma 14.7, we have

$$\mathrm{ord}_{p_l}(\alpha_1) \geq \min_{2\leq i\leq 1+\nu+r} \mathrm{ord}_{p_l}(\alpha_i) \quad \text{and} \quad \mathrm{ord}_{p_l}(\alpha_{1h}) \geq \min_{2\leq i\leq 1+\nu+r}(\alpha_{ih}) \quad h = (1,\ldots,s).$$

and

$$\mathrm{ord}_{p_l}(\delta_1) = 0.$$

Let I be the set of all indices $i' \in \{2,\ldots,1+\nu+r\}$ for which

$$\mathrm{ord}_{p_l}(\alpha_{i'}) = \min_{2\leq i\leq 1+\nu+r} \mathrm{ord}_{p_l}(\alpha_i).$$

We will identify two cases, the *special case* and the *general case*. The special case occurs when there is some index $i' \in I$ such that $\alpha_i/\alpha_{i'} \in \mathbb{Q}_{p_l}$ for $i = 1,\ldots,1+\nu+r$. The general case is when there is no such index.

We now assume that our Thue-Mahler equation has degree 3 to assure that our linear form in p-adic logs has coefficients in $\mathbb{Q}_p$. DETAILS NEEDED HERE [p51 of HAMBROOK]. This means that we are indeed always in the Special Case of TdW/Hambrook.

Thus, let $\hat{i}$ be an arbitrary index in I for which $\alpha_i/\alpha_{\hat{i}} \in \mathbb{Q}_{p_l}$ for every $i = 1,\ldots,1+\nu+r$. We further define

$$\beta_i = -\frac{\alpha_i}{\alpha_{\hat{i}}} \quad i = 1,\ldots,1+\nu+r,$$

and

$$\Lambda_l' = \frac{1}{\alpha_{\hat{i}}}\Lambda_l = \sum_{i=1}^{1+\nu+r} b_i(-\beta_i).$$

Now, we have $\beta_i \in \mathbb{Z}_{p_l}$ for $i = 1, \dots, 1+\nu+r$.

Lemma 14.8. *Suppose* $\operatorname{ord}_{p_l}(\delta_1) = 0$ *and*

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

Then

$$\operatorname{ord}_{p_l}(\Lambda_l') = \sum_{i=1}^{v} n_i a_{li} + \operatorname{ord}_{p_l}(\delta_2) - \operatorname{ord}_{p_l}(\alpha_{\hat{i}}).$$

Proof. Immediate from Lemma 14.5 and Lemma 14.6. □

We now describe the p_l-adic reduction procedure. Recall that l_v is a constant such that

$$\frac{l_v}{\log(p)} \geq \max\left(\frac{1}{p-1}, \operatorname{ord}_{p_v}(\delta_1)\right) - \operatorname{ord}_{p_v}(\delta_2).$$

Now, let l_v' (denoted μ in BeGhKr and m in TdW) be the largest element of $\mathbb{Z}_{\geq 0}$ at most

$$l_v' \leq \frac{l_v}{\log(p)} - \operatorname{ord}_{p_l}(\alpha_{\hat{i}}) + \operatorname{ord}_{p_l}(\delta_2).$$

We will use the notation l_v' and μ interchangeably. Eventually we should use consistent notation here, but we will just use μ for now in place of l_v'.

For each $x \in \mathbb{Z}_{p_l}$, let $x^{\{\mu\}}$ denote the unique rational integer in $[0, p_l^{\mu} - 1]$ such that $\operatorname{ord}_{p_l}(x - x^{\mu}) \geq \mu$ (ie. $x \equiv x^{\{\mu\}} \pmod{p_l^{\mu}}$). That is,

$$x \equiv x^{\{\mu\}} \pmod{p_l^{\mu}} \implies x - x^{\{\mu\}} = \alpha p_l^{\mu}$$

for some $\alpha \in \mathbb{Z}$. Hence $x \equiv x^{\{\mu\}} \pmod{p_l^{j}}$ for $j = 1, \dots, \mu$. In other words, we must have

$$x = a_0 + a_1 p + \cdots + a_n p^n + \cdots \quad \text{and} \quad x^{\{\mu\}} = a_0 + a_1 p + \cdots + a_{\mu-1} p^{\mu-1}.$$

Then

$$x - x^{\{\mu\}} = a_{\mu} p^{\mu} + \cdots + a_n p^n + \cdots \implies x - x^{\{\mu\}} \equiv 0 \pmod{p^{\mu}}$$

so that the highest power dividing $x - x^{\{\mu\}}$ is at least μ. Recall, the order is the first non-zero term appearing in the series expansion of $x - x^{\{\mu\}}$, and thus a_μ may or may not be the first non-zero term, hence the order is at least μ, though can be larger.

Let Γ_μ be the $(\nu + r)$-dimensional translated lattice $A_\mu x + w$, where A_μ is the diagonal matrix having $\hat{i}^{\text{th}}$ row

$$\left(\beta_2^{\{\mu\}}, \cdots, \beta_{\hat{i}-1}^{\{\mu\}}, p_l^\mu, \beta_{\hat{i}+1}^{\{\mu\}}, \cdots, \beta_{1+\nu+r}^{\{\mu\}}\right) \in \mathbb{Z}^{\nu+r}.$$

Here, p_l^μ is the $(\hat{i}, \hat{i})$ entry of A_μ. That is,

$$A_\mu = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & 0 & & \\ & & 1 & & & & \\ \beta_2^{\{\mu\}} & \cdots & \beta_{\hat{i}-1}^{\{\mu\}} & p_l^\mu & \beta_{\hat{i}+1}^{\{\mu\}} & \cdots & \beta_{1+\nu+r}^{\{\mu\}} \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

Additionally, w is the vector whose only non-zero entry is the $\hat{i}^{\text{th}}$ element, $\beta_1^{\{\mu\}}$,

$$w = (0, \dots 0, \beta_1^{\{\mu\}}, 0, \dots, 0)^T \in \mathbb{Z}^{\nu+r}.$$

Of course, we must compute the β_i to p_l-adic precision at least μ in order to avoid errors here. Let $\gamma = (n_1, \dots, n_\nu, a_1, \dots, a_r) \in \mathbb{R}^{\nu+r}$ be a solution to our S-unit equation.

Lemma 14.9. *Suppose* $\operatorname{ord}_{p_l}(\delta_1) = 0$ *and*

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

Then the following equivalence holds:

$$\begin{aligned} \sum_{i=1}^{v} n_i a_{li} \geq \mu - \operatorname{ord}_{p_l}(\delta_2) + \operatorname{ord}_{p_l}(\alpha_{\hat{i}}) \quad & \textit{if and only if} \quad \operatorname{ord}_{p_l}(\Lambda_l') \geq \mu \\ & \textit{if and only if} \quad \gamma \in \Gamma_v. \end{aligned}$$

Remark 14.10. Note that the conditions $\mathrm{ord}_{p_l}(\delta_1) = 0$ and

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

are equivalent to

$$\sum_{i=1}^{v} n_i a_{li} > \max\left\{\frac{1}{p_l - 1}, \mathrm{ord}_{p_l}(\delta_1)\right\} - \mathrm{ord}_{p_l}(\delta_2).$$

Proof. By Lemma 14.8, the assumption means that

$$\mathrm{ord}_{p_l}(\Lambda_l') = \sum_{i=1}^{v} n_i a_{li} + \mathrm{ord}_{p_l}(\delta_2) - \mathrm{ord}_{p_l}(\alpha_{\hat{i}}).$$

Now, suppose

$$\sum_{i=1}^{v} n_i a_{li} \geq \mu - \mathrm{ord}_{p_l}(\delta_2) + \mathrm{ord}_{p_l}(\alpha_{\hat{i}}).$$

We thus have

$$\begin{aligned}
\mathrm{ord}_{p_l}(\Lambda_l') &= \sum_{i=1}^{v} n_i a_{li} + \mathrm{ord}_{p_l}(\delta_2) - \mathrm{ord}_{p_l}(\alpha_{\hat{i}}) \\
&\geq \mu - \mathrm{ord}_{p_l}(\delta_2) + \mathrm{ord}_{p_l}(\alpha_{\hat{i}}) + \mathrm{ord}_{p_l}(\delta_2) - \mathrm{ord}_{p_l}(\alpha_{\hat{i}}) \\
&= \mu.
\end{aligned}$$

Conversely, suppose $\mathrm{ord}_{p_l}(\Lambda_l') \geq \mu$. Then

$$\mu \leq \mathrm{ord}_{p_l}(\Lambda_l') = \sum_{i=1}^{v} n_i a_{li} + \mathrm{ord}_{p_l}(\delta_2) - \mathrm{ord}_{p_l}(\alpha_{\hat{i}}).$$

That is,

$$\sum_{i=1}^{v} n_i a_{li} \geq \mu - \mathrm{ord}_{p_l}(\delta_2) + \mathrm{ord}_{p_l}(\alpha_{\hat{i}}).$$

Hence, it follows that $\sum_{i=1}^{v} n_i a_{li} \geq \mu - \mathrm{ord}_{p_l}(\delta_2) + \mathrm{ord}_{p_l}(\alpha_{\hat{i}})$ if and only if $\mathrm{ord}_{p_l}(\Lambda_l') \geq \mu$.

Now, suppose $\gamma = (n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{\nu+r}$ is a solution to our S-unit equation.

Suppose further that $\sum_{i=1}^{v} n_i a_{li} \geq \mu - \mathrm{ord}_{p_l}(\delta_2) + \mathrm{ord}_{p_l}(\alpha_{\hat{i}})$ so that $\mathrm{ord}_{p_l}(\Lambda_l') \geq \mu$. Let

$$\lambda = \frac{1}{p^\mu} \sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})$$

and consider the $(\nu + r)$-dimensional vector

$$x = (n_1, \ldots, n_{\hat{i}-1}, \lambda, n_{\hat{i}+1}, \ldots, n_\nu, a_1, \ldots, a_r)^T.$$

We claim $x \in \mathbb{Z}^{\nu+r}$. That is, $\lambda \in \mathbb{Z}$, meaning that $\sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})$ is divisible by p^μ, or equivalently,

$$\mathrm{ord}_p\left(\sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})\right) \geq \mu.$$

Indeed, since

$$\mathrm{ord}_{p_l}\left(\beta_i^{\{\mu\}} - \beta_i\right) \geq \mu \quad \text{for } i = 1, \ldots, 1 + \nu + r,$$

by definition, it follows that $\beta_i^{\{\mu\}}$ and β_i share the first $\mu - 1$ terms and thus $\mathrm{ord}_p(\beta_i) = \mathrm{ord}_p(\beta_i^{\{\mu\}})$. Now, to compute this order, we only need to concern ourselves with the first non-zero term in the series expansion of $\sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})$. Since $\beta_i^{\{\mu\}}$ and β_i share the first $\mu - 1$ terms, it follows that showing

$$\mathrm{ord}_p\left(\sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}})\right) \geq \mu$$

is equivalent to showing that

$$\mathrm{ord}_p\left(\sum_{i=1}^{\nu+r+1} b_i(-\beta_i)\right) \geq \mu \implies \mathrm{ord}_{p_l}(\Lambda_l') \geq \mu.$$

This latter inequality is true by assumption. Thus $\lambda \in \mathbb{Z}$.

Then, computing $A_\mu x + w$ yields

$$A_\mu x + w = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & 0 & & \\ & & 1 & & & & \\ \beta_2^{\{\mu\}} & \cdots & \beta_{\hat{i}-1}^{\{\mu\}} & p_l^\mu & \beta_{\hat{i}+1}^{\{\mu\}} & \cdots & \beta_{1+\nu+r}^{\{\mu\}} \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \begin{pmatrix} n_1 \\ \vdots \\ n_{\hat{i}-1} \\ \lambda \\ n_{\hat{i}+1} \\ \vdots \\ n_\nu \\ a_1 \\ \vdots \\ a_r \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \beta_1^{\{\mu\}} \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & 0 & & \\ & & 1 & & & & \\ \beta_2^{\{\mu\}} & \cdots & \beta_{\hat{i}-1}^{\{\mu\}} & p_l^\mu & \beta_{\hat{i}+1}^{\{\mu\}} & \cdots & \beta_{1+\nu+r}^{\{\mu\}} \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \begin{pmatrix} b_2 \\ \vdots \\ b_{\hat{i}-1} \\ \lambda \\ b_{\hat{i}+1} \\ \vdots \\ b_{\nu+r+1} \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \beta_1^{\{\mu\}} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} b_2 \\ \vdots \\ b_{\hat{i}-1} \\ b_2\beta_2^{\{\mu\}} + \cdots + b_{\hat{i}-1}\beta_{\hat{i}-1}^{\{\mu\}} + \lambda p_l^\mu + b_{\hat{i}+1}\beta_{\hat{i}+1}^{\{\mu\}} + \cdots + b_{\nu+r+1}\beta_{1+\nu+r}^{\{\mu\}} + \beta_1^{\{\mu\}} \\ b_{\hat{i}+1} \\ \vdots \\ b_{\nu+r+1} \end{pmatrix}$$

Now,

$$\lambda p_l^\mu = p^\mu \frac{1}{p^\mu} \sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}}) = \sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}}),$$

hence

$$
\begin{aligned}
& b_2\beta_2^{\{\mu\}} + \cdots + b_{\hat{i}-1}\beta_{\hat{i}-1}^{\{\mu\}} + b_{\hat{i}+1}\beta_{\hat{i}+1}^{\{\mu\}} + \cdots + b_{\nu+r+1}\beta_{1+\nu+r}^{\{\mu\}} + \lambda p_l^{\mu} + \beta_1^{\{\mu\}} \\
& = b_1\beta_1^{\{\mu\}} + b_2\beta_2^{\{\mu\}} + \cdots + b_{\hat{i}-1}\beta_{\hat{i}-1}^{\{\mu\}} + b_{\hat{i}+1}\beta_{\hat{i}+1}^{\{\mu\}} + \cdots + b_{\nu+r+1}\beta_{1+\nu+r}^{\{\mu\}} + \sum_{i=1}^{\nu+r+1} b_i(-\beta_i^{\{\mu\}}) \\
& = b_{\hat{i}}(-\beta_{\hat{i}}^{\{\mu\}}) \\
& = b_{\hat{i}}
\end{aligned}
$$

where the last equality follows from the fact that

$$-\beta_i = \frac{\alpha_{\hat{i}}}{\alpha_{\hat{i}}} = 1.$$

Thus,

$$A_\mu x + w = \begin{pmatrix} b_2 \\ \vdots \\ b_{\hat{i}-1} \\ b_{\hat{i}} \\ b_{\hat{i}+1} \\ \vdots \\ b_{\nu+r+1} \end{pmatrix} = \begin{pmatrix} n_1 \\ \vdots \\ n_\nu \\ a_1 \\ \vdots \\ a_r \end{pmatrix} = \gamma.$$

Thus, it follows that $\gamma \in \Gamma_v$. CONVERSELY STILL NEED TO SHOW THE CONVERSE, THAT IS

$$m' \in \Gamma_v \quad \text{implies} \quad \sum_{i=1}^{v} n_i a_{li} \geq \mu - \operatorname{ord}_{p_l}(\delta_2) + \operatorname{ord}_{p_l}(\alpha_{\hat{i}}).$$

□

Remark 14.11. In the case $n = 3$, the construction of Λ'_p is simpler since there are only two cases to consider (either g_p splits completely over $\mathbb{Q}_p$, or it has square factor).

We define

$$c_p = \log p\left(\max\left(\tfrac{1}{p-1}, \operatorname{ord}_{p_l}(\delta_1)\right) - \operatorname{ord}_{p_l}(\delta_2)\right).$$

Corollary 14.12. *Assume that $h_{p_l}(z) > \max(0, c_p)$. Then the following equivalence holds:*

$$h_{p_l}(z) \geq \log p_l\left(\mu - \operatorname{ord}_{p_l}(\delta_2) + \operatorname{ord}_{p_l}(\alpha_{\hat{i}})\right) \quad \text{if and only if} \quad \gamma \in \Gamma_v.$$

Proof. Recall from Proposition 13.3 that

$$h_{p_l}(z) = \begin{cases} \log(p_l)|u_l - r_l| \\ 0 \end{cases}.$$

Since $h_{p_l}(z) > 0$, it follows that $h_{p_l}(z) = \log(p_l)|u_l - r_l|$. Hence the assumption becomes

$$\begin{aligned}
&\log(p_l)|u_l - r_l| = h_{p_l}(z) > \log p \left(\max\left(\tfrac{1}{p-1}, \mathrm{ord}_{p_l}(\delta_1)\right) - \mathrm{ord}_{p_l}(\delta_2)\right) \\
&|u_l - r_l| = h_{p_l}(z) > \left(\max\left(\tfrac{1}{p-1}, \mathrm{ord}_{p_l}(\delta_1)\right) - \mathrm{ord}_{p_l}(\delta_2)\right) \\
&\sum_{j=1}^{\nu} n_j a_{lj} > \left(\max\left(\tfrac{1}{p-1}, \mathrm{ord}_{p_l}(\delta_1)\right) - \mathrm{ord}_{p_l}(\delta_2)\right)
\end{aligned}$$

with conclusion

$$\begin{aligned}
h_{p_l}(z) &\geq \log p_l \left(\mu - \mathrm{ord}_{p_l}(\delta_2) + \mathrm{ord}_{p_l}(\alpha_{\hat{i}})\right) \quad \text{if and only if} \quad \gamma \in \Gamma_v \\
\log(p_l)|u_l - r_l| &\geq \log p_l \left(\mu - \mathrm{ord}_{p_l}(\delta_2) + \mathrm{ord}_{p_l}(\alpha_{\hat{i}})\right) \quad \text{if and only if} \quad \gamma \in \Gamma_v \\
|u_l - r_l| &\geq \left(\mu - \mathrm{ord}_{p_l}(\delta_2) + \mathrm{ord}_{p_l}(\alpha_{\hat{i}})\right) \quad \text{if and only if} \quad \gamma \in \Gamma_v \\
\sum_{j=1}^{\nu} n_j a_{lj} &\geq \left(\mu - \mathrm{ord}_{p_l}(\delta_2) + \mathrm{ord}_{p_l}(\alpha_{\hat{i}})\right) \quad \text{if and only if} \quad \gamma \in \Gamma_v,
\end{aligned}$$

which is the previous lemma.

□

Recall that we wish to prove the following lemma:

Lemma 14.13. *Any $(x, y) \in \Sigma_v(l, h)$ is determined by some $\gamma \in \Gamma_v \cap \mathcal{E}_v$.*

Proof of Lemma 14.13. If $(n_1, \ldots, n_\nu, a_1, \ldots, a_r) \in \mathbb{R}^{r+\nu}$ is a solution which lies in $\Sigma_v(l, h)$, then, by definition, it corresponds to a solution (x, y) satisfying

$$\Sigma_v(l, h) = \{(x, y) \in \Sigma \mid (h_w(z)) \leq h \text{ and } (h_w(z)) \nleq 0 \text{ and } h_v(z) > l_v\}.$$

Hence $h_v(z) > l_v$, where l_v is a constant such that

$$\frac{l_v}{\log(p)} \geq \max\left(\frac{1}{p-1}, \mathrm{ord}_{p_v}(\delta_1)\right) - \mathrm{ord}_{p_v}(\delta_2).$$

That is,

$$h_v(z) > l_v \geq \log(p)\left(\max\left(\frac{1}{p-1}, \mathrm{ord}_{p_v}(\delta_1)\right) - \mathrm{ord}_{p_v}(\delta_2)\right) = c_p.$$

Now, recall that $l \geq 0$ so that $l_v \geq 0$. It thus follows that

$$h_v(z) > l_v \geq \begin{cases} 0 \\ c_p \end{cases} \implies h_v(z) > \max(0, c_p).$$

In other words, the condition of the previous corollary is satisfied.

Now, recall that l'_v (sometimes denoted μ) is the largest element of $\mathbb{Z}_{\geq 0}$ at most

$$l'_v \leq \frac{l_v}{\log(p)} - \mathrm{ord}_{p_l}(\alpha_{\hat{i}}) + \mathrm{ord}_{p_l}(\delta_2).$$

That is

$$\frac{l_v}{\log(p)} \geq l'_v + \mathrm{ord}_{p_l}(\alpha_{\hat{i}}) - \mathrm{ord}_{p_l}(\delta_2)$$

so that

$$h_v(z) > l_v \geq \log(p)\left(l'_v + \mathrm{ord}_{p_l}(\alpha_{\hat{i}}) - \mathrm{ord}_{p_l}(\delta_2)\right).$$

Now, by the previous corollary, we must have $\gamma \in \Gamma_v$. This shows that (x, y) is determined by $\gamma = m' \in \Gamma_v$, which proves Lemma 14.13. □

14.2 Non-Archimedean ellipsoid.

Recall that

$$h\left(\frac{\delta_2}{\lambda}\right) = \frac{1}{[K:\mathbb{Q}]}\sum_{l=1}^{\nu} \log(p_l)|u_l - r_l| + \frac{1}{[L:\mathbb{Q}]}\sum_{w:L\to\mathbb{C}} \log\max\left\{\left|w\left(\frac{\delta_2}{\lambda}\right)\right|, 1\right\}.$$

We now restrict our attention to those $p \in \{p_1, \ldots, p_\nu\}$ and study the p-adic valuations of the numbers appearing in (23). Let $l \in \{1, \ldots, \nu\}$, corresponding to $p_l \in \{p_1, \ldots, p_\nu\}$. Take $\mathbf{h} \in \mathbb{R}^{r+\nu}$ such that $\mathbf{h} \geq \mathbf{0}$. Let

$$b = \frac{1}{\log(2)^2}\sum_{k=1}^{\nu} h_k^2$$

where

$$\log(2)^2 q_f(\mathbf{n}) = \log(2)^2 \sum_{k=1}^{\nu} \left\lfloor \frac{\log(p_k)^2}{\log(2)^2} \right\rfloor |u_k - r_k|^2 \leq \sum_{k=1}^{\nu} \log(p_k)^2 |u_k - r_k|^2 \leq \sum_{k=1}^{\nu} h_k^2.$$

For each ε_l in $\{\varepsilon_1, \ldots, \varepsilon_r\}$, we define

$$|a_l|^2 \leq \left(\frac{1}{[K:\mathbb{Q}]} \sum_{k=1}^{\nu} w_{\gamma lk} h_k + \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma: L \to \mathbb{C}} w_{\varepsilon l \sigma} h_\sigma \right)^2 =: b_{\varepsilon_l}.$$

Note that here, we do not distinguish any ε_l^*.

We define the ellipsoid $\mathcal{E}_l \subseteq \mathbb{R}^{\nu+r}$ by

$$\mathcal{E}_l = \{q_l(\mathbf{x}) \leq (1+r)(bb_{\varepsilon_1} \cdots b_{\varepsilon_r});\ \mathbf{x} \in \mathbb{R}^{r+\nu}\}, \quad \text{where} \tag{26}$$

$$q_l(\mathbf{x}) = (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) \left(q_f(x_1, \ldots, x_\nu) + \sum_{i=1}^{r} \frac{b}{b_{\varepsilon_i}} x_{\varepsilon_i}^2 \right) \tag{27}$$

$$q_l(\mathbf{x}) = \left((b_{\varepsilon_1} \cdots b_{\varepsilon_r}) \cdot q_f(x_1, \ldots, x_\nu) + (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) \sum_{i=1}^{r} \frac{b}{b_{\varepsilon_i}} x_{\varepsilon_i}^2 \right) \tag{28}$$

$$q_l(\mathbf{x}) = \left((b_{\varepsilon_1} \cdots b_{\varepsilon_r}) \cdot q_f(x_1, \ldots, x_\nu) + \sum_{i=1}^{r} b(b_{\varepsilon_1} \cdots b_{\varepsilon_{i-1}} b_{\varepsilon_{i+1}} b_{\varepsilon_r}) x_{\varepsilon_i}^2 \right) \tag{29}$$

where

$$q_f(\mathbf{y}) = (A\mathbf{y})^{\mathrm{T}} D^2 A\mathbf{y}.$$

To generate the matrix for this ellipsoid, recall that I is the set of all indices $i' \in \{2, \ldots, 1+\nu+r\}$ for which

$$\mathrm{ord}_{p_l}(\alpha_{i'}) = \min_{2 \leq i \leq 1+\nu+r} \mathrm{ord}_{p_l}(\alpha_i).$$

We note that we are always in the so-called *special case*, where there is some index $i' \in I$ such that $\alpha_i/\alpha_{i'} \in \mathbb{Q}_{p_l}$ for $i = 1, \ldots, 1+\nu+r$.

Now we state several relatively-easy-to-check conditions that each imply that we are always in the special case for degree 3 Thue-Mahler equations. Moreover, each condition implies that we have $\frac{\alpha_{i_1}}{\alpha_{i_2}} \in \mathbb{Q}_p$ for every $i_1, i_2 \in \{1, \ldots, 1+\nu+r\}$.

(a) $\alpha_1, \ldots, \alpha_{1+\nu+r} \in \mathbb{Q}_p$

(b) $g(t)$ has three or more linear factors in $\mathbb{Q}_p[t]$ and $\theta^{(i_0)}, \theta^{(j)}, \theta^{(k)}$ are roots of such polynomials.

(c) $g(t)$ has an irreducible factor in $\mathbb{Q}_p[t]$ of degree two, and $\theta^{(j)}, \theta^{(k)}$ are roots of this

(d) $g(t)$ has a non-linear irreducible factor in $\mathbb{Q}_p[t]$ that splits completely in the extension of $\mathbb{Q}_p$ that it generates and $\theta^{(j)}, \theta^{(k)}$ are roots of this factor

Proof. It is obvious that (a) implies $\alpha_{i_1}/\alpha_{i_2} \in \mathbb{Q}_p$ for every $i_1, i_2 \in \{1, \ldots, 1+\nu+r\}$. If (b) holds, then $\delta_1, \gamma_i^{(k)}/\gamma_i^{(j)} (i = 1, \ldots, \nu), \varepsilon_i^{(k)}/\varepsilon_i^{(j)} (i = 1, \ldots, r)$ all belong to $\mathbb{Q}_p$, which, since $\mathbb{Q}_p$ is complete, implies (a). Now, (c) implies (d). We claim that (d) implies $\alpha_{i_1}/\alpha_{i_2} \in \mathbb{Q}_p$ for every $i_1, i_2 \in \{1, \ldots, 1+\nu+r\}$. To see this, assume (d), let L be the extension of $\mathbb{Q}_p$ generated by the factor of $g(t)$ in question, and consider any $\alpha, \beta \in L$. The automorphisms on L that maps $\theta^{(j)}$ to $\theta^{(k)}$ multiplies the logarithms $\log_{p_l}\left(\alpha^{(k)}/\alpha^{(j)}\right)$ and $\log_{p_l}\left(\beta^{(k)}/\beta^{(j)}\right)$ by -1 and hence fixes the quotient

$$\frac{\log_{p_l}\left(\alpha^{(k)}/\alpha^{(j)}\right)}{\log_{p_l}\left(\beta^{(k)}/\beta^{(j)}\right)}. \tag{30}$$

Therefore, since L is Galois, this quotient belongs to $\mathbb{Q}_p$. Since $\alpha_{i_1}/\alpha_{i_2}$ is of the form (30) for every $i_1, i_2 \in \{1, \ldots, 1+\nu+r\}$, the claim is proved. □

Now, recall that if our Thue-Mahler is only of degree 3, it follows that $g(t)$ can only split in 3 ways in $\mathbb{Q}_p$.

(a) $g(t) = g_1(t)$, where $\deg(g_1(t)) = 3$

(b) $g(t) = g_1(t)g_2(t)$ where $\deg(g_1(t)) = 1$ and $\deg(g_2(t)) = 2$ (without loss of generality)

(c) $g(t) = g_1(t)g_2(t)g_3(t)$ where $\deg(g_i(t)) = 3$ for $i = 1, 2, 3$.

In the event that that $g(t)$ is irreducible (a), the corresponding prime ideal $\mathfrak{p}$ in K has $ef = 3$, and is therefore bounded. That is, it does not appear in the set of unbounded ideals $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_\nu\}$, and we can ignore this case. The other 2 cases appear in the list above, therefore guaranteeing that $\alpha_{i_1}/\alpha_{i_2} \in \mathbb{Q}_p$ for every $i_1, i_2 \in \{1, \ldots, 1+\nu+r\}$.

Finally, suppose that $\gamma \in \Gamma_v \cap \mathcal{E}_v$. Let $M = M_v$ be the matrix defining the ellipsoid

$$\mathcal{E}_\tau : z^t M^t M z \leq (1+r)(bb_{\varepsilon_1} \cdots b_{\varepsilon_r}),$$

that is,

$$M = \sqrt{b_{\varepsilon_1} \cdots b_{\varepsilon_r}} \begin{pmatrix} DA & 0 & \dots & 0 & 0 \\ 0 & \sqrt{\frac{b}{b_{\varepsilon 1}}} & \dots & 0 & 0 \\ 0 & 0 & \sqrt{\frac{b}{b_{\varepsilon 2}}} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \sqrt{\frac{b}{b_{\varepsilon}}} \end{pmatrix}.$$

Note that we never need to compute M, but rather $M^T M$ so that we do not need to worry about precision. In this case,

$$M^T M = b_{\varepsilon_1} \cdots b_{\varepsilon_r} \begin{pmatrix} A^T D^2 A & 0 & \dots & 0 & 0 \\ 0 & \frac{b}{b_{\varepsilon 1}} & \dots & 0 & 0 \\ 0 & 0 & \frac{b}{b_{\varepsilon 2}} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \frac{b}{b_{\varepsilon}} \end{pmatrix}$$

$$= \begin{pmatrix} (b_{\varepsilon_1} \cdots b_{\varepsilon_r}) A^T D^2 A & 0 & \dots & 0 & 0 \\ 0 & b b_{\varepsilon_2} \cdots b_{\varepsilon_r} & \dots & 0 & 0 \\ 0 & 0 & b b_{\varepsilon_1} b_{\varepsilon_3} \cdots b_{\varepsilon_r} & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & b b_{\varepsilon_1} \cdots b_{\varepsilon_{r-1}} \end{pmatrix}.$$

Recall that

$$A_\mu = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & 0 & & \\ & & 1 & & & & \\ \beta_2^{\{\mu\}} & \dots & \beta_{\hat{i}-1}^{\{\mu\}} & p_l^\mu & \beta_{\hat{i}+1}^{\{\mu\}} & \dots & \beta_{1+\nu+r}^{\{\mu\}} \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

$A_\mu x + w$ define the lattice Γ_v where $\gamma \in \Gamma_v \cap \mathcal{E}_v$. In particular, since $\gamma \in \Gamma_v \cap \mathcal{E}_v$, there exists $x \in \mathbb{R}^{r+\nu}$ such that $\gamma = \Gamma_v x + w$ and $\gamma^t M^t M \gamma \leq (1+r)(b b_{\varepsilon_1} \cdots b_{\varepsilon_r})$. We thus have

$$(\Gamma_v x + w)^t M^t M (\Gamma_\tau x + w) \leq (1+r)(b b_{\varepsilon_1} \cdots b_{\varepsilon_r}).$$

As A_τ is clearly invertible, with matrix inverse

$$A_\tau^{-1} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & 0 & & \\ & & 1 & & & & \\ -\frac{\beta_2^{\{\mu\}}}{p_l^\mu} & \cdots & -\frac{\beta_{\hat{i}-1}^{\{\mu\}}}{p_l^\mu} & \frac{1}{p_l^\mu} & -\frac{\beta_{\hat{i}+1}^{\{\mu\}}}{p_l^\mu} & \cdots & -\frac{\beta_{1+\nu+r}^{\{\mu\}}}{p_l^\mu} \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix},$$

we can find a vector c such that $A_\tau c = -w$. Indeed, this vector is $c = A_\tau^{-1}(-w)$, where

$$c = A_\tau^{-1} w = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & 0 & & \\ & & 1 & & & & \\ -\frac{\beta_2^{\{\mu\}}}{p_l^\mu} & \cdots & -\frac{\beta_{\hat{i}-1}^{\{\mu\}}}{p_l^\mu} & \frac{1}{p_l^\mu} & -\frac{\beta_{\hat{i}+1}^{\{\mu\}}}{p_l^\mu} & \cdots & -\frac{\beta_{1+\nu+r}^{\{\mu\}}}{p_l^\mu} \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -\beta_1^{\{\mu\}} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -\frac{\beta_1^{\{\mu\}}}{p^{\{\mu\}}} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Now,

$$\begin{aligned} (1+r)(bb_{\varepsilon_1}\cdots b_{\varepsilon_r}) &\geq (\Gamma_\tau x + w)^t M^t M(\Gamma_\tau x + w) \\ &= (\Gamma_\tau x - (-w))^t M^t M(\Gamma_\tau x - (-w)) \\ &= (\Gamma_\tau x - \Gamma_\tau c)^t M^t M(\Gamma_\tau x - \Gamma_\tau c) \\ &= (\Gamma_\tau (x-c))^t M^t M(\Gamma_\tau (x-c)) \\ &= (x-c)^t (M\Gamma_\tau)^t M\Gamma_\tau (x-c) \\ &= (x-c)^t B^t B(x-c) \end{aligned}$$

where $B = M\Gamma_\tau$. That is, we are left to solve

$$(x-c)B^t B(x-c) \leq (1+r)(bb_{\varepsilon_1}\cdots b_{\varepsilon_r}).$$

Recall that $\gamma \in \Gamma_v$ means

$$A_\mu x + w = \begin{pmatrix} b_2 \\ \vdots \\ b_{\hat{i}-1} \\ b_{\hat{i}+1} \\ \vdots \\ b_{\nu+r+1} \\ b_{\hat{i}} \end{pmatrix} = \gamma.$$

START TESTING LOWER/UPPER BOUNDS; NO SOLUTIONS OR ALL, THEN REPEAT REDUCTION UNTIL EXPONENT SIZE SAY 10 REFINED SIEVE - IS USEFUL OR NOT? CHECK BENJAMIN+RAFAEL'S SUNIT SOLVER TO SEE WHERE IT SWITCHES

HAVE CODE CONVERT FROM Hs TO EXPONENTS SO THAT WE CAN COMPARE THE REDUCTION ON THE EXPONENTS