AN ABSTRACT OF THE DISSERTATION OF

Emerald Tatiana Stacy for the degree of Doctor of Philosophy in Mathematics presented on June 13, 2018.

Title: On Small Heights of Totally p-adic Numbers.

Abstract approved: _____

Clayton J. Petsche

The height of an algebraic number α is a measure of how arithmetically complicated α is. We say α is totally p-adic if the minimal polynomial of α splits completely over the field $\mathbb{Q}_p$ of p-adic numbers. In this paper, we investigate what can be said about the smallest nonzero height of a degree d totally p-adic number. In particular, we look at the cases that α is either contained within an abelian extension of $\mathbb{Q}$, or has degree 2 or degree 3 over $\mathbb{Q}$. Additionally, we determine an upper bound on the smallest limit point of the height of totally p-adic numbers for each fixed prime p.

On Small Heights of Totally p-adic Numbers

by
Emerald Tatiana Stacy

A DISSERTATION

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

Presented June 13, 2018
Commencement June 2018

Doctor of Philosophy dissertation of Emerald Tatiana Stacy presented on June 13, 2018

APPROVED:

Major Professor, representing Mathematics

Chair of the Department of Mathematics

Dean of the Graduate School

I understand that my dissertation will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my dissertation to any reader upon request.

Emerald Tatiana Stacy, Author

ACKNOWLEDGEMENTS

It is with deepest gratitude that I thank my advisor, Clayton Petsche. I have wanted to be a number theorist since I was eleven years old. Thank you for helping me realize that dream.

For their support, advice, and encouragement while I found my voice as a teacher, I thank Tevian Dray and Jessica Beck. Good mentors are invaluable, and I am incredibly grateful to have both of you on my team.

I have been surrounded by a wonderful group of women who have supported me. Claire Gibbons, thank you for reminding me that I always have a choice, and that everything "counts" as work. Kathryn Williams, less than four. Always. Melissa Saiz-Matheny, you always know where to find a dustpan, and Applebees. I know you think I would have done this with or without out you, and maybe you are right, but I am so glad I didn't have to.

Jesse, thank you for making me my morning smoothie, even when it means you have to wash the blender. Mom, thank you for teaching me to quilt and to look at a problem through a different lens when I get stuck. Jacob, thank you for all of the video-game filled weekends, and reminding me that there is more to life than graduate school. Dad, I wish you could be here for this.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF TABLES

To my pumpkin.

On Small Heights of Totally p-adic Numbers

1 Introduction

1.1 A Historical Overview

The height (or more formally, the logarithmic Weil height) of a rational number $\frac{a}{b}$ is

$$h\left(\tfrac{a}{b}\right) = \log \max\{|a|, |b|\},$$

provided $\gcd(a, b) = 1$. This quantity gives a measure of how arithmetically complicated a rational number is. Rational numbers can be close together on the real line, and yet have radically different height. For example, $h\left(\frac{1}{3}\right) = \log 3 \approx 1.0986$ and $h\left(\frac{10001}{30000}\right) = \log 30000 \approx 10.30895$.

There are two ways to extend the height function from rational numbers to the field $\overline{\mathbb{Q}}$ of all algebraic numbers. The first uses the theory of places of number fields, and is developed in Section 2.2. The second method is better suited to doing explicit calculations, and will prove useful in Chapters 3 and 4. Each algebraic number α has a unique irreducible polynomial $f_\alpha \in \mathbb{Z}[x]$ of degree d with roots $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$, leading coefficient $a > 0$, and $f_\alpha(\alpha) = 0$. Then we define the height of α by

$$h(\alpha) = \tfrac{1}{d}\left(\log a + \sum_{j=1}^{d} \log^+ |\alpha_j|\right),$$

where $\log^+ x = \max\{0, \log x\}$, and e is the base of the logarithm.

The height function has many interesting properties. From the definition above, we see that if α_i and α_j are both roots of f_α, then $h(\alpha_i) = h(\alpha_j)$. Additionally,

(a) for all $n \in \mathbb{Z}$, $h(\alpha^n) = |n| h(\alpha)$,

(b) $h(\alpha) = h(\alpha^{-1})$,

(c) $h(\alpha) \geq 0$, with equality if and only if α is zero or a root of unity, and

(d) for any $A > 0$ and $B > 0$, there are finitely many algebraic numbers α with $\deg(f_\alpha) \leq A$ and $h(\alpha) \leq B$; we call this the Northcott property.

The Northcott property allows for the arrangment of all algebraic numbers of a fixed degree $d \geq 1$ in order of nondecreasing height. In 1874, Cantor used this fact to prove that $\overline{\mathbb{Q}}$ is countable [Can74]. Since the real numbers are uncountable, this implies the existence of transcendental numbers.

Following Cantor, heights were used to prove many important results in number theory in the twentieth century. In 1928, Weil used heights in his doctoral dissertation to prove the Mordell-Weil Theorem, which states that the group of rational points on an elliptic curve over a number field is finitely generated [WP28]. In 1950, Northcott proved that for a rational function $\phi(x) \in K(x)$ over a number field K, the set of all points in $\mathbb{P}^1(K)$ that are preperiodic with respect to iteration of the function ϕ is finite [Nor50]. In 1922, Mordell conjectured that a curve of genus at least 2 over a number field K contains only finitely many K-rational points. Faltings used heights to prove this to be true in 1983 [Fal83].

In addition to the height function being a useful tool, there has been considerable interest in the study of the height function itself. Lehmer discovered a method to construct large prime numbers using algebraic numbers with height positive but as small as possible in terms of the degree. Thus he was led to the following question in 1933. Observe that

$$h(\sqrt[d]{2}) = \tfrac{1}{d} \log 2,$$

so since

$$\lim_{d\to\infty} h(\sqrt[d]{2}) = \lim_{d\to\infty} \tfrac{1}{d} \log 2 = 0,$$

there are algebraic numbers of arbitrarily small, nonzero height. Lehmer searched for numbers of small, nonzero height, which he used to calculate large primes. The

question he posed is equivalent to the following: Does there exist an $\epsilon > 0$ such that

$$h(\alpha) \geq \tfrac{\epsilon}{d}$$

for all nonzero, non-root of unity, algebraic numbers α of degree d? Lehmer's polynomial,

$$f(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1,$$

has two real roots, one of which falls outside the unit circle, and eight roots on the unit circle. Let $\lambda > 1$ be the largest real root of $f(x)$. Note that

$$h(\lambda) = \tfrac{1}{10} \log \lambda \approx 0.01623576.$$

Thus, if such an ϵ exists, it must be the case that $\epsilon \leq \log \lambda$. Although Lehmer found this polynomial and value by hand, no smaller value of $d\,h(\alpha)$ has been found since, either by hand or via computer. It is now understood that Lehmer's question fits into the larger study of the behavior of small points in height theory.

One avenue of research seeks to give lower bounds on $h(\alpha)$ that depend on the degree of α. So far, none of these results has quite resolved Lehmer's question. The second avenue seeks to provide lower bounds with additional hypotheses on α, and these results often have the strength $h(\alpha) \geq \frac{\epsilon}{d}$ or even $h(\alpha) \geq \epsilon$. For all of these results, we assume that α is a nonzero, non-root of unity algebraic number of degree d.

In 1971, Blanksby and Montgomery [BM71] used Fourier series in several variables to prove that

$$h(\alpha) > \tfrac{1}{d} \log(1 + (52d \log(6d))^{-1}).$$

Seven years later, Stewart [Ste78] used Diophantine approximation to prove that there is some value C so that

$$h(\alpha) > \tfrac{1}{d} \log\left(1 + \frac{C}{d \log(d)}\right).$$

Although Stewart's bound was not an improvement on the work of Blanksby and Montgomery, his method was used one year later by Dobrowolski [Dob79] to obtain

what is still the best known lower bound on $h(\alpha)$ in terms of d:

$$h(\alpha) > \tfrac{1}{d} \log\left(1 + \frac{1}{1200}\left(\frac{\log\log d}{\log d}\right)^3\right).$$

Although Dobrowolski's bound is an improvement on previous results, it still does not answer Lehmer's question.

With additional hypotheses on α, there is a series of interesting results in the literature. We say α is **totally real** (or **totally p-adic**) if the minimal poynomial f_α of α over $\mathbb{Q}$ splits completely over $\mathbb{R}$ (or $\mathbb{Q}_p$). In 1973, Schinzel used the arithmetic-geometric mean inequality to prove that if α is totally real, then

$$h(\alpha) \geq \tfrac{1}{2} \log\left(\tfrac{1+\sqrt{5}}{2}\right)$$

with equality if $\alpha = \frac{1+\sqrt{5}}{2}$ [Sch73]. In 1993, Höhn and Skoruppa used an auxiliary function to provide an alternate proof of Schinzel's bound [HS93].

The existence of Schinzel's bound can also be shown via a theorem of Bilu, which states that given a sequence of distinct algebraic numbers $\{\alpha_k\}$ such that $h(\alpha_k) \to 0$, the algebraic conjugates of α_k are equidistributed with respect to the unique rotation invariant measure supported on the unit circle of $\mathbb{C}$ [Bil97]. If such a sequence were totally real, then equidistribution would be impossible. In principle, an explicit constant could be obtained by applying a quantitative version of Bilu's Theorem due to Petsche [Pet05], but the resulting inequality would be inferior to the sharp inequality of Schinzel.

An algebraic number α is said to be reciprocal if it is conjugate to (has the same minimal polynomial as) α^{-1}. In 1951, Breusch [Bre51] used resultants to prove that if α is not reciprocal, then

$$h(\alpha) \geq \tfrac{0.16517}{d}.$$

Breusch's result went unnoticed for several decades by many number theorists working on Lehmer's problem and related questions, until it was rediscovered by Narkiewicz. In the meantime, Smyth [Smy71] proved in 1971 that if α is not reciprocal, and α_0 is

a root of $x^3 - x - 1$, then

$$h(\alpha) \geq \frac{3}{d} h(\alpha_0) \approx \frac{0.28118}{d}.$$

Smyth's result is sharp, since it is achieved by α_0. He used methods from complex analysis and Fourier analysis.

It is a result of Amoroso and David [AD99] that if $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$, then there exists an $\epsilon > 0$ so that

$$h(\alpha) \geq \frac{\epsilon}{d}.$$

Additionally, for each positive integer m there exists a constant ϵ_m that depends on m, such that if the degree of a Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is bounded above by d^m, then

$$h(\alpha) \geq \frac{\epsilon_m}{d}.$$

In 2000, Amoroso and Dvornicich [AD00] proved that if α is contained within an abelian extension of $\mathbb{Q}$, then

$$h(\alpha) \geq \frac{\log 5}{12}.$$

It is not yet known if this inequality is sharp. Currently, the lowest known height of an algebraic number contained within an abelian extension of $\mathbb{Q}$ is $\frac{\log 7}{12}$.

Garza has shown lower bounds on $h(\alpha)$ for three separate conditions on α. If α has r real conjugates [Gar07], then

$$h(\alpha) \geq \frac{r}{2d} \log\left(\frac{2^{1-d/r} + \sqrt{4^{1-d/r} + 4}}{2}\right).$$

If α is contained within a dihedral extension of $\mathbb{Q}$ [Gar08], then

$$h(\alpha) \geq \frac{1}{2} \log \frac{1+\sqrt{5}}{2}.$$

If $p > d$ is a prime that ramifies completely in $\mathbb{Q}(\alpha)$ [Gar09], then

$$h(\alpha) \geq \frac{1}{d} \log(\sqrt{5} - 1).$$

In 2010, Garza, Ishak, Mossinghoff, Pinner, and Wiles [GIM+10] proved that if the minimal polynomial of α has all odd coefficients, then

$$h(\alpha) \geq \frac{0.4278}{d+1}.$$

Bombieri and Zannier [BZ01] proved that an analogue to Schinzel's Theorem holds in $\mathbb{Q}_p$ for each prime p, although the analogous best possible lower bound is unknown. Suppose that S is a nonempty subset of places of $\mathbb{Q}$, and let L_S be a subfield of $\overline{\mathbb{Q}}$ such that for all $\alpha \in L_S$, and all $p \in S$, α is totally p-adic (or totally real if $p = \infty$). If $\infty \notin S$, Bombieri and Zannier showed that

$$\liminf_{\alpha \in L_S} h(\alpha) \geq \frac{1}{2} \sum_{p \in S} \frac{\log p}{p+1}.$$

Using potential theory, Petsche and Fili [FP13] improved on this bound in two ways: first by allowing for the possibilty that S contains the archimedean place ∞, and second, by improving the constants at the non-archimedean places to:

$$\liminf_{\alpha \in L_S} h(\alpha) \geq \begin{cases} \frac{1}{2} \sum_{p \in S} \frac{p \log p}{2(p^2-1)} & \text{if } \infty \notin S \\ \frac{1}{2} \sum_{p \in S, p \neq \infty} \frac{p \log p}{2(p^2-1)} + \frac{7\zeta(3)}{4\pi^2} & \text{if } \infty \in S. \end{cases}$$

In the opposite direction of providing lower bounds on the heights of totally p-adic and totally real numbers, one might try to construct algebraic numbers with height as small as possible. There have been some results in this direction. For example, Petsche [Peta] proved that for odd primes p, there exists some totally p-adic $\alpha \in \overline{\mathbb{Q}}$ of degree $d \leq p-1$, and

$$0 < h(\alpha) \leq \frac{1}{p-1} \log\left(\frac{p+\sqrt{p^2+4}}{2}\right).$$

Recently, Pottmeyer [Pot18] has improved upon Petsche's upper bound, and obtained the existence of totally p-adic α such that

$$0 < h(\alpha) \leq \frac{\log p}{p}.$$

In 1980, Smyth created a set of totally real numbers of small height by taking all preimages of 1 under the map $\phi(x) = x + \frac{1}{x}$. The heights of the points in this set

have a limit point $\ell \approx 0.27328$ [Smy80]. We use an argument inspired by this result of Smyth to provide an upper bound on the smallest limit point of heights of totally p-adic numbers of degree d. This result is stated as Theorem 1.5 in the following section, and proved in Chapter 5.

1.2 Summary of New Results

Recall that an algebraic number α is **totally p-adic** if the minimal poynomial f_α of α over $\mathbb{Q}$ splits completely over $\mathbb{Q}_p$. Previous results have investigated what can be said about small heights of totally p-adic numbers for a fixed prime, and allowing d to vary. In this paper, we fix the degree d, and let the prime p vary. In particular, we define $\tau_{d,p}$ to be the smallest height attained by a totally p-adic, nonzero, non-root of unity, algebraic number of degree d. We know such a smallest height number exists by Northcott's Theorem. For each pair d and p, we will create an irreducible polynomial of degree d that splits completely over $\mathbb{Q}_p$, thus guaranteeing the finiteness of $\tau_{d,p}$. For brevity, we introduce the notation

$$\mathcal{T}_p = \{\alpha \in \overline{\mathbb{Q}} \mid h(\alpha) > 0 \text{ and } \alpha \text{ totally } p\text{-adic}\}$$

for the set of all nonzero, non-root of unity, totally p-adic algebraic numbers.

We begin in Chapter 3 by looking at degree 2 numbers. Since a quadratic polynomial splits completely over $\mathbb{Q}_p$ if and only if its discriminant is a square modulo p, we search for degree 2 numbers of small height. The two smallest nontrivial heights attained by quadratic numbers are $\frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right)$ and $\frac{1}{2}\log 2$. The first is only attained by the roots of $x^2 \pm x - 1$.

TABLE 1.1: Discriminants of Quadratic Numbers of Small Height

$h(\alpha_i)$	f_{α_i}	Discriminant of f_{α_i}
$\frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right)$	$x^2 \pm x - 1$	5
$\frac{1}{2}\log 2$	$x^2 + 2$	-2
$\frac{1}{2}\log 2$	$x^2 - 2$	2
$\frac{1}{2}\log 2$	$x^2 + 2x + 2$	-1

The Legendre symbol, $\left(\frac{a}{p}\right)$, detects when a is a square modulo p. It returns 0 if $p \mid a$, 1 if a is a square modulo p, and -1 is a is not a square modulo p. By properties of the Legendre symbol,

$$\left(\tfrac{-1}{p}\right)\left(\tfrac{2}{p}\right) = \left(\tfrac{-2}{p}\right).$$

For odd p, $\left(\frac{-2}{p}\right) \neq 0$, and therefore at least one of the symbols has a value of 1. The associated polynomial splits over $\mathbb{Q}_p$, and since $x^2 \pm x - 1$ splits if and only if $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$, we obtain the following theorem:

Theorem 1.1. For any prime p,

$$\tau_{2,p} = \begin{cases} \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right) & \text{if } p \equiv 1, 4 \pmod 5 \\ \frac{1}{2}\log 2 & \text{if } p \equiv 0, 2, 3 \pmod 5. \end{cases}$$

One of the goals of this thesis is an attempt to generalize Theorem 1.1 for larger degrees. Although quadratic reciprocity provides a nice way to prove Theorem 1.1, in Chapter 3 we shall see that the deeper reason that $\tau_{2,p}$ depends only on $p \pmod 5$ is that all quadratic extensions of $\mathbb{Q}$ are abelian.

The subfield of all algebraic numbers contained in an abelian extension of $\mathbb{Q}$ is denoted $\mathbb{Q}^{\mathrm{ab}}$. Let $\mathcal{T}_p^{\mathrm{ab}} = \mathcal{T}_p \cap \mathbb{Q}^{\mathrm{ab}}$. We define $\tau_{d,p}^{\mathrm{ab}}$ to be the smallest height of $\alpha \in \mathcal{T}_p^{\mathrm{ab}}$ of degree d. Note that for all primes p, $\tau_{2,p} = \tau_{2,p}^{\mathrm{ab}}$. To generalize Theorem 1.1 from quadratic numbers to arbitrary degree, we look at what can be said about $\tau_{d,p}^{\mathrm{ab}}$ for $d \geq 3$.

The Kronecker-Weber Theorem states that all abelian extensions of $\mathbb{Q}$ are contained within a cyclotomic extension of $\mathbb{Q}$, so we leverage the Galois theory of cyclotomic extensions. For $\alpha \in \mathbb{Q}^{\text{ab}}$, the conductor of the number field $K = \mathbb{Q}(\alpha)$ is the smallest positive integer m such that K is contained in $\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m^{th} root of unity. Then $(\mathbb{Z}/m\mathbb{Z})^\times$ is isomorphic to the Galois group of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ by the map $[i] \to \sigma_i$, where σ_i is the element of the Galois group which sends $\zeta_m \to \zeta_m^i$. For $\alpha \in \overline{\mathbb{Q}}$, we define A_α to be the set of all $j \in \mathbb{Z}$ such that $\sigma_j(\alpha) = \alpha$.

Theorem 1.2. Let $d \geq 2$ and let $\alpha_1, \alpha_2, \alpha_3, \ldots$ be an enumeration of all elements of $\mathcal{T}_p^{\text{ab}}$ of degree d, written in order of nondecreasing height, so that

$$h(\alpha_1) \leq h(\alpha_2) \leq h(\alpha_3) \leq \ldots.$$

Let m_i denote the conductor of $\mathbb{Q}(\alpha_i)$.

(a) There exists an integer $k \geq 1$ such that $\bigcup_{i=1}^{k} A_{\alpha_i}$ contains all primes p not dividing any of the conductors $m_1, \ldots, m_k$.

(b) Let $k \geq 1$ be the smallest positive integer satisfying **(a)**, and let

$$N_d = \text{lcm}(m_1, \ldots, m_k).$$

Then $\tau_{d,p}^{\text{ab}}$ depends only on $p \pmod{N_d}$.

Theorem 1.2 provides an alternate proof of the finiteness of $\tau_{d,p}^{\text{ab}}$. By finding a k that satisfies the criterion described in Theorem 1.2, we can calculate N_d. For example, we calculate N_3 to be 228979643050431.

Next, we take a closer look at $\tau_{3,p}$. Since not all roots of cubic polynomials are contained within an abelian extension of $\mathbb{Q}$, we can no longer rely on quadratic reciprocity, and must turn to other techniques. In particular, we use the method of Cardano to detect when a polynomial splits over $\mathbb{Q}_p$. The first step is to depress the cubic, so without loss of generality we consider only polynomials of the form $x^3 + Ax + B \in \mathbb{Q}[x]$. The conditions that determine if a polynomial splits completely

over $\mathbb{Q}_p$ depend whether or not $\mathbb{Q}_p$ contains a primitive cube root of unity, which happens exactly when $p \equiv 1 \pmod 3$.

Theorem 1.3. Let p be a prime, with $p \equiv 1 \pmod 3$, $f(x) = x^3 + Ax + B \in \mathbb{Q}[x]$, and $\Delta = B^2 + 4A^3/27$. If $A = 0$, let $C = -B$, and if $A \neq 0$, let C be either square root of Δ in $\overline{\mathbb{Q}_p}$. Then f splits completely over $\mathbb{Q}_p$ if and only if

(a) Δ is a square in $\mathbb{Q}_p$, and

(b) $\frac{-B+C}{2}$ is a cube in $\mathbb{Q}_p$.

Theorem 1.4. Let p be a prime, with $p \equiv 2 \pmod 3$, $f(x) = x^3 + Ax + B \in \mathbb{Q}[x]$ with $B \neq 0$, $\Delta = B^2 + 4A^3/27$, and ζ a primitive cube root of unity. If $A = 0$, let $C = -B$, and if $A \neq 0$, let C be either square root of Δ in $\overline{\mathbb{Q}_p}$. Then f splits completely over $\mathbb{Q}_p$ if and only if

(a) Δ is a square in $\mathbb{Q}_p(\zeta)$ and not a square in $\mathbb{Q}_p$, and

(b) $\frac{-B+C}{2}$ is a cube in $\mathbb{Q}_p(\zeta)$ and not a cube in $\mathbb{Q}_p$.

Theorem 1.3 and Theorem 1.4 give rise to algorithms to solve for $\tau_{3,p}$ explicitly. We implement these algorithms in Sage, and obtain the results in Table 1.2, where f_α is an irreducible polynomial with roots of height $\tau_{3,p}$.

TABLE 1.2: Some values of $\tau_{3,p}$

p	$\tau_{3,p}$	f_α
5	0.36620	$x^3 - 2x^2 - x - 3$
7	0.12741	$x^3 - x^2 - 1$
11	0.23105	$x^3 - x^2 - 2$
13	0.093733	$x^3 - x^2 + 1$

Continued on next page

TABLE 1.2 – continued from previous page

p	$\tau_{3,p}$	f_α
17	0.23105	$x^3 - 2x - 2$
19	0.12741	$x^3 + x + 1$
23	0.20313	$x^3 - x^2 + x + 1$
29	0.093733	$x^3 - x - 1$
31	0.093733	$x^3 + x^2 - 1$
37	0.20313	$x^3 + x^2 + x - 1$
41	0.093733	$x^3 - x - 1$
43	0.23105	$x^3 - 2x + 2$
47	0.23105	$2x^3 - 2x^2 + 1$
53	0.20313	$x^3 - x^2 - x - 1$
59	0.12741	$x^3 - x^2 - 1$

Shifting focus, we then look at an upper bound on the smallest limit point of nontrivial heights of totally p-adic numbers. This work builds on previous results of Bombieri-Zannier and Fili-Petsche. They have established lower bounds, which are not sharp, for $\liminf_{d\to\infty} \tau_{d,p}$. We use techniques from arithmetic dynamical systems to establish an upper bound on $\liminf_{d\to\infty} \tau_{d,p}$. The exact value of $\liminf_{d\to\infty} \tau_{d,p}$ is not known, but we offer the following upper bound, which is approximately twice the lower bound provided by Fili-Petsche.

Theorem 1.5. For each prime p, there are infinitely many $\alpha \in \mathcal{T}_p^{\mathrm{ab}}$ such that $h(\alpha) \le \frac{\log(p+1)}{p-1}$. In particular,

$$\liminf_{d\to\infty} \tau_{d,p} \le \frac{\log(p+1)}{p-1}.$$

The proof of Theorem 1.5 is inspired by an argument of Smyth, where he used the preimages of 1 under the map $\phi(x) = x + \frac{1}{x}$ to create an upper bound on the

smallest limit point of nontrivial heights of totally real numbers. We use instead the map $\phi_p(x) = \frac{1}{p}(x^p - x)$, and take preimages of 1 to create an infinite set of nontrivial heights bounded above by $\frac{\log(p+1)}{p-1}$.

In Chapter 2, we provide background on absolute values, heights, Mahler measure and Newton polygons. In Chapter 3, we consider heights of totally p-adic numbers in abelian extensions of $\mathbb{Q}$, and we prove Theorem 1.2. In Chapter 4, we prove Theorem 1.3 and Theorem 1.4. In Chapter 5, we use techniques from arithmetic dynamical systems to establish an upper bound on $\liminf_{d\to\infty} \tau_{d,p}$. The appendices contain all code used in Sage to compute results of degree 3 algebraic numbers.

2 Preliminaries

This section contains standard results that are used throughout this paper. We assume the reader has a background in basic abstract algebra, Galois theory, and the theory of algebraic number fields. We review the basic definitions of absolute value and p-adic numbers. The main sources are *Heights in Diophantine Geometry* by Enrico Bombieri and Walter Gubler [BG06], *Local Fields* by J.W.S. Cassels [Cas86], *p-adic Numbers: An Introduction* by Fernando Q. Gouvêa [Gou97], and *Algebraic Number Theory Course Notes (Fall 2006)* by Matt Baker [Bak06].

2.1 Absolute Values

All results in this section, along with proofs, can be found within *p-adic Numbers: An Introduction* by Fernando Q. Gouvêa in Sections 3.1 and 3.2 [Gou97].

Definition. Let k be a field. An **absolute value** on k is a function $|\cdot| : k \to [0, \infty)$ that satisfies the following properties for all $x, y \in k$:

i) $|x| = 0$ if and only if $x = 0$;

ii) $|xy| = |x||y|$;

iii) $|x + y| \leq |x| + |y|$.

If $|\cdot|$ further satisfies the strong triangle inequality, $|x+y| \leq \max\{|x|, |y|\}$ for all $x, y \in k$, then $|\cdot|$ is a **non-archimedean** absolute value. If $|\cdot|$ does not satisfy the strong triangle inequality for all $x, y \in k$, then $|\cdot|$ is an **archimedean** absolute value. Two absolute values, $|\cdot|_1$ and $|\cdot|_2$, are **equivalent** if there is some $\theta > 0$ such that, for all $x \in k$, $|x|_1 = |x|_2^{\theta}$. If $|\cdot|_1$ is equivalent to $|\cdot|_2$, we write $|\cdot|_1 \sim |\cdot|_2$.

Example 1. The **trivial absolute value**, $|\cdot|_0 : k \to [0, \infty)$ is defined by

$$|x|_0 = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0. \end{cases}$$

Example 2. The standard archimedean absolute value on $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}$ is given by $|z|_\infty = \sqrt{z\overline{z}}$.

When $k = \mathbb{Q}$, in addition to the standard archimedean absolute value, there are countably many p-adic absolute values, one for each prime p (up to equivalence).

Definition. Let $x \in \mathbb{Q}$, p be a prime, and write $x = p^k \frac{a}{b}$, where $a, b, k \in \mathbb{Z}$, and $p \nmid ab$. Then the ***p*-adic absolute value** of $x \neq 0$ is

$$|x|_p = p^{-k}.$$

The p-adic absolute value measures the divisibility of p; it is small when the numerator of x is highly divisible by p, and large when the denominator of x is highly divisible by p. To illustrate,

$$\lim_{n\to\infty} |p^n|_p = \lim_{n\to\infty} p^{-n} = 0.$$

Proposition 2.1. $|\cdot|_p$ is a non-archimedean absolute value on $\mathbb{Q}$.

Proof. The first two axioms follow directly from the definition of $|\cdot|_p$. It remains to prove that the strong triangle inequality holds. Let $x = p^k \frac{a}{b}$ and $y = p^\ell \frac{c}{d} \in \mathbb{Q}$, where $p \nmid abcd$. Without loss of generality, suppose that $|x|_p \leq |y|_p$. Thus $k \geq \ell$. It follows that

$$\begin{aligned} |x + y|_p &= \left|p^k \tfrac{a}{b} + p^\ell \tfrac{c}{d}\right|_p \\ &= \left|p^\ell \left(p^{k-l} \tfrac{a}{b} + \tfrac{c}{d}\right)\right|_p \\ &= p^{-\ell} \left|p^{k-l} \tfrac{a}{b} + \tfrac{c}{d}\right|_p \\ &= p^{-\ell} \left|\tfrac{p^{k-l}ad+bc}{bd}\right|_p \end{aligned}$$

$$\leq p^{-\ell}$$
$$= |y|_p$$
$$= \max\{|x|_p, |y|_p\}. \qquad \square$$

The next proposition is often referred to as "the case of equality in the strong triangle inequality."

Proposition 2.2. Let k be a field, and let $|\cdot|$ be a non-archimedean absolute value on k. Let $x, y \in k$ with $|x| \neq |y|$. Then $|x + y| = \max\{|x|, |y|\}$.

Proof. Without loss of generality, suppose $|x| < |y|$. By the strong triangle inequality,

$$|x + y| \leq \max\{|x|, |y|\} = |y|.$$

Since $|x| < |y|$,

$$|y| = |x + y - x| \leq \max\{|x + y|, |x|\} = |x + y|. \tag{2.1}$$

If the last equality in (2.1) did not hold, then we would have $|y| \leq \max\{|x+y|, |x|\} = |x|$, which would contradict $|x| < |y|$. Since $|y| \leq |x + y| \leq |y|$, $|x + y| = |y|$. $\square$

Theorem 2.3 (Ostrowski's Theorem)**.** [Gou97, Theorem 3.1.3] Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.

A **place** of a number field K is defined to be an equivalence class of nontrivial absolute values, and we denote by M_K the set of places of K. Ostrowski's Theorem allows us to write

$$M_{\mathbb{Q}} = \{\infty, 2, 3, 5, 7, 11, 13, 17, \dots\},$$

where ∞ denotes the archimedean place, and abusing notation slightly we use p to denote both a prime number as well as its corresponding equivalence class of absolute values on $\mathbb{Q}$. The archimedean place is often refered to as the "place at infinity," where the non-archimedean places are considered the "finite places." The absolute values on K satisfy a version of Ostrowski's Theorem. For more details, see [Gou97].

Given $v \in M_K$, we may restrict one of its absolute values to $\mathbb{Q}$, and by Ostrowski's Theorem on $\mathbb{Q}$, v must correspond to a place p of $\mathbb{Q}$; in this case we write $v \mid p$.

The field of rational numbers is not complete with respect to any of its nontrivial absolute values. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is denoted by $\mathbb{Q}_p$ and is called the **field of p-adic numbers**. The absolute value $|\cdot|_p$ extends uniquely to an absolute value on $\mathbb{Q}_p$. Just as $\mathbb{Q}$ is dense in $\mathbb{R}$, $\mathbb{Q}$ is also dense in $\mathbb{Q}_p$. $\mathbb{Z}_p$ is the **ring of p-adic integers** and is defined as:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Although $\mathbb{Q}_p$ is complete, it is not algebraically closed. The algebraic closure of $\mathbb{Q}_p$ is $\overline{\mathbb{Q}_p}$, and the completion of $\overline{\mathbb{Q}_p}$ is denoted by $\mathbb{C}_p$, which is both complete and algebraically closed [BGR84].

Example 3. The polynomial $x^2 - p$ does not split in $\mathbb{Q}_p$, since the p-adic absolute value of an element in $\mathbb{Q}_p$ must be equal to p^k for $k \in \mathbb{Z}$, and $\left|\sqrt{p}\right|_p = p^{-1/2}$.

Definition. The **local degree** of a number field K over $\mathbb{Q}$ at the place v is $d_v = [K_v : \mathbb{Q}_v]$, where K_v is the completion of K under $|\cdot|_v$ and $\mathbb{Q}_v$ is the completion of $\mathbb{Q}$ under $|\cdot|_v$. The **global degree** of K over $\mathbb{Q}$ is $d = [K : \mathbb{Q}]$.

Example 4. Let K be a number field, and v be the archimedean place. Then $\mathbb{Q}_v = \mathbb{R}$ and either $K_v = \mathbb{C}$ or $K_v = \mathbb{R}$, so $d_v = 1$ or $d_v = 2$.

Theorem 2.4 (Local-Global Degree Formula)**.** [BG06, Corollary 1.3.2] Let L be a finite extension of a number field K. Then, for $v \in M_K$,

$$[L : K] = \sum_{\substack{w \in M_L \\ w \mid v}} [L_w : K_v].$$

Definition. Let v be a place of K. If v is archimedean, we will say $v \mid \infty$, and denote by $|\cdot|_v$ the unique absolute value on K such that $|x|_v = |x|_\infty$ for all $x \in \mathbb{Q}$. If v is non-archimedean with $v \mid p$, then $|\cdot|_v$ is the unique absolute value on K such that $|x|_v = |x|_p$ for all $x \in \mathbb{Q}$.

One of the most important results in p-adic analysis is Hensel's Lemma. The proof is essentially a p-adic version of Newton's root-finding method from Calculus. We include a standard proof of Hensel's Lemma, this version of which appears in [Petb]; see also [Con18b] for essentially the same proof but for a stronger version of the result.

Lemma 2.5 (Hensel's Lemma)**.** [Con18b, Theorem 1.2] If $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ satisfies

i) $f(a) \equiv 0 \pmod{p}$, and

ii) $f'(a) \not\equiv 0 \pmod{p}$,

then there is a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv a \pmod{p}$.

Proof. Beginning with a, we create a sequence of elements of $\mathbb{Z}_p$ which converge to a root α of f, and show that $\alpha \equiv a \pmod{p}$. To begin, we let $a_1 = a$, and define the sequence $a_1, a_2, a_3, \ldots$ recursively as follows:

$$a_{k+1} = a_k - \tfrac{f(a_k)}{f'(a_k)}. \tag{2.2}$$

We show by induction, that

$$\begin{aligned} |f(a_k)|_p &\le |f(a)|_p^{2^{k-1}}, \text{ and} \\ |f'(a_k)|_p &= 1 \end{aligned} \tag{2.3}$$

for all choices of $k \ge 1$. Notice that (2.3) implies that $f'(a_k)$ is nonzero, and therefore (2.2) makes sense.

Assume (2.3) holds for $a_1, a_2, \ldots, a_k$. We show that (2.3) holds for a_{k+1}. By definition of a_k and the induction hypothesis,

$$|a_{k+1} - a_k|_p = \left|\tfrac{f(a_k)}{f'(a_k)}\right|_p = |f(a_k)|_p \le |f(a)|_p^{2^{k-1}} < 1.$$

Expanding f about a_k, we obtain

$$f(x) = b_0 + b_1(x - a_k) + \cdots + b_d(x - a_k)^d.$$

Since $\mathbb{Z}_p$ is a ring containing a_k and the coefficients of f, and since b_j are the coefficients of $f(x + a_k)$, we have that $b_j \in \mathbb{Z}_p$ for all j. Additionally, $b_0 = f(a_k)$ and $b_1 = f'(a_k)$. By (2.2), $f(a_k) + f'(a_k)(a_{k+1} - a_k) = 0$ and thus

$$\begin{aligned} f(a_{k+1}) &= b_0 + b_1(a_{k+1} - a_k) + b_2(a_{k+1} - a_k)^2 + \cdots + b_d(a_{k+1} - a_k)^d \\ &= f(a_k) + f'(a_k)(a_{k+1} - a_k) + b_2(a_{k+1} - a_k)^2 + \cdots + b_d(a_{k+1} - a_k)^d \\ &= b_2(a_{k+1} - a_k)^2 + \cdots + b_d(a_{k+1} - a_k)^d. \end{aligned}$$

By the strong triangle inequality,

$$|f(a_{k+1})|_p \leq |a_{k+1} - \alpha_k|_p^2 \leq (|f(a)|_p^{2^{k-1}})^2 = |f(a)|_p^{2^k}.$$

Further,

$$f'(a_{k+1}) = f'(a_k) + 2b_2(a_{k+1} - a_k) + \cdots + db_d(a_{k+1} - a_k)^{d-1}$$

and thus by Proposition 2.2, $|f'(a_{k+1})|_p = |f'(a_k)|_p = 1$. Thus, we have shown that a_{k+1} satisfies (2.3), so by induction (2.3) holds for all $k \in \mathbb{N}$.

To show that the sequence $\{a_k\}$ converges to some $\alpha \in \mathbb{Z}_p$, we must first show that $\{a_k\}$ is a Cauchy sequence in $\mathbb{Z}_p$. If $k_1 \leq k_2$ are integers, then

$$\begin{aligned} |a_{k_2} - a_{k_1}|_p &= \left| \sum_{k=k_1}^{k_2-1} (a_{k+1} - a_k) \right|_p \\ &\leq \max_{k_1 \leq k \leq k_2 - 1} |a_{k+1} - a_k|_p \\ &\leq \max_{k_1 \leq k \leq k_2 - 1} |f(a)|_p^{2^{k-1}} \\ &= |f(a)|_p^{2^{k_1 - 1}}. \end{aligned}$$

Since $\lim_{k_1 \to \infty} |f(a)|_p^{2^{k_1-1}} = 0$, we have that $\{a_k\}$ is a Cauchy sequence. Let $\alpha = \lim a_k$. Since $\mathbb{Z}_p$ is complete, $\alpha \in \mathbb{Z}_p$. By continuity of polynomials,

$$f(\alpha) = f(\lim a_k) = \lim f(a_k) = 0.$$

Lastly, we verify that $\alpha \equiv a \pmod{p}$:

$$\begin{aligned} |a-\alpha|_p &= |a_1 - a_k + a_k - \alpha|_p \\ &\leq \max\{|a_1 - a_k|_p, |a_k - \alpha|_p\} \\ &\leq \max\{|f(a)|_p, |a_k - \alpha|_p\} \\ &= |f(a)|_p < 1 \end{aligned}$$

for large enough k. □

Example 5. Let $f(x) = x^2 + x + 2$. Since

$$|f(1)|_2 = |4|_2 = \tfrac{1}{4}, \text{ and}$$

$$|f'(1)|_2 = |3|_2 = 1,$$

there exists an $\alpha \in \mathbb{Z}_2$ such that $f(\alpha) = 0$, and $\alpha \equiv 1 \pmod{2}$. Further, since α is in the field $\mathbb{Q}_2$, both roots of f must be in $\mathbb{Q}_2$, and f splits completely over $\mathbb{Q}_2$.

Proposition 2.6. Let p be an odd prime. Then $\mathbb{Q}_p$ contains the $(p-1)^{\text{st}}$ roots of unity.

Remark. To see that the $(p-1)^{\text{st}}$ roots of unity are the only roots of unity in $\mathbb{Q}_p$, see [Gou97, page 72-73].

Proof. We use Hensel's Lemma to show that in fact the $(p-1)^{\text{st}}$ roots of unity are in $\mathbb{Q}_p$. Let $f(x) = x^{p-1} - 1$, and $a \in \{1, 2, \ldots, p-1\}$. By Fermat's Little Theorem, we have that $a^{p-1} \equiv 1 \pmod{p}$. In other words, $p \mid a^{p-1} - 1$. Hence

$$|f(a)|_p = |a^{p-1} - 1|_p < 1.$$

Since

$$|f'(a)|_p = |(p-1)a^{p-2}|_p = 1,$$

Hensel's Lemma guarantees a unique root of f in $\mathbb{Q}_p$ congruent to a, for all $a \in \{1, 2, \ldots, p-1\}$. Thus, all $p-1$ of the $(p-1)^{\text{st}}$ roots of unity are in $\mathbb{Q}_p$. □

2.2 Logarithmic Weil Height

Let $\frac{a}{b} \in \mathbb{Q}$ be in lowest terms. Recall that the height of $\frac{a}{b}$ is $\log \max\{|a|, |b|\}$. To precisely extend the height function to number fields, we use the machinery of places.

Definition. Let K be a number field containing α, $d_v = [K_v : \mathbb{Q}_v]$, and $d = [K : \mathbb{Q}]$. The **logarithmic Weil height** of α is defined by the function

$$h(\alpha) = \sum_{v \in M_K} \log \max\{1, |\alpha|_v^{d_v/d}\}.$$

Throughout this paper, $h(\alpha)$ shall be referred to as "the height of α."

To show that $h(\alpha)$ does not depend on the choice of K, let L be a field extension of K. For each place v of K, the local-global degree formula for the extension L/K states that $[L : K] = \sum_{w|v} [L_w : K_w]$. The following calculation shows $h(\alpha)$ remains the same if we view α as an element of K or as an element of L.

$$\begin{aligned}
\sum_{w \in M_L} \log \max\left\{1, |\alpha|_w^{[L_w:\mathbb{Q}_w]/[L:\mathbb{Q}]}\right\} &= \sum_{v \in M_K} \sum_{w|v} \log \max\left\{1, |\alpha|_v^{[L_w:\mathbb{Q}_w]/[L:\mathbb{Q}]}\right\} \\
&= \sum_{v \in M_K} \sum_{w|v} \tfrac{[L_w:\mathbb{Q}_w]}{[L:\mathbb{Q}]} \log \max\{1, |\alpha|_v\} \\
&= \sum_{v \in M_K} \sum_{w|v} \tfrac{[L_w:K_w][K_v:\mathbb{Q}_v]}{[L:K][K:\mathbb{Q}]} \log \max\{1, |\alpha|_v\} \\
&= \sum_{v \in M_K} \tfrac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]} \sum_{w|v} \tfrac{[L_w:K_w]}{[L:K]} \log \max\{1, |\alpha|_v\} \\
&= \sum_{v \in M_K} \tfrac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]} \log \max\{1, |\alpha|_v\} \\
&= \sum_{v \in M_K} \log \max\left\{1, |\alpha|_v^{[K_v:\mathbb{Q}_v]/[K:\mathbb{Q}]}\right\}
\end{aligned}$$

Since $\mathbb{Q}(\alpha)$ is a subfield of all number fields containing α, the above calculation is sufficient to show equality for all number fields containing α.

Theorem 2.7 (Northcott's Theorem)**.** [BG06, Theorem 1.6.8] For each $A > 0$, $B > 0$, the set

$$\left\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq A \text{ and } h(\alpha) \leq B\right\}$$

is finite.

Theorem 2.8. Let α be an algebraic number. Then $h(\alpha) = 0$ if and only if $\alpha = 0$ or is a root of unity.

Proof. From the definiton of height, we see that $h(0) = 0$ and $h(1) = 0$. Let α be a root of unity with $\alpha^m = 1$. Then $m\,h(\alpha) = h(\alpha^m) = h(1) = 0$, and thus $h(\alpha) = 0$.

Conversely, suppose that $h(\alpha) = 0$. Then $h(\alpha^n) = |n|h(\alpha) = 0$ for all positive integers n. Since the sequence $\alpha, \alpha^2, \alpha^3, \ldots$ has bounded height and bounded degree, by Northcott's Theorem, the sequence can only contain finitely many values. Thus, for some $m > n$, $\alpha^m = \alpha^n$. Moreover, $0 = \alpha^n(\alpha^{m-n} - 1)$. Thus $\alpha = 0$ or is a root of unity. □

2.3 Mahler Measure

The results in this section come from *Heights in Diophantine Geometry* by Enrico Bomieri and Walter Gubler [BG06].

Definition. Let $f(x) \in \mathbb{C}[x]$ be a nonzero polynomial of degree d with roots $\alpha_1, \ldots, \alpha_d$ (allowing for multiplicity) and leading coefficient a. The **Mahler measure** of f is

$$M(f) = |a| \prod_{|\alpha_j| \geq 1} |\alpha_j|,$$

where $|z| = \sqrt{z\overline{z}}$.

Definition. The n^{th} cyclotomic polynomial, $\Phi_n(x)$, is the minimal polynomial for a primitive n^{th} root of unity.

Theorem 2.9. [BG06, Proposition 1.6.6] Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of $\alpha \neq 0$, and $d = \deg(f)$. Then

$$h(\alpha) = \tfrac{1}{d} \log M(f).$$

Theorem 2.10. Let $f \in \mathbb{Z}[x]$. Then $M(f) = 1$ if and only if $f(x) = \pm x^k \prod \Phi_n(x)$, for some $k \in \mathbb{N}$ and cyclotomic polynomials Φ_n.

Proof. If $M(f) = 1$, then all irreducible factors of f have Mahler measure 1, so then Theorem 2.9 implies that all roots are either zero or roots of unity. For the other direction, it follows directly from the definiton of Mahler measure that $M(\pm x^k \prod \Phi_n(x)) = 1$ because the leading coefficient is 1 and all roots are inside the closed unit disc. □

Definition. Let $f \in \mathbb{Z}[x]$ with

$$f(x) = \sum_{i=0}^{d} a_i x^i.$$

The **length** of f is $L(f) = \sum_{i=0}^{d} |a_i|$ where $|\cdot|$ is the archimedean absolute value on $\mathbb{Z}$.

Proposition 2.11. (Height-Length Bound) Let $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$, Then

$$L(f) \leq 2^d M(f).$$

Proof. Note that for a nonzero complex number γ, $L(\gamma f) = |\gamma| L(f)$ and $M(\gamma f) = |\gamma| M(f)$. Thus, without loss of generality we may asssume that f is monic, and can be written

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = \prod_{i=1}^{d} (x - \alpha_i).$$

By the symmetric function theorem, for $0 \leq i \leq d-1$, a_i is equal to the sum over all subsets of the roots of f of size $d - i$, of $\pm$ the product of the roots in that subset. The Mahler measure is the product of all roots with absolute value greater than one. Thus, each product being summed is bounded above by the Mahler measure $M(f)$, and there are $\binom{d}{i}$ terms being summed, so we have

$$\begin{aligned} L(f) &= 1 + \sum_{i=0}^{d-1} |a_i| \\ &\leq \sum_{i=0}^{d} \binom{d}{i} M(f) \\ &= 2^d M(f). \end{aligned}$$

□

2.4 Newton Polygons

For this section, we rely on Section 6.3 in *Local Fields* by J.W.S Cassels [Cas86] and Section 6.4 in *p-adic Numbers: An Introduction* by Fernando Q. Gouvêa [Gou97]. The Newton polygon of a polynomial f is a geometric object that encodes information about the placement of the roots of f.

Definition. The **p-adic valuation** $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{+\infty\}$ on $\mathbb{Q}_p$ is defined by

$$|x|_p = p^{-v_p(x)}$$

for $x \neq 0$, and $v_p(0) = +\infty$.

Definition. Let p be a prime, and

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d \in \mathbb{Q}_p[x].$$

Consider the set of points $\{(i, v_p(a_i)) \mid 0 \leq i \leq d\}$ in $\mathbb{R}^2$. The **Newton polygon** of $f(x)$ is the lower boundary of the convex hull of this set of points.

Definition. The **Newton slopes** are the slopes of the line segments of a Newton polygon. The point $(i, v(a_i))$ is a **vertex** of the Newton polygon if the slopes of the line segments change at $(i, v(a_i))$. We then say that i is a **break**. The **length** of a line segment is the length of the projection of the corresponding segment onto the x-axis.

Definition. A polynomial is **pure** if its Newton polygon has only one Newton slope.

Example 6. Figure 2.1 shows the Newton polygon of

$$f(z) = z^7 + \frac{3}{16}z^6 + \frac{1}{32}z^5 - 8z^4 + \frac{7}{16}z^3 - \frac{1}{12}z + 28 \in \mathbb{Q}_2[z].$$

There are breaks at $i = 1, 3, 5, 6, 7$ and the Newton slopes are $-4, -1, -\frac{1}{2}, 1, 4$.

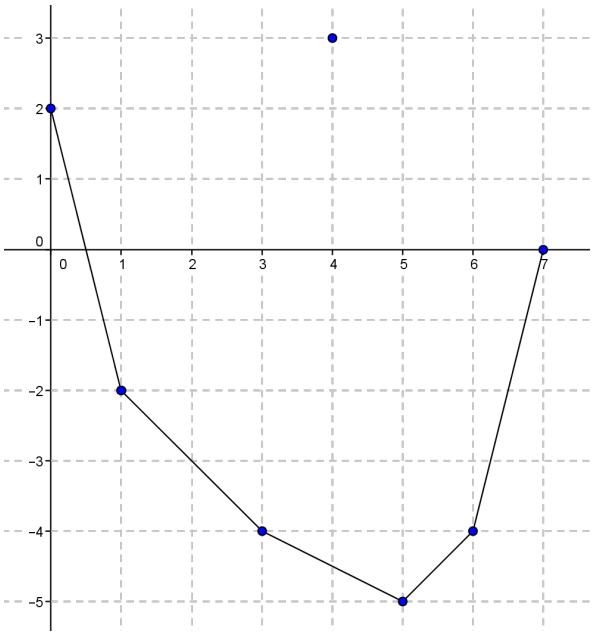

FIGURE 2.1: Newton Polygon of $f(z) = z^7 + \frac{3}{16}z^6 + \frac{1}{32}z^5 - 8z^4 + \frac{7}{16}z^3 - \frac{1}{12}z + 28$.

Theorem 2.12. [Gou97, Theorem 6.4.7] Let $f(x) = a_d x^d + \cdots + a_1 x + 1 \in \mathbb{Q}_p[x]$. Let $\alpha_1, \ldots, \alpha_d$ be the roots of $f(x)$ in $\mathbb{C}_p$, counting multiplicities, so that

$$f(x) = \prod_{i=1}^{d} \left(1 - \tfrac{x}{\alpha_i}\right).$$

Let $\lambda_i = v(1/\alpha_i)$. Then λ is a slope of the Newton polygon of $f(z)$ with length ℓ if precisely ℓ of the λ_i are equal to λ. That is, $f(x)$ has exactly ℓ roots with absolute value p^λ.

Proposition 2.13. [Gou97, Proposition 6.4.2] All irreducible polynomials in $\mathbb{Q}_p[x]$ are pure.

Definition. A polynomial $f \in \mathbb{Q}_p[x]$ is of **type**

$$(\ell_1, m_1 : \ell_2, m_2 : \cdots : \ell_r, m_r) \tag{2.4}$$

if the segments of the Newton polygon of f are length ℓ_i with slope m_i, and $m_1 < m_2 < \cdots < m_r$.

Theorem 2.14. [Cas86, Theorem 3.1] Suppose $f(x) \in \mathbb{Q}_p[x]$ is of type

$$(\ell_1, m_1 : \ell_2, m_2 : \cdots : \ell_r, m_r)\,.$$

Then,

$$f(x) = g_1(x)g_2(x)\cdots g_r(x),$$

where $g_i(x)$ is pure of type (ℓ_i, m_i).

Remark. Theorem 2.14 implies that if $f(x) \in \mathbb{Q}_p[x]$ is of type

$$(\ell_1, 1 : \ell_2, 1 : \cdots : \ell_r, 1)\,,$$

then f splits completely over $\mathbb{Q}_p$.

3 Totally p-adic Numbers with Abelian Galois Group

Definition. Let $\alpha \in \overline{\mathbb{Q}}$. We say that α is **abelian** if α is contained within an abelian extension of $\mathbb{Q}$. The subfield of all abelian algebraic numbers is denoted $\mathbb{Q}^{\text{ab}}$.

For brevity, we will denote the set of all nonzero, non-root of unity, algebraic, totally p-adic numbers by $\mathcal{T}_p$, and $\mathcal{T}_p^{\text{ab}} = \mathcal{T}_p \cap \mathbb{Q}^{\text{ab}}$.

Definition. Given a prime p and a positive integer d, we define

$$\tau_{d,p} = \min\{h(\alpha) \mid \alpha \in \mathcal{T}_p \text{ and } \deg(\alpha) = d\}, \text{ and}$$
$$\tau_{d,p}^{\text{ab}} = \min\{h(\alpha) \mid \alpha \in \mathcal{T}_p^{\text{ab}} \text{ and } \deg(\alpha) = d\}.$$

We establish the finiteness of $\tau_{d,p}$ for all choices of p and d in two ways. First, Proposition 3.1 uses Newton polygons to create a polynomial of degree d that is irreducible over $\mathbb{Q}$ and splits completely over $\mathbb{Q}_p$. Later, Theorem 3.8 will provide an alternate proof via Galois theory.

Proposition 3.1. Let p be a prime, and $d \geq 2$. There exists an $\alpha \in \mathcal{T}_p$ of degree d.

Proof. Let q be a prime, distinct from p. We will show that the polynomial

$$f(x) = p^{(d+1)d/2}x^d + \sum_{i=0}^{d-1} qp^{i(i-1)/2}x^i.$$

is irreducible over $\mathbb{Z}$ and splits completely over $\mathbb{Q}_p$. Since $p^{(d+1)d/2} \neq \pm 1$, f is not cyclotomic. Thus the roots of f are not roots of unity.

Let a_i be the coefficient of x^i. For all $0 \leq i \leq d-1$, $q \mid a_i$ and $q^2 \nmid a_0$. By the Eisenstein criterion, f is irreducible over $\mathbb{Z}$.

Next we determine the Newton polygon type of f for the prime p. If $\ell_i = 1$ for all i, then by Theorem 2.14, f splits completely over $\mathbb{Q}_p$. Since $v_p(a_i) = \frac{i(i-1)}{2}$,

$$v_p(a_{i+1}) - v_p(a_i) = \tfrac{(i+1)i}{2} - \tfrac{i(i-1)}{2} = i.$$

Therefore, f is of type $(1, 0 : 1, 1 : 1, 2 : \cdots : 1, i : \cdots : 1, d-1)$ and splits completely over $\mathbb{Q}_p$. $\square$

3.1 Totally p-adic Numbers of Degree 2

Proposition 3.2. Let $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ be irreducible with $a \neq 0$, and let $\alpha \in \overline{\mathbb{Q}}$ be a root of f.

(a) If $f(x)$ is equal to $\pm\Phi_3(x), \pm\Phi_4(x)$, or $\pm\Phi_6(x)$, then $h(\alpha) = 0$.

(b) If $f(x) = \pm(x^2 \pm x - 1)$, then $h(\alpha) = \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right)$.

(c) If $f(x)$ is not equal to $\pm\Phi_3(x), \pm\Phi_4(x), \pm\Phi_6(x)$ or $\pm(x^2 \pm x - 1)$, then $h(\alpha) \geq \frac{1}{2}\log 2$.

Proof. Let α be a root of unity contained in a number field K. For all $v \in M_K$, $|\alpha|_v = 1$, and thus part **(a)** holds. Part **(b)** follows from the quadratic formula and definition of height.

We now verify part **(c)**. Suppose $f(x) = a(x-\alpha)(x-\beta)$ is not equal to $\pm\Phi_3(x), \pm\Phi_4(x), \pm\Phi_6(x)$, or $\pm(x^2 \pm x - 1)$.

If $|a| \geq 2$, then $M(f) \geq 2$, and $h(\alpha) \geq \frac{1}{2}\log 2$. Therefore, we may assume $a = 1$. We then consider two cases: either the roots of f are real or non-real.

Case 1: Suppose $\alpha, \beta \in \mathbb{R}$ are the roots of f, and for sake of contradiction that $0 < h(\alpha) < \frac{1}{2}\log 2$. In terms of Mahler measure, this can be written as $1 < M(f) < 2$. Since f is irreducible, $c \neq 0$. Thus

$$1 \leq |c| = |\alpha\beta| \leq \max\{1, |\alpha|\}\max\{1, |\beta|\} = M(f) < 2.$$

Thus $c = \pm 1$. Note that α and β are not roots of unity, since we have excluded all quadratic cyclotomic polynomials. By Kronecker's Theorem, $h(\alpha) > 0$. Since $|\alpha\beta| = 1$, we know exactly one of the roots must fall outside the unit circle, and the other inside. Without loss of generality, suppose $|\alpha| < 1 < |\beta|$, so $M(f) = |\beta|$. Since f is irreducible with real roots, $b^2 - 4ac$ is a positive non-square in $\mathbb{Z}$.

To show $|b| = 1$, we elimiminate $|b| = 0$ and $|b| \geq 2$ by contradiction. If $b = 0$, then $b^2 - 4ac = -4c$, which is negative when $c = 1$, and is a square if $c = -1$. Suppose $|b| \geq 2$.

Then

$$M(f) = \max\left\{\left|\frac{-b+\sqrt{b^2-4c}}{2}\right|, \left|\frac{-b-\sqrt{b^2-4c}}{2}\right|\right\} = \frac{|b|+\sqrt{b^2-4c}}{2}.$$

If $c = -1$, then

$$M(f) = \frac{|b|+\sqrt{b^2+4}}{2} > \frac{|b|+|b|}{2} = |b| \geq 2,$$

which contradicts the assumption that $M(f) < 2$. If $c = 1$, $b^2 - 4ac = b^2 - 4$, which cannot be zero by the irreducibilty hypothesis. Hence, $|b| \geq 3$, so

$$M(f) = \frac{|b|+\sqrt{b^2-4}}{2} \geq \frac{|b|+\sqrt{5}}{2} > 2,$$

which contradicts the assumption that $M(f) < 2$. Therefore, $|b| = 1$.

Considering all polynomials with $|a| = |b| = |c| = 1$, we find that $\pm(x^2 \pm x - 1)$ are the only such polynomials that have real roots.

Case 2: Suppose the roots of f are non-real, say α and $\overline{\alpha}$. Since $a = 1$, $\alpha\overline{\alpha} = c$. Since f is not a cyclotomic polynomial, by Kronecker's Theorem, $|\alpha| > 1$ and $|\overline{\alpha}| > 1$. Thus $|c| \geq 2$. Therefore $h(\alpha) = \frac{1}{2}\log M(f) = \frac{1}{2}|c| \geq \frac{1}{2}\log 2$. □

Remark. Proposition 3.1 implies the smallest nonzero height of a degree 2 algebraic number is achieved only by the the roots of $\pm(x^2 \pm x - 1)$.

Definition. Let p be an odd prime. The **Legendre symbol**, for an integer a, is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a square} \pmod p, \\ -1 & \text{if } a \text{ is not a square} \pmod p, \text{ and} \\ 0 & \text{if } p \mid a. \end{cases}$$

The **law of quadratic reciprocity** states that for odd primes p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Theorem 3.3. For any prime p,

$$\tau_{2,p} = \begin{cases} \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right) & \text{if } p \equiv 1, 4 \pmod 5 \\ \frac{1}{2}\log 2 & \text{if } p \equiv 0, 2, 3 \pmod 5. \end{cases}$$

Proof. Let p be an odd prime. We consider a few polynomials whose roots have height $\frac{1}{2}\log 2$,

$$g(x) = x^2 + 2,$$
$$h(x) = x^2 - 2, \text{ and}$$
$$k(x) = x^2 + 2x + 2.$$

A quadratic polynomial splits in $\mathbb{Q}_p$ if and only if its discriminant is a square mod p. Thus g splits over $\mathbb{Q}_p$ if and only if $\left(\frac{-2}{p}\right) = 1$, h splits over $\mathbb{Q}_p$ if and only if $\left(\frac{2}{p}\right) = 1$, and k splits over $\mathbb{Q}_p$ if and only if $\left(\frac{-1}{p}\right) = 1$, where $\left(\frac{a}{p}\right)$ is the Legendre symbol. By properties of the Legendre symbol,

$$\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right). \tag{3.1}$$

Since p is odd, $\left(\frac{-2}{p}\right) \neq 0$, and therefore at least one of the symbols has a value of 1. The associated polynomial must split over $\mathbb{Q}_p$.

By Proposition 3.1, $\pm(x^2 \pm x - 1)$ are the only irreducible polynomials over $\mathbb{Z}$ with root α such that $0 < h(\alpha) < \frac{1}{2}\log 2$. Thus $\tau_{2,p} = \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right)$ if one of $\pm(x^2 \pm x - 1)$ splits over $\mathbb{Q}_p$. If not, then $\tau_{2,p} = \frac{1}{2}\log 2$.

Note that $\pm(x^2 \pm x - 1)$ splits over $\mathbb{Q}_p$ if and only if its discriminant 5 is a square in $\mathbb{Q}_p$. By quadratic reciprocity, if $p \equiv 1, 4 \pmod 5$, then $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$. If $p \equiv 2, 3 \pmod 5$, then $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$.

It remains to determine $\tau_{2,2}$ and $\tau_{2,5}$. Since the value group of $\mathbb{Q}_p$ is $p^{\mathbb{Z}}$, 5 is not a square in $\mathbb{Q}_5$ since $|\sqrt{5}|_5 = 5^{-1/2}$. Thus $\tau_{2,5} \neq \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right)$, and $\tau_{2,5} = \frac{1}{2}\log 2$.

Note that $x^2 + x + 2$ splits over $\mathbb{Q}_2$ by Hensel's Lemma, and the roots have height $\frac{1}{2}\log 2$. Further, $x^2 \pm x - 1$ do not split over $\mathbb{Q}_2$ since they do not split over $\mathbb{Z}_2$, and thus $\tau_{2,2} = \frac{1}{2}\log 2$. □

3.2 Dependence of $\tau_{d,p}^{\mathrm{ab}}$ on a Congruence Condition

In Section 3.1 we showed that $\tau_{2,p}$ depends only on $p \pmod 5$. In this section we show that for any degree d, $\tau_{d,p}^{\mathrm{ab}}$ depends only on p modulo some integer N_d. Theorem 3.8 verifies the finiteness of $\tau_{d,p}^{\mathrm{ab}}$ for $d \geq 2$ and prime p, and since $\tau_{d,p} \leq \tau_{d,p}^{\mathrm{ab}}$, $\tau_{d,p}$ must also be finite.

Lemma 3.4. Let G be a finite abelian group of order n. If $m \mid n$, then there exists a subgroup of G of order m.

Proof. We induct on the order of $|G|$. The case $|G| = 1$ is trivial. For nontrivial G, suppose that the Lemma holds for all groups with smaller order than G. Let m be a divisor of $|G|$ and let p be a prime divisor of m. Let $\alpha \in G$ of order p. Such an element exists by Cauchy's Theorem. Then $G/\langle\alpha\rangle$ has a subgroup $H/\langle\alpha\rangle$ of order m/p, and H is therefore a subgroup of G of order m. □

Lemma 3.5. If H is a subgroup of a finite abelian group G, and $|H| \mid m \mid |G|$, then there exists $K \leqslant G$ such that $H \leqslant K \leqslant G$ and $|K| = m$.

Proof. Consider G/H, and note that

$$\tfrac{m}{|H|} \mid \tfrac{|G|}{|H|} = \mid G/H \mid .$$

By Lemma 3.4, there must exist a subgroup of G/H with order $\frac{m}{|H|}$. Call this group K/H. Then the group K has order m, and $H \leqslant K \leqslant G$. □

Example 7. Let $d = 2$. Note that $3, 5 \equiv 1 \pmod 2$. So $n = 15$, and

$$(\mathbb{Z}/15\mathbb{Z})^{\times} = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Subgroups of $(\mathbb{Z}/15\mathbb{Z})^{\times}$ of index 2 are

$$G_{\alpha_1} = \{1, 2, 4, 8\},$$
$$G_{\alpha_2} = \{1, 4, 7, 13\}, \text{ and}$$

$$G_{\alpha_3} = \{1, 4, 11, 14\}.$$

Note that $(\mathbb{Z}/15\mathbb{Z})^\times = G_{\alpha_1} \cup G_{\alpha_2} \cup G_{\alpha_3}$. Thus, for all primes p except 3 and 5, $[p] \in G_{\alpha_1} \cup G_{\alpha_2} \cup G_{\alpha_3}$. In this way, we can think of the G_{α_i} "covering" all but finitely many primes. We would like to ensure that we can find such a collection of groups for any degree d.

Lemma 3.6. Let $d \geq 2$. There exists an $n \in \mathbb{N}$ such that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the union of all subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$ of index d.

Proof. Let q, r be distinct prime numbers such that $q \equiv 1 \pmod{d}$ and $r \equiv 1 \pmod{d}$. Such primes are guaranteed to exist by Dirichlet's Theorem on primes in arithmetic progressions. Let $n = qr$. By the Chinese Remainder Theorem,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$

Thus

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/r\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/(r-1)\mathbb{Z}. \tag{3.2}$$

Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. We aim to construct a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ of index d that contains a. By (3.2), $\operatorname{ord}(a) \mid \operatorname{lcm}(q-1, r-1)$, where $\operatorname{ord}(a)$ is the smallest positive integer m such that $a^m \equiv 1 \pmod{n}$. Since $d \mid q-1$ and $d \mid r-1$,

$$d \mid \gcd(q-1, r-1) = \tfrac{(q-1)(r-1)}{\operatorname{lcm}(q-1, r-1)}.$$

Therefore, $\frac{(q-1)(r-1)}{d} \in \mathbb{Z}$, and we have

$$\operatorname{ord}(a) \mid \frac{(q-1)(r-1)}{d} \mid (q-1)(r-1).$$

By Lemma 3.5, there is a group G such that $\langle a \rangle \leqslant G \leqslant (\mathbb{Z}/n\mathbb{Z})^\times$ with $|G| = \frac{(q-1)(r-1)}{d}$, and thus $[(\mathbb{Z}/n\mathbb{Z})^\times : G] = d$. □

We now reivew the basic Galois theory of cyclotomic extensions. See [DF04, Chapter 14, Theorem 26] for more details. Let $n \geq 3$, and let ζ_n be a primitive n^{th}

root of unity. Then $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ via the isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$
$$[i] \mapsto \sigma_i$$

where $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ characterized by $\sigma_i(\zeta_n) = \zeta_n^i$.

Definition. Let $d \geq 1$ be an integer, and n be as described in Lemma 3.6. Let $\alpha \in \mathbb{Q}(\zeta_n)$, with $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. We define G_α and A_α as follows:

$$G_\alpha = \{[i] \in (\mathbb{Z}/n\mathbb{Z})^\times \mid \sigma_i(\alpha) = \alpha\}, \text{ and}$$
$$A_\alpha = \{i \in \mathbb{Z} \mid [i] \in G_\alpha\}.$$

Figure 3.1 shows the Galois correspondence of subfields of $\mathbb{Q}(\zeta_n)$ of degree d with subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$ of index d.

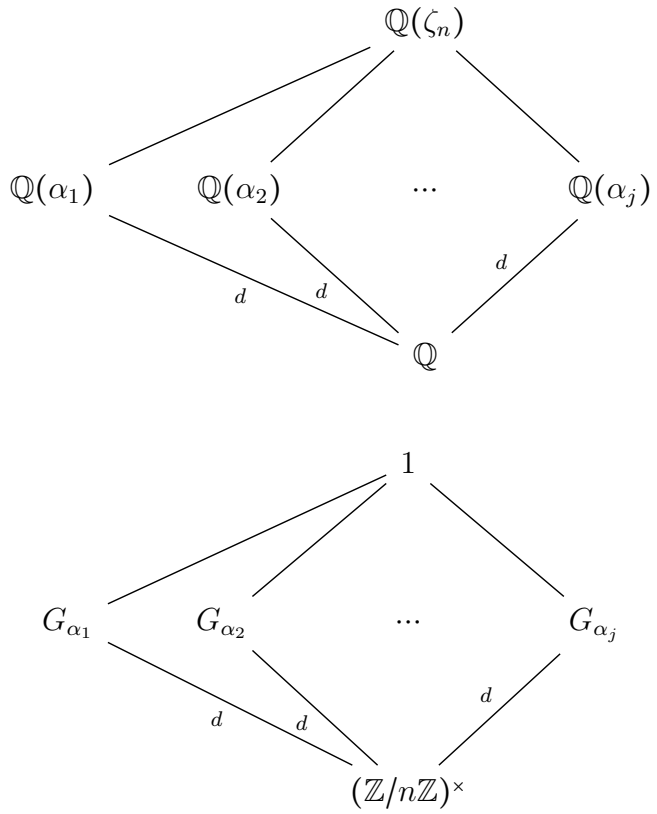

FIGURE 3.1: Galois Correspondence of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ with $(\mathbb{Z}/n\mathbb{Z})^\times$

The following lemma is well known, but for lack of a convenient reference, we provide a proof.

Lemma 3.7. Let $\alpha \in \mathbb{Q}(\zeta_n)$ have minimal polynomial $f_\alpha \in \mathbb{Z}[x]$, and let

$$G_\alpha = \{[i] \in (\mathbb{Z}/n\mathbb{Z})^\times \mid \sigma_i(\alpha) = \alpha\}.$$

Thus G_α is the subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ corresponding to $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\alpha))$ via the isomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let $p \nmid n$ be a prime. Then f_α splits completely in $\mathbb{Q}_p$ if and only if $[p] \in G_\alpha$.

Proof. The automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ satisfies $\sigma_p(x) \equiv x \pmod{p}$ for all $x \in \mathbb{Z}[\zeta_n]$ [Bak06, Lemma 4.51]. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an abelian extension, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension and therefore σ_p restricts to an automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$; the above congruence implies that σ_p is the Frobenius element of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ associated to the prime p.

If $[p] \in G_\alpha$, then σ_p is the identity element of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$, which implies that p splits completely in $\mathbb{Q}(\alpha)$ [Bak06, Proposition 4.36]; that is $p\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathfrak{p}_1 \dots \mathfrak{p}_d$, where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. It follows that each local degree $e(\mathfrak{p}_i/p)f(\mathfrak{p}_i/p) = [\mathbb{Q}(\alpha)_{\mathfrak{p}_i} : \mathbb{Q}_p]$ is equal to 1 [Bak06, Theorem 5.25], which means that $\mathbb{Q}(\alpha)_{\mathfrak{p}_i} = \mathbb{Q}_p$ for $i = 1, 2, \dots, d$. In particular, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}_p$, and therefore as $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, all d of the Galois conjugates of α are in $\mathbb{Q}_p$ as well. Hence $f_\alpha(x)$ splits completely in $\mathbb{Q}_p$. The converse follows from a straightforward reversal of this argument. □

Remark. By Lemma 3.7, for each prime $p \nmid n$, p splits completely in $\mathbb{Q}(\alpha)$ if and only if $p \in G_\alpha$.

Theorem 3.8. Let $d \geq 2$ be an integer. Then there exists a constant C_d such that for each prime p, there exists $\alpha \in \mathcal{T}_p^{\mathrm{ab}}$ of degree d and height $h(\alpha) \leq C_d$. In particular, $\tau_{d,p}^{\mathrm{ab}} \leq C_d$ for all primes p.

Proof. Let $d \geq 2$ be an integer. For primes $q, r \equiv 1 \pmod{d}$, we fix $n = qr$. By Lemma 3.6,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \bigcup_{\substack{G_i \leqslant (\mathbb{Z}/n\mathbb{Z})^\times \\ [(\mathbb{Z}/n\mathbb{Z})^\times : G_i] = d}} G_i.$$

Let $[p]$ denote the reduction of $p \pmod{n}$. Let p be a prime with $[p] \in G_1$, and let K_1 be the fixed field of the subset of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ that corresponds to G_1. By the primitive element theorem, there exists some $\alpha_1 \in K_1$ so that $\mathbb{Q}(\alpha_1) = K_1$. Moreover, we can choose a primitive element α_1 that is not a root of unity. This follows from the observation that, in the standard proof of the Primitive Element Theorem [Mil17, Theorem 5.1], any finite separable extension of infinite fields actually has infinitely many primitive elements, but a number field contains only finitely many roots of unity.

Let f_{α_1} be the minimal polynomial for α_1. By Lemma 3.7, since p splits completely in K_1, α_1 is totally p-adic. Let $h_1 = h(\alpha_1)$. Then $\tau_{d,p}^{\mathrm{ab}} \leq h_1$. Repeating this process for all G_i, we obtain a finite list of heights, $h_1, h_2, \ldots, h_l$. Thus, for $p \neq q, r$,

$$\tau_{d,p}^{\mathrm{ab}} \leq \max\{h_1, h_2, \ldots, h_l\}.$$

We repeat this argument for $n' = q'r'$, where $q', r' \equiv 1 \pmod{d}$ and q' and r' are distinct from n and q. Thus we may deduce that $\tau_{d,q}^{\mathrm{ab}}$ and $\tau_{d,r}^{\mathrm{ab}}$ are finite, and that for all primes p,

$$\tau_{d,p}^{\mathrm{ab}} \leq \max\{h_1, h_2, \ldots, h_l, \tau_{d,q}^{\mathrm{ab}}, \tau_{d,r}^{\mathrm{ab}}\} = C_d. \qquad \square$$

Remark. For $d \geq 2$ and prime p, Theorem 3.8 implies the finiteness of $\tau_{d,p}$ since $\tau_{d,p} \leq \tau_{d,p}^{\mathrm{ab}}$. This provides an alternate proof of Proposition 3.1.

Corollary 3.9. For each $d \geq 2$, $\{\tau_{d,p} \mid p \text{ is a prime}\}$ is bounded.

Proof. Note that $\tau_{d,p} \leq \tau_{d,p}^{\mathrm{ab}}$, since $\tau_{d,p}^{\mathrm{ab}}$ considers only abelian algebraic numbers. Thus, since $\{\tau_{d,p}^{\mathrm{ab}} \mid p \text{ is a prime}\}$ is bounded, so must $\{\tau_{d,p} \mid p \text{ is a prime}\}$ be. $\square$

Definition. Let $\alpha \in \mathbb{Q}^{\text{ab}}$ and $K = \mathbb{Q}(\alpha)$. By the Kronecker-Weber Theorem, K is contained within a cyclotomic extension of $\mathbb{Q}$. The **conductor** of K is the smallest positive integer m for which K is contained within $\mathbb{Q}(\zeta_m)$.

Remark. Let $\alpha \in \mathbb{Q}^{\text{ab}}$ and m be the conductor of $\mathbb{Q}(\alpha)$. H_α and B_α will now play the roles of G_α and A_α, only now with the modulus being the conductor instead of the n described in Lemma 3.6. That is,

$$H_\alpha = \{[i] \in (\mathbb{Z}/m\mathbb{Z})^\times \mid \sigma_i(\alpha) = \alpha\}, \text{ and}$$
$$B_\alpha = \{i \in \mathbb{Z} \mid [i] \in H_\alpha\}.$$

Theorem 3.10. Let $d \geq 2$ and let $\alpha_1, \alpha_2, \ldots$ be an enumeration of all $\alpha \in \mathcal{T}_p^{\text{ab}}$ of degree d, written in order of nondecreasing height $h(\alpha_1) \leq h(\alpha_2) \leq \ldots$. Let m_i denote the conductor of $\mathbb{Q}(\alpha_i)$.

(a) There exists an integer $k \geq 1$ such that $\bigcup_{i=1}^{k} B_{\alpha_i}$ contains all primes p not dividing any of the conductors $m_1, \ldots, m_k$.

(b) Let $k \geq 1$ be the smallest positive integer satisfying **(a)**, and let

$$N_d = \text{lcm}(m_1, \ldots, m_k).$$

Then $\tau_{d,p}^{\text{ab}}$ depends only on $p \pmod{N_d}$.

Proof. **(a)** It follows from Northcott's Theorem that such an enumeration exists and that $h(\alpha_i) \to \infty$ as $i \to \infty$. By Theorem 3.8 there exists some $k \geq 1$ such that

$$\{\alpha_1, \ldots, \alpha_k\} = \left\{\alpha \in \mathbb{Q}^{\text{ab}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] = d \text{ and } h(\alpha_i) \leq C_d\right\}$$

where C_d is as established in Theorem 3.8. It follows from Theorem 3.8 that $\bigcup_{i=1}^{k} B_{\alpha_i}$ contains all prime numbers not dividing the conductors $m_1, \ldots m_k$.

(b) Suppose p and p' are two primes such that $p \equiv p' \pmod{N_d}$. Then for each $1 \leq i \leq k$, we know that $p \equiv p' \pmod{m_i}$ and so p splits completely in $\mathbb{Q}(\alpha_i)$ if and

only if p' splits completely in $\mathbb{Q}(\alpha_i)$. Let i_0 be the smallest index i for which p splits completely in $\mathbb{Q}(\alpha_i)$. Since i_0 is also the smallest index for which p' splits completely in $\mathbb{Q}(\alpha_i)$, we have

$$h(\alpha_{i_0}) = \tau_{d,p}^{\mathrm{ab}} = \tau_{d,p'}^{\mathrm{ab}}.$$

If p is a prime with $p \mid m_i$ for some $1 \leq i \leq k$, then p is the only prime in the congruence class $p \pmod{N_d}$. $\square$

3.3 Determining N_2

As an alternative to Theorem 3.3, we use Theorem 3.10 to determine N_2. We begin by creating a list of degree 2 algebraic numbers with $h(\alpha) \leq \frac{1}{2}\log 2$.

TABLE 3.1: Degree 2 Algebraic Numbers of Small Height

i	α_i	$h(\alpha_i)$	m_i	B_{α_i} is the union of	α_i totally p-adic iff
$1,2,3,4$	$\frac{\pm 1 \pm \sqrt{5}}{2}$	$\frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right)$	5	$1 \pmod 5, 4 \pmod 5$	$p \equiv 1,4 \pmod 5$
$5,6$	$\pm\sqrt{2}$	$\frac{1}{2}\log 2$	8	$1 \pmod 8, 7 \pmod 8$	$p \equiv 1,7 \pmod 8$
$7,8$	$\pm i\sqrt{2}$	$\frac{1}{2}\log 2$	8	$1 \pmod 8, 3 \pmod 8$	$p \equiv 1,3 \pmod 8$
$9,10$	$\pm 1 \pm i$	$\frac{1}{2}\log 2$	4	$1 \pmod 4$	$p \equiv 1 \pmod 4$, or $p = 2$

Observe that

$$\begin{aligned}\bigcup_{i=1}^{10} B_{\alpha_i} &= \{\text{primes } p \mid p \equiv 1,4 \pmod 5, p \equiv 1,3,5,7 \pmod 8, \text{ or } p = 2\} \\ &= \{\text{all primes}\}.\end{aligned}$$

Since $(\mathbb{Z}/8\mathbb{Z})^\times = \{1,3,5,7\}$ and $2 \in B_{1+i}$, by Theorem 3.10

$$N_2 = \operatorname{lcm}(5,8) = 40.$$

In Theorem 3.3, we found that $\tau_{2,p}^{\mathrm{ab}}$ depends only on the reduction of p modulo 5, and yet by applying Theorem 3.10 we obtain $N_2 = 40$. It is worth noting that with Theorem 3.10, we are not guaranteed to find the smallest such modulus.

3.4 Determining N_3

We begin by using SAGE [The18] to run the code found in Appendix A, which creates a list of all irreducible, cubic polynomials in $\mathbb{Z}[x]$ with Mahler measure bounded above by 8.5 and stores the list in ascending order of Mahler measure. Theorem 3.13 verifies that this list is sufficient to determine N_3.

If the determinant of a polynomial of degree n is a perfect square in $\mathbb{Q}$, then the Galois group of that polynomial is a subgroup of A_n. The Galois group of a cubic polynomial f_α is either S_3 or A_3. S_3 is not an abliean group. A_3 is the cyclic group of order 3 and is abelian. Thus, the roots of f_α in $\mathbb{Z}[x]$ are contained in an abelian extension of $\mathbb{Q}$ if and only if the discriminant of f_α is a perfect square in $\mathbb{Q}$.

Let K be the number field created by adjoining the roots of f_α to $\mathbb{Q}$, Δ be the discriminant of K, and let m be the conductor of K. The code in Appendix B extracts from the list created above all polynomials with abelian roots, calculates Δ, m, and the cyclic decomposition of $(\mathbb{Z}/m\mathbb{Z})^\times$. Table 3.2 contains the complete results of this process. To calculate the conductor, we turn to a special case of the Hasse Conductor-Discriminant formula, as follows.

Theorem 3.11. [Has30, Theorem 6] Let K be an abelian extension of $\mathbb{Q}$, with $[K : \mathbb{Q}] = 3$ and discriminant Δ. Let $p_1, p_2, \ldots, p_n$ be all the primes (aside from 3) that divide Δ. If 3 divides Δ, then the conductor of K is $9p_1p_2 \ldots p_n$. If 3 not does divide Δ, then the conductor of K is $p_1p_2 \ldots p_n$.

TABLE 3.2: Irreducible Cubic Polynomials with Abelian Galois Group and Mahler Measure ≤ 8.5

$h(\alpha_i)$	f_{α_i}	Δ_i	m_i	$(\mathbb{Z}/m_i\mathbb{Z})^\times$
0.2698623053	$x^3 - 2\,x^2 - x + 1$	49	7	C_6
0.2698623053	$x^3 - x^2 - 2\,x + 1$	49	7	C_6
				Continued on next page

TABLE 3.2 – continued from previous page

$h(\alpha_i)$	f_{α_i}	Δ_i	m_i	$(\mathbb{Z}/m_i\mathbb{Z})^\times$
0.2698623053	$x^3 + x^2 - 2\,x - 1$	49	7	C_6
0.2698623053	$x^3 + 2\,x^2 - x - 1$	49	7	C_6
0.3525256045	$x^3 - 3\,x^2 + 1$	81	9	C_6
0.3525256045	$x^3 - 3\,x - 1$	81	9	C_6
0.3525256045	$x^3 - 3\,x + 1$	81	9	C_6
0.3525256045	$x^3 + 3\,x^2 - 1$	81	9	C_6
0.4090481645	$x^3 - 3\,x^2 + 3$	81	9	C_6
0.4090481645	$x^3 + 3\,x^2 - 3$	81	9	C_6
0.4090481645	$3\,x^3 - 3\,x - 1$	81	9	C_6
0.4090481645	$3\,x^3 - 3\,x + 1$	81	9	C_6
0.4316755623	$x^3 - 4\,x^2 + x + 1$	169	13	C_{12}
0.4316755623	$x^3 - x^2 - 4\,x - 1$	169	13	C_{12}
0.4316755623	$x^3 + x^2 - 4\,x + 1$	169	13	C_{12}
0.4316755623	$x^3 + 4\,x^2 + x - 1$	169	13	C_{12}
0.4661498406	$x^3 - 4\,x^2 + 3\,x + 1$	49	7	C_6
0.4661498406	$x^3 - 3\,x^2 - 4\,x - 1$	49	7	C_6
0.4661498406	$x^3 + 3\,x^2 - 4\,x + 1$	49	7	C_6
0.4661498406	$x^3 + 4\,x^2 + 3\,x - 1$	49	7	C_6
0.5009113655	$2\,x^3 - 4\,x^2 - 2\,x + 2$	49	7	C_6
0.5009113655	$2\,x^3 - 2\,x^2 - 4\,x + 2$	49	7	C_6
0.5009113655	$2\,x^3 + 2\,x^2 - 4\,x - 2$	49	7	C_6
0.5009113655	$2\,x^3 + 4\,x^2 - 2\,x - 2$	49	7	C_6
0.5018786268	$x^3 - 5\,x^2 + 2\,x + 1$	361	19	C_{18}
0.5018786268	$x^3 - 2\,x^2 - 5\,x - 1$	361	19	C_{18}
0.5018786268	$x^3 + 2\,x^2 - 5\,x + 1$	361	19	C_{18}

Continued on next page

TABLE 3.2 – continued from previous page

$h(\alpha_i)$	f_{α_i}	Δ_i	m_i	$(\mathbb{Z}/m_i\mathbb{Z})^\times$
0.5018786268	$x^3+5\,x^2+2\,x-1$	361	19	C_{18}
0.5364793041	$x^3-2\,x^2-3\,x+5$	169	13	C_{12}
0.5364793041	$x^3+2\,x^2-3\,x-5$	169	13	C_{12}
0.5364793041	$5\,x^3-3\,x^2-2\,x+1$	169	13	C_{12}
0.5364793041	$5\,x^3+3\,x^2-2\,x-1$	169	13	C_{12}
0.5397246107	$x^3-6\,x^2+5\,x-1$	49	7	C_6
0.5397246107	$x^3-5\,x^2+6\,x-1$	49	7	C_6
0.5397246107	$x^3+5\,x^2+6\,x+1$	49	7	C_6
0.5397246107	$x^3+6\,x^2+5\,x+1$	49	7	C_6
0.5420244156	$2\,x^3-5\,x^2-x+2$	961	31	C_{30}
0.5420244156	$2\,x^3-x^2-5\,x+2$	961	31	C_{30}
0.5420244156	$2\,x^3+x^2-5\,x-2$	961	31	C_{30}
0.5420244156	$2\,x^3+5\,x^2-x-2$	961	31	C_{30}
0.5628405126	$x^3-6\,x^2+3\,x+1$	81	9	C_6
0.5628405126	$x^3-3\,x^2-6\,x-1$	81	9	C_6
0.5628405126	$x^3+3\,x^2-6\,x+1$	81	9	C_6
0.5628405126	$x^3+6\,x^2+3\,x-1$	81	9	C_6
0.5835746647	$2\,x^3-6\,x^2+2$	81	9	C_6
0.5835746647	$2\,x^3-6\,x-2$	81	9	C_6
0.5835746647	$2\,x^3-6\,x+2$	81	9	C_6
0.5835746647	$2\,x^3+6\,x^2-2$	81	9	C_6
0.5988214758	$x^3-6\,x^2-x+5$	169	13	C_{12}
0.5988214758	$x^3+6\,x^2-x-5$	169	13	C_{12}
0.5988214758	$5\,x^3-x^2-6\,x+1$	169	13	C_{12}
0.5988214758	$5\,x^3+x^2-6\,x-1$	169	13	C_{12}

Continued on next page

TABLE 3.2 – continued from previous page

$h(\alpha_i)$	f_{α_i}	Δ_i	m_i	$(\mathbb{Z}/m_i\mathbb{Z})^\times$
0.6098176693	$3\,x^3 - 5\,x^2 - 4\,x + 3$	3721	61	C_{60}
0.6098176693	$3\,x^3 - 4\,x^2 - 5\,x + 3$	3721	61	C_{60}
0.6098176693	$3\,x^3 + 4\,x^2 - 5\,x - 3$	3721	61	C_{60}
0.6098176693	$3\,x^3 + 5\,x^2 - 4\,x - 3$	3721	61	C_{60}
0.6158739226	$x^3 - 7\,x^2 + 4\,x + 1$	1369	37	C_{36}
0.6158739226	$x^3 - 4\,x^2 - 7\,x - 1$	1369	37	C_{36}
0.6158739226	$x^3 + 4\,x^2 - 7\,x + 1$	1369	37	C_{36}
0.6158739226	$x^3 + 7\,x^2 + 4\,x - 1$	1369	37	C_{36}
0.6193630725	$x^3 - 6\,x^2 + 9\,x - 3$	81	9	C_6
0.6193630725	$x^3 + 6\,x^2 + 9\,x + 3$	81	9	C_6
0.6193630725	$3\,x^3 - 9\,x^2 + 6\,x - 1$	81	9	C_6
0.6193630725	$3\,x^3 + 9\,x^2 + 6\,x + 1$	81	9	C_6
0.6241036381	$2\,x^3 - 7\,x^2 + x + 2$	1849	43	C_{42}
0.6241036381	$2\,x^3 - x^2 - 7\,x - 2$	1849	43	C_{42}
0.6241036381	$2\,x^3 + x^2 - 7\,x + 2$	1849	43	C_{42}
0.6241036381	$2\,x^3 + 7\,x^2 + x - 2$	1849	43	C_{42}
0.6360664016	$3\,x^3 - 6\,x^2 - 3\,x + 3$	49	7	C_6
0.6360664016	$3\,x^3 - 3\,x^2 - 6\,x + 3$	49	7	C_6
0.6360664016	$3\,x^3 + 3\,x^2 - 6\,x - 3$	49	7	C_6
0.6360664016	$3\,x^3 + 6\,x^2 - 3\,x - 3$	49	7	C_6
0.6400972247	$2\,x^3 - 6\,x^2 + 6$	81	9	C_6
0.6400972247	$2\,x^3 + 6\,x^2 - 6$	81	9	C_6
0.6400972247	$6\,x^3 - 6\,x - 2$	81	9	C_6
0.6400972247	$6\,x^3 - 6\,x + 2$	81	9	C_6
0.6486367163	$x^3 - x^2 - 6\,x + 7$	361	19	C_{18}

Continued on next page

TABLE 3.2 – continued from previous page

$h(\alpha_i)$	f_{α_i}	Δ_i	m_i	$(\mathbb{Z}/m_i\mathbb{Z})^\times$
0.6486367163	$x^3 + x^2 - 6\,x - 7$	361	19	C_{18}
0.6486367163	$7\,x^3 - 6\,x^2 - x + 1$	361	19	C_{18}
0.6486367163	$7\,x^3 + 6\,x^2 - x - 1$	361	19	C_{18}
0.6486367163	$x^3 - 7\,x - 7$	49	7	C_6
0.6486367163	$x^3 - 7\,x + 7$	49	7	C_6
0.6486367163	$7\,x^3 - 7\,x^2 + 1$	49	7	C_6
0.6486367163	$7\,x^3 + 7\,x^2 - 1$	49	7	C_6
0.6622071408	$x^3 - 6\,x^2 - 9\,x - 3$	81	9	C_6
0.6622071408	$x^3 + 6\,x^2 - 9\,x + 3$	81	9	C_6
0.6622071408	$3\,x^3 - 9\,x^2 + 6\,x + 1$	81	9	C_6
0.6622071408	$3\,x^3 + 9\,x^2 + 6\,x - 1$	81	9	C_6
0.6624373759	$x^3 - 8\,x^2 + 5\,x + 1$	49	7	C_6
0.6624373759	$x^3 - 5\,x^2 - 8\,x - 1$	49	7	C_6
0.6624373759	$x^3 + 5\,x^2 - 8\,x + 1$	49	7	C_6
0.6624373759	$x^3 + 8\,x^2 + 5\,x - 1$	49	7	C_6
0.6627246225	$2\,x^3 - 8\,x^2 + 2\,x + 2$	169	13	C_{12}
0.6627246225	$2\,x^3 - 2\,x^2 - 8\,x - 2$	169	13	C_{12}
0.6627246225	$2\,x^3 + 2\,x^2 - 8\,x + 2$	169	13	C_{12}
0.6627246225	$2\,x^3 + 8\,x^2 + 2\,x - 2$	169	13	C_{12}
0.6633392513	$3\,x^3 - 7\,x^2 - 2\,x + 3$	4489	67	C_{66}
0.6633392513	$3\,x^3 - 2\,x^2 - 7\,x + 3$	4489	67	C_{66}
0.6633392513	$3\,x^3 + 2\,x^2 - 7\,x - 3$	4489	67	C_{66}
0.6633392513	$3\,x^3 + 7\,x^2 - 2\,x - 3$	4489	67	C_{66}
0.6663004651	$2\,x^3 - 7\,x^2 + 3\,x + 4$	961	31	C_{30}
0.6663004651	$2\,x^3 + 7\,x^2 + 3\,x - 4$	961	31	C_{30}

Continued on next page

TABLE 3.2 – continued from previous page

$h(\alpha_i)$	f_{α_i}	Δ_i	m_i	$(\mathbb{Z}/m_i\mathbb{Z})^\times$
0.6663004651	$4\,x^3 - 3\,x^2 - 7\,x - 2$	961	31	C_{30}
0.6663004651	$4\,x^3 + 3\,x^2 - 7\,x + 2$	961	31	C_{30}
0.6696162679	$x^3 - 7\,x^2 + 7$	49	7	C_6
0.6696162679	$x^3 + 7\,x^2 - 7$	49	7	C_6
0.6696162679	$7\,x^3 - 7\,x - 1$	49	7	C_6
0.6696162679	$7\,x^3 - 7\,x + 1$	49	7	C_6
0.6795133581	$x^3 - 5\,x^2 + 4\,x + 5$	169	13	C_{12}
0.6795133581	$x^3 + 5\,x^2 + 4\,x - 5$	169	13	C_{12}
0.6795133581	$5\,x^3 - 4\,x^2 - 5\,x - 1$	169	13	C_{12}
0.6795133581	$5\,x^3 + 4\,x^2 - 5\,x + 1$	169	13	C_{12}
0.6910644552	$3\,x^3 - 8\,x^2 - x + 3$	5329	73	C_{72}
0.6910644552	$3\,x^3 - x^2 - 8\,x + 3$	5329	73	C_{72}
0.6910644552	$3\,x^3 + x^2 - 8\,x - 3$	5329	73	C_{72}
0.6910644552	$3\,x^3 + 8\,x^2 - x - 3$	5329	73	C_{72}
0.6931471806	$x^3 - 6\,x^2 + 8$	81	9	C_6
0.6931471806	$x^3 + 6\,x^2 - 8$	81	9	C_6
0.6931471806	$x^3 - 4\,x^2 - 4\,x + 8$	49	7	C_6
0.6931471806	$x^3 + 4\,x^2 - 4\,x - 8$	49	7	C_6
0.6931471806	$x^3 - 5\,x^2 - 2\,x + 8$	961	31	C_{30}
0.6931471806	$x^3 + 5\,x^2 - 2\,x - 8$	961	31	C_{30}
0.6931471806	$8\,x^3 + 2\,x^2 - 5\,x - 1$	961	31	C_{30}
0.6931471806	$8\,x^3 - 2\,x^2 - 5\,x + 1$	961	31	C_{30}
0.6931471806	$2\,x^3 - 5\,x^2 - 3\,x + 8$	1849	43	C_{42}
0.6931471806	$2\,x^3 + 5\,x^2 - 3\,x - 8$	1849	43	C_{42}
0.6931471806	$8\,x^3 - 3\,x^2 - 5\,x + 2$	1849	43	C_{42}

Continued on next page

TABLE 3.2 – continued from previous page

$h(\alpha_i)$	f_{α_i}	Δ_i	m_i	$(\mathbb{Z}/m_i\mathbb{Z})^\times$
0.6931471806	$8\,x^3+3\,x^2-5\,x-2$	1849	43	C_{42}
0.6931471806	$8\,x^3-6\,x-1$	81	9	C_6
0.6931471806	$8\,x^3-6\,x+1$	81	9	C_6
0.6931471806	$8\,x^3-4\,x^2-4\,x+1$	49	7	C_6
0.6931471806	$8\,x^3+4\,x^2-4\,x-1$	49	7	C_6
0.6943241113	$x^3-7\,x^2+12\,x-5$	169	13	C_{12}
0.6943241113	$x^3+7\,x^2+12\,x+5$	169	13	C_{12}
0.6943241113	$5\,x^3-12\,x^2+7\,x-1$	169	13	C_{12}
0.6943241113	$5\,x^3+12\,x^2+7\,x+1$	169	13	C_{12}
0.6971989008	$2\,x^3-8\,x^2+6\,x+2$	49	7	C_6
0.6971989008	$2\,x^3-6\,x^2-8\,x-2$	49	7	C_6
0.6971989008	$2\,x^3+6\,x^2-8\,x+2$	49	7	C_6
0.6971989008	$2\,x^3+8\,x^2+6\,x-2$	49	7	C_6
0.6990306738	$2\,x^3-9\,x^2+3\,x+2$	3969	63	$C_6\times C_6$
0.6990306738	$2\,x^3-3\,x^2-9\,x-2$	3969	63	$C_6\times C_6$
0.6990306738	$2\,x^3+3\,x^2-9\,x+2$	3969	63	$C_6\times C_6$
0.6990306738	$2\,x^3+9\,x^2+3\,x-2$	3969	63	$C_6\times C_6$
0.7037615930	$x^3-9\,x^2+6\,x+1$	3969	63	$C_6\times C_6$
0.7037615930	$x^3-6\,x^2-9\,x-1$	3969	63	$C_6\times C_6$
0.7037615930	$x^3+6\,x^2-9\,x+1$	3969	63	$C_6\times C_6$
0.7037615930	$x^3+9\,x^2+6\,x-1$	3969	63	$C_6\times C_6$
0.7050512090	$x^3-9\,x^2+6\,x-1$	81	9	C_6
0.7050512090	$x^3-6\,x^2+9\,x-1$	81	9	C_6
0.7050512090	$x^3+6\,x^2+9\,x+1$	81	9	C_6
0.7050512090	$x^3+9\,x^2+6\,x+1$	81	9	C_6

Continued on next page

TABLE 3.2 – continued from previous page

$h(\alpha_i)$	f_{α_i}	Δ_i	m_i	$(\mathbb{Z}/m_i\mathbb{Z})^\times$
0.7121464707	$4\,x^3 - 7\,x^2 - 5\,x + 4$	11881	109	C_{108}
0.7121464707	$4\,x^3 - 5\,x^2 - 7\,x + 4$	11881	109	C_{108}
0.7121464707	$4\,x^3 + 5\,x^2 - 7\,x - 4$	11881	109	C_{108}
0.7121464707	$4\,x^3 + 7\,x^2 - 5\,x - 4$	11881	109	C_{108}

For each polynomial f_{α_i} in Table 3.2, we run the code contained in Appendix C to determine the congruence classes modulo m_i on a prime p for f_{α_i} to split completely in $\mathbb{Q}_p$. When $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic, the congruence classes are the unique index 3 subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$. When $(\mathbb{Z}/m\mathbb{Z})^\times$ is not cyclic, there may be more than one index 3 subgroup.

If $(\mathbb{Z}/m\mathbb{Z})^\times$ is not cyclic, the code checks the first 200 primes to determine if there is a root in $\mathbb{Q}_p$ via Hensel's Lemma. When a root of f_α is determined to be in $\mathbb{Q}_p$, we know that for all primes q with $q \equiv p \pmod{m}$, f_α must have a root in $\mathbb{Q}_p$, by Lemma 3.7. We know there are $\frac{|(\mathbb{Z}/m\mathbb{Z})^\times|}{3}$ congruence classes for which f_α has a root in $\mathbb{Q}_p$. Thus, after testing the first 200 primes, the code checks the cardinality of the set of congruences to ensure all were found. Note that the code only checks for one root via Hensel's Lemma. The following Lemma establishes that showing one root is within $\mathbb{Q}_p$ is sufficient to guarantee all roots are in $\mathbb{Q}_p$.

Lemma 3.12. Let α be an abelian algebraic number of degree 3 with Galois conjugates β and γ. If $\alpha \in \mathbb{Q}_p$ for a prime p, then $\beta, \gamma \in \mathbb{Q}_p$ as well.

Proof. Since $\alpha \in \mathbb{Q}_p$, $\mathbb{Q}(\alpha) \subset \mathbb{Q}_p$. As $\alpha \in K$ for K abelian, $\mathbb{Q}(\alpha)$ is Galois, so $\beta, \gamma \in \mathbb{Q}(\alpha)$ and thus $\beta, \gamma \in \mathbb{Q}_p$. □

For each polynomial f_{α_i} in Table 3.2, Table 3.3 contains the congruence classes modulo m_i for which f_{α_i} will split completely over $\mathbb{Q}_p$.

TABLE 3.3: Abelian Cubic Polynomials and Congruence Classes $\pmod{m_i}$ for Splitting over $\mathbb{Q}_p$

$h(\alpha_i)$	f_{α_i}	α_i is totally p-adic iff
0.2698623053	$x^3 - 2x^2 - x + 1$	$p \equiv 1, 6 \pmod 7$
0.2698623053	$x^3 - x^2 - 2x + 1$	$p \equiv 1, 6 \pmod 7$
0.2698623053	$x^3 + x^2 - 2x - 1$	$p \equiv 1, 6 \pmod 7$
0.2698623053	$x^3 + 2x^2 - x - 1$	$p \equiv 1, 6 \pmod 7$
0.3525256045	$x^3 - 3x^2 + 1$	$p \equiv 1, 8 \pmod 9$
0.3525256045	$x^3 - 3x - 1$	$p \equiv 1, 8 \pmod 9$
0.3525256045	$x^3 - 3x + 1$	$p \equiv 1, 8 \pmod 9$
0.3525256045	$x^3 + 3x^2 - 1$	$p \equiv 1, 8 \pmod 9$
0.4090481645	$x^3 - 3x^2 + 3$	$p \equiv 1, 8 \pmod 9$
0.4090481645	$x^3 + 3x^2 - 3$	$p \equiv 1, 8 \pmod 9$
0.4090481645	$3x^3 - 3x - 1$	$p \equiv 1, 8 \pmod 9$
0.4090481645	$3x^3 - 3x + 1$	$p \equiv 1, 8 \pmod 9$
0.4316755623	$x^3 - 4x^2 + x + 1$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.4316755623	$x^3 - x^2 - 4x - 1$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.4316755623	$x^3 + x^2 - 4x + 1$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.4316755623	$x^3 + 4x^2 + x - 1$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.4661498406	$x^3 - 4x^2 + 3x + 1$	$p \equiv 1, 6 \pmod 7$
0.4661498406	$x^3 - 3x^2 - 4x - 1$	$p \equiv 1, 6 \pmod 7$
0.4661498406	$x^3 + 3x^2 - 4x + 1$	$p \equiv 1, 6 \pmod 7$
0.4661498406	$x^3 + 4x^2 + 3x - 1$	$p \equiv 1, 6 \pmod 7$
0.5009113655	$2x^3 - 4x^2 - 2x + 2$	$p \equiv 1, 6 \pmod 7$
0.5009113655	$2x^3 - 2x^2 - 4x + 2$	$p \equiv 1, 6 \pmod 7$

Continued on next page

TABLE 3.3 – continued from previous page

$h(\alpha_i)$	f_{α_i}	α_i is totally p-adic iff
0.5009113655	$2\,x^3+2\,x^2-4\,x-2$	$p \equiv 1,6 \pmod 7$
0.5009113655	$2\,x^3+4\,x^2-2\,x-2$	$p \equiv 1,6 \pmod 7$
0.5018786268	$x^3-5\,x^2+2\,x+1$	$p \equiv 1,7,8,11,12,18 \pmod{19}$
0.5018786268	$x^3-2\,x^2-5\,x-1$	$p \equiv 1,7,8,11,12,18 \pmod{19}$
0.5018786268	$x^3+2\,x^2-5\,x+1$	$p \equiv 1,7,8,11,12,18 \pmod{19}$
0.5018786268	$x^3+5\,x^2+2\,x-1$	$p \equiv 1,7,8,11,12,18 \pmod{19}$
0.5364793041	$x^3-2\,x^2-3\,x+5$	$p \equiv 1,5,8,12 \pmod{13}$
0.5364793041	$x^3+2\,x^2-3\,x-5$	$p \equiv 1,5,8,12 \pmod{13}$
0.5364793041	$5\,x^3-3\,x^2-2\,x+1$	$p \equiv 1,5,8,12 \pmod{13}$
0.5364793041	$5\,x^3+3\,x^2-2\,x-1$	$p \equiv 1,5,8,12 \pmod{13}$
0.5397246107	$x^3-6\,x^2+5\,x-1$	$p \equiv 1,6 \pmod 7$
0.5397246107	$x^3-5\,x^2+6\,x-1$	$p \equiv 1,6 \pmod 7$
0.5397246107	$x^3+5\,x^2+6\,x+1$	$p \equiv 1,6 \pmod 7$
0.5397246107	$x^3+6\,x^2+5\,x+1$	$p \equiv 1,6 \pmod 7$
0.5420244156	$2\,x^3-5\,x^2-x+2$	$p \equiv 1,2,4,8,15,16,23,27,29,30 \pmod{31}$
0.5420244156	$2\,x^3-x^2-5\,x+2$	$p \equiv 1,2,4,8,15,16,23,27,29,30 \pmod{31}$
0.5420244156	$2\,x^3+x^2-5\,x-2$	$p \equiv 1,2,4,8,15,16,23,27,29,30 \pmod{31}$
0.5420244156	$2\,x^3+5\,x^2-x-2$	$p \equiv 1,2,4,8,15,16,23,27,29,30 \pmod{31}$
0.5628405126	$x^3-6\,x^2+3\,x+1$	$p \equiv 1,8 \pmod 9$
0.5628405126	$x^3-3\,x^2-6\,x-1$	$p \equiv 1,8 \pmod 9$
0.5628405126	$x^3+3\,x^2-6\,x+1$	$p \equiv 1,8 \pmod 9$
0.5628405126	$x^3+6\,x^2+3\,x-1$	$p \equiv 1,8 \pmod 9$
0.5835746647	$2\,x^3-6\,x^2+2$	$p \equiv 1,8 \pmod 9$
0.5835746647	$2\,x^3-6\,x-2$	$p \equiv 1,8 \pmod 9$

Continued on next page

TABLE 3.3 – continued from previous page

$h(\alpha_i)$	f_{α_i}	α_i is totally p-adic iff
0.5835746647	$2\,x^3 - 6\,x + 2$	$p \equiv 1, 8 \pmod 9$
0.5835746647	$2\,x^3 + 6\,x^2 - 2$	$p \equiv 1, 8 \pmod 9$
0.5988214758	$x^3 - 6\,x^2 - x + 5$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.5988214758	$x^3 + 6\,x^2 - x - 5$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.5988214758	$5\,x^3 - x^2 - 6\,x + 1$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.5988214758	$5\,x^3 + x^2 - 6\,x - 1$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.6098176693	$3\,x^3 - 5\,x^2 - 4\,x + 3$	$p \equiv 1, 3, 8, 9, 11, 23, 27, 28, 37, 41, 50, 52, 53 \pmod{61}$
0.6098176693	$3\,x^3 - 4\,x^2 - 5\,x + 3$	$p \equiv 1, 3, 8, 9, 11, 23, 27, 28, 37, 41, 50, 52, 53 \pmod{61}$
0.6098176693	$3\,x^3 + 4\,x^2 - 5\,x - 3$	$p \equiv 1, 3, 8, 9, 11, 23, 27, 28, 37, 41, 50, 52, 53 \pmod{61}$
0.6098176693	$3\,x^3 + 5\,x^2 - 4\,x - 3$	$p \equiv 1, 3, 8, 9, 11, 23, 27, 28, 37, 41, 50, 52, 53 \pmod{61}$
0.6158739226	$x^3 - 7\,x^2 + 4\,x + 1$	$p \equiv 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36 \pmod{37}$
0.6158739226	$x^3 - 4\,x^2 - 7\,x - 1$	$p \equiv 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36 \pmod{37}$
0.6158739226	$x^3 + 4\,x^2 - 7\,x + 1$	$p \equiv 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36 \pmod{37}$
0.6158739226	$x^3 + 7\,x^2 + 4\,x - 1$	$p \equiv 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36 \pmod{37}$
0.6193630725	$x^3 - 6\,x^2 + 9\,x - 3$	$p \equiv 1, 8 \pmod 9$
0.6193630725	$x^3 + 6\,x^2 + 9\,x + 3$	$p \equiv 1, 8 \pmod 9$

Continued on next page

TABLE 3.3 – continued from previous page

$h(\alpha_i)$	f_{α_i}	α_i is totally p-adic iff
0.6193630725	$3\,x^3 - 9\,x^2 + 6\,x - 1$	$p \equiv 1, 8 \pmod 9$
0.6193630725	$3\,x^3 + 9\,x^2 + 6\,x + 1$	$p \equiv 1, 8 \pmod 9$
0.6241036381	$2\,x^3 - 7\,x^2 + x + 2$	$p \equiv 1, 2, 4, 8, 11, 16, 21, 22, 27, 39, 41 \pmod{43}$
0.6241036381	$2\,x^3 - x^2 - 7\,x - 2$	$p \equiv 1, 2, 4, 8, 11, 16, 21, 22, 27, 39, 41 \pmod{43}$
0.6241036381	$2\,x^3 + x^2 - 7\,x + 2$	$p \equiv 1, 2, 4, 8, 11, 16, 21, 22, 27, 39, 41 \pmod{43}$
0.6241036381	$2\,x^3 + 7\,x^2 + x - 2$	$p \equiv 1, 2, 4, 8, 11, 16, 21, 22, 27, 39, 41 \pmod{43}$
0.6360664016	$3\,x^3 - 6\,x^2 - 3\,x + 3$	$p \equiv 1, 6 \pmod 7$
0.6360664016	$3\,x^3 - 3\,x^2 - 6\,x + 3$	$p \equiv 1, 6 \pmod 7$
0.6360664016	$3\,x^3 + 3\,x^2 - 6\,x - 3$	$p \equiv 1, 6 \pmod 7$
0.6360664016	$3\,x^3 + 6\,x^2 - 3\,x - 3$	$p \equiv 1, 6 \pmod 7$
0.6400972247	$2\,x^3 - 6\,x^2 + 6$	$p \equiv 1, 8 \pmod 9$
0.6400972247	$2\,x^3 + 6\,x^2 - 6$	$p \equiv 1, 8 \pmod 9$
0.6400972247	$6\,x^3 - 6\,x - 2$	$p \equiv 1, 8 \pmod 9$
0.6400972247	$6\,x^3 - 6\,x + 2$	$p \equiv 1, 8 \pmod 9$
0.6486367163	$x^3 - x^2 - 6\,x + 7$	$p \equiv 1, 7, 8, 11, 12, 18 \pmod{19}$
0.6486367163	$x^3 + x^2 - 6\,x - 7$	$p \equiv 1, 7, 8, 11, 12, 18 \pmod{19}$
0.6486367163	$7\,x^3 - 6\,x^2 - x + 1$	$p \equiv 1, 7, 8, 11, 12, 18 \pmod{19}$
0.6486367163	$7\,x^3 + 6\,x^2 - x - 1$	$p \equiv 1, 7, 8, 11, 12, 18 \pmod{19}$
0.6486367163	$x^3 - 7\,x - 7$	$p \equiv 1, 6 \pmod 7$
0.6486367163	$x^3 - 7\,x + 7$	$p \equiv 1, 6 \pmod 7$
0.6486367163	$7\,x^3 - 7\,x^2 + 1$	$p \equiv 1, 6 \pmod 7$
0.6486367163	$7\,x^3 + 7\,x^2 - 1$	$p \equiv 1, 6 \pmod 7$
0.6622071408	$x^3 - 6\,x^2 - 9\,x - 3$	$p \equiv 1, 8 \pmod 9$
0.6622071408	$x^3 + 6\,x^2 - 9\,x + 3$	$p \equiv 1, 8 \pmod 9$

Continued on next page

TABLE 3.3 – continued from previous page

$h(\alpha_i)$	f_{α_i}	α_i is totally p-adic iff
0.6622071408	$3\,x^3 - 9\,x^2 + 6\,x + 1$	$p \equiv 1, 8 \pmod 9$
0.6622071408	$3\,x^3 + 9\,x^2 + 6\,x - 1$	$p \equiv 1, 8 \pmod 9$
0.6624373759	$x^3 - 8\,x^2 + 5\,x + 1$	$p \equiv 1, 6 \pmod 7$
0.6624373759	$x^3 - 5\,x^2 - 8\,x - 1$	$p \equiv 1, 6 \pmod 7$
0.6624373759	$x^3 + 5\,x^2 - 8\,x + 1$	$p \equiv 1, 6 \pmod 7$
0.6624373759	$x^3 + 8\,x^2 + 5\,x - 1$	$p \equiv 1, 6 \pmod 7$
0.6627246225	$2\,x^3 - 8\,x^2 + 2\,x + 2$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.6627246225	$2\,x^3 - 2\,x^2 - 8\,x - 2$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.6627246225	$2\,x^3 + 2\,x^2 - 8\,x + 2$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.6627246225	$2\,x^3 + 8\,x^2 + 2\,x - 2$	$p \equiv 1, 5, 8, 12 \pmod{13}$
0.6633392513	$3\,x^3 - 7\,x^2 - 2\,x + 3$	$p \equiv 1, 3, 5, 15, 22, 40, 42, 43, 45, 53, 59, 64 \pmod{67}$
0.6633392513	$3\,x^3 - 2\,x^2 - 7\,x + 3$	$p \equiv 1, 3, 5, 15, 22, 40, 42, 43, 45, 53, 59, 64 \pmod{67}$
0.6633392513	$3\,x^3 + 2\,x^2 - 7\,x - 3$	$p \equiv 1, 3, 5, 15, 22, 40, 42, 43, 45, 53, 59, 64 \pmod{67}$
0.6633392513	$3\,x^3 + 7\,x^2 - 2\,x - 3$	$p \equiv 1, 3, 5, 15, 22, 40, 42, 43, 45, 53, 59, 64 \pmod{67}$
0.6663004651	$2\,x^3 - 7\,x^2 + 3\,x + 4$	$p \equiv 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$
0.6663004651	$2\,x^3 + 7\,x^2 + 3\,x - 4$	$p \equiv 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$
0.6663004651	$4\,x^3 - 3\,x^2 - 7\,x - 2$	$p \equiv 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$
0.6663004651	$4\,x^3 + 3\,x^2 - 7\,x + 2$	$p \equiv 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$
0.6696162679	$x^3 - 7\,x^2 + 7$	$p \equiv 1, 6 \pmod 7$
0.6696162679	$x^3 + 7\,x^2 - 7$	$p \equiv 1, 6 \pmod 7$

Continued on next page

TABLE 3.3 – continued from previous page

$h(\alpha_i)$	f_{α_i}	α_i is totally p-adic iff
0.6696162679	$7x^3 - 7x - 1$	$p \equiv 1, 6 \pmod 7$
0.6696162679	$7x^3 - 7x + 1$	$p \equiv 1, 6 \pmod 7$
0.6795133581	$x^3 - 5x^2 + 4x + 5$	$p \equiv 1, 5, 12 \pmod{13}$
0.6795133581	$x^3 + 5x^2 + 4x - 5$	$p \equiv 1, 5, 12 \pmod{13}$
0.6795133581	$5x^3 - 4x^2 - 5x - 1$	$p \equiv 1, 5, 12 \pmod{13}$
0.6795133581	$5x^3 + 4x^2 - 5x + 1$	$p \equiv 1, 5, 12 \pmod{13}$
0.6910644552	$3x^3 - 8x^2 - x + 3$	$p \equiv 1, 3, 7, 8, 10, 17, 21, 24, 27, 30, 43, 64, 65, 66 \pmod{73}$
0.6910644552	$3x^3 - x^2 - 8x + 3$	$p \equiv 1, 3, 7, 8, 10, 17, 21, 24, 27, 30, 43, 64, 65, 66 \pmod{73}$
0.6910644552	$3x^3 + x^2 - 8x - 3$	$p \equiv 1, 3, 7, 8, 10, 17, 21, 24, 27, 30, 43, 64, 65, 66 \pmod{73}$
0.6910644552	$3x^3 + 8x^2 - x - 3$	$p \equiv 1, 3, 7, 8, 10, 17, 21, 24, 27, 30, 43, 64, 65, 66 \pmod{73}$
0.6931471806	$x^3 - 6x^2 + 8$	$p \equiv 1, 8 \pmod 9$
0.6931471806	$x^3 + 6x^2 - 8$	$p \equiv 1, 8 \pmod 9$
0.6931471806	$x^3 - 4x^2 - 4x + 8$	$p \equiv 1, 6 \pmod 7$
0.6931471806	$x^3 + 4x^2 - 4x - 8$	$p \equiv 1, 6 \pmod 7$
0.6931471806	$x^3 - 5x^2 - 2x + 8$	$p \equiv 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$
0.6931471806	$x^3 + 5x^2 - 2x - 8$	$p \equiv 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$
0.6931471806	$8x^3 + 2x^2 - 5x - 1$	$p \equiv 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$
0.6931471806	$8x^3 - 2x^2 - 5x + 1$	$p \equiv 1, 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$
0.6931471806	$2x^3 - 5x^2 - 3x + 8$	$p \equiv 1, 2, 4, 8, 11, 16, 21, 22, 27, 39, 41 \pmod{43}$
0.6931471806	$2x^3 + 5x^2 - 3x - 8$	$p \equiv 1, 2, 4, 8, 11, 16, 21, 22, 27, 39, 41 \pmod{43}$

Continued on next page

TABLE 3.3 – continued from previous page

$h(\alpha_i)$	f_{α_i}	α_i is totally p-adic iff
0.6931471806	$8\,x^3 - 3\,x^2 - 5\,x + 2$	$p \equiv 1, 2, 4, 8, 11, 16, 21, 22, 27, 39, 41 \pmod{43}$
0.6931471806	$8\,x^3 + 3\,x^2 - 5\,x - 2$	$p \equiv 1, 2, 4, 8, 11, 16, 21, 22, 27, 39, 41 \pmod{43}$
0.6931471806	$8\,x^3 - 4\,x^2 - 4\,x + 1$	$p \equiv 1, 6 \pmod{7}$
0.6931471806	$8\,x^3 + 4\,x^2 - 4\,x - 1$	$p \equiv 1, 6 \pmod{7}$
0.6931471806	$8\,x^3 - 6\,x - 1$	$p \equiv 1, 8 \pmod{9}$
0.6931471806	$8\,x^3 - 6\,x + 1$	$p \equiv 1, 8 \pmod{9}$
0.6943241113	$x^3 - 7\,x^2 + 12\,x - 5$	$p \equiv 1, 5, 12 \pmod{13}$
0.6943241113	$x^3 + 7\,x^2 + 12\,x + 5$	$p \equiv 1, 5, 12 \pmod{13}$
0.6943241113	$5\,x^3 - 12\,x^2 + 7\,x - 1$	$p \equiv 1, 5, 12 \pmod{13}$
0.6943241113	$5\,x^3 + 12\,x^2 + 7\,x + 1$	$p \equiv 1, 5, 12 \pmod{13}$
0.6971989008	$2\,x^3 - 8\,x^2 + 6\,x + 2$	$p \equiv 1, 6 \pmod{7}$
0.6971989008	$2\,x^3 - 6\,x^2 - 8\,x - 2$	$p \equiv 1, 6 \pmod{7}$
0.6971989008	$2\,x^3 + 6\,x^2 - 8\,x + 2$	$p \equiv 1, 6 \pmod{7}$
0.6971989008	$2\,x^3 + 8\,x^2 + 6\,x - 2$	$p \equiv 1, 6 \pmod{7}$
0.6990306738	$2\,x^3 - 9\,x^2 + 3\,x + 2$	$p \equiv 1, 2, 4, 8, 16, 31, 32, 47, 55, 59, 61, 62 \pmod{63}$
0.6990306738	$2\,x^3 - 3\,x^2 - 9\,x - 2$	$p \equiv 1, 2, 4, 8, 16, 31, 32, 47, 55, 59, 61, 62 \pmod{63}$
0.6990306738	$2\,x^3 + 3\,x^2 - 9\,x + 2$	$p \equiv 1, 2, 4, 8, 16, 31, 32, 47, 55, 59, 61, 62 \pmod{63}$
0.6990306738	$2\,x^3 + 9\,x^2 + 3\,x - 2$	$p \equiv 1, 2, 4, 8, 16, 31, 32, 47, 55, 59, 61, 62 \pmod{63}$
0.7037615930	$x^3 - 9\,x^2 + 6\,x + 1$	$p \equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}$

Continued on next page

TABLE 3.3 – continued from previous page

$h(\alpha_i)$	f_{α_i}	α_i is totally p-adic iff
0.7037615930	$x^3 - 6\,x^2 - 9\,x - 1$	$p \equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}$
0.7037615930	$x^3 + 6\,x^2 - 9\,x + 1$	$p \equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}$
0.7037615930	$x^3 + 9\,x^2 + 6\,x - 1$	$p \equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}$

Theorem 3.13. Let p be a prime. Then $\tau_{3,p}^{\mathrm{ab}}$ depends only on $p \pmod{228979643050431}$.

Proof. This proof is an application of the proof of Theorem 3.10. From Table 3.3 we determine

$$\tau_{3,3}^{\mathrm{ab}} = 0.609817669, \text{ and}$$

$$\tau_{3,7}^{\mathrm{ab}} = 0.501878627,$$

by finding the first congruence classes that contain 3 and 7. All primes $p \neq 3, 7$, when reduced modulo 63, are contained in $(\mathbb{Z}/63\mathbb{Z})^{\times}$. Observe that

$$(\mathbb{Z}/63\mathbb{Z})^{\times} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20, 22, 23, 25, 26, 29, 31, 32, 34, 37, 38, 40, 41,$$

$$43, 44, 46, 47, 50, 52, 53, 55, 58, 59, 61, 62\}.$$

By the first eight lines of Table 3.3, we observe that

$$\tau_{3,p}^{\mathrm{ab}} = \begin{cases} 0.269862305 & \text{if } p \equiv 1, 6 \pmod 7, \\ 0.352525605 & \text{if } p \equiv 1, 8 \pmod 9 \text{ and } p \not\equiv 1, 6 \pmod 7. \end{cases}$$

Thus

$$\tau_{3,p}^{\mathrm{ab}} = 0.269862305 \text{ for } p \equiv 1, 13, 20, 22, 29, 34, 41, 43, 47, 55, 62 \pmod{63}, \text{ and}$$

$$\tau_{3,p}^{\mathrm{ab}} = 0.352525605 \text{ for } p \equiv 17, 19, 26, 37, 44, 46, 53 \pmod{63}.$$

It remains to determine $\tau_{3,p}^{\mathrm{ab}}$ for

$$p \equiv 2, 4, 5, 11, 16, 23, 25, 31, 32, 38, 40, 47, 52, 58, 59, 61 \pmod{63}.$$

Note that each of the above numbers falls into one of the following two sets:

$$p \equiv 1, 2, 4, 8, 16, 31, 32, 47, 55, 59, 61, 62 \pmod{63}$$

$$p \equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}$$

Therefore, by the final eight lines of Table 3.3, given any prime p, one of the polynomials in the table must split completely over $\mathbb{Q}_p$. By Theorem 3.10,

$$N_3 = \operatorname{lcm}(7, 9, 13, 19, 31, 37, 43, 61, 63, 67, 73) = 228979643050431. \qquad \square$$

4 Totally p-adic Numbers of Degree 3

As we have seen in Section 3.1, $\tau_{2,p}$ depends only on p modulo 5. We calculated this in two ways, one using quadratic reciprocity and the other using the Kronekcer-Weber Theorem. By the Kronecker-Weber method, we found that $\tau_{3,p}^{\text{ab}}$ depends only on p modulo 228979643050431. Determining $\tau_{3,p}$ is a more delicate endeavor, since neither quadratic reciprocity nor the Kronecker-Weber theorem apply to determine the splitting behavior of primes in nonabelian extensions of $\mathbb{Q}$. In particular, not all cubic extensions are abelian, and quadratic reciprocity is unavailable. Note that Proposition 3.1 guarantees finiteness of $\tau_{d,p}$ for all $d \geq 2$ and primes p.

In this section, we develop tools to determine $\tau_{3,p}$ for all $p \geq 5$. We exclude the calculations of $\tau_{3,2}$ and $\tau_{3,3}$ since detecting squares and cubes in $\mathbb{Q}_2$ and $\mathbb{Q}_3$ is a bit different than it is in $\mathbb{Q}_p$ for $p \geq 5$. However, in principle the ideas outlined here, suitably modified, could be made to perform these calculations as well.

In *Ars Magna*, Cardano proves a method to find the roots of a cubic polynomial f as elements of $\mathbb{C}$ [CS68]. This method is an analogue to completing the square for a quadratic polynomial. We use Cardano's method to determine if a cubic polynomial in $K[y]$ splits completely over K, where K is an arbitrary field of characteristic not equal to 2 or 3. Beginning with an arbitrary cubic polynomial in $K[y]$,

$$g(y) = ay^3 + by^2 + cy + d$$

we divide through by the leading coefficient,

$$y^3 + \tfrac{b}{a}y^2 + \tfrac{c}{a}y + \tfrac{d}{a}$$

and then perform a change of variables $y = x - \frac{b}{3}$ to eliminate the quadratic term. Thus our polynomial becomes

$$\left(x - \tfrac{b}{3a}\right)^3 + \tfrac{b}{a}\left(x - \tfrac{b}{3a}\right)^2 + \tfrac{c}{a}\left(x - \tfrac{b}{3a}\right) + \tfrac{d}{a}$$

which simplifies to

$$x^3 + \left(\frac{3ac-b^2}{3a^2}\right)x + \frac{27a^2d-9abc+2b^3}{27a^3}.$$

Setting $A = \frac{3ac-b^2}{3a^2}$ and $B = \frac{27a^2d-9abc+2b^3}{27a^3}$, we have the monic depressed cubic polynomial with coefficients in K,

$$f(x) = x^3 + Ax + B.$$

Note that since the transformations to depress the cubic are field operations, g splits over K if and only if f splits over K.

Lemma 4.1 (Cardano)**.** [CS68] Let L be an algebraically closed field of characteristic not equal to 2 or 3, and let ζ be a primitive cube root of unity in L. Let $f(x) = x^3 + Ax + B \in L[x]$, and let $\Delta = B^2 + 4A^3/27$. If $A = 0$, let $C = -B$, and if $A \neq 0$, let C be either square root of Δ in L. Let u be a cube root of $\frac{-B+C}{2}$ and let $v = -\frac{A}{3u}$. Then the roots of f are

$$\alpha_1 = u + v$$
$$\alpha_2 = \zeta u + \zeta^2 v$$
$$\alpha_3 = \zeta^2 u + \zeta v.$$

Proof. If $A = 0$, then $f(x) = x^3 + B$ and the roots of f are $u, \zeta u$, and $\zeta^2 u$, as desired. If $A \neq 0$, note that $3uv + A = 0$, and

$$\begin{aligned}
u^3 + v^3 &= \frac{-B+C}{2} - \frac{A^3}{27u^3} \\
&= \frac{-B+C}{2} - \frac{2A^3}{27(-B+C)} \\
&= \frac{27(-B+C)^2 - 4A^3}{54(-B+C)} \\
&= \frac{27(-B+C)^2 - 27(C^2-B^2)}{54(-B+C)} \\
&= \frac{(-B+C)-(B+C)}{2} \\
&= -B.
\end{aligned}$$

Let $g(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$. Then

$$g(x) = x^3 - (\alpha_1+\alpha_2+\alpha_3)x^2 + (\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3.$$

Since $1+\zeta+\zeta^2 = 0$, we have the following:

$$\begin{aligned}\alpha_1+\alpha_2+\alpha_3 &= u+v+\zeta u+\zeta^2 v+\zeta^2 u+\zeta v\\ &= u(1+\zeta+\zeta^2)+v(1+\zeta+\zeta^2)\\ &= 0,\end{aligned}$$

$$\begin{aligned}\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= (u+v)(\zeta u+\zeta^2 v)+(u+v)(\zeta^2 u+\zeta v)+(\zeta u+\zeta^2 v)(\zeta^2 u+\zeta v)\\ &= \zeta u^2+3\zeta vu+3\zeta^2 vu+\zeta^2 v^2+\zeta^2 u^2+\zeta v^2+u^2+v^2\\ &= (1+\zeta+\zeta^2)u^2+(3\zeta+3\zeta^2)uv+(1+\zeta+\zeta^2)v^2\\ &= -3uv\\ &= A,\end{aligned}$$

and

$$\begin{aligned}\alpha_1\alpha_2\alpha_3 &= (u+v)(\zeta u+\zeta^2 v)(\zeta^2 u+\zeta v)\\ &= u^3+\zeta^2 u^2 v+\zeta u^2 v+uv^2+u^2 v+\zeta^2 uv^2+\zeta uv^2+v^3\\ &= (u^3+v^3)+(1+\zeta+\zeta^2)u^2 v+(1+\zeta+\zeta^2)u^2 v\\ &= -B.\end{aligned}$$

Therefore, $f(x) = g(x)$ and α_1, α_2, and α_3 are the roots of f. □

To determine when a cubic polynomial $f(x) \in \mathbb{Q}_p[x]$ splits completely over $\mathbb{Q}_p$, the method will depend on whether $\mathbb{Q}_p$ contains a primitive cube root of unity, which happens exactly when $p \equiv 1 \pmod 3$. Thus, we consider two cases: $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$.

4.1 Splitting Condition for $p \equiv 1 \pmod 3$

Theorem 4.2. Let K be a field of characteristic not equal to 2 or 3, let L be an algebraic closure of K, and assume that K contains a primitive cube root of unity, ζ. Let $f(x) = x^3 + Ax + B \in K[x]$, and $\Delta = B^2 + 4A^3/27$. If $A = 0$, let $C = -B$, and if $A \neq 0$, let C be either square root of Δ in L. Then f splits completely over K if and only if

(a) Δ is a square in K, and

(b) $\frac{-B+C}{2}$ is a cube in K.

Proof. Suppose $A = 0$. Then $\Delta = B^2$ is a square in K, so **(a)** is true. Additionally, $C = -B$ and $f(x) = x^3 + B$, which splits completely over K if and only if $-B$ is a cube in K, which happens exactly when **(b)** holds.

Now suppose $A \neq 0$. Let u be a cube root of $\frac{-B+C}{2}$ and let $v = -\frac{A}{3u}$. Let F be a Galois extension of K containing C and u.

Suppose the conditions **(a)** and **(b)** are met. By Lemma 4.1, the roots of f are

$$\alpha_1 = u + v$$
$$\alpha_2 = \zeta u + \zeta^2 v$$
$$\alpha_3 = \zeta^2 u + \zeta v,$$

and thus f splits completely over K.

Conversely, suppose that f splits completely over K. Let $\sigma \in \mathrm{Gal}(F/K)$. Since σ fixes α_1 and α_2,

$$u + v = \sigma(u) + \sigma(v), \text{ and } \zeta u + \zeta^2 v = \zeta\sigma(u) + \zeta^2\sigma(v). \tag{4.1}$$

Note that $\left(\begin{smallmatrix} 1 & 1 \\ \zeta & \zeta^2 \end{smallmatrix}\right)$ has a non-zero determinant and thus

$$\begin{pmatrix} 1 & 1 \\ \zeta & \zeta^2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \sigma(u) + \sigma(v) \\ \zeta\sigma(u) + \zeta^2\sigma(v) \end{pmatrix} \tag{4.2}$$

has a unique solution. By (4.1), $x = u, y = v$ is a solution to (4.2) and $x = \sigma(u)$, $y = \sigma(v)$ is a solution to (4.2) as well. Therefore $u = \sigma(u)$. By the Galois correspondence, $u \in K$, and thus **(b)** holds. Thus $u^3 = \frac{-B+C}{2} \in K$. Since $C = 2u^3 + B$, $C \in K$ and therefore $\Delta = B^2 + 4A^3/27 = C^2$ is a square in K, and **(a)** is true. □

Lemma 4.3. Let p be a prime, $p \neq 3$, and let $a \in \mathbb{Z}_p$ with $|a|_p = 1$. Then a is a cube in $\mathbb{Q}_p$ if and only if $a \pmod p$ is a cube in $\mathbb{Z}_p/p\mathbb{Z}_p$.

Proof. Suppose that a is a cube in $\mathbb{Z}_p$. Then a is a cube in $\mathbb{Z}_p/p\mathbb{Z}_p$ by the nature of quotient rings.

Conversely, suppose a_0 is a cube in $\mathbb{Z}/p\mathbb{Z}$ where $a_0 = [a]$, and let $b_0 \in \mathbb{Z}/p\mathbb{Z}$ satisfy $b_0^3 \equiv a_0 \pmod p$. Let $f(x) = x^3 - a$. Note that $p \nmid 3, b_0$. By the strong triangle inequality,

$$\begin{aligned} |f(b_0)|_p &= \left|b_0^3 - a\right|_p \\ &= \left|b_0^3 - a_0 + a_0 - a\right|_p \\ &\leq \max\left\{\left|b_0^3 - a_0\right|_p, |a_0 - a|_p\right\} \\ &\leq \tfrac{1}{p}. \end{aligned}$$

Further,

$$\begin{aligned} |f'(b_0)|_p &= \left|3b_0^2\right|_p \\ &= 1. \end{aligned}$$

By Hensel's Lemma, a is a cube in $\mathbb{Q}_p$. □

Theorem 4.4. Let p be a prime, with $p \equiv 1 \pmod 3$. Then the following algorithm yields $\tau_{3,p}$.

(1) Create a list, in ascending order of Mahler measure, of all irreducible, non-cyclotomic cubic polynomials in $\mathbb{Z}[x]$ with Mahler measure bounded above by 8.5. Let $f(x)$ be the first polynomial on the list.

(2) Convert $f(x)$ into depressed form $g(x) = x^3 + Ax + B$ and let $\Delta = B^2 + 4A^3/27$.

(3) If Δ is not a square in $\mathbb{Q}_p$, return to step **(2)** with the next polynomial on the list.

(4) If $A = 0$, let $C = -B$, and otherwise let C be a square root of Δ in $\mathbb{Q}_p$. If $\frac{-B+C}{2}$ is not a cube in $\mathbb{Q}_p$, return to step **(2)** with the next polynomial on the list. Otherwise, terminate, $\tau_{3,p} = \frac{1}{3}\log M(f)$.

Proof. Since $\tau_{3,p} \leq \tau_{3,p}^{\mathrm{ab}}$, by Proposition 3.13 we know that $\tau_{3,p} \leq 0.70376$. By Proposition 2.11, a list of all polynomials with length less than 68 will contain all irreducible, non-cyclotomic, cubic polynomials with Mahler measure bounded above by 8.5. Any degree 3 algebraic number of height less than or equal to 0.70376 will be a root of a polynomial in the list. Thus, this algorithm will always terminate successfully.

Let f be the polynomial being considered. By Theorem 4.2, steps **(3)**, and **(4)** will detect exactly when f splits completely over $\mathbb{Q}_p$. □

4.2 Splitting Condition for $p \equiv 2 \pmod 3$

Theorem 4.5. Let K be a field of characteristic not equal to 2 or 3, L be an algebraic closure of K, ζ be a primitive cube root of unity in L, and assume that $\zeta \notin K$. Let $f(x) = x^3 + Ax + B \in K[x]$ with $B \neq 0$ and let $\Delta = B^2 + 4A^3/27$. If $A = 0$, let $C = -B$, and if $A \neq 0$, let C be either square root of Δ in L. Then f splits completely over K if and only if

(a) Δ is a square in $K(\zeta)$ and not a square in K, and

(b) $\frac{-B+C}{2}$ is a cube in $K(\zeta)$ and not a cube in K.

Proof. Suppose $A = 0$. Then $\Delta = B^2$ is a square in K, so **(a)** is false. Additionally, $C = -B$ and $f(x) = x^3 + B$, which will never split completely over K since $\zeta \notin K$.

Next, suppose $A \neq 0$, let u be a cube root of $\frac{-B+C}{2}$ and let $v = \frac{-A}{3u}$. Then the roots of f are

$$\alpha_1 = u + v$$
$$\alpha_2 = \zeta u + \zeta^2 v$$
$$\alpha_3 = \zeta^2 u + \zeta v.$$

We first suppose f splits completely in K. Let L be a Galois extension of K that contains u and ζ. Let $\sigma \in \mathrm{Gal}(L/K(\zeta))$. We want to show that σ must also fix u. Since we are assuming that f splits completely over K, σ must also fix α_1, α_2, and α_3,

$$u + v = \sigma(u) + \sigma(v), \tag{4.3}$$
$$\zeta u + \zeta^2 v = \zeta\sigma(u) + \zeta^2\sigma(v),$$
$$\zeta^2 u + \zeta v = \zeta^2\sigma(u) + \zeta\sigma(v). \tag{4.4}$$

By multiplying (4.3) by ζ and subtracting (4.4), we obtain

$$(\zeta - \zeta^2)u = (\zeta - \zeta^2)\sigma(u), \tag{4.5}$$

so $\sigma(u) = u$ because $\zeta \neq \zeta^2$. Thus, since every $\sigma \in \mathrm{Gal}(L/K(\zeta))$ fixes u, it follows from the Galois correspondence that $u \in K(\zeta)$. It remains show $u \notin K$. Let $\tau \in \mathrm{Gal}(L/K)$ such that τ permutes ζ and ζ^2. We now show that τ does not fix u. Since α_1, α_2, and α_3 must all be fixed by τ,

$$u + v = \tau(u) + \tau(v),$$

$$\zeta u + \zeta^2 v = \zeta^2 \tau(u) + \zeta \tau(v), \tag{4.6}$$

$$\zeta^2 u + \zeta v = \zeta \tau(u) + \zeta^2 \tau(v). \tag{4.7}$$

By multiplying (4.7) by ζ, and subtracting (4.6), we obtain

$$(1 - \zeta)u = (1 - \zeta)\tau(v) \tag{4.8}$$

and note that $\tau(v) = u$, so τ does not fix u. Thus $u \notin K$ and **(b)** holds.

Further, $u \in K(\zeta)$, so $u^3 = \frac{-B+C}{2} \in K(\zeta)$, and thus Δ is a square in $K(\zeta)$ since $C \in K(\zeta)$. Since $K(u)$ is contained within $K(\zeta)$, a quadratic extension of K, and $u \notin K$, $[K(u) : K] = 2$. For sake of contradiction, suppose Δ is a square in K. Then $u^3 \in K$, so $[K(u) : K] = 3$ which is not true. Thus Δ is not a square in K, and **(a)** holds.

Conversely, suppose that **(a)** and **(b)** are true. Note that if $A = 0$, then Δ is a square in K, contradicting **(a)**. Thus, $A \neq 0$. Let σ denote the non trivial element of $\mathrm{Gal}(K(\zeta)/K)$. Since ζ and ζ^2 share a degree 2 minimal polynomial, σ must permute ζ and ζ^2.

By **(a)** and **(b)**, $u, u^3 \notin K$ and $u, u^3 \in K(\zeta)$. Since u^3 and v^3 are the roots of $r(z) = z^2 + Bz - \frac{A^3}{27}$, $\sigma(u)^3 = \sigma(u^3) = v^3$. Therefore, either $\sigma(u) = v$, $\sigma(u) = \zeta v$, or $\sigma(u) = \zeta^2 v$.

We will now show that $\sigma(u) = v$ by eliminating the other two options by way of contradiction. We rely on the fact that elements of the Galois group send roots of f to roots of f, and that $\sigma^2(u) = u$. If $\sigma(u) = \zeta v$, then $u = \zeta^2 \sigma(v)$, and $\sigma(u + v) = \sigma(u) + \sigma(v) = \zeta v + \zeta u$. Since $\zeta v + \zeta u$ is not a root of f, $\sigma(u) \neq \zeta v$. If $\sigma(u) = \zeta^2 v$, then $u = \zeta \sigma(v)$, and $\sigma(u + v) = \zeta^2 u + \zeta^2 v$. Since $\zeta^2 u + \zeta^2 v$ is not a root of f, $\sigma(u) \neq \zeta^2 v$.

Therefore, $\sigma(u) = v$ and $\sigma(v) = u$. Thus

$$\sigma(\alpha_1) = \sigma(u+v) = \sigma(u) + \sigma(v) = v + u = \alpha_1,$$
$$\sigma(\alpha_2) = \sigma(\zeta u + \zeta^2 v) = \sigma(\zeta u) + \sigma(\zeta^2 v) = \zeta^2 v + \zeta u = \alpha_2,$$
$$\sigma(\alpha_3) = \sigma(\zeta^2 u + \zeta v) = \sigma(\zeta^2 u) + \sigma(\zeta v) = \zeta v + \zeta^2 v = \alpha_3.$$

Since σ fixes α_1, α_2 and α_3, by the Galois correspondence, f splits completely in K. □

Let $p \equiv 2 \pmod 3$. The third cyclotomic polynomial, $\Phi_3(x) = x^2 + x + 1$, has discriminant -3 and is the minimal polynomial for ζ. Since -3 is not a square in $\mathbb{Q}_p$, $\Phi_3(x)$ is irreducible over $\mathbb{Q}_p$, and thus $\mathbb{Q}_p$ does not contain a primitive cube root of unity. There are exactly three quadratic extensions of $\mathbb{Q}_p$: $\mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{-3})$, and $\mathbb{Q}_p(\sqrt{-3p})$. Let $K = \mathbb{Q}_p(\sqrt{-3}) = \mathbb{Q}_p(\zeta)$, the unique unramified quadratic extension of $\mathbb{Q}_p$. The p-adic absolute value on $\mathbb{Q}_p$ extends uniquely to $\mathbb{Q}_p(\sqrt{-3})$ by

$$|a + b\sqrt{-3}|_p = \left|N_{K/\mathbb{Q}_p}(a + b\sqrt{-3})\right|_p^{1/2} = \left|a^2 + 3b^2\right|_p^{1/2}.$$

The following three lemmas summarize some basic facts about this field.

Lemma 4.6. Let $p \equiv 2 \pmod 3$, and $K = \mathbb{Q}_p(\sqrt{-3})$. For $x \in K^\times$, $|x|_p \in p^{\mathbb{Z}}$.

Proof. Let $x = a + b\sqrt{-3}$, with $a, b \in \mathbb{Q}_p$ and $x \neq 0$. Suppose $|a|_p \neq |b|_p$. Then

$$|x|_p = \left|a^2 + 3b^2\right|_p^{1/2} = \max\{|a|_p, |b|_p\} \in p^{\mathbb{Z}}.$$

Suppose instead that $|a|_p = |b|_p = p^\ell$. Set $a_0 = p^\ell a$ and $b_0 = p^\ell b$. Note that since $a_0, b_0 \in \mathbb{Q}_p$, $|a_0|_p, |b_0|_p \in p^{\mathbb{Z}}$. Note that if $|a_0^2 + 3b_0^2|_p < 1$, then reducing modulo p we obtain that $a_0^2 + 3b_0^3 \equiv 0 \pmod p$ which is a contradiction since -3 is not a quadratic residue modulo p. Thus

$$|x|_p = \left|a^2 + 3b^2\right|_p^{1/2} = \left|p^{-2\ell}(a_0^2 + 3b_0^2)\right|_p^{1/2} = p^\ell |a_0^2 + 3b_0^2|_p^{1/2} = p^\ell \in p^{\mathbb{Z}}.$$ □

Lemma 4.7. Let p be a prime with $p \equiv 2 \pmod 3$, $K = \mathbb{Q}_p(\sqrt{-3})$, and $C \in K$. Let $k \in \mathbb{N}$, $p \nmid k$. Then $f(x) = x^k - C$ has a root in K if and only if

(a) $|C|_p = p^{k\ell}$ for some $l \in \mathbb{Z}$, and

(b) $p^{k\ell}C \pmod p$ is a k^{th} power in $\mathbb{F}_{p^2} = \mathbb{Z}_p[\sqrt{-3}]/p$.

Proof. First we assume the existence of $r \in K$ so that $f(r) = 0$, and verify that **(a)** and **(b)** hold. By Lemma 4.6, $|r|_p = p^\ell$ for some $\ell \in \mathbb{Z}$. Since $C = r^k$, **(a)** is true, as

$$|C|_p = |r^k|_p = p^{k\ell}.$$

Further,

$$p^{kl}C = p^{kl}r^k = (p^l r)^k$$

and thus $p^{kl}C$ is the k^{th} power of $p^l r \pmod p$ in $\mathbb{Z}[\sqrt{-3}]/p$, so **(b)** holds.

Conversely, we suppose $C \in \mathbb{Q}_p(\sqrt{-3})$ satisfies conditions **(a)** and **(b)**, and show that C is a k^{th} power in K. Replacing C with $p^{kl}C$, without loss of generality we may assume $|C|_p = 1$. By condition **(b)**, there exist $a \in \mathbb{F}_{p^2}$ such that

$$C \equiv a^k \pmod p.$$

Then

$$|f(a)|_p = \left|a^k - C\right|_p \leq \tfrac{1}{p}.$$

Additionally,

$$|f'(a)|_p = \left|ka^{k-1}\right|_p = 1.$$

By Hensel's Lemma f has a root in K. □

Lemma 4.8. Let p be a prime with $p \equiv 2 \pmod 3$, and $K = \mathbb{Q}_p(\sqrt{-3})$. Let $x \in \mathbb{Q}_p$ be nonzero and the square of an element in K. Then exactly one of the following two cases is true:

(a) $x = a^2$ for some $a \in \mathbb{Q}_p$, or

(b) $x = -3b^2$ for some $b \in \mathbb{Q}_p$.

Proof. Suppose $x = (a + b\sqrt{-3})^2$ for $a, b \in \mathbb{Q}_p$. Then $x = a^2 - 3b^2 + 2ab\sqrt{-3}$. Since $\sqrt{-3} \notin \mathbb{Q}_p$, $ab = 0$. If $a = 0$, then $x = -b^2$ and **(b)** holds. If $b = 0$, then $x = a^2$ and **(a)** holds. □

The previous lemma gives us the machinery to detect and solve for a square root in K, since x is a square in K and not in $\mathbb{Q}_p$ if and only if $\frac{x}{-3} = b^2$ for some $b \in \mathbb{Q}_p$. In Appendix $A.4$, the function **IsCubeInK** applies this lemma.

Theorem 4.9. Let p be an odd prime, with $p \equiv 2 \pmod 3$. Then the following algorithm yields $\tau_{3,p}$.

(1) Create a list, in ascending order of Mahler measure, of all irreducible, non-cyclotomic cubic polynomials in $\mathbb{Z}[x]$ with Mahler measure less than 8.5. Let $f(x)$ be the first polynomial on the list.

(2) Convert $f(x)$ into depressed form $g(x) = x^3 + Ax + B$ and let $\Delta = B^2 + 4A^3/27$.

(3) If Δ is a square in $\mathbb{Q}_p$ or is not a square in $\mathbb{Q}_p(\sqrt{-3})$, return to step **(2)** with the next polynomial on the list.

(4) If $A = 0$, let $C = -B$, and otherwise let C be a square root of Δ in $\mathbb{Q}_p(\sqrt{-3})$. If $\frac{-B+C}{2}$ is not a cube in $\mathbb{Q}_p(\sqrt{-3})$, return to step (2) with the next polynomial on the list.

(5) If $\frac{-B+C}{2}$ is a cube in $\mathbb{Q}_p$, return to step **(2)** with the next polynomial on the list. Otherwise, terminate, $\tau_{3,p} = \frac{1}{3}\log M(f)$.

Proof. Since $\tau_{3,p} \leq \tau_{3,p}^{\text{ab}}$, by Proposition 3.13 we know that $\tau_{3,p} \leq 0.70376$. By Proposition 2.11, a list of all polynomials with length less than 68 will contain all irreducible, non-cyclotomic, cubic polynomials with Mahler measure bounded above by 8.5. Any degree 3 algebraic number of height less than or equal to 0.70376 will be a root of a polynomial in the list. Thus, this algorithm will always terminate successfully.

Let f be the polynomial being considered. By Theorem 4.5, steps **(3)**, **(4)**, and **(5)** will detect exactly when f splits completely over $\mathbb{Q}_p$. □

4.3 Implementing the Algorithms to Determine $\tau_{3,p}$

First, we create a list of all irreducible, non-cyclotomic, cubic polynomials in $\mathbb{Z}[x]$ with Mahler measure less than 8.5. By Theorem 3.13, this list will be sufficient to determine $\tau_{3,p}$ for all primes p. The code to create this list can be found in Appendix A. The list contains $26,796$ polynomials. Using the code in Appendix D to determine $\tau_{3,p}$ for all primes p with $5 \leq p \leq 197$, we obtain Table 4.1. For each prime p, f_α is the minimal polynomial of α, where $h(\alpha) = \tau_{3,p}$.

TABLE 4.1: Some values of $\tau_{3,p}$

p	$\tau_{3,p}$	f_α
5	0.36620	$x^3 - 2x^2 - x - 3$
7	0.12741	$x^3 - x^2 - 1$
11	0.23105	$x^3 - x^2 - 2$
13	0.093733	$x^3 - x^2 + 1$
17	0.23105	$x^3 - 2x - 2$
19	0.12741	$x^3 + x + 1$
23	0.20313	$x^3 - x^2 + x + 1$
29	0.093733	$x^3 - x - 1$
31	0.093733	$x^3 + x^2 - 1$
37	0.20313	$x^3 + x^2 + x - 1$
41	0.093733	$x^3 - x - 1$
43	0.23105	$x^3 - 2x + 2$
47	0.23105	$2x^3 - 2x^2 + 1$
53	0.20313	$x^3 - x^2 - x - 1$

Continued on next page

TABLE 4.1 – continued from previous page

p	$\tau_{3,p}$	f_α
59	0.12741	$x^3 - x^2 - 1$
61	0.23105	$x^3 + x^2 + x + 2$
67	0.12741	$x^3 - x^2 - 1$
71	0.12741	$x^3 - x^2 - 1$
73	0.093733	$x^3 - x - 1$
79	0.23105	$x^3 + x^2 + 2$
83	0.28612	$2\,x^3 + 2\,x - 1$
89	0.20313	$x^3 - x^2 - x - 1$
97	0.12741	$x^3 - x^2 - 1$
101	0.12741	$x^3 - x^2 - 1$
103	0.20313	$x^3 - x^2 + x + 1$
107	0.23105	$x^3 - x^2 - x + 2$
109	0.12741	$x^3 - x^2 - 1$
113	0.12741	$x^3 - x^2 - 1$
127	0.18747	$x^3 - x^2 + 2\,x - 1$
131	0.093733	$x^3 - x^2 + 1$
137	0.20313	$x^3 - x^2 - x - 1$
139	0.18747	$x^3 - x^2 + 2\,x - 1$
149	0.23105	$x^3 - x^2 - 2$
151	0.093733	$x^3 - x - 1$
157	0.12741	$x^3 - x^2 - 1$
163	0.093733	$x^3 - x - 1$

Continued on next page

TABLE 4.1 – continued from previous page

p	$\tau_{3,p}$	f_α
167	0.093733	$x^3 - x - 1$
173	0.12741	$x^3 - x^2 - 1$
179	0.23105	$2\,x^3 - 2\,x^2 + 2\,x - 1$
181	0.20313	$x^3 - x^2 - x - 1$
191	0.12741	$x^3 + x - 1$
193	0.093733	$x^3 - x + 1$
197	0.093733	$x^3 - x^2 + 1$

5 An Upper Bound on $\liminf_{d\to\infty} \tau_{d,p}$

The previous two chapters have focused on calculating the height $\tau_{d,p}$ of the smallest non-root of unity totally p-adic algebraic numbers of fixed degree d. In this section, we fix a prime p and consider the set $\{\tau_{d,p} \mid d \geq 2\}$. In particular, what can we say about the smallest accumulation point of the set? In 2006, Bombieri and Zannier [BG06] determined that

$$\liminf_{d\to\infty} \tau_{d,p} \geq \tfrac{\log p}{2(p+1)}.$$

This bound was improved by Fili and Petsche [FP13] to

$$\liminf_{d\to\infty} \tau_{d,p} \geq \tfrac{p\log p}{2(p^2-1)}.$$

In this chapter, we use techniques from arithmetic dynamical systems to establish an upper bound on $\liminf_{d\to\infty} \tau_{d,p}$. The exact value of $\liminf_{d\to\infty} \tau_{d,p}$ is not known, but in the following result we establish an upper bound on this limit infimum that is approximately twice the lower bound provided by Fili-Petsche.

Theorem 5.1. For each prime p, there exist infinitely many $\alpha \in \mathcal{T}_p$ such that $h(\alpha) \leq \frac{\log(p+1)}{p-1}$. In particular,

$$\liminf_{d\to\infty} \tau_{d,p} \leq \tfrac{\log(p+1)}{p-1}.$$

Lemma 5.2. Let p be a prime, and $\phi_p(x) = \frac{1}{p}(x^p - x)$. Then $\phi_p : \mathbb{Z}_p \to \mathbb{Z}_p$ is surjective and p-to-1.

Proof. We first establish that $\phi_p(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$. Let $\alpha \in \mathbb{Z}_p$. By Fermat's Little Theorem,

$$|\phi_p(\alpha)|_p = \left|\tfrac{1}{p}\right|_p |\alpha^p - \alpha|_p \leq p \cdot \tfrac{1}{p} = 1.$$

Let $\beta \in \mathbb{Z}_p$. We want to show that there are p distinct points α that satisfy $\phi_p(\alpha) = \beta$. For this, we apply Hensel's Lemma to the polynomial

$$g(x) = x^p - x - p\beta,$$

noting that $g(x) = 0$ if and only if $\phi_p(x) = \beta$. Let $a \in \{0, 1, 2, \cdots, p-1\}$. By Fermat's Little Theorem and the strong triangle inequality,

$$|g(a)|_p = |(a^p - a) - p\beta|_p \leq \tfrac{1}{p}.$$

Since $|pa^{p-1}|_p < 1$, we have equality in the strong triangle inequality, and thus

$$|g'(a)|_p = \left|pa^{p-1} - 1\right|_p = 1.$$

For each a, Hensel's Lemma indicates that there is a unique root in $\mathbb{Z}_p$ congruent to a. This finds p distinct roots, and this ϕ_p is p-to-1. □

Remark. Given $\alpha \in \phi^{-k}(1)$, we note that all of the algebraic conjugates of α are also in $\phi^{-k}(1)$, because α is a root of $\phi^k(x) - 1$ and hence its minimal polynomial over $\mathbb{Q}$ is a divisor of $\phi^k(x) - 1$. We can conclude from this observation and Lemma 5.2 that the set $\phi^{-k}(1)$ consists entirely of totally p-adic algebraic numbers.

Lemma 5.3. For distinct nonnegative integers k and k', the sets $\phi_p^{-k}(1)$ and $\phi_p^{-k'}(1)$ are disjoint.

Proof. For a proof by contradiction, suppose there exists some α such that $\phi_p^k(\alpha) = \phi_p^{k'}(\alpha) = 1$. Without loss of generality, suppose $k' > k$, with $k' = k + \ell$. Then

$$1 = \phi_p^{k'}(\alpha) = \phi_p^{\ell}\left(\phi_p^k(\alpha)\right) = \phi_p^{\ell}(1).$$

This implies that 1 is a periodic point. However, 1 is not a periodic point since $\phi_p(1) = 0$, 0 is fixed. Thus, no such α exists. □

For each $k \in \mathbb{N}$, select $\alpha_k \in \phi_p^{-k}(1)$. Let $\mathcal{A}$ be the set of α_k chosen. By Lemma 5.3, the α_k are distinct, and thus $\mathcal{A}$ contains infinitly many distinct totally p-adic numbers.

Lemma 5.4. Let K be a number field containing α_k, and v a place of K. Then

(a) $|\alpha_k|_v \leq 1$ for $v \nmid \infty$, and

(b) $|\alpha_k|_v \le (1+p)^{1/(p-1)}$ for $v \mid \infty$.

Proof. **(a)** Suppose v is a non-archimedean place of K, with $v \nmid p$. Then α_k is a root of $f(x) = \phi_p^k(x) - 1$. The polynomial $f(x)$ has v-integral coefficients. In particular, the leading coefficient, a power of $\frac{1}{p}$, is a v-adic unit, and thus α_k is v-integral.

Now suppose $v \mid p$. By Lemma 5.2, all points in the backwards orbit of 1 are in $\mathbb{Z}_p$, so $|\alpha_k|_v \le 1$.

Since α_k is a preperiodic point, it has bounded forward orbit. Therefore, to prove part **(b)**, it will suffice to show that if $\alpha \in K$ satisfies $|\alpha|_v > (1+p)^{1/(p-1)}$, then $|\phi_p^n(\alpha)|_v \to +\infty$ as $n \to +\infty$.

Let $\alpha \in K$ with $|\alpha|_v > (1+p)^{1/(p-1)}$, and let $\epsilon > 0$ such that

$$|\alpha| > (1 + p + p\epsilon)^{1/(p-1)}.$$

Then

$$\begin{aligned}
|\phi_p(\alpha)|_v &= \left|\tfrac{1}{p}(\alpha^p - \alpha)\right|_v \\
&= \tfrac{1}{p}\,|\alpha|_v \left|\alpha^{p-1} - 1\right|_v \\
&\ge \tfrac{1}{p}\,|\alpha|_v \left(\left|\alpha^{p-1}\right|_v - 1\right) \\
&\ge \tfrac{1}{p}\,|\alpha|_v\,|p + p\epsilon|_v \\
&= |\alpha|_v\,(1+\epsilon).
\end{aligned}$$

Iterating this inequality gives $|\phi_p^n(\alpha)|_v \ge |\alpha|_v(1+\epsilon)^n$ and therefore $|\phi_p^n(\alpha)|_v \to +\infty$ as $n \to +\infty$. □

Proof of Theorem 5.1. Let $\alpha_k \in \mathcal{A}$. Then

$$\begin{aligned}
h(\alpha_k) &= \sum_{v \in M_K} \log \max\{1, |\alpha_k|_v^{d_v/d}\} \\
&\le \sum_{v \mid \infty} \log \max\{1, |\alpha_k|_v^{d_v/d}\} \\
&\le \sum_{v \mid \infty} \frac{d_v}{d} \log(1+p)^{1/(p-1)}
\end{aligned}$$

$$= \log(1+p)^{1/(p-1)}.$$

Since $\mathcal{A}$ contains infinitely many totally p-adic algebraic numbers, all of which satisfy the inequality above, it must be the case that

$$\liminf_{d\to\infty} \tau_{d,p} \leq \log(1+p)^{1/(p-1)}. \qquad \square$$

Remark. Using the results of Pestche, Szpiro, and Tucker in [PST12], it can be shown that the upper bound of $\frac{\log(p+1)}{p-1}$ can be replaced by the value of the Arakelov-Zhang pairing $\langle \phi_p(x), x^2 \rangle$ of the map ϕ_p with the squaring map. Although this value is smaller than $\frac{\log(p+1)}{p-1}$, it is probably difficult to calculate explicitly in closed form.

The inspiration for the proof for Theorem 5.1 comes from [Smy80], in which Smyth uses a similar dynamical approach to create a small limit of point of heights of totally real algebraic numbers. In Theorem 3 of

Bibliography

AD99. Francesco Amoroso and Sinnou David. Le probleme de Lehmer en dimension supérieure. *Journal fur die Reine und Angewandte Mathematik*, pages 145–179, 1999.

AD00. Francesco Amoroso and Roberto Dvornicich. A lower bound for the height in abelian extensions. *J. Number Theory*, 80(2):260–272, 2000.

Bak06. Matt Baker. Algebraic number theory course notes (fall 2006) Math 8803, Georgia Tech. `http://people.math.gatech.edu/~mbaker/pdf/ANTBook.pdf`, 2006. Accessed: 2017-12-31.

Bil97. Yuri Bilu. Limit distribution of small points on algebraic tori. *Duke Mathematical Journal*, 89(3):465–476, 1997.

BG06. Enrico Bombieri and Walter Gubler. *Heights in Diophantine Geometry*. Number 4 in New Mathematical Monographs. Cambridge University Press, Cambridge, 2006.

BGR84. S. Bosch, U. Güntzer, and R. Remmert. *Non-Archimedean analysis*, volume 261 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1984.

BM71. P. E. Blanksby and H. L. Montgomery. Algebraic integers near the unit circle. *Acta Arith.*, 18:355–369, 1971.

Bre51. Robert Breusch. On the distribution of the roots of a polynomial with integral coefficients. *Proceedings of the American Mathematical Society*, 2(6):939–941, 1951.

BZ01. Enrico Bombieri and Umberto Zannier. A note on heights in certain infinite extensions of $\mathbb{Q}$. *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni*, 12(1):5–14, 2001.

Can74. Georg Cantor. Ueber eine eigenschaft des inbegriffs aller reellen algebraischen zahlen. *Journal für die reine und angewandte Mathematik*, 77:258–262, 1874.

CS68. Girolamo Cardano and C Spon. Ars magna (1545). *Opera Omnia*, 4:221–302, 1968.

Cas86. John William Scott Cassels. *Local fields*, volume 3. Cambridge University Press Cambridge, 1986.

Con18a. Keith Conrad. Galois groups of cubics and quartics (not in characteristic 2). `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf`, 2018. Accessed: 2018-06-14.

Con18b. Keith Conrad. Hensel's lemma. `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/hensel.pdf`, 2018. Accessed: 2018-01-15.

DF04. David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

Dob79. E. Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34:391–401, 1979.

Fal83. Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

FP13. Paul Fili and Clayton Petsche. Energy integrals over local fields and global height bounds. *International Mathematics Research Notices*, page rnt250, 2013.

Gar07. John Garza. On the height of algebraic numbers with real conjugates. *Acta Arith.*, 128(4):385–389, 2007.

Gar08. John Garza. The Mahler measure of dihedral extensions. *Acta Arithmetica*, 131:201–215, 2008.

Gar09. John Garza. The Lehmer strength bounds for total ramification. *Acta Arithmetica*, 137:171–176, 2009.

GIM+10. J. Garza, M. I. M. Ishak, M. J. Mossinghoff, C. G. Pinner, and B. Wiles. Heights of roots of polynomials with odd coefficients. *J. Théor. Nombres Bordeaux*, 22(2):369–381, 2010.

Gou97. Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, second edition, 1997.

Has30. Helmut Hasse. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. *Math. Z.*, 31(1):565–582, 1930.

HS93. G. Höhn and N.-P. Skoruppa. Un résultat de Schinzel. *J. Théor. Nombres Bordeaux*, 5(1):185, 1993.

Mil17. James S. Milne. Fields and Galois theory (v4.53), 2017. Available at www.jmilne.org/math/.

Nor50. D. G. Northcott. Periodic points on an algebraic variety. *Ann. of Math. (2)*, 51:167–177, 1950.

Peta. Clayton Petsche. The height of algebraic units in local fields. *unpublished preprint*.

Petb. Clayton Petsche. Number theory seminar, Spring 2012, Introduction to Arithmetic Dynamics.

Pet05. Clayton Petsche. A quantitative version of Bilu's equidistribution theorem. *International Journal of Number Theory*, 1(02):281–291, 2005.

PST12. Clayton Petsche, Lucien Szpiro, and Thomas Tucker. A dynamical pairing between two rational maps. *Transactions of the American Mathematical Society*, 364(4):1687–1710, 2012.

Pot18. Lukas Pottmeyer. Small totally p-adic algebraic numbers. *arXiv preprint arXiv:1802.05923*, 2018.

The18. The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.2)*, 2018. `http://www.sagemath.org`.

Sch73. A. Schinzel. On the product of the conjugates outside the unit circle of an algebraic number. *Acta Arith.*, 24:385–399, 1973. Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday. IV.

Smy71. C.J. Smyth. On the product of the conjugates outside the unit circle of an algebraic integer. *Bull. London Math. Soc.*, 3:169–175, 1971.

Smy80. C.J. Smyth. On the measure of totally real algebraic integers. *Journal of the Australian Mathematical Society*, 30(2):137–149, 1980.

Ste78. Cameron L. Stewart. Algebraic integers whose conjugates lie near the unit circle. *Bull. Soc. Math. France*, 106(2):169–176, 1978.

WP28. André Weil and Emile Picard. L'arithmétique sur les courbes algébraiques: thèses présentées à la faculté des sciences de l'université de paris pour obtenir le grade de docteur ès sciences mathématiques. 1928.

APPENDICES

A Code to Create a List of Polynomials

All code was written for SageMath, Version 8.2 [The18]. The function **MahlerMeasureCubic** calculates the Mahler measure of the cubic polynomial $f(x) = ax^3 + bx^2 + cx + d$. The function accepts the integers a, b, c, and d as input, and returns the Mahler measure of f, rounded to ten decimal places. We use the built in Sage function **roots()** to find the roots of f, and then calculate the Mahler measure.

```
def MahlerMeasureCubic(a,b,c,d):
    M=a
    Poly=a*x^3+b*x^2+c*x+d
    Roots=Poly.roots(CC)
    for i in [0..len(Roots)-1]:
        M=M*max(1,abs(Roots[i][0]))
    return M.n(digits=10)
```

The following program creates a list of all irreducible cubic polynomials with Mahler measure bounded above by 8.5. This threshold is high enough to obtain the covering property needed in the proof of Theorem 3.13. By the height-length bound, we know to find all such polynomials it is sufficient to check all irreducible polynomials with length bounded above by 68. The program culls any polynomial that is either reducible or has Mahler measure greater than 8.5. We use the built in Sage function **is_irreducible()** to determine if a polynomial is irreducible over $\mathbb{Q}$.

In addition to the polynomial and Mahler measure, the list also contains the coeffcients of the depressed cubic, A and B, and discriminant of the polynomial, and the height of the roots. The output of this program is saved as the file **irred_polynomials_L68**, and is used by the programs in Appendix B and Appendix D.

```
R.<x> = QQ[]
Polynomials=[]
L=68
for a in [1..L]:
    for b in [-L+abs(a)..L-abs(a)]:
        for c in [-L+abs(a)+abs(b)..L-abs(a)-abs(b)]:
            for d in [-L+abs(a)+abs(b)+abs(c)..L-abs(a)-abs(b)-abs(c)]:
                Poly=a*x^3+b*x^2+c*x+d
                if Poly.is_irreducible()==True:
                    MM=MahlerMeasureCubic(a,b,c,d)
                    A=(3*a*c-b^2)/(3*a^2)
                    B=(27*a^2*d-9*a*b*c+2*b^3)/(27*a^3)
                    Delta=B^2+4*A^3/27
                    h=1/3*log(MM);
                    if MM <= L/8:
                        Polynomials.append([MM,a,b,c,d,A,B,Delta,h])
Polynomials=sorted(Polynomials)
print 'done'
save(Polynomials,'irred_polynomials_L68')
```

B Code to Create a List of Cubic Abelian Numbers

This function loads the list of all irreducible cubic polynomials in $\mathbb{Z}[x]$ with Mahler measure bounded above by 8.5, as created in Appendix A. For each polynomial f, this program calculates the discriminant of the polynomial.

In general, the Galois group of a polynomial $f(x) \in \mathbb{Z}[x]$ of degree d is a subgroup of A_d if and only if the discrimant of f is a square in $\mathbb{Q}$ [Con18a, Theorem 1.3]. If f is a cubic polynomial, as it is here, then the Galois group of f is A_3, and thus abelian, if and only if the discriminant of f is a square in $\mathbb{Q}$.

If f is abelian, then the program calculates the discriminant of K, the number field obtained by adjoining the roots of f to $\mathbb{Q}$, by applying the built in function **absolute_discriminant()**. It then applies Theorem 3.11 and uses the built in Sage command **factor()** to determine the conductor of K. All of this data is stored in the array **AbelianCubics**, and the array is printed as a LaTeX ready table.

```
Polynomials=load('irred_polynomials_L68')
L=len(Polynomials)
AbelianCubics=[]

for i in [0..L-1]:
    Poly=Polynomials[i];
    a=Poly[1];
    b=Poly[2];
    c=Poly[3];
    d=Poly[4];
    D=b^2*c^2-4*a*c^3-4*b^3*d-27*a^2*d^2+18*a*b*c*d;

    if D.is_square()==True:
        K.<j>=NumberField(a*x^3+b*x^2+c*x+d)
        DD=K.absolute_discriminant()
        MM=Poly[0];
        h=Poly[8];
        Factors=DD.factor()
        ListOfFactors=list(Factors)
        L=len(ListOfFactors)
        Cond=1

        for i in [0..L-1]:
            Cond=Cond*ListOfFactors[i][0]
            if ListOfFactors[i][0]==3:
                Cond=Cond*3
        C=Cond
        AbelianCubics.append([h,a*x^3+b*x^2+c*x+d,DD,C]);

latex(table(AbelianCubics))
```

C Code to Determine Congruence Condtions for Splitting

After running the code in Appendix B, we run the following program, which checks the array **AbelianCubics**, and for each polynomial f_{α_i} with conductor m_i, determines the elements of the subgroup of $(\mathbb{Z}/m_i\mathbb{Z})^\times$, B_{α_i}, for which f_{α_i} splits over $\mathbb{Q}_p$ if $[p] \in B_{\alpha_i}$.

```
AbelianCubics=load('AbelianCubics')
L=len(AbelianCubics);
P = Primes();

for i in [0..L-1]:
    Poly=AbelianCubics[i][1]
    PolyList=Poly.list()
    a=PolyList[3]
    b=PolyList[2]
    c=PolyList[1]
    d=PolyList[0]
    Cond=AbelianCubics[i][3]
    v=[1];

    for j in [0..50]:
        for k in [1..P[j]-1]:
            A=Integer(a*k^3+b*k^2+c*k+d)
            A=A%P[j]
            B=Integer(3*a*k^2+2*b*k+c)
            B=B%P[j]
            if A==0 and B>0:
                v.append(P[j]%Cond)

    V=sorted(v)
    V=set(V)
    AbelianCubics[i]
    V
```

D Code to Determine $\tau_{d,p}$ for all $5 \leq p \leq N$

The function **IsCubeInFp** takes in integers a and p. It returns **True** if a is a cube in $\mathbb{Z}/p\mathbb{Z}$, and **False** otherwise.

```
def IsCubeInFp(a,p):
    b=0
    while b<p:
        if Mod(b,p)^3==Mod(a,p):
            return True
        b=b+1
    return False
```

The function **IsCubeInQp** determines if the p-adic number A is a cube in $\mathbb{Q}_p$ by applying Lemma 4.3.

```
def IsCubeInQp(A,p):
    val=A.ordp();
    if 3.divides(val)==True:
        L=A.list();
        a=L[0];
        if IsCubeInFp(a,p)==True:
            return True;
    return False
```

The function **IsCubeInK** checks to see if $A + B\sqrt{-3}$ is a cube in $K = \mathbb{Q}_p(\sqrt{-3})$ by applying Lemma 4.8.

```
def IsCubeInK(A,B,p):
    A=K(A);
    B=K(B);
    AA=A.list();
    BB=B.list();
    A0=AA[0];
    B0=BB[0];

    if A.abs()<1:
        A0=0
    if B.abs()<1:
        B0=0
    for c in [0..p-1]:
        for d in [0..p-1]:
            if (c*c*c-9*c*d*d)%p==A0:
                if (3*c*c*d-3*d*d*d)%p==B0:
                    return True
    return False
```

The function **TauDP1mod3** determines $\tau_{3,p}$ for the prime p where $p \equiv 1 \pmod 3$, by implementing the algorithm described in Theorem 4.4. We use the built in Sage command **is_padic_square()** to determine if a number is a square in $\mathbb{Q}_p$.

```
def TauDP1mod3(p):
    i=0;
    while i < L-1:
        A=Polynomials[i][5];
        B=Polynomials[i][6];
        D=Polynomials[i][7];
        A=K(A);
        B=K(B);
        D=K(D);

        if QQ(D).is_padic_square(p)==True:
            if A==0:
                C=-B;
            if A!=0:
                C=D.square_root();
            Check=(C-B)/2;
            if IsCubeInQp(Check,p)==True:
                return Polynomials[i]
        i=i+1;
    return False
```

The function **TauDP2mod3** determines $\tau_{3,p}$ for the prime p where $p \equiv 2 \pmod 3$, by implementing the algorithm described in Theorem 4.9. We use the built in Sage command **is_padic_square()** to determine if a number is a square in $\mathbb{Q}_p$.

```
def TauDP2mod3(p):
    i=0;
    while i < L-1:
        D=Polynomials[i][7];

        if D.is_padic_square(p)==False:
            b=D/(-3);

            if b.is_padic_square(p)==True:
                a=Polynomials[i][6]/2;
                b=K(b);
                b=sqrt(b);

                if IsCubeInK(a,b,p)==True:
                    return Polynomials[i]
        i=i+1;
    return False
```

The following code determines $\tau_{3,p}$ for all primes p greater than 5, up to and including the N^{th} prime. The output is a LaTeX ready table.

```
Polynomials=load('irred_polynomials_L68')
L=len(Polynomials)
P=Primes(); # P is now a list of all primes
N=25
rows = [['P', '$\tau_{3,p}$', 'Polynomial']]

for i in[2..N]:
    p=P.unrank(i);
    K = Qp(p, prec = 6, type = 'capped-rel', print_mode = 'series');

    if p%3==1:
        tdp=TauDP1mod3(p)
        Poly=tdp[1]*x^3+tdp[2]*x^2+tdp[3]*x+tdp[4];
        h=tdp[8].n(digits=5);
        rows.append([p,h,Poly])

    if p%3==2:
        tdp=TauDP2mod3(p)
        Poly=tdp[1]*x^3+tdp[2]*x^2+tdp[3]*x+tdp[4];
        h=tdp[8].n(digits=5);
        rows.append([p,h,Poly])

latex(table(rows=rows, frame=True))
```