2021-12-09

Totally p-adic Numbers of Degree 4

Melissa Janet Ault
Brigham Young University

Totally p-adic Numbers of Degree 4

Melissa Janet Ault

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Darrin Doud, Chair
David Cardon
Jasbir Chahal

Department of Mathematics

Brigham Young University

ABSTRACT

Totally p-adic Numbers of Degree 4

Melissa Janet Ault
Department of Mathematics, BYU
Master of Science

In this thesis, we extend results of Emerald Stacy to compute an upper bound on the minimal height of a totally p-adic algebraic integer α of degree 4 independent of p. We also compute actual values of the minimal height of a totally p-adic algebraic integer α of degree 4 for small primes p.

Keywords: totally p-adic, algebraic numbers, logarithmic height, number fields

Acknowledgements

Thanks to my adviser, Dr. Darrin Doud, for all the help with writing this thesis. Thanks to my parents, roommates, and friends for giving me moral support throughout my time here.

Contents

List of Tables

List of Figures

Chapter 1. Introduction

For an algebraic number α with minimal polynomial f_α over $\mathbb{Q}$, we define the Mahler measure of f_α to be

$$M(f_\alpha) = |a| \prod_{i=1}^{n} \max\{1, |\alpha_i|\}$$

where a is the leading coefficient of f_α, $n = \deg(f_\alpha)$, and $\{\alpha_1, \ldots, \alpha_n\}$ are the roots of f_α.

The logarithmic Weil height of α [1] is then

$$h(\alpha) = \frac{1}{n} \log M(f_\alpha)$$

where d is the degree of f_α. The Mahler measure of the minimal polynomial of α and the Weil height of α are measures of the complexity of α and allow us to sort algebraic numbers by height, which is useful in many applications.

In 1975, Schinzel proved [4] that if α is a totally real algebraic integer not equal to 0 or ± 1 then

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

In a recent paper [5], Emerald Stacy studied a p-adic analogue of this theorem. She proved that for any p, there exists a real number $\tau_{3,p}$ such that every totally p-adic algebraic number α of degree 3 has $h(\alpha) \geq \tau_{3,p}$. Stacy also calculated an upper bound for $\tau_{3,p}$ independent of p and computed actual values of $\tau_{3,p}$ for small primes.

In this thesis, we extend Stacy's results to prove that for every prime p, there exists a real number $\tau_{4,p}$ such that every totally p-adic algebraic number α of degree 4 has $h(\alpha) \geq \tau_{4,p}$. (See theorem 5.1) We will also calculate a bound for $\tau_{4,p}$ independent of p, and compute actual values of $\tau_{4,p}$ for primes less than or equal to 500.

Our ideas are based on the methods that Stacy used. We begin by studying two different types of Galois extension, generated by degree 4 number fields, which we will use to find the bound $\tau_{4,p}$. We use the fact that given a Galois number field, every prime number has a Frobenius in the Galois group of that number field, and if the number field is abelian, p

splits completely in the fixed field of the Frobenius. We also use the fact that if α generates a number field in which p splits completely, then α is totally p-adic. Using these facts, we are able to show that there is a finite set of number fields such that every prime, with finitely many exceptions, splits completely in at least one of the number fields. We search the number fields to find a generator α of each number field with small Mahler measure. Since every prime p splits in one of the number fields, the largest Mahler measure of these α's will give an upper bound for $\tau_{4,p}$ for all p except for the finitely many exceptional primes. We deal with these exceptional primes separately. We thus find that for any prime p, there is a totally p-adic α whose minimal polynomial has Mahler measure less than or equal to 9. Hence we find that for any prime p, $\tau_{4,p} \leq \frac{\log 9}{4} = \frac{\log 3}{2}$.

In addition, we created a sorted list of all irreducible polynomials of degree 4 with Mahler measure smaller than 9. We used bounds from [1] to bound the coefficients of any polynomial of Mahler measure less than 9. This produced a finite list of polynomials containing all of the polynomials of degree 4 with Mahler measure less than 9. We searched through them, sifted out the ones with Mahler measure actually less than 9 and put them into a sorted list. For a given prime p, we can search this list to find the polynomial with smallest Mahler measure that defines a number field in which p splits completely. The height $h(\alpha)$ of a root α of this smallest polynomial will be the actual value of $\tau_{4,p}$.

Chapter 2. Algebraic Number Theory Background

2.1 Splitting of primes in number fields

We'll begin by introducing and defining some terminology that comes from [2].

Definition 2.1. A *number field* is a subfield of $\mathbb{C}$ that has finite degree over $\mathbb{Q}$. Every such field can be written as $\mathbb{Q}(\alpha)$ for some algebraic number α.

Definition 2.2. A *Dedekind domain* is an integral domain R that satisfies the following conditions:

(i) Every ideal is finitely generated.

(ii) Every nonzero prime ideal is a maximal ideal

(iii) R is integrally closed in its field of fractions

$$K = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in R, \beta \neq 0 \right\}.$$

This brings us to a theorem proved in [2]:

Theorem 2.3. *Every ideal in a Dedekind domain is uniquely representable as a product of prime ideals.*

Now let $\mathbb{A}$ be the set of algebraic integers in $\mathbb{C}$ and let K be a number field.

Definition 2.4. A *number ring* is a subring $\mathcal{O}_K = \mathbb{A} \cap K$ of K.

Theorem 2.5. *Every number ring is a Dedekind domain.*

This tells us that the ring $\mathbb{A}$ is a Dedekind domain. Let L, K be number fields where $K \subset L$ and let $\mathcal{O}_L$ and $\mathcal{O}_K$ be their number rings, respectively. Let $\mathfrak{p} \subset \mathcal{O}_K$ and $\mathfrak{P} \subset \mathcal{O}_L$ be prime ideals. We can easily see that $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$, so Theorem 2.3 tells us that it has a unique factorization into prime ideals of $\mathcal{O}_L$.

Definition 2.6. The *ramification index* e of $\mathfrak{P}$ over $\mathfrak{p}$ is the exact power of $\mathfrak{P}$ that divides $\mathfrak{p}\mathcal{O}_L$. The notation is $e(\mathfrak{P}/\mathfrak{p})$.

Definition 2.7. We say that $\mathfrak{P}$ *lies over* $\mathfrak{p}$ if the following conditions hold (which also end up being equivalent):

(i) $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$

(ii) $\mathfrak{P} \supset \mathfrak{p}\mathcal{O}_L$

(iii) $\mathfrak{P} \supset \mathfrak{p}$

(iv) $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$

(v) $\mathfrak{P} \cap K = \mathfrak{p}$.

We know that $\mathcal{O}_K$ and $\mathcal{O}_L$ are Dedekind domains from Theorem 2.5, which means that every nonzero prime ideal in these rings is a maximal ideal. Let $\mathfrak{P}$ and $\mathfrak{p}$ be primes with $\mathfrak{P}$ lying over $\mathfrak{p}$. Then $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{P}$ are fields.

In the proof of Theorem 14 in [2], we get the following theorem:

Theorem 2.8. *If I is a nonzero ideal in a number ring R, then R/I is finite.*

This gives us the fact that every prime ideal in a number ring has finite index.

Definition 2.9. The *residue fields* associated with $\mathfrak{p}$ and $\mathfrak{P}$ are the fields $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{P}$, respectively.

We see that $\mathcal{O}_K \subset \mathcal{O}_L$ since $K \subset L$, and if $\mathfrak{P}$ lies over $\mathfrak{p}$, there is a natural inclusion $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}$. Hence, $\mathcal{O}_L/\mathfrak{P}$ is an extension over $\mathcal{O}_K/\mathfrak{p}$ of finite degree since both residue fields are finite.

Definition 2.10. The *inertial degree* f of $\mathfrak{P}$ over $\mathfrak{p}$ is the degree of the finite extension $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$. The notation is $f(\mathfrak{P}/\mathfrak{p})$.

Definition 2.11. $\mathfrak{p}$ is *ramified* in $\mathcal{O}_L$ if and only if $e(\mathfrak{P}/\mathfrak{p}) > 1$ for some prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying over $\mathfrak{p}$.

Definition 2.12. A prime ideal $\mathfrak{p}$ of K *splits completely* in L if and only if $\mathfrak{p}$ splits into $[L : K]$ distinct primes, where each prime has ramification index and inertial degree of 1.

2.2 Completion of number fields at prime ideals

First we want to define $\mathfrak{p}$-adic valuations. Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$.

Definition 2.13. The discrete $\mathfrak{p}$-*adic valuation* $v_{\mathfrak{p}}(x)$ on $\mathcal{O}_K$ (where $x \in \mathcal{O}_K$) is the power of $\mathfrak{p}$ in the factorization of the ideal $\mathcal{O}_K x$ if $x \neq 0$. If $x = 0$, we say that $v_{\mathfrak{p}}(x) = \infty$. We can also say that $(x) = \mathfrak{p}^{v_{\mathfrak{p}}(x)} \cdot I$ for $x \in \mathcal{O}_K$, where I is an ideal that is prime to $\mathfrak{p}$.

Theorem 2.14. *The function $v_{\mathfrak{p}} : \mathcal{O}_K \to \mathbb{Z} \cup \{\infty\}$ satisfies the following conditions:*

(i) $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$.

Proof. Let $(x) = \mathfrak{p}^{v_{\mathfrak{p}}(x)} \cdot I$ and $(y) = \mathfrak{p}^{v_{\mathfrak{p}}(y)} \cdot J$. Using properties of ideals, we see that

$$\begin{aligned} (xy) &= (x)(y) \\ &= \mathfrak{p}^{v_{\mathfrak{p}}(x)} \cdot I \cdot \mathfrak{p}^{v_{\mathfrak{p}}(y)} \cdot J \qquad \text{where } I \text{ and } J \text{ are relatively prime ideals} \\ &= \mathfrak{p}^{v_{\mathfrak{p}}(x)+v_{\mathfrak{p}}(y)} \cdot I \cdot J. \end{aligned}$$

Hence, we see that $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$. □

(ii) $v_{\mathfrak{p}}(x + y) \geq \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}$.

Proof. Again let $(x) = \mathfrak{p}^{v_{\mathfrak{p}}(x)} \cdot I$ and $(y) = \mathfrak{p}^{v_{\mathfrak{p}}(y)} \cdot J$ and let $m = \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}$. Then $x \in \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ and $y \in \mathfrak{p}^{v_{\mathfrak{p}}(y)}$. We can also see that both $\mathfrak{p}^{v_{\mathfrak{p}}(x)}$ and $\mathfrak{p}^{v_{\mathfrak{p}}(y)}$ are subsets of $\mathfrak{p}^m$. This means that $x + y \in \mathfrak{p}^m$, so then $\mathfrak{p}^m \mid (x + y)$. Thus, $v_{\mathfrak{p}}(x + y) \geq m$. □

We can also extend $v_{\mathfrak{p}}$ to K by the property

$$v_{\mathfrak{p}}\left(\frac{x}{y}\right) = v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(y).$$

We now define $\|x\|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$, where $N(\mathfrak{p}) = \|\mathcal{O}_K/\mathfrak{p}\|$.

Theorem 2.15.

$$\|x + y\|_{\mathfrak{p}} \leq \|x\|_{\mathfrak{p}} + \|y\|_{\mathfrak{p}}.$$

Proof.

$$\begin{aligned}\|x + y\|_{\mathfrak{p}} &= N(\mathfrak{p})^{-v_{\mathfrak{p}}(x+y)} \\ &\leq N(\mathfrak{p})^{-\min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}} \\ &= \max\{\|x\|_{\mathfrak{p}}, \|y\|_{\mathfrak{p}}\} \\ &\leq \|x\|_{\mathfrak{p}} + \|y\|_{\mathfrak{p}}.\end{aligned}$$

□

Now we recall some definitions:

Definition 2.16. An *absolute value* on a field K is a function $\|\cdot\| : K \to \mathbb{R}$ satisfying

(i) $\|\alpha\beta\| = \|\alpha\|\|\beta\|$

(ii) $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$

(iii) $\|\alpha\| = 0 \iff \alpha = 0$.

Examples:

1. The restriction of the absolute value on $\mathbb{C}$ to K and to its conjugates are absolute values on K.

2. The $\mathfrak{p}$-adic absolute value $\|\cdot\|_{\mathfrak{p}}$ on K is an absolute value on K.

Remarks:

1. The $\mathfrak{p}$-adic absolute value on K satisfies a stronger version of part (ii) in Theorem 2.14:

$$\|\alpha + \beta\|_{\mathfrak{p}} \leq \max\{\|\alpha\|_{\mathfrak{p}}, \|\beta\|_{\mathfrak{p}}\}. \tag{2.1}$$

An absolute value satisfying 2.1 is a non-archimedean absolute value. Otherwise, it is archimedean.

2. Ostrowski has a theorem that states that the $\mathfrak{p}$-adic valuations are the only (not equivalent) non-archimedean valuations on K, whereas by the Gelfand-Tornheim theorem, the archimedean valuation of K given in example 1 are the only such valuations on K.

3. The archimedean absolute value on $\mathbb{Q}$ is usually denoted by $\|\cdot\|_\infty$ and is said to correspond to the infinite prime $p = \infty$.

Definition 2.17. A *Cauchy sequence* in a field K with absolute value $\|\cdot\|$ is a sequence $\{a_n\}$ ($a_n \in K$) such that for any $\varepsilon > 0$, there is an N such that

$$\|a_n - a_m\| < \varepsilon \quad \text{for all} \quad m, n > N.$$

A sequence $\{a_n\}$ converges to a number a if

$$\lim_{n\to\infty} \|a - a_n\| = 0.$$

We define multiplication and addition of Cauchy sequences as

(i) $\{a_n\} + \{b_n\} = \{a_n + b_n\}$

(ii) $\{a_n\} \cdot \{b_n\} = \{a_n b_n\}$.

Now we want to prove some theorems:

Theorem 2.18. *The set $\mathfrak{C}$ of all Cauchy sequences in a field K with absolute value $\|\cdot\|$ is a ring.*

Proof. First we check that $\mathfrak{C}$ is an abelian additive group. Let $\{a_n\}, \{b_n\} \in \mathfrak{C}$. Then for $\varepsilon > 0$, there exist N_1, N_2 such that

$$\|a_n - a_m\| < \frac{\varepsilon}{2} \quad \text{for } n, m > N_1$$
$$\|b_n - b_m\| < \frac{\varepsilon}{2} \quad \text{for } n, m > N_2.$$

Let $N = \max\{N_1, N_2\}$. Then we see that

$$\begin{aligned}
\|(a_n + b_n) - (a_m + b_m)\| &= \|a_n - a_m + b_n - b_m\| \\
&\leq \|a_n - a_m\| + \|b_n - b_m\| \\
&< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.
\end{aligned}$$

So $\{a_n\} + \{b_n\} \in \mathfrak{C}$.

We see that addition is commutative because addition in K is commutative, so

$$\begin{aligned}
\{a_n\} + \{b_n\} &= \{a_n + b_n\} \\
&= \{b_n + a_n\} \\
&= \{b_n\} + \{a_n\}.
\end{aligned}$$

Now let $\{c_n\} \in \mathfrak{C}$. Consider

$$\begin{aligned}
(\{a_n\} + \{b_n\}) + \{c_n\} &= \{a_n + b_n\} + \{c_n\} \\
&= \{a_n + b_n + c_n\} \\
&= \{a_n\} + \{b_n + c_n\} \\
&= \{a_n\} + (\{b_n\} + \{c_n\}).
\end{aligned}$$

So addition is associative. Clearly, $\{\mathbf{0}\} = \{0, 0, \ldots, 0\}$ is a Cauchy sequence, and $\{a_n\} + \{\mathbf{0}\} = \{a_n\} = \{\mathbf{0}\} + \{a_n\}$, so $\mathfrak{C}$ has an additive identity. Then if we consider the element $\{-a_n\} \in \mathfrak{C}$, we see

$$\begin{aligned}
\{a_n\} + \{-a_n\} &= \{a_n - a_n\} \\
&= \{0\} \\
&= \{-a_n + a_n\} \\
&= \{-a_n\} + \{a_n\}.
\end{aligned}$$

So every element has an additive inverse. Thus, $\mathfrak{C}$ is an abelian additive group. Now we consider multiplication. We show $\mathfrak{C}$ is closed under multiplication. It is known that Cauchy sequences are bounded, so $\|a_n\| \leq B_1$ and $\|b_n\| \leq B_2$. Since $\{a_n\}$ and $\{b_n\}$ are Cauchy sequences, we have that there exist N_1, N_2 such that for $\varepsilon > 0$,

$$\|a_n - a_m\| < \frac{\varepsilon}{2B_2} \quad \text{for } n, m > N_1$$
$$\|b_n - b_m\| < \frac{\varepsilon}{2B_1} \quad \text{for } n, m > N_2.$$

We see that

$$\begin{aligned}\|a_n b_n - a_m b_m\| &= \|a_n b_n - a_n b_m + a_n b_m - a_m b_m\| \\ &\leq \|a_n b_n - a_n b_m\| + \|a_n b_m - a_m b_m\| \\ &= \|a_n\| \|b_n - b_m\| + \|b_m\| \|a_n - a_m\| \\ &< B_1\left(\frac{\varepsilon}{2B_1}\right) + B_2\left(\frac{\varepsilon}{2B_2}\right) = \varepsilon.\end{aligned}$$

So $\{a_n\}\{b_n\} \in \mathfrak{C}$. We see that since K is a field,

$$\begin{aligned}\{a_n\} \cdot \{b_n\} &= \{a_n b_n\} \\ &= \{b_n a_n\} \\ &= \{b_n\} \cdot \{a_n\}.\end{aligned}$$

So multiplication is commutative. We also see that

$$\begin{aligned}(\{a_n\} \cdot \{b_n\}) \cdot \{c_n\} &= \{a_n b_n\} \cdot \{c_n\} \\ &= \{a_n b_n c_n\} \\ &= \{a_n\} \cdot \{b_n c_n\} \\ &= \{a_n\} \cdot (\{b_n\} \cdot \{c_n\}).\end{aligned}$$

So multiplication is associative. Clearly, $\{1\} = \{1, 1, \ldots, 1\}$ is a Cauchy sequence, and $\{a_n\} \cdot \{1\} = \{a_n\} = \{1\} \cdot \{a_n\}$, so $\mathfrak{C}$ has a multiplicative identity. Finally, consider

$$\begin{aligned}(\{a_n\} + \{b_n\}) \cdot \{c_n\} &= \{a_n + b_n\} \cdot \{c_n\} \\ &= \{(a_n + b_n) \cdot c_n\} \\ &= \{a_n c_n + b_n c_n\} \\ &= \{a_n\}\{c_n\} + \{b_n\}\{c_n\}.\end{aligned}$$

Because the ring is commutative, the left distributive law also holds. Thus, $\mathfrak{C}$ is a commutative ring with identity. □

Now let $\mathfrak{N}$ be the set of all Cauchy sequences that converge to 0.

Theorem 2.19. *The set $\mathfrak{N}$ of all Cauchy sequences in a field K that go to 0 is a maximal ideal. Hence $K_p = \mathfrak{C}/\mathfrak{N}$ is a field, containing K as a subfield.*

Proof. First we show that $\mathfrak{N}$ is an ideal. Clearly $\{0\} \in \mathfrak{N}$, so $\mathfrak{N} \neq \varnothing$. Let $\{a_n\}, \{b_n\} \in \mathfrak{N}$. Then $\|a_n\| < \frac{\varepsilon}{2}$ and $\|b_n\| < \frac{\varepsilon}{2}$. Consider

$$\|a_n + b_n\| \leq \|a_n\| + \|b_n\| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

so $\{a_n\}, \{b_n\} \in \mathfrak{N}$. and it is closed under addition. Now say $\|a_n\| < \sqrt{\varepsilon}$ and $\|b_n\| < \sqrt{\varepsilon}$. Then

$$\|a_n b_n\| = \|a_n\| \cdot \|b_n\| < \sqrt{\varepsilon} \cdot \sqrt{\varepsilon} = \varepsilon.$$

So $\{a_n\} \cdot \{b_n\} \in \mathfrak{N}$ and $\mathfrak{N}$ is closed under multiplication. Now let $\{a_n\} \in \mathfrak{N}$ and $\{b_n\} \in \mathfrak{C}$. Again, since Cauchy sequences are bounded, we have that $\|b_n\| \leq B$. Now let $\|a_n\| < \frac{\varepsilon}{B}$, so

$$\|a_n b_n\| = \|a_n\| \cdot \|b_n\| < \frac{\varepsilon}{B} \cdot B = \varepsilon$$

and thus $\{a_n\} \cdot \{b_n\} \in \mathfrak{N}$. It is similar for $\{b_n\} \cdot \{a_n\}$ since K is a field and multiplication is commutative. Thus, $\mathfrak{N}$ is an ideal.

Now we show $\mathfrak{N}$ is maximal. Let $\{a_n\} \in \mathfrak{C} \backslash \mathfrak{N}$, and say $\lim_{n\to\infty} \|a_n\| = c$, where $c \neq 0$. This means there exists an N_1 such that $\big|\|a_n\| - c\big| < \frac{c}{2}$ for all $n > N_1$, so $\frac{c}{2} < \|a_n\| < \frac{3c}{2}$. Since $\{a_n\}$ is a Cauchy sequence, we have that there is an N_2 such that $\|a_n - a_m\| < \frac{\varepsilon c^2}{4}$ for $n, m > N_2$. By assumption, $a_n \neq 0$ for $n > N'$, so all a_n except for a finite many are nonzero. Let $b_n = \frac{1}{a_n}$ for all a_n except the finitely many terms. We see that

$$
\begin{aligned}
\|b_n - b_m\| &= \left\| \frac{1}{a_n} - \frac{1}{a_m} \right\| \\
&= \frac{\|a_n - a_m\|}{\|a_n a_m\|} \\
&< \frac{\varepsilon c^2/4}{c^2/4} \\
&= \varepsilon.
\end{aligned}
$$

So $\{b_n\}$ is a Cauchy sequence.

Then $\{a_n\}\{b_n\} = \{1\} + \{c_n\}$, $\{c_n\} \in \mathfrak{N}$. This means $\mathfrak{N}$ is a maximal ideal and thus $K_p = \mathfrak{C}/\mathfrak{N}$ is a field. □

Definition 2.20. A field K is *complete* if every Cauchy sequence in K converges to an element in K.

Theorem 2.21. *$K_\mathfrak{p}$ is a complete field, with $\|\cdot\| : K_\mathfrak{p} \to \mathbb{R}$ defined by $\|\{\alpha_i\}\| = \lim_{n\to\infty} \|\alpha_n\|$. Moreover, K is dense in $K_\mathfrak{p}$.*

Remarks:

1. The same construction gives $\mathbb{R} = \mathbb{Q}_\mathfrak{p}$ for $p = \infty$.

2. The algebraic closure $\overline{\mathbb{Q}_\mathfrak{p}}$ of $\mathbb{Q}_\mathfrak{p}$ for $p = \infty$ is $\mathbb{R}$.

2.3 Totally p-adic algebraic numbers and algebraic number fields

Definition 2.22. An algebraic number α is *totally p-adic* if every root in $\overline{\mathbb{Q}}_p$ of its minimal polynomial over $\mathbb{Q}$ lies in $\mathbb{Q}_p$.

Remark: If $p = \infty$, totally p-adic is the same as totally real.

Definition 2.23. A number field K is *totally p-adic* if the image of every embedding of K into $\overline{\mathbb{Q}}_p$ lies inside $\mathbb{Q}_p$.

Theorem 2.24. *A number field K is totally p-adic if and only if $K = \mathbb{Q}(\alpha)$, where α is totally p-adic.*

Proof. Suppose K is totally p-adic. Then since K is a number field, we can write $K = \mathbb{Q}(\alpha)$ [2]. Then we can get embeddings of K into $\overline{\mathbb{Q}}_p$ by sending α to a root of its minimal polynomial. Since K was totally p-adic, then α is totally p-adic.

Conversely, assume that $K = \mathbb{Q}(\alpha)$ where α is totally p-adic. Then we can again get embeddings of K into $\overline{\mathbb{Q}}_p$ by sending α to any root of its minimal polynomial. Since α was assumed to be totally p-adic, all of these roots are contained in $\mathbb{Q}_p$. Then the image of K is contained in $\mathbb{Q}_p$ and K is totally p-adic. □

Now that we've talked about totally p-adic algebraic numbers and number fields, we need another lemma to prove our main theorem.

Lemma 2.25. *Let K be a number field. For each embedding $\phi : K \to \overline{\mathbb{Q}}_p$, there is a prime $\mathfrak{p}$ of K lying over p, so that the closure of the image of ϕ is ismorphic to the completion $K_{\mathfrak{p}}$.*

Proof. Let $K = \mathbb{Q}(\alpha)$, where α has minimal polynomial f. The minimal polynomial of α over $\mathbb{Q}$ factors over $\mathbb{Q}_p$ as

$$\prod_{i=1}^{d} m_i$$

where there is a bijection between the factors m_i and the primes $\mathfrak{p}_i$ of K lying over p such that $\deg(m_i) = e_i f_i$, where e_i is the ramification index of $\mathfrak{p}_i$ over $\mathfrak{p}$ and f_i is the inertial degree of $\mathfrak{p}_i$ over $\mathfrak{p}$.

Let α_j be a root of m_j in $\overline{\mathbb{Q}}_p$. By Proposition 4.31 in [3], the primes of K that lie over p are in bijective correspondence with the embeddings of K into $\overline{\mathbb{Q}}_p$ that take α to some α_j; under this correspondence, and with the definitions above, $\mathfrak{p}_i$ corresponds to the embedding that send α to α_j.

Then by Proposition 4.31 [3], we have that $K_{\mathfrak{p}_i}$ is isomorphic to $\mathbb{Q}_p(\alpha_i)$ so that the completion of the image of $K(\alpha)$ inside $\overline{\mathbb{Q}}_p$ is isomorphic to $K_{\mathfrak{p}_i}$. □

Finally, we can prove the main theorem of this section:

Theorem 2.26. *Let $K = \mathbb{Q}(\alpha)$ be a number field. Then K (and hence α) is totally p-adic if and only if p splits completely in $K/\mathbb{Q}$.*

Proof. Assume that K is totally p-adic, and let $\mathfrak{p}$ be a prime of K lying over p with ramification index e and inertial degree f. Then $K_\mathfrak{p}$ is a degree ef extension of $\mathbb{Q}_p$. Since K is dense in $K_\mathfrak{p}$, and K is totally p-adic, we see that $ef = 1$. Since this is true for every prime of K lying over p, we see that p splits completely in K.

Conversely, assume that p splits completely in K. Then by Lemma 2.25, every embedding of K into $\overline{\mathbb{Q}}_p$ has image with closure isomorphic to $K_\mathfrak{p}$. Since p splits completely in K, we know that $K_\mathfrak{p} = \mathbb{Q}_p$. Hence, K is totally p-adic. □

2.4 Frobenius elements and splitting in abelian extensions

Let K, L be number fields where L is a Galois extension of K. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ be their rings of algebraic integers, respectively. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Let G be the Galois group of L/K.

Definition 2.27. The *decomposition group* D is defined as

$$D = D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Definition 2.28. The *inertia group* E is defined as

$$E = E(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P} \quad \forall \alpha \in \mathcal{O}_L\}.$$

This brings us to a theorem from [2]:

Theorem 2.29. *Assume $\mathfrak{p}$ is unramified in L, which means $e(\mathfrak{P}/\mathfrak{p}) = 1$ and $E(\mathfrak{P}/\mathfrak{p})$ is trivial. Then there is an isomorphism from $D(\mathfrak{P}/\mathfrak{p})$ to $H = \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$.*

H has a special generator: $x \mapsto x^{|\mathcal{O}_K/\mathfrak{p}|}$, where $x \in \mathcal{O}_L/\mathfrak{P}$. Then the corresponding automorphism $\phi \in D$ is such that for every $\alpha \in \mathcal{O}_L$,

$$\phi(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \bmod \mathfrak{P}.$$

Definition 2.30. ϕ is called the *Frobenius automorphism* of $\mathfrak{P}$ over $\mathfrak{p}$. The notation is $\phi(\mathfrak{P}/\mathfrak{p})$.

This next theorem is proved in [2]:

Theorem 2.31. *Let L/K be a Galois extension of number fields with* $\mathrm{Gal}(L/K)$ *abelian, let $\mathfrak{p}$ be a prime in K, and let $\mathfrak{P}$ be a prime in L lying over $\mathfrak{p}$. Let $D = D(\mathfrak{P}/\mathfrak{p})$ be the decomposition group of $\mathfrak{P}$ over $\mathfrak{p}$. Then the fixed field L^D is Galois over K, and $\mathfrak{p}$ splits completely in L^D/K and in any subfield K'/K with $K' \subset L^D$.*

Chapter 3. Prior Work

3.1 Emerald Stacy's work for degree 3

In this section, we will look at Emerald Stacy's work on totally p-adic numbers of degree 3 [5]. First we'll need some definitions.

Definition 3.1. An algebraic number α is *totally p-adic* if its minimal polynomial f_α over $\mathbb{Q}$ splits completely over $\mathbb{Q}_\mathfrak{p}$.

Definition 3.2. The *Mahler measure*, denoted $M(f)$, of a polynomial $f(x)$ with leading coefficient a and zeros $\alpha_1, \alpha_2, \ldots, \alpha_n$ is defined as

$$M(f) = |a| \prod_{i=1}^{n} \max\{1, |\alpha_i|\}.$$

Definition 3.3. The *logarithmic Weil height of an algebraic number α of degree 3*, denoted by $h(\alpha)$ is defined by

$$h(\alpha) = \frac{1}{3} \log M(f_\alpha).$$

Definition 3.4. Let $f(x) = \sum_{i=1}^{n} a_i x^i$. The *length of f* is defined by

$$L(f) = \sum_{i=0}^{n} |a_i|.$$

Note: There are only finitely many f of bounded length.

She denotes the smallest height attained by a totally p-adic, nonzero, non-root of unity, algebraic number of degree n as $\tau_{n,p}$. In her paper, she finds the following bound:

Theorem 3.5. $\tau_{3,p} \leq 0.70376$.

She begins by doing a computer search using SageMath to find a list of all cubic polynomials with length less than 68, and she establishes that this list will contain all irreducible and cubic polynomials with roots of height less than 0.70376. Then she removes polynomials that do not have an abelian Galois group. For each of the remaining polynomials, she determines the congruence classes of p for which a root α is totally p-adic. Then she finds 4 polynomials $f_1, \ldots, f_4$ such that all but finitely many primes are in the union of these 4 sets of congruence classes. The primes not included in the union of these congruence classes are 3 and 7, and she finds $\tau_{3,3}$ and $\tau_{3,7}$ separately. Letting α_i be a root of f_i, we then know that for every $p \neq 3, 7$, one of the α_i is totally p-adic. Hence, she finds that $\tau_{3,p} \leq \max\{\tau_{3,3}, \tau_{3,7}, h(\alpha_1), \ldots, h(\alpha_4)\}$, independent of p. So she has an upper bound for $\tau_{3,p}$ for all primes p.

After this, she uses her original list of polynomials to compute the exact value of $\tau_{3,p}$ for primes up to 500.

3.2 Stacy's results in light of Frobenius elements

In her paper, Stacy found 4 cubic extensions $K_1 = \mathbb{Q}(\alpha_1)$, $K_2 = \mathbb{Q}(\alpha_2)$, $K_3 = \mathbb{Q}(\alpha_3)$, and $K_4 = \mathbb{Q}(\alpha_4)$, with the property that for every prime p (with finitely many exceptions, in this case 3 and 7) at least one of the α_i is totally p-adic. She found these α_i by examining cubic polynomials with abelian Galois groups, and computing the congruence classes of primes for which a root of the polynomials is totally p-adic. By combining different sets of congruence classes, she put together this set of four fields.

It turns out that the α_i that she found generate four $\mathbb{Z}/3\mathbb{Z}$ extensions of $\mathbb{Q}$ which are contained in a single $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$-extension of $\mathbb{Q}$. Call this extension L.

The subfield diagram is as follows:

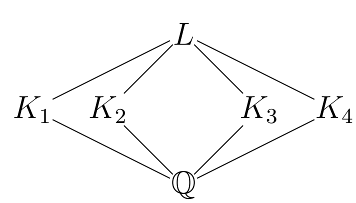

Figure 3.1: Subfield Diagram of a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$-extension $L/\mathbb{Q}$ (all lines denote degree 3 extensions).

We note that in Gal($L/\mathbb{Q}$), every unramified prime has a Frobenius element. Since Gal($L/\mathbb{Q}$) has only elements of order 1 and 3, each Frobenius element has order 1 or 3.

If the Frobenius element of a prime p is of order 1, then its fixed field is L. Hence by Theorem 2.31, p splits completely in L, and hence in each of the K_i. Then Theorem 2.23 tells us that each α_i is totally p-adic.

On the other hand, if the Frobenius element of a prime p is of order 3, then its fixed field is one of the K_i. Hence by Theorem 2.31 p splits completely in one of the K_i. Then Theorem 2.23 tells us that the corresponding α_i is totally p-adic.

Note that this will work for any $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$-extension L; we can obtain a set of four cubic fields with abelian Galois group such that for every prime (except the finitely many primes that ramify in L) one of the four fields is totally p-adic.

We will adapt this new description of the fields found by Stacy to determine a similar set of fields for the degree four problem.

4.1 $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$-extensions

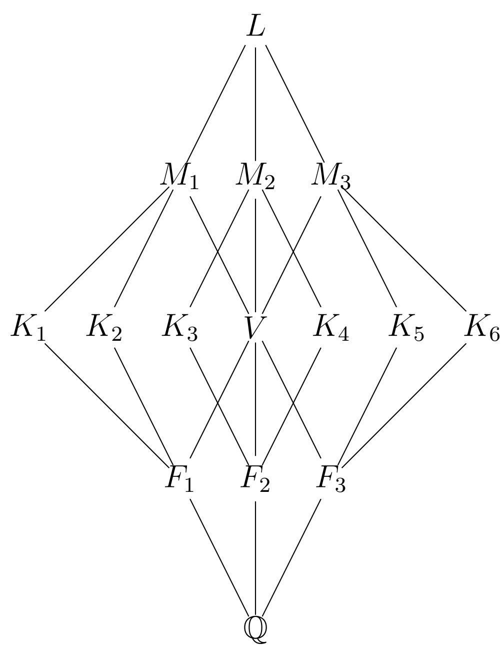

Figure 4.1: Subfield diagram of a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$-extension $L/\mathbb{Q}$ (all lines denote degree 2 extensions).

In order to generalize Stacy's work to degree four polynomials, we wish to find a finite set of number fields in which every prime (with finitely many exceptions) splits completely. We found two ways to do this.

The first way that we found was to look at a Galois extension with Galois group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. In such an extension, the possible orders of Frobenius elements are 1, 2 or 4. By examining the subfield diagram of a $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ extension (see Figure 4.1), we find that such an extension has three degree 8 extensions (the M_i in the diagram), six degree 4 subextensions with cyclic Galois group (the K_i in the diagram) and one Klein four subextension (the V in the diagram). If the Frobenius of a prime p has order 4, the Frobenius would fix a degree four field that is Galois with Galois group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$; i.e., one of the K_i. Hence, p would split completely in this field. If the Frobenius of a prime p has order 2, it will fix a degree 8 field that will contain two of the K_i, in both of which p will split completely. Finally, if the Frobenius of p has order 1, then it fixes the entire field, which contains all six of the K_i in which p would then split completely. Hence, we find that any unramified prime in a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ extension will split completely in at least one of the six degree four cyclic subextensions.

4.2 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-extensions

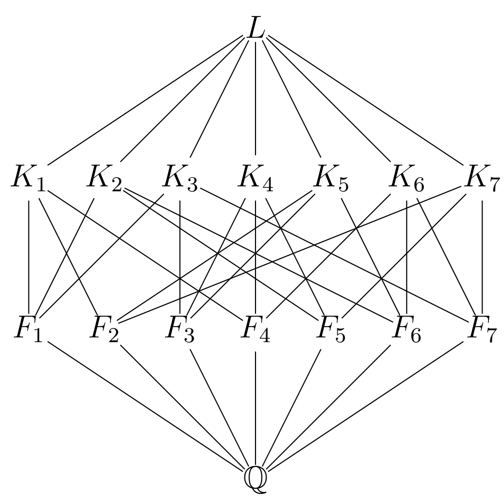

Figure 4.2: Subfield diagram of a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-extension $L/\mathbb{Q}$ (all lines denote degree 2 extensions).

A second way to accomplish this task is to start with an extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (see Figure 4.2). Such a field has seven degree four subextensions, each of which has Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, labeled K_i in the diagram. For any unramified prime p, the Frobenius of p will have order 1 or 2 in this Galois group. If it has order 2, then it fixes one of the K_i, and p will split completely in that K_i. If the Frobenius of p has order 1, then it fixes the entire field, and p splits completely in all seven of the K_i. Hence each prime that is unramified in the larger field will split completely in one or more of the seven K_i.

Because a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extension is easily described as $\mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{c})$ for certain a, b, c, we chose to use this type of extension. In the computations in the next section, we will use three different $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ extensions, namely, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3})$, and $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt{5})$ to get an upper bound on $\tau_{4,p}$.

Chapter 5. Bounding $\tau_{4,p}$ for all p

5.1 Use a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-extension to get a bound that works for all p

Throughout this chapter we use code from PARI/GP [6].

First we need to choose an L that will satisfy the diagram in Figure 4.2. We will choose $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Then we have that $K_1 = \mathbb{Q}(\sqrt{5}, \sqrt{6})$, $K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K_3 = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, $K_4 = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, $K_5 = \mathbb{Q}(\sqrt{2}, \sqrt{15})$, $K_6 = \mathbb{Q}(\sqrt{3}, \sqrt{10})$, and $K_7 = \mathbb{Q}(\sqrt{10}, \sqrt{15})$. Now we define a program `mahler(f)` that will use 3.2 to calculate the Mahler measure of a polynomial f:

```
mahler(f,{M=0})=
    roots=polroots(f);
    M=polcoeff(f,poldegree(f));
    for(i=1,matsize(roots)[1],
        M=M*max(1,abs(roots[i]))
     );
     M
```

Then we define a program `minimum(f)`:

```
minimum(f)=
    M=10000;
    r=polroots(f)[1];
    basis=subst(nfbasis(f),x,r);
    for(a=0,10,
        for(b=-10,10,
            for(c=-10,10,
```

```
                    for(d=-10,10,
                        alpha=basis*[a,b,c,d]~;
                        g=algdep(alpha,4);
                        if(polisirreducible(g),
                            if(poldegree(g)==4,
                                if(mahler(g)<M,
                                        if(mahler(g)>1,
                                            M=mahler(g);
                                            G=g;
                                            print([M,g]);
                                    )
                                )
                            )
                        )
                    )
                )
            )
        )
```

This program takes a polynomial f and uses the command `nfbasis` to find an integral basis for the number field defined by that polynomial. Then it uses the `subst` command to substitute one of the roots of f into the integral basis for the field defined by f. It then runs through linear combinations of the basis (the ~ command transposes $[a, b, c, d]$ to a column vector so matrix multiplication is valid) and finds the minimal polynomial for each linear combination. It then checks the Mahler measure of the minimal polynomial, and if it is smaller than the previous M it has stored (and greater than 1, to account for the roots of unity), it sets that as the new M. Otherwise, it moves on. Then it prints the polynomial and its Mahler measure. Thus we get a list of irreducible degree 4 polynomials with decreasing

Field	Defining polynomial	Mahler measure	Height
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	$x^4 - 4x^2 + 1$	3.732	0.329236
$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	$x^4 - 6x^2 + 4$	5.236	0.413889
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	$x^4 + 6x^3 + 2x^2 - 6x + 1$	7.873	0.515860
$\mathbb{Q}(\sqrt{10}, \sqrt{15})$	$x^4 - 8x^2 + 1$	7.873	0.515860
$\mathbb{Q}(\sqrt{3}, \sqrt{10})$	$x^4 + 8x^3 - 2x^2 - 12x + 6$	11.477	0.610086
$\mathbb{Q}(\sqrt{5}, \sqrt{6})$	$x^4 - 14x^3 + 9x^2 + 10x - 5$	14.348	0.665903
$\mathbb{Q}(\sqrt{2}, \sqrt{15})$	$x^4 + 12x^3 - 16x^2 - 12x + 1$	21.954	0.772237

Table 5.1: Computational results for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Mahler measure.

We can use the `polcompositum` command to find a defining polynomial for each K_i, and then the `minimum(f)` program will give us the smallest Mahler measure for that field if we input the defining polynomial.

This proves that $\tau_{4,p} \leq 0.772237$ for $p \neq 2, 3, 5$.

Now we can use the same methods to check another L, namely $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt{5})$. Note that $\mathbb{Q}(\sqrt{-1}, \sqrt{3})$ is generated by a root of unity, so we look at the defining polynomial with the next smallest Mahler measure.

Field	Defining polynomial	Mahler measure	Height
$\mathbb{Q}(\sqrt{-1}, \sqrt{5})$	$x^4 + 3x^2 + 1$	2.618	0.240603
$\mathbb{Q}(\sqrt{5}, \sqrt{-3})$	$x^4 + x^3 + 2x^2 - x + 1$	2.618	0.240603
$\mathbb{Q}(\sqrt{-1}, \sqrt{3})$	$x^4 + 2x^3 + 2x^2 - 2x + 1$	3.732	0.329236
$\mathbb{Q}(\sqrt{3}, \sqrt{-5})$	$x^4 + x^2 + 4$	4.000	0.346574
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	$x^4 + 6x^3 + 2x^2 - 6x + 1$	7.873	0.515860
$\mathbb{Q}(\sqrt{-1}, \sqrt{15})$	$x^4 - 4x^3 - x^2 + 10x + 10$	10.000	0.575646
$\mathbb{Q}(\sqrt{-3}, \sqrt{-5})$	$x^4 + 16x^2 + 4$	15.746	0.689147

Table 5.2: Computational results for $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt{5})$.

This would give a bound as follows: for $p \neq 3, 5$, $\tau_{4,p} \leq 0.689147$.

We again use the same methods to check $L = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3})$. Note that as before, $\mathbb{Q}(\sqrt{-1}, \sqrt{3})$ is generated by a root of unity, along with $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$, so we check the defining polynomial with the next smallest Mahler measure.

This field then gives that for $p \neq 2, 3$, $\tau_{4,p} \leq 0.549306$.

Field	Defining polynomial	Mahler measure	Height
$\mathbb{Q}(\sqrt{-1}, \sqrt{2})$	$x^4 + 2x^2 + 4x + 2$	3.414	0.306971
$\mathbb{Q}(\sqrt{-1}, \sqrt{3})$	$x^4 + 2x^3 + 2x^2 - 2x + 1$	3.732	0.329236
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	$x^4 - 4x^2 + 1$	3.732	0.329236
$\mathbb{Q}(\sqrt{3}, \sqrt{-2})$	$x^4 + 4x^2 + 1$	3.732	0.329236
$\mathbb{Q}(\sqrt{2}, \sqrt{-3})$	$x^4 + 2x^2 + 4$	4.000	0.346574
$\mathbb{Q}(\sqrt{-2}, \sqrt{-3})$	$x^4 - 2x^2 + 4$	4.000	0.346574
$\mathbb{Q}(\sqrt{-1}, \sqrt{6})$	$x^4 + 9$	9.000	0.549306

Table 5.3: Computational results for $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3})$.

Now we note that 2 and 3 both ramify in $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3})$. From the next section, we see that $\tau_{4,2} = 0.346574$ and $\tau_{4,3} = 0.274653$. Thus, we get the following theorem:

Theorem 5.1. *For every prime p, $\tau_{4,p} \leq 0.549306$.*

5.2 Actual values of $\tau_{4,p}$

Now we want to calculate some actual values for $\tau_{4,p}$. To do this, we create a list of polynomials with Mahler measure smaller than some bound. In our case we'll use 9, since that was the smallest Mahler measure we found in the previous section. On page 25 in [1], we get that if $f = a_n x^n + \cdots + a_1 x + a_0$, then $|a_{n-r}| \leq \binom{n}{r} M(f)$, where $M(f)$ is the Mahler measure of f. We use the following code:

```
list=[];
for(a=1,L,
    for(b=-4L,4L,
        for(c=-6L,6L,
            for(d=-4L,4L,
                for(e=-L,L,
                    f=ax^4+bx^3+cx^2+dx+e;
                     M=mahler(f);
                     if(M<L,
```

```
                        if(polisirreducible(f),
                            list=concat(list,[[M,f]])
                        )
                    )
                )
            )
        )
    )
```

This code will search through degree four polynomials using the bounds from [1] and put the polynomials that are irreducible and have Mahler measure 9 or less into a vector called `list`. We sort this list of polynomials by Mahler measure.

After we obtain this list, we need to define a program that determines whether p splits completely in a field:

```
{splitscompletely(p,f)=
        K=nfinit(polredabs(f));
        pr=idealprimedec(K,p);
        if(length(pr)==poldegree(f),1,0)
}
```

This program takes in a prime p and a defining polynomial f of a number field. The `polredabs` command takes in a polynomial f and will find a monic generating polynomial of the number field defined by f, and the `nfinit` command takes in a polynomial and creates a vector that contains information about the number field generated by that polynomial. Then the `idealprimedec` command takes in a number field K and a prime p and returns the prime ideal decomposition of p in the number field K as a vector of prime ideals. Then we check that the number of prime ideals in that vector is equal to the degree of f (in our case we look at polynomials with degree 4), and if the length is equal, then p splits completely in the number field defined by f.

Now that we have this, we run the code

```
{smallest(p)=
    flag=0;
    i=4;
    while(!flag,
        i=i+1;
        if(splitscompletely(p,list[i][2]),
            flag=mahler(list[i][2])
        )
    );
[flag,list[i][2]]
}
```

This code takes as input a prime number p. It loops through the polynomials in `list` (our list of all irreducible quartic polynomials sorted by Mahler measure) until it finds the first (smallest Mahler measure) polynomial defining a field in which p splits completely. As we have shown, a root α of this polynomial will be totally p-adic, and, since our list is sorted by Mahler measure, $h(\alpha) = M(f)$ will be the minimal height of a totally p-adic algebraic number of degree 4. Hence, $h(\alpha) = \tau_{4,p}$.

Using this code for each prime $p \leq 569$, we obtain the following table of actual values of $\tau_{4,p}$. Note that, since we have previously proven that there is a totally p-adic α whose minimal polynomial has Mahler measure less than or equal to 9 for any prime p, we could extend this table indefinitely without having to expand our list of polynomials.

Prime	$\tau_{4,p}$	Minimal polynomial
2	0.346574	$2x^4 - x^3 + 2x^2 + x + 4$
3	0.274653	$3x^4 - 4x^3 + 4x^2 - 4x + 3$
5	0.274653	$2x^4 + 3$
7	0.274653	$3x^4 - 4x^2 + 3$
11	0.173287	$2x^4 - 3x^2 + 2$
13	0.235153	$2x^4 - x^2 + 2$
17	0.232996	$2x^4 + x^3 - x^2 + 2x + 1$
19	0.173287	$2x^4 + x^2 + 2$
23	0.158244	$x^4 - 2x^3 + x^2 - 2x + 1$
29	0.120303	$x^4 - x^2 - 1$
31	0.173287	$2x^4 - x^2 + 2$
37	0.173287	$x^4 - x^3 + x - 2$
41	0.173287	$x^4 - 2x^2 + 2$
43	0.135884	$x^4 - x^3 + 2x^2 - 2x + 1$
47	0.173287	$2x^4 - 4x^3 + 5x^2 - 4x + 2$
53	0.173287	$2x^4 - 2x^3 + x^2 - 2x + 2$
59	0.156051	$x^4 - 2x^3 + x - 1$
61	0.207861	$x^4 + 2x^3 + 2x + 1$
67	0.173287	$x^4 + x^2 - x + 2$
71	0.156051	$x^4 - 2x^3 + x - 1$
73	0.173287	$x^4 - 2$
79	0.173287	$x^4 - x^3 - x^2 + 2$
83	0.0805712	$x^4 - x^3 - 1$
89	0.120303	$x^4 - x^2 - 1$
97	0.173287	$2x^4 - 2x^3 + 3x^2 - 2x + 2$
101	0.120303	$x^4 - x^2 - 1$
103	0.135884	$x^4 - x^3 + 2x^2 - 2x + 1$
107	0.173287	$2x^4 - 3x^2 + 2$
109	0.173287	$2x^4 - 2x^3 + x^2 - 2x + 2$
113	0.144611	$x^4 - x^3 - x^2 + x - 1$
127	0.158244	$x^4 - 2x^3 + x^2 - 2x + 1$
131	0.173287	$2x^4 + 2x^3 + 3x^2 + 2x + 2$
137	0.158244	$x^4 - 2x^3 + x^2 - 2x + 1$
139	0.135884	$x^4 - x^3 + 2x^2 - 2x + 1$
149	0.173287	$2x^4 - 2x^3 + x^2 - 2x + 2$
151	0.158244	$x^4 - 2x^3 + x^2 - 2x + 1$
157	0.110534	$x^4 - x^3 + x^2 + 1$
163	0.173287	$x^4 - x + 2$
167	0.173287	$x^4 - x^3 - x + 2$
173	0.173287	$x^4 - 2x^3 + 2x - 2$
179	0.164064	$x^4 - x^3 - x^2 - x - 1$
181	0.120303	$x^4 - x^2 - 1$
191	0.173287	$x^4 - x^3 + x^2 - x + 2$
193	0.0843445	$x^4 - x^3 + 1$

Bibliography

[1] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[2] Daniel A. Marcus. *Number fields*. Universitext. Springer, 2018. Second edition.

[3] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier analysis on number fields*, volume 186 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[4] A. Schinzel. Addendum to the paper: "On the product of the conjugates outside the unit circle of an algebraic number" (Acta Arith. **24** (1973), 385–399). *Acta Arith.*, 26(3):329–331, 1974/75.

[5] Emerald Stacy. Totally p-adic numbers of degree 3. In *Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *The Open Book Series*, pages 387–401. Mathematical Sciences Publishers, 2020.

[6] The PARI Group, Univ. Bordeaux. *PARI/GP version* ***2.13.1***, 2019. available from `http://pari.math.u-bordeaux.fr/`.