2014-01-14

# Applications of the Hypergeometric Method

Sorvisto, Dayne

UNIVERSITY OF CALGARY

# Applications of the Hypergeometric Method

by

Dayne Sorvisto

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTERS OF SCIENCE

DEPARTMENT OF MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

January, 2014

# Abstract

Abstract: We define an irrationality measure and show how irrationality measures can be used to bound the size of solutions to Thue equations. We give a review of some of the major results about binary Thue equations.

We study the Hypergeometric Method. We prove an important theorem which shows how irrationality measures can be constructed from sequences of rational numbers. We explicitly construct irrationality measures for some degree 3 algebraic irrationalities.

We look at the application of irrationality measures to binary Thue equations. Throughout this chapter we illustrate each theorem with an example equation using the irrationality measures we constructed.

We look at applications of restricted irrationality measures to continued fractions and exponential Diophantine equations. We prove a theorem about the size of solutions to the generalized Ramanujan-Nagell equation.

# Acknowledgements

I would like to express my deepest appreciation to my supervisor, Dr. Mark Bauer for all of the guidance and encouragement he has given me during the last two years. There are very few professors that are as committed to his students as he is and his patience, vast knowledge and insight have contributed immensely to my experience at the University of Calgary. In particular, I would like to acknowledge him for the many hours he spent editing this thesis and the countless comments he's given me to make this thesis the best that it can be. I'm extremely lucky to have had him as a supervisor and I can honestly say he went above and beyond my expectations. I would also like to thank all the professors I've had that have contributed to my understanding of mathematics and ultimately made this thesis possible. I dedicate this thesis to my mom, Allison Sorvisto for all her love and support during my education.

# Table of Contents

# Chapter 1

# Liouville's Approximation Theorem and its Generalizations

## 1.1 Introduction

In number theory, Diophantine approxmation is concerned with the approximation of real numbers by rational numbers. The basic problem in Diophantine approximation is to know how well a real number $\alpha$ can be approximated by a rational number $\frac{a}{b}$. The approximation is good if $\left|\alpha - \frac{a}{b}\right|$ does not decrease if $\frac{a}{b}$ is replaced by another rational number with a smaller denominator. The theory of simple continued fractions was used to find good approximations of a real number in the 18th century. With this in mind, it was natural to ask whether or not it is possible to find sharp upper or lower bounds on the above absolute value in terms of the denominator. This turned out to be a very profound question and is the subject of this thesis.

It is the goal of this thesis to develop the idea of an irrationality measure, which in some sense quantifies how well an irrational number can be approximated by rational numbers. We start by giving sufficient background information including very simple definitions and theorems on irrationality and culminating with the Hypergeometric Method. This background will be used to explicitly construct irrationality measures and the explicit computation of some nontrivial examples. The secondary goal of this thesis is to show some applications of irrationality measures to Diophantine equations; this is done by considering both a particular family of Thue equations as well as some exponential Diophantine equations. Throughout the thesis simple continued fractions will play an important role when we compute specific examples of irrationality measures. As such, a supplementary goal of this thesis is to show

how simple continued fractions are related to irrationality measures.

We begin by discussing irrationality and some of its basic properties. An irrational number is a real number that is not rational. In general deciding whether or not a real number is irrational is an extremely difficult problem (for example, the irrationality of $e+\pi$ is not known). However, there exist many equivalent ways to describe what it means for a real number to be irrational. A good introduction to the mathematics of irrational numbers is Irrational Numbers by Ivan Niven (see [19]).

## 1.2 Criterion for Irrationality

The following theorem gives an equivalent characterization for the irrationality of a real number. The theorem follows from a basic fact of Diophantine approximation, namely that any nonzero integer has absolue value at least one. A simple corollary of this is if a real number is rational then it cannot be well approximated by any rational number other than itself. We state this formally below.

**Theorem 1.** *Let $\alpha$ be a real number, then the following are equivalent:*

*(1) $\alpha$ is irrational.*

*(2) For any $\epsilon > 0$ there exists $\frac{p}{q} \in \mathbb{Q}$ such that*

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{\epsilon}{q}.$$

*(3) For any real number $Q > 1$, there exists an integer $q$ in the range $1 \leq q \leq Q$ and a rational integer $p$ such that*

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ}.$$

*Proof.* We begin by proving that (1) $\implies$ (3)

Let $Q > 1$ and define N to be the ceiling of Q. This implies that N is an integer such that $N - 1 < Q \leq N$. Also since $Q > 1$ this implies $N \geq 2$. For $x \in \mathbb{R}$ write $x = \lfloor x \rfloor + \{x\}$,

where $\lfloor x \rfloor$ is the integer part of x and $\{x\}$ is the fractional part. Let $\alpha \in \mathbb{R} - \mathbb{Q}$.

Consider the subset E of the unit interval which consist of the $N-1$ elements $\{q\alpha\}, q = 1, ...N-1$ as well as the endpoints of the interval 0 and 1. Since $\alpha$ is irrational, these $N+1$ elements are pairwise distinct. We can also split the unit interval into N subintervals $I_j = [\frac{j}{N}, \frac{j+1}{N}], 0 \leq j \leq N-1$. By the pidgeonhole principle it follows that at least one of these intervals contains at least 2 of the elements of our set E, call this interval $I_{j_0}$.

If $j_0 = N-1$ then $I_{j_0} = [1-1/N, 1]$ contains 1 as well as one other element $\{q\alpha\}, 1 \leq q \leq N-1$. Set $p = \lfloor q\alpha \rfloor + 1$. Then we have $1 \leq q \leq N-1 < Q$ and $p - q\alpha = 1 - \{q\alpha\}$ and hence $0 < p - q\alpha < \frac{1}{N} \leq \frac{1}{Q}$. The case where $j_0 = 0$ is similar.

Apart from 0 and 1, our $N+1$ elements of E are irrational and hence are contained in the union of the open intervals $(\frac{j}{N}, \frac{j+1}{N}), 1 \leq j \leq N-2$. In this case we have $1 \leq j_0 \leq N-2$ and $I_{j_0}$ contains 2 elements of the form $\{q_1\alpha\}, \{q_2\alpha\}$ with $0 \leq q_1 < q_2 \leq N-1$. We then set q to be the difference $q_2 - q_1$ and p to be the difference $\lfloor q_2\alpha \rfloor - \lfloor q_1\alpha \rfloor$. Thus the conditons of (3) are satisfied since we have $0 < q = q_2 - q_1 \leq N-1 < Q$ and

$$|q\alpha - p| = |q_2\alpha - q_1\alpha - (\lfloor q_2\alpha \rfloor - \lfloor q_1\alpha \rfloor)| = |\{q_2\alpha\} - \{q_1\alpha\}| < 1/N \leq \frac{1}{Q}.$$

We see (2) $\implies$ (1) by noting if $\alpha = \frac{a}{b}$ then we can choose $c = \frac{1}{b}$ so that for any rational number $\frac{p}{q} \neq \alpha$,

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q}.$$

The above inequality holds since $aq - bp$ is a nonzero integer with absolute value at least 1.

Finally, (3) $\implies$ (2) follows immediately by fixing $\epsilon > 0$ and invoking the Archimedian property of the reals to choose a natural number $Q > 1$ with $\frac{1}{Q} < \epsilon$.

□

The following is a sharper version of Theorem 1 due to Adolf Hurwitz and is known in the literature as "Hurwitz's Theorem".

**Theorem 2** (Hurwitz's Theorem)**.** *A real number $\alpha$ is irrational iff there are infinitely many rational numbers $p/q$ that satisfy the inequality*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$$

Classical proofs of Hurwitz's Theorem use Farey series or continued fractions. A proof can be found in Adolf Hurwitz's paper [15].

In 1844, Liouville gave the first examples of transcendental numbers (later to be called Liouiville numbers). His results were based on his observation that algebraic numbers cannot be approximated by rationals "too well" and at the same time, "too frequently". What later became known as Liouville's approximation theorem that Liouville used to construct these transcendental numbers has since become a major object of study in diophantine approximation. An inequality of the type given in Liouville's Approximation Theorem is called a Liouiville inequality. A natural way to construct a class of transcendental numbers is by using Liouville inequalities as in the definition of a Liouville number. We will now explicitly define both algebraic numbers and Liouville numbers.

**Definition 1** (Algebraic number)**.** *A real algebraic number is a real number that is a root of a non-zero polynomial in one variable with rational coefficients. The degree of an algebraic number is the degree of its minimal polynomial over $\mathbb{Q}$. A real number that is not algebraic is called transcendental.*

**Definition 2** (Liouville Number)**.** *A Liouville number is a real number $\alpha$ such that for any positive integer $n$, there exists integers $a$ and $b > 1$ such that $\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^n}$*

It turns out that there is a close relationship between Liouville inequalities and algebraic numbers. This relationship is stated formally in Liouville's Approximation Theorem.

**Theorem 3** (Liouville's Approximation Theorem)**.** *Let $\alpha$ be a real algebraic number of degree $n \geq 2$ and $p$ and $q$ be integers, then*

$$\left|\alpha - \frac{p}{q}\right| > \frac{A}{q^n} \tag{1.1}$$

*where $A$ is a positive constant that only depends on $\alpha$.*

*Proof.* Since $\alpha$ is algebraic, it is the root of some degree n polynomial $f(x)$ with integer coefficients. Let M be the max of $|f'(x)|$ over the compact set $[\alpha-1, \alpha+1]$ and $\alpha_1, \alpha_2, .., \alpha_m$ be the distinct roots of f not equal to $\alpha$ with $m < n$.

Choose a value $A > 0$ that satisfies the inequality

$$A < \min\left\{1, \frac{1}{M}, |\alpha - \alpha_i|\right\}.$$

Suppose that there exists integers p and q that contradict the theorem, that is,

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{A}{q^n} \leq A < \min\left\{1, \frac{1}{M}, |\alpha - \alpha_i|\right\}.$$

It follows that $\frac{p}{q}$ is in the interval $[\alpha - 1, \alpha + 1]$ and is not equal to any of the $\alpha_i$ since $\left|\alpha - \frac{p}{q}\right| < |\alpha - \alpha_i|$. Hence, $\frac{p}{q}$ is not a root of f and there is no root of f between $\alpha$ and $p/q$. By the mean value theorem, there exists an $x_0$ between $\frac{p}{q}$ and $\alpha$ such that

$$f(\alpha) - f\left(\frac{p}{q}\right) = \left(\alpha - \frac{p}{q}\right) f'(x_0).$$

Since $\alpha$ is a root of f but $p/q$ is not, it follows that $|f'(x_0)| > 0$ and hence,

$$\left|\alpha - \frac{p}{q}\right| = \frac{\left|f(\alpha) - f(\frac{p}{q})\right|}{|f'(x_0)|} = \left|\frac{f\left(\frac{p}{q}\right)}{f'(x_0)}\right|.$$

Now f can be written in the form

$$f(x) = \sum_{i=0}^{n} c_i x^i$$

where the coefficients are integers. Hence,

$$\left|f\left(\frac{p}{q}\right)\right| = \left|\sum_{i=0}^{n} c_i \left(\frac{p}{q}\right)^i\right| = \frac{|\sum_{i=0}^{n} c_i p^i q^{n-i}|}{q^n} \geq \frac{1}{q^n}.$$

The final inequality is true since $\frac{p}{q}$ is not a root of f and $|\sum_{i=0}^{n} c_i p^i q^{n-i}|$ is a nonzero integer. From the above we get the inequality $|f(\frac{p}{q})| \geq \frac{1}{q^n}$. Also, since $|f'(x_0)| \leq M$ (by construction) and $\frac{1}{M} > A$ (by the definition of A), we have that

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{f\left(\frac{p}{q}\right)}{f'(x_0)}\right| \geq \frac{1}{Mq^n} > \frac{A}{q^n}.$$

□

We remark that Liouville numbers are clearly transcendental by Liouvilles Approximation Theorem. One might wonder how typical Liouville numbers are amongst all real numbers, that is, how many reals do we expect to be Liouville numbers? The following theorem shows that almost no real numbers are Liouville numbers in the sense of Lebesgue measure.

**Theorem 4.** *The set of Liouville numbers in* $[0, 1]$ *has Lebesgue measue 0.*

*Proof.* Fix $\epsilon > 0$, we want to show that the Lebesgue measure of the Liouville numbers in the interval [0,1] is less than $\epsilon$. Note that for any positive integer n,

$$\sum_{b=2}^{\infty} \frac{4}{b^{n-1}} < \frac{4}{2^{n-3}} \sum_{b=2}^{\infty} \frac{1}{b^2}$$

and since the rightmost sum converges we can choose a positive integer $n$ such that

$$\sum_{b=2}^{\infty} \frac{4}{b^{n-1}} < \epsilon.$$

By definition if $\alpha$ is a Liouville number in [0,1] then there exist integers $a$ and $b$ with $b > 1$ such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^n}.$$

Since

$$\frac{1}{b^n} < \frac{1}{2}$$

and $\alpha \in [0, 1]$ we must have that

$$-\frac{1}{2} < \frac{a}{b} < \frac{3}{2}$$

or equivalently $-\frac{b}{2} < a < \frac{3b}{2}$. Hence, a is in an open interval of length $2b$. This implies that for any integer $b > 1$, there are at most $2b$ possible values of $a$ for which our inequality can hold. Hence we conclude that $\alpha$ can be in at most $2b$ intervals of length $\frac{2}{b^n}$ and therefore the Lebesgue measure of all such $\alpha$ is at most

$$\sum_{i=2}^{\infty} \frac{2i}{i^n} < \epsilon$$

by how $n$ was chosen. □

One might wonder if it is possible to improve the inequality in Theorem 3 further and reduce n to arrive at a sharper one of the form (1.1). In fact sharpenings of Liouville's inequality to be of the form

$$\left|\alpha - \frac{p}{q}\right| > \frac{\lambda(q)}{q^n} \tag{1.2}$$

(where $\lambda(q)$ is some monotonically increasing function that tends to infinity as $q \to \infty$) are of immense importance because, as we will see, they can be used to bound solutions to Diophantine equations.

## 1.3 The Existence of a Computable Bound for Thue Equation

Diophantine approximation is concerned with the approximation of real numbers by rational numbers. One reason that Liouville inequalities are important in Diophantine approximation is because they can often be applied to Diophantine equations to show that they only have certain solutions.

**Definition 3.** *A binary form $f(x, y)$ of degree $n \in \mathbb{Z}$ with $n \geq 1$ is a homogeneous bivariate polynomial $f(x, y) = a_0x^n + a_1x^{n-1}y + a_2x^{n-2}y^2 + ... + a_{n-1}xy^n + a_ny^n$ where $a_i \in \mathbb{Z}$ for each $i$*

Let $f(x, y)$ be an integral binary form of degree $n \geq 3$ and $N \neq 0$ a nonzero integer.

We consider solutions to the equation $f(x, y) = N$. This equation is often called Thue's equation after Axel Thue who proved in 1909 that this equation has only finitely many

solutions in integers (see [24]). The study of this equation in the early 20th century ultimately led Mordell to the theorem on the finite rank of the group of rational points on an elliptic curve as well as Siegel's theorem that there are only finitely many integral points on an algebraic curve with genus greater than zero. Although an elliptic curve is homogeneous in three variables with an affine model inhomogeneous in two variables whereas a Thue equation is homogeneous in two variables; the method of showing the finiteness of Thue equations lead to the study of homogeneous forms in 3 or more variables. Hence, Thue equations played a central part in the development of Diophantine analysis in the early 20th century.

It was not until long after Thue published his work on this equation that an explicit bound on the number of solutions (in terms of just parameters of the equation such as $|N|$ or the height or degree of the form) was known. Therefore, the proof we will present in this thesis is different from the one due to Thue.

In this thesis we will use improvements of Liouville inequalities to find explicit bounds on solutions to particular Thue equations in terms of its parameters. However, we will not go into theory of linear forms in logs which give general improvements of Liouville's theorem for algebraic numbers. A good introduction to the theory of linear forms in logarithms is Linear Forms in Logarithms of Rational Numbers by Yuri Nesterenko (see [18] ).

Instead, we will use the Hypergeometric method to derive improvements of Liouville's theorem for particular algebraic numbers. These improvements are often significantly sharper than the improvements we would get by using the more general theory of linear forms in logs and so the bounds that we will derive will be very sharp. In fact, later we will show how the Hypergeometric method can be used to bound the number of solutions for an infinite family of Thue equations by deriving very sharp effective improvements of Liouville's approximation theorem for a particular class of algebraic numbers (called irrationality measures).

Towards this goal we will prove that the Thue equation has only finitely many integral solutions, but we will assume without proof that we have an improvement of Liouville's

inequality for the algebraic numbers we consider in the proof. We note that this assumption is actually true but invokes the extremely deep theory of linear forms in logarithms to show there is an improvement of Liouville's inequality for any algebraic irrationality. The following is a fortaste for some of the main ideas of the thesis.

First we will give some motivation for why we should expect these effective inequalities to be useful in proving there are finitely many integral solutions to the Thue equation. Let $f(x, y)$ be an irreducible binary form of degree $n \geq 3$ and suppose that $N \neq 0$ is an integer. If inequality 3.5 admits a sharpening of the form 1.2 for some $\lambda(q) \to \infty$ then the Diophantine equation $f(x, y) = N$ has only finitely many solutions. We note that $f(x, y)$ irreducible implies $f(x, 1)$ is irreducibe (see section 4.1 for a proof). We remark that if $f(x, y)$ is not irreducible then the equation $f(x, y) = N$ can be reduced to finitely many equations of this type where the binary form is irreducible.

Now if $f(x, 1)$ is a polynomial without real roots then the equation $f(x, y) = N$ has only a finite number of solutions. We see this by noting if there are infinitely many solutions $(x_k, y_k)$ in integers then $y_k^n f(\frac{x_k}{y_k}, 1) = A$ and hence $f(\frac{x_k}{y_k}, 1) = \frac{N}{y_k^n}$. Taking the limit as $k \to \infty$ it follows that $f(x, 1)$ has a real root.

Suppose instead that $\alpha$ is a real root of $f(x, 1)$ and $\alpha^{(i)}$ (i = 1, 2,..., n) are its conjugates. It follows from the equation and $y \neq 0$ that

$$\prod_{i=1}^{n} \left| \alpha^{(i)} - \frac{x}{y} \right| = \frac{N}{|a||y|^n}$$

where $a$ is the leading coefficient of the polynomial $f(x, 1)$. Assuming the equation has solutions $(x, y)$ for infinitely many $y$, we see the product on the left takes arbitrarily small values for solutions $x$ and $y$. Since $\alpha^{(i)}$ are all distinct, there are infinitely many $\frac{x}{y}$ close to one of the real roots, say $\alpha^{(j)}$.

From the above (after some nontrivial manipulations that we will show in the next theorem) we obtain an inequality $\left| \alpha - \frac{x}{y} \right| < \frac{c_2}{|y|^n}$ where $c_2$ depends on $\alpha$. If $\lambda(q) \to \infty$ this contradicts the Liouiville inequality 1.2 and hence there are not infinitely many solutions.

These ideas illustrate how we can take a Diophantine equation and associate a set of algebraic irrationalities to it and if we can find sharp Liouville inequalities for each algebraic irrationality, we can bound the solutions to the equation in such a way that the constants are explicit and depend on the constants given in the inequalities. We will now explicitly show this in the next theorem.

**Theorem 5.** *Let $f(x,y)$ be an irreducible binary form of degree $n \geq 3$ and $N$ a nonzero integer. Consider the Diophantine equation $f(x,y) = N$. If $\alpha^{(1)}, ..., \alpha^{(n)}$ are the $n$ distinct roots of the polynomial $f(x,1)$ and for each root we have an effective improvement of Liouville's Approximation Theorem of the form $|\alpha^{(i)} - p/q| > C/q^{\omega}$ for some effective constant $C > 0$ depending on $\alpha^{(i)}$, it follows that there is an effective bound on $|y|$ of the form*

$$|y|^{n-\omega} < 2^{(n-1)} \frac{|N|}{c_3 \, |f'(\alpha^{(1)})|}$$

*Proof.* Let $\alpha^{(1)}, ..., \alpha^{(n)}$ be the n distinct roots of the polynomial $f(x,1)$. If integers X and Y satisfy (1.1) and $Y \neq 0$ (if Y=0 then the inequality in the theorem follows trivially) then define $\alpha^{(1)}$ as the root with

$$\left| \alpha^{(1)} - \frac{X}{Y} \right| = \min_i \left| \alpha^{(i)} - \frac{X}{Y} \right|.$$

From the equation

$$\prod_{i=1}^{n} |\alpha^{(i)} - \frac{X}{Y}| = \frac{N}{|a_0||Y|^n}$$

we have that

$$\left| \alpha^{(1)} - \frac{X}{Y} \right| \leq \frac{c}{Y}$$

where

$$c = \left( \frac{|N|}{|a_0|} \right)^{1/n}$$

and $a_0$ is the leading coefficient of $f(x,1)$.

Then for $i \neq 1$ we have that

$$2\left|\alpha^{(i)} - \frac{X}{Y}\right| \geq \left|\alpha^{(i)} - \frac{X}{Y}\right| + \left|\alpha^{(1)} - \frac{X}{Y}\right| \geq \left|\alpha^{(i)} - \alpha^{(1)}\right|.$$

by the triangle inequality.

Since the above inequality holds for $i \neq 1$ and

$$|Y| \leq 2\left(\frac{|N|}{|a_0|}\right)^{\frac{1}{n}} |\alpha^{(1)} - \alpha^{(i)}|^{-1}$$

we obtain

$$\frac{|N|}{|a_0|} = |Y|^n \prod_{i=1}^{n} \left|\alpha^{(i)} - \frac{X}{Y}\right| \geq |Y|^n 2^{-n+1} \left|\alpha^{(1)} - \frac{X}{Y}\right| \prod_{i=2}^{n} |\alpha^{(1)} - \alpha^{(i)}|. \tag{1.3}$$

Hence we arrive at the following

$$\left|\alpha^{(1)} - \frac{X}{Y}\right| \leq \frac{c_2}{|Y|^n} \tag{1.4}$$

where

$$c_2 = 2^{(n-1)} \frac{|N|}{|f'(\alpha^{(1)})|}.$$

It is at this stage of the proof that we will use our assumption that we have an improvement on Liouiville's approximation theorem for $\alpha^{(1)}$ (note that this uses assumption that $\alpha^{(1)}$ is real). From this assumption and ( 1.4) we have that

$$\frac{c_3}{|Y|^{\omega}} < \left|\alpha^{(1)} - \frac{X}{Y}\right| < \frac{c_2}{|Y|^n}$$

for some effectively computable constant $c_3$ from which it follows that

$$|Y|^{n-\omega} < 2^{(n-1)} \frac{|N|}{c_3 f'(\alpha^{(1)})} \tag{1.5}$$

□

We remark that Roths' theorem implies we can take $\omega = 2+\epsilon$ for any $\epsilon > 0$ but $c_3$ (which depends on $\alpha^{(1)}, \epsilon$) is then ineffective. However this is sufficient to prove the finiteness of the

number of solutions. If an effective improvement exists as in the statement of the theorem then (1.5 ) gives a bound on $|y|$ and consequently on $|x|$.

In particular the kind of Thue equation that we will study in this thesis is the case where $n = 3$ and there is no $xy$ term, sometimes called a binary Thue equation in the literature. We discuss its history as well as some recent results which give very tight upper bounds on the number of solutions to this equation in positive integers.

## 1.4 A History of the Binary Thue Equation

A special case of the equation Axel Thue originally considered in his paper [24] is the equation $ax^n - by^n = N$ for a,b and n and N fixed nonzero integers, $n \geq 3$. This equation is also referred to as a binary Thue equation and in the special case $N = 1$ there is an abundance of literature on the subject. Both Delone and Nagell [17] showed independently that if $n = 3$ this equation has at most one positive integer solution in $x$ and $y$ and furthermore if this solution exists it must correspond to the fundamental unit in the number field $\mathbb{Q}\left(\left(\frac{a}{b}\right)^{1/3}\right)$ (when all embeddings are complex). This result was extended by Ljunggren in his paper [16] where the the equation

$$\left|ax^4 - by^4\right| = 1$$

was shown to have at most one positive integer solution in $x$ and $y$.

A recent improvement is due to Michael Bennett and Benjamin M.M. De Weger in their paper "On the Diophantine Equation $|ax^n - by^n| = 1$" (see [8]). The main theorem of Bennett and De Weger's paper shows the equation under consideration has at most one solution in positive integers except possibly in two cases. The theorem is given as follows.

**Theorem 6.** *If a,b and n are integers with $b > a \geq 1$ and $n \geq 3$ , then the equation $|ax^n - by^n| = 1$ has at most one solution in positive integers $(x, y)$, except possibly the cases where $b = 1$ and $2 \leq a \leq \min\{0.3n, 83\}$ and $17 \leq n \leq 347$.*

The proof of this result depends on techniques discussed in this thesis such as the Hypergeometric Method as well as techniques beyond the scope of this thesis (such as the theory of linear forms in logarithms and lattice-basis reduction methods).

Bennett and De Weger first prove a version of the above theorem for n 'small' relative to $\max\{a, b\}$ using arguments related to the Hypergeometric Method. The next stage of the proof is considering some special cases for "small" $n$ between 5 and 13 where the Hypergeometric Method is insufficient. In order to handle these cases, the more general theory of linear forms in logarithms is invoked as well as some computational methods in lattice-basis reduction. The major computational difficulty is finding fundamental units of corresponding algebraic number fields. Finally, a lower bound on some linear forms in logarithms for pairs of algebraic numbers is invoked to prove the main theorem of the paper.

For values other than $N = 1$, the binary Thue equation $ax^n - by^n = N$ (which we consider from the Diophantine approximation perspective in this thesis) was first studied in 1937 by Siegel who extended the work of Thue (what later would be known as the Thue-Siegel method). Siegel [23] was able to prove that the Thue inequality $|ax^n - by^n| \leq c$ has at most one solution in positive integers $(x, y)$ provided that

$$|ab|^{n/2-1} \geq 4n \left( \prod_{p|n} p^{\frac{1}{p^{p-1}}} \right)^n e^{2n-2}.$$

This result was further sharpened by Jan-Hendrik Evertse in his PhD thesis titled "Upper Bounds for the Numbers of Solutions of Diophantine Equations" [12]. The main result of his thesis is the following.

**Theorem 7.** *The Thue inequality $|ax^n - by^n| \leq c$ has at most one solution in positive integers (x,y) for $n \geq 3$ and $c$ a positive real number given that $\max\{|ax^n|, |by^n|\} > \beta_n c^{\alpha_n}$ where $\beta_n, \alpha_n$ are effectively computable positive constants satisfying $\beta_3 = 1152.2, \beta_4 = 98.53$ and $\beta_n < n^2$ for $n \geq 5$.*

The techniques used in the proof of Evertse's theorem include the Hypergeometric Method

but also more advanced techniques such as the iterated gap principle which are beyond the scope of this thesis but can be found in [12]. The part of this proof that we will focus on in this thesis is the the existence of effective improvements of Liouville inequalities. The Liouville inequality given in Theorem 3 of the form

$$\left|\alpha - \frac{p}{q}\right| > \frac{A}{q^n}$$

is called effective because the constant A can be explicitly computed.

The first improvements to Liouville inequalities were given by Thue in 1909 [1] who reduced n to $\frac{n}{2} + 1 + \epsilon$ for any $\epsilon > 0$ and the constant A depends only on $\epsilon$ and $\alpha$. Later in 1921 Siegel [22] improved Thue's bound considerably giving rise to the Thue-Siegel theorem which states

$$\left|\alpha - \frac{p}{q}\right| > c|q|^{-\lambda-\epsilon}$$

where $c(\alpha, \epsilon) > 0$ and

$$\lambda = \min\{\frac{n}{s+1}, s\}, s = 1, 2, ..., n-1.$$

The technique used in the proof of this theorem involves constructing a multivariate polynomial that vanishes to high order at the algebraic point $(\alpha, \alpha)$. We note that Theorem 5 and Thue-Siege theorem imply that a Thue equation has ony finitey many integral solutions.

In fact as mentioned previously, it was proven by Roth that $\lambda$ can be reduced to $2 + \epsilon$ in the above bound (it is not known whether the $\epsilon$ is necessary or not). However, the constant c is not effective in any of the above inequalities; that is the proofs of the resulting inequalities do not provide any insights into how to compute c and thus cannot be applied to explicitly solve Diophnatine equations.

**Definition 4.** *For a real number $\alpha$ we define its* ***irrationality measure*** *to be* $\inf_{\omega \in S}\{\omega\}$ *where $S$ is the set of positive real numbers $\omega$ such that there are only finitely many integers $p, q$ that satisfy*

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\omega}$$

For instance, it is known that for any irrational algebraic number and any $\epsilon > 0$ there is a constant c depending only on $\alpha$ and $\epsilon$ such that $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{2+\epsilon}}$. This is known as Roth's theorem or the Thue-Siegel-Roth theorem. The exponent $2 + \epsilon$ is referrred to as an irrationality exponent and 2 is an irrationality measure (in the literature these terms are sometimes interchanged depending on the context). However, as in the theorem of Thue and Siegel, the inequality in Roth's theorem is not effective. We remark that if the set $S$ is nonempty then it is infinite since if it contains a positive real number $\omega$ then it also must contain all positive reals larger than $\omega$. However, $S$ can be empty for example in the case of Liouville numbers. It is also worth noting that Theorem 1 implies the irrationality measure of any irrational number is at least 2.

Roth's theorem is a statement about the irrationality measure of irrational algebraic numbers, but one might wonder what the irrationality measure of a typical real number is, a problem that Aleksandr Khinchin provided the answer to in 1926. This famous result known as Khinchin's Theorem was first of many results in Diophantine approxmiation which are valid for almost all real numbers except outside of a set of Lebesgue measure 0. Results of this kind form the metric theory of Diophantine approximiation. Although Khinchin's Theorem is not relavent to this thesis, we include it as an interesting related result.

**Theorem 8** ( Khinchin's Theorem)**.** *If* $\sum_q \phi(q) < \infty$ *for* $\phi(q) \geq 0$ *then* $\left|x - \frac{p}{q}\right| < \frac{\phi(q)}{|q|}$ *has finitely many solutions p and q for almost all real numbers (on a set of Lebesgue measure zero).*

Khinchin's Theorem will not be proved here, but Theorem 4 can be viewed as a much weaker version of this result. We remark that Khinchin's Theorem shows that almost all real numbers behave like algebraic irrationalities from the perspective of Diophantine approximiation, meaning that real numbers have irrationality measure 2 except outside of a set of Lebesgue measure 0. However, this does not say anything about how to compute irrationality measures for fixed real numbers and in general, finding effective sharpenings of

Liouville inequalities for algebraic irrationalities is a very difficult problem. Thue and Siegel were the first mathematicians to develop this idea and we briefly summarize their methods below.

## 1.5 Thue and Siegel Methods

Suppose that $\beta$ is an irrational algebraic number. The Thue and Siegel method is used to construct sequeneces of rational numbers with desirable properties (to be defined later) that converge to $\beta$. The main idea is to define analytic functions called Pade approximants to approximate algebraic functions. The properties of these Pade approximants are used to show that the corresponding sequences of rational numbers have the desired properties that lead to improvements of Liouville's approximation theorem. Finally, these effective improvements can then be used to solve certain Diophantine equations.

The Thue-Siegel method requires one "good" initial approximation to $\beta$. In particular, the algebraic function $z^{\frac{1}{n}}$ is used to analyze the class of numbers $\beta = (\frac{a}{b})^{\frac{1}{n}}$ where a,b and n are rational integers by evauating the Pade approximants at this initial approximation.

The motivation behind this idea is as follows: Let $\frac{p_0}{q_0}$ be a good initial approximation to $\beta$ so that $\zeta = \frac{p_0^n}{q_0^n}\frac{b}{a}$ is close to 1.

Using diagonal Pade approximants (these will be defined formally later) it can be shown that there are meromorphic functions $P_r(z), Q_r(z)$ and $E_r(z)$ such that

$$\frac{P_r(z)}{Q_r(z)} = z^{\frac{1}{n}} + E(_r z)$$

where $E_r(z)$ is some function that can be viewed as an error term that is small for z close to 1 (it has a zero of order $2r+1$ at z=1).

Since $\zeta$ is a rational number and $P_r(z), Q_r(z)$ are rational functions of z, $\frac{P_r(\zeta)}{Q_r(\zeta)}$ is a rational number say $\frac{A_r}{B_r}$. Since $E_r(\zeta)$ is small, a rational approximation to $\beta$ is immediate ($\beta \sim \frac{B_r p_0}{A_r q_0}$ ). This process is used to generate a sequence of rational approximants to $\beta$.

This "good" sequence of approximations can sometimes immediately be transferred into a lower bound on the irrationality of $\beta$. Depending on how good the initial approximation was, this may be better than Liouville's Theorem. The proof of this fact relies on determining asymptotics for $|P_r(z)|, |Q_r(z)|$ and $|\beta Q_r(z) - P_r(z)|$ These ideas of Thue and Segel came to be known as the Hypergeometric Method.

# Chapter 2

# The Hypergeometric Method

In this chapter we discuss the Hypergeometric Method and use the method to explicitly construct irrationality measures for some degree 3 algebraic numbers that will see later have many applications to Thue equations. Since we previously defined an irrationality measure as a real number, it is worth nothing that 'constructing an irrationality measure' in this context really means finding an upperbound on the irrationality measure of an irrational number. We start by stating and proving a theorem which says if we have a "good" sequence of rational approximants to an irrational number then we can construct an upperbound on the irrationality measure of that number. This theorem is the backbone of the Hypergeometric Method and a version of it is used in all constructions of irrationality measures which use the Hypergeometric Method.

This chapter can be outlined as follows. We first prove an improved version of the aforementioned theorem. We then show how this theorem has been applied to construct irrationality measures, relying heavily on Pade approximants and a paper by Michael Bennett in order to construct arithmetic and analytic bounds. Finally, we compute some irrationality measures which will involve a considerable analysis of continued fractions. We conclude this chapter with a discussion of restricted irrationality measures.

## 2.1 Constructing an Upperbound on Irrationality Measure

In this section we show in detail how a sequence of rational approximants to an irrational number can be used to construct an irrationality measure. We define 3 bounds such a sequence must satisfy, concentrating first on the so called arithmetic and analytic bounds. We conclude the section by showing how a third bound, called the arithmetic bound, gives

a twofold improvement of the irrationality exponent. We assume that $\alpha$ is an irrational number and $\frac{P_k}{Q_k}$ is a sequence of distinct rational numbers (without loss of generality assume $Q_k > 0$) indexed by $\mathbb{N}$ that satisfies these properties.

$$|P_k - \alpha Q_k| \leq a\beta^k, \beta < 1 \tag{2.1}$$

$$|Q_k| \leq cQ^k, Q > 1 \tag{2.2}$$

$$G'_k \geq G^k, \text{where } G'_k | \gcd(P_k, Q_k), \text{and } G > 1 \tag{2.3}$$

We will concentrate on the first 2 conditions (called the analytic bounds) and then see how the third condition, called the arithmetic bound leads to further improvements on the irrationality measure of $\alpha$. First we will prove the following theorem.

**Theorem 9.** *Given an irrational number $\alpha$ and a sequence satisfying conditions (2.1) and (2.2) above, there exists a constant $C$ depending on only on $a$, $c$, $Q$ and $\beta$ such that*

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{Cq^{1+\frac{\log Q}{\log \beta}}}$$

*for all $\frac{p}{q}$ with $q > 0$.*

*Proof.* We first fix $\frac{p}{q}$ with $q > 0$.

From (2.1), we have the inequality

$$\left|\frac{P_k}{Q_k} - \alpha\right| \leq a\frac{\beta^{-k}}{Q_k}. \tag{2.4}$$

Now, we use the triangle inequality to get

$$\left|\frac{p}{q} - \alpha\right| + \left|\frac{P_k}{Q_k} - \alpha\right| \geq \left|\frac{p}{q} - \frac{P_k}{Q_k}\right|.$$

The idea is that the quantity on the right will be large because there are large gaps between distinct rational numbers as was shown in Theorem 1.

More formally,

$$\left|\frac{p}{q}-\frac{P_k}{Q_k}\right| = \left|\frac{Q_k p - P_k q}{qQ_k}\right| \geq \frac{1}{qQ_k}.$$

Here we are assuming that $\frac{p}{q} \neq \frac{P_k}{Q_k}$, otherwise just replace $\frac{P_k}{Q_k}$ with $\frac{P_{k+1}}{Q_{k+1}}$ since the sequence was assumed to be distinct. The last inequality follows from the fact that an integer has modulus at least 1, a version of the pigeonhole principle that is often humorously referred to as the 'fundamental theorem of diophantine approximation'.

It follows that

$$\left|\frac{p}{q}-\alpha\right| + \left|\frac{P_k}{Q_k}-\alpha\right| \geq \frac{1}{qQ_k}. \tag{2.5}$$

We now ask how large does k have to be so that $\left|\frac{P_k}{Q_k}-\alpha\right|$ is small, that is

$$\left|\frac{P_k}{Q_k}-\alpha\right| \leq \frac{1}{2}\frac{1}{qQ_k}$$

By (2.4) it suffices to choose k such that

$$\frac{a\beta^{-k}}{Q_k} \leq \frac{1}{2}\frac{1}{qQ_k}.$$

The $Q_k'$s cancel out in this inequality and we are left with $\beta^{-k} \leq \frac{1}{2aq}$. Taking the log of both sides implies that $k \geq \frac{\log 2aq}{\log \beta}$.

This is a lowerbound on k. In general, choosing a small value of k will result in a smaller irrationality exponent. An additional requirement is that k needs to be an integer so we should choose k to be $\lceil \frac{\log 2aq}{\log \beta} \rceil$. We note that an upperbound on k is

$$1 + \frac{\log 2aq}{\log \beta}.$$

Hence, if k is larger than this upperbound, it follows from equation (2.5) that

$$\left|\frac{p}{q}-\alpha\right| \geq \frac{1}{2qQ_k}.$$

Since we know that $\log Q_k \leq \log(cQ^k) = \log c + k \log Q$ we substitute the upperbound on k and get

$$\log Q_k \leq \log c + \frac{\log 2aq}{\log \beta} \log Q + \log Q.$$

Dividing both sides of the above inequality through by $\log q$ implies that $\frac{\log Q_k}{\log q}$ is less than or equal to

$$\frac{\log c}{\log q} + \frac{\log 2a}{\log \beta \log q} \log Q + \frac{\log Q}{\log \beta} + \frac{\log Q}{\log q}.$$

Now we use the fact that $Q_k = q^{\frac{\log Q_k}{\log q}}$ which gives

$$Q_k \leq q^{\frac{\log q}{\log \beta}} q^{\frac{\log(2a)}{\log \beta \log q} \log Q + \frac{\log Q}{\log q} + \frac{\log c}{\log q}} = q^{\frac{\log q}{\log \beta}} cQe^{\frac{\log 2a \log Q}{\log \beta}}.$$

Thus we have

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{1}{Cq^{\lambda}}$$

where in this case

$$\lambda = 1 + \frac{\log Q}{\log \beta}$$

and

$$C = 2cQe^{\frac{\log 2a \log Q}{\log \beta}}.$$

□

Next we will see how an arithmetic upperbound can be used to improve the irrationality exponent further. We will discuss how the arithmetic upperbound on the quantity $G'_k$ is derived in a later section but the purpose here is to show if we have an arithmetic upperbound then we get an improvement of the irrationaliy exponent given in the previous theorem. The improvement will be twofold by reducing the numerator and increasing the denominator of the irrationality exponenent. In applications of the Hypergeometric Method,

any improvement of the irrationality exponent is valuable and so the following theorem is useful.

**Theorem 10.** *Given an irrational number $\alpha$, and a sequence of integers satisfying conditions (2.1), (2.2) and (2.3) , there exists a constant $C$ depending only on $a$, $c$, $Q$ and $\beta$ such that*

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{Cq^{\lambda}}$$

*for all $\frac{p}{q}$ with $q > 0$. Futhermore,*

$$\lambda = 1 + \frac{\log Q - \log G}{\log \beta + \log G}$$

*and*

$$C = 2cQe^{\frac{\log 2a \log Q}{\log \beta}}.$$

*Proof.* Let $G'_k | \gcd(P_k, Q_k)$, hence we can write $P'_k G'_k = P_k$ and $Q'_k G'_k = Q_k$.
Note that condition (2.2) implies that

$$|Q'_k| \leq c\frac{Q^k}{G'_k}. \tag{2.6}$$

Next, we proceed as before using our reduced fraction.

$$\left|\frac{p}{q} - \alpha\right| + \left|\frac{P_k}{Q_k} - \alpha\right| = \left|\frac{p}{q} - \alpha\right| + \left|\frac{P'_k}{Q'_k} - \alpha\right| \geq \frac{1}{qQ'_k}. \tag{2.7}$$

As above ,we may still assume that $\frac{p}{q} \neq \frac{P_k}{Q_k}$, otherwise we replace $\frac{P_k}{Q_k}$ with $\frac{P_{k+1}}{Q_{k+1}}$.

From condition (2.2)

$$|Q_k\alpha - P_k| \leq a\beta^{-k}$$

implies that

$$|Q'_k\alpha - P'_k| \leq \frac{a\beta^{-k}}{G'_k} \leq \frac{a\beta^{-k}}{G^k}.$$

Hence,

$$\left|\alpha - \frac{P'_k}{Q'_k}\right| \leq \frac{a\beta^{-k}}{G^k Q'_k}.$$

It now suffices to choose k such that

$$\frac{a\beta^{-k}}{G^k Q'_k} \leq \frac{1}{2qQ'_k}$$

in order to guarantee that,

$$\left|\alpha - \frac{P'_k}{Q'_k}\right| \leq \frac{1}{2qQ'_k}.$$

It is sufficient to require that

$$\frac{a\beta^{-k}}{G^k} \leq \frac{1}{2q}$$

which is satisfied iff

$$k \geq \frac{\log(2aq)}{\log G + \log \beta}.$$

As we stated before, it is this sharper lowerbound on k that will lead to further improvements in the irrationality exponent. Formally,

$$\left|\alpha - \frac{P'_k}{Q'_k}\right| \leq \frac{1}{2qQ'_k} \implies \left|\alpha - \frac{p}{q}\right| \geq \frac{1}{2qQ'_k}$$

by inequality (2.7). But,

$$\frac{1}{2qQ'_k} = \frac{1}{2q^{\hat{\lambda}}}$$

where

$$\hat{\lambda} = 1 + \frac{\log Q'_k}{\log q}$$

Therefore, it suffices to bound this quantity $\hat{\lambda}$. We can achieve this by using our lowerbound on k as follows. We know from (2.6) and condition (2.3) that

$$\log Q'_k \leq \log c + k \log Q - k \log G.$$

Choosing k to be

$$\left\lceil \frac{\log(2aq)}{\log G + \log \beta} \right\rceil$$

we get

$$k \leq \frac{\log(2aq)}{\log G + \log \beta} + 1.$$

Since $Q > G$,

$$\log Q'_k \leq \log c + \frac{\log(2aq)}{\log \beta + \log G}(\log Q - \log G) + (\log Q - \log G).$$

From this inequality it follows that

$$\frac{\log Q'_k}{\log q} \leq \frac{\log Q - \log G}{\log \beta + \log G} + \frac{\log c}{\log q} + \frac{\log(2a)}{\log q(\log \beta + \log G)}(\log Q - \log G) + \frac{\log Q - \log G}{\log q}.$$

The last three terms tend to 0 as $q \to \infty$. As we saw in the previous proof by exponentiating, these terms only affect the constant, not the irrationality exponent.

Finally, we take

$$\lambda = 1 + \frac{\log Q - \log G}{\log \beta + \log G}$$

and

$$C = ce^{\frac{\log(2a)(\log Q - \log G)}{\log \beta + \log G} + (\log Q - \log G)}.$$

We conclude that

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{Cq^{\lambda}}$$

for all $\frac{p}{q}$ with $q > 0$.

□

## 2.2 Pade Approximants

An inequality of the shape given in Theorem 10 is called a lower bound on irrationality measure of $\alpha$. The $\lambda$ is an upperbound on the irrationality measure but is also sometimes referred to as an irrationality exponent or an irrationality measure in the literature. We will use these terms interchangeably throughout the remaining sections since it should be clear from the context what we mean.

The challenge now in deriving the above inequality is actually constructing such a sequence. If we restrict $\alpha$ to irrational numbers of the form $(\frac{p}{q})^{1/n}$ for some integers $p$ and $q$, then one way to do this is via Pade approximants to the binomial function $(1+x)^{1/n}$. First we define big-O notation since it is used throughout the remaining sections.

**Definition 5.** *Given functions $f(z), g(z)\,\mathbb{R} \to \mathbb{R}$, $g(z)$ is said to be $O(f(z))$ if there exists a constant $M > 0$ such that $|g(z)| < M|f(z)|$ holds for all sufficiently large $z$.*

Given a formal power series $f(z)$ and positive integers $r$ and $s$, we will use linear algebra to deduce polynomials $P_r(z), Q_s(z)$ with rational coefficients of degrees $r$ and $s$, respectively, such that

$$P_r(z) - f(z)Q_s(z) = z^{r+s+1}E_{r,s}(z).$$

Here, $E_{r,s}(z)$ is a power series in the variable $z$. If we let $r = s$ then the polynomials $P_r(z)$ and $Q_r(z)$ are called diagonal pade approximants and we have for each natural number n, polynomials $P_n(z)$ and $Q_n(z)$ of degree n with rational integer coefficients such that

$$P_n(z) - f(z)Q_n(z) = z^{2n+1}E_n(z).$$

We remark that the word "hypergeometric" in the Hypergeometric Method is a reference to hypergeometric functions. A Hypergeometric function is any function $F(\alpha, \beta, \gamma, z)$ that satisfies the second order differential equation

$$z(1-z)F'' + (\gamma - (1+\alpha+\beta)z)F' - \alpha\beta F = 0.$$

We remark that $P_n(z)$ and $Q_n(z)$ can be shown to satisfy this differential equation and in general, most families of Pade approximants are hypergeometric functions. This is where the method gets its name.

It is also worth noting that the Pade approximants (considered as functions of a complex variable) may be analytically continued to include algebaic numbers such which could be

used to extend the Hypergeometric Method to other algebraic numbers like the Gaussian integers (where a version of Liouville's Approximation theorem also holds). However, we are not concerned with generalizations of the Hypergeometric Method in this thesis.

The existence of these Pade approximants will now be demonstrated. Let $f(z)$ be a function with a power series representation. That is,

$$f(z) = c_0 + c_1 z + c_2 z^2 + c_3 z^3 + \cdots$$

be a given formal power series. Given a pair of integers $(m, n)$, we want to find polynomials

$$p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m$$

and

$$q(z) = b_0 + b_1 z + b_2 z^2 + \cdots + b_n z^n$$

such that

$$f(z) = \frac{a_0 + a_1 z + ... + a_L z^L}{b_0 + b_1 z + ... + b_M z^M} + O(z^{L+M+1})$$

or equivalently,

$$f(z)q(z) - p(z) = \beta_{m+n+1} z^{m+n+1} + \beta_{m+n+2} z^{m+n+2} + \cdots \quad (*).$$

Condition (*) is equivalent to the following linear system

$$(1) \begin{cases} c_0 b_0 = a_0 \\ c_1 b_0 + c_0 b_1 = a_1 \\ c_2 b_0 + c_1 b_1 + c_0 b_2 = a_2 \\ \cdots \\ c_m b_0 + c_{m-1} b_1 + c_{m-2} b_2 + \cdots + c_0 b_m = a_m \end{cases}$$

$$(2)\ \begin{cases} c_{m+1}b_0 + c_m b_1 + c_{m-1}b_2 + \cdots + c_0 b_{m+1} = 0 \\ c_{m+2}b_0 + c_{m+1}b_1 + c_m b_2 + \cdots + c_0 b_{m+2} = 0 \\ \cdots \\ c_{m+n}b_0 + c_{m+n-1}b_1 + c_{m+n-2}b_2 + \cdots + c_0 b_{m+n} = 0 \end{cases}$$

in which $b_k = 0$ for $k > n$. When system (2) has a nontrivial solution, the coefficients $a_0$, $a_1, \cdots, a_m$ are determined from (1). This is solution is unique in the sense that if

$$f(z)q^*(z) - p^*(z) = \beta^*_{m+n+1} z^{m+n+1} + \beta^*_{m+n+2} z^{m+n+2} + \cdots$$

then

$$p(z)q^*(z) = p^*(z)q(z).$$

We can see this as follows. Since

$$fqq^* - pq^* = *z^{m+n+1} + \cdots$$

and

$$fq^*q - p^*q = *z^{m+n+1} + \cdots.$$

Hence,

$$p^*q - pq^* = *z^{m+n+1} + \cdots$$

where there asterisk $*$ is used as a stand-alone to represent the coefficients. Since $\deg(p^*q - pq^*) \leq m + n$ and the coefficients of $z^k$ on the right-hand side is zero for $k \leq n + n$, we conclude that $p^*q - pq^* = 0$.

Together, these two sets of relations determine all the coefficients and are termed Pade equations. Thus, we have constructed a rational function called the Pade approximant with 2 parameters $m$ and $n$ (sometimes written $[m/n]$ ) which agrees with the formal power series up to $z^{m+n}$. It should be noted that this construction says nothing about whether the sequence of Pade approximants converges to the function $f(z)$ and a formal power series is sufficient to construct the Pade approximant.

Although, it often happens that if a power series converges to a function g on some disk of radius R , the sequence of Pade approximants may converge on a larger domain and thus Pade approximants have practical applications to analytic continuation. However, this is beyond the scope of this section. A good reference for Pade approximants is given in the book "Pade Approximants" by George A. Baker Jr. and Peter Graves-Morris [4].

The binomial function $(1+\frac{x}{N})^{1/n}$ evaluated at particular integers is important for constructing irrationality measures because the diagonal Pade approximants to this function can be given explicitly. Although one can show that Pade approximants always exist for more general functions by using linear algebra, the Pade approximants to the binomial function are constructed by considering a contour integral and applying Cauchy's integral formula.

One considers two contour integrals,

$$I_0(z) = \frac{1}{2\pi i}\int_\gamma \frac{(1+zx)^{k+1/3}}{z^2(z-a)}dz$$

and

$$I_1(z) = \frac{1}{2\pi i}\int_\gamma \frac{(1+zx)^{k+1/3}}{(z-a)^2 z}dz$$

where $|x| < 1/a$ and $\gamma$ is a closed positively oriented countour enclosing both 0 and a.

Applying Cauchy's Integral Formula implies that,

$$I_1(x) = p_{10}(x) + (1+ax)^{1/3}p_{11}(x)$$

and

$$I_0(x) = p_{00}(x) + (1+ax)^{1/3}p_{01}(x).$$

where

$$p_{11}(x) = a^{-2k} \sum_{r=0}^{k_{11}} (-1)^{r+k_{11}} \binom{k+1/3}{r} \binom{2k-r-1}{k_{11}-r} (ax)^r (1+ax)^{k-r},$$

$$p_{00}(x) = a^{-2k} \sum_{r=0}^{k_{00}} (-1)^{k_{lm}} \binom{k+1/3}{r} \binom{2k-r-1}{k_{00}-r} (ax)^r,$$

and

$$p_{01}(x) = a^{-2k} \sum_{r=0}^{k_{01}} (-1)^{r+k_{01}} \binom{k+1/3}{r} \binom{2k-r-1}{k_{01}-r} (ax)^r (1+ax)^{k-r}.$$

Here $k_{lm} = k - 1 + \delta_{lm}$ and $0 \leq l, m \leq 1$.

In order to show how the above formulas were derived, we consider the case where $l = 0$ and

$$I_0(z) = \frac{1}{2\pi i} \int_\gamma \frac{(1+zx)^{k+1/3}}{z^2(z-a)} dz$$

where $(1+xz)^{k+1/3}$ represents the function whose value at $z = 0$ is 1 (the principal branch).

Using the binomial series $(1+t)^v = \sum_{k=0}^{\infty} \binom{t}{k} t^k$ for $|t| < 1$, we have the following series representations . In powers of z,

$$(1+xz)^{k+1/3} = \sum_{\nu=0}^{\infty} \binom{k+1/3}{\nu} (xz)^\nu$$

and in powers of $z - a$,

$$(1+xz)^{k+1/3} = (ax+1)^{k+1/3} + \sum_{n=0}^{\infty} \binom{k+1/3}{n} x^n (z-a)^n.$$

Also using the geometric series we have in powers of $z$,

$$z^{-2}(z-a)^{-1} = \sum_{n=0}^{\infty} z^{-3-n} a^n = -\frac{1}{az^2} - \frac{1}{a^2 z} - \frac{1}{a^3} - \frac{z}{a^4} + \dots$$

and in powers of $z - a$,

$$z^{-2}(z-a)^{-1} = \frac{1}{a^2(z-a)} - \frac{2}{a^3} + 3 + \frac{z-a}{a^4} - 4\frac{(z-a)^2}{a^5} + \dots.$$

Since our integrand is

$$\frac{(1+zx)^{k+1/3}}{z}^{-2}(z-a)^{-1},$$

we can expand this as a series in powrs of $z-a$ by taking the Cauchy product

$$\left((ax+1)^{k+1/3} + \sum_{n=0}^{\infty}\binom{k+1/3}{n}x^n(z-a)^n\right)\left(\frac{1}{a^2(z-a)} - \frac{2}{a^3} + 3 + \frac{z-a}{a^4} - 4\frac{(z-a)^2}{a^5} + \dots\right).$$

From this it follows that the coefficient of $\frac{1}{z-a}$ is $p_{00}(x)$, which is the residue of our integrand at the pole $z=a$. Similiarly, by taking the Cauchy product

$$\left(\sum_{\nu=0}^{\infty}\binom{k+1/3}{\nu}(xz)^{\nu}\right)\left(\sum_{n=0}^{\infty}z^{-3-n}a^n = -\frac{1}{az^2} - \frac{1}{a^2z} - \frac{1}{a^3} - \frac{z}{a^4} + \dots\right)$$

we find that the residue of the integrand at the pole $z=0$ is $P_{01}(x)$ .The case where $l=1$ follows similarly. An in depth computation of these formulas can be found in Lemma 3.3 of [20].

In order to generate the good sequence of rational approximations, one needs to choose an initial approximation, usually a convergent of the irrational being approximated. If we take $x = 1/N$ then it will be shown that this method gives a good measure of irrationality for numbers of the form $(1+\frac{a}{N})^{1/3}$. The sequence of rational approximations is generated by evaluating the pade approximants at particular integers corresponding to our initial approximation. The Hypergeometric Method is based on the idea that if the pade approximants are "good" approximations of the binomial function, then the rational numbers we get by evaluating them at these integer values will be good approximations to the binomial function evaluated at $x=a$. In order to show this in detail we present the following four lemmas from Bennett's paper [6].

**Lemma 1.** *Suppose that $\alpha$ is real and there exist postive integers c,d, C and D with $D>1$ such that for each positive integer k, we can find integers $p_{lmk}$ for $0 \le l, m \le 1$ with nonzero determinant such that:*

$$|p_{lmk}| \leq cC^k \text{ for } (0 \leq l, m \leq 1)$$

$$|p_{l0k} + p_{lk}\alpha| \leq dD^{-k} \text{ for } (0 \leq l \leq 1)$$

*Then for all positive integers p and q,*

$$\left|\alpha - \frac{p}{q}\right| > (3Cc\max\{1, 1.5d\}^{\frac{\log C}{logD}})^{-1} q^{-1-\frac{\log C}{logD}}$$

*Proof.* This lemma is just a slight modification of Theorem 10 of the last section.

□

We choose $x = 1/N$ to be our initial approximation to $(1 + \frac{a}{N})^{1/3}$. Although we have not yet shown that this approximation is "good" enough, it is a reasonable approximation as it depends on N. The next step in the Hypergeometric Method is to derive bounds for the contour integral $|I_l(1/N)|$.

**Lemma 2.** *If* $0 \leq l \leq 1$ *and* $N \geq 4a$ *then*

$$|I_l(1/N)| \leq \left(N(\sqrt{N} + \sqrt{N+a})^2\right)^{-k}.$$

*Proof.* From a detailed analysis of the contour integrals $I_l(z)$ given in Lemma 3.2 of the paper "Simultaneous Rational Approximation of Binomial Functions" by Michael Bennett [9], we have the integral representation of $I_l(1/N)$:

$$|I_l(1/N)| \leq \frac{\sqrt{3}}{2\pi} N^{-2k} \int_0^\infty \frac{x^{k+1/3}}{(x+1+al/N)\left((x+1)(x+1+a/N)\right)^k}. \tag{2.8}$$

For $1 \leq k \leq 10$ using the fact that $N \geq 4a$,

$$|I_l(1/N)| \leq \left(N(\sqrt{N} + \sqrt{N+a})^2\right)^{-k}.$$

We verify this by explicitly evaluating

$$\int_0^\infty \frac{x^{k+1/3}}{(x+1+al/N)\left((x+1)(x+1+a/N)\right)^k}.$$

For $1 \leq k \leq 10$ we have that

$$\int_0^\infty \frac{x^{k+1/3}}{(x+1+al/N)\left((x+1)(x+1+a/N)\right)^k}dx \leq \int_0^\infty \frac{x^{k+1/3}}{(x+1)^{k+2}}dx \leq \int_0^\infty \frac{x^{k+1/3}}{(x+1)^{k+2}}dx = \frac{4\pi}{9\sqrt{3}}.$$

Plugging this into inequality 2.8 we have

$$|I_l(1/N)| \leq \frac{\sqrt{3}}{2\pi}N^{-2k}\int_0^\infty \frac{x^{k+1/3}}{(x+1+al/N)\left((x+1)(x+1+a/N)\right)^k} \leq \frac{2\pi}{9}N^{-2k} \leq N^{-2k}.$$

Now using the fact that $a \leq \frac{1}{4}N$ we have

$$\left(N(\sqrt{N}+\sqrt{N+a})^2\right)^{-k} \leq N^2$$

from which the inequality follows.

If $k > 10$ then $|x^{1/3}/(x+1)| \leq \frac{4^{1/3}}{3}$ for $x \geq 0$ (2.8) implies that

$$|I_l(1/N)| \leq \frac{4^{1/3}\sqrt{3}}{6\pi}N^{-2k}\int_0^\infty \left(\frac{x}{(x+1)(x+1+\frac{a}{N})}\right)^k dx.$$

We split the above integral as

$$\int_0^4 \left(\frac{x}{(x+1)(x+1+a/N)}\right)^k dx + \int_4^\infty \left(\frac{x}{(x+1)(x+1+\frac{a}{N})}\right)^k dx$$

so we can apply estimates on both integrals.

We note that

$$\int_0^4 \left(\frac{x}{(x+1)(x+1+a/N)}\right)^k dx \leq 4\left(\frac{N}{\sqrt{N}+\sqrt{N+a})^2}\right)^k$$

since the derivative of

$$\frac{x}{(x+1)(x+1+\frac{a}{N})}$$

is

$$\frac{N(a-Nx^2+N)}{(x+1)^2(a+Nx+N)^2}$$

which has a root at $\frac{\sqrt{a+N}}{N}$ corresponding to the maximum of this function on the set $0 \leq x \leq 4$. Plugging this into our integrand we have

$$\frac{\sqrt{a+N}}{(\sqrt{a+N}+\sqrt{N})(\frac{a}{N}+\frac{\sqrt{a+N}}{\sqrt{N}}+1)} \leq \frac{N}{\sqrt{N}+\sqrt{N+a})^2}$$

since $N \geq 4a$.

We also have

$$\int_4^\infty \left(\frac{x}{(x+1)(x+1+a/N)}\right)^k dx \leq \int_4^\infty \left(\frac{x}{(x+1)^2)}\right)^k dx < \int_4^\infty \left(\frac{1}{x+1}\right)^k dx = \int_5^\infty \left(\frac{1}{x}\right)^k dx = \frac{5^{1-k}}{k-1}.$$

But for $k > 10$ this estimate is very small. In fact, it is strictly less than $5^{-k}$.

Now we apply the fact that $N \geq 4a$ and we get

$$\frac{N}{\sqrt{N}+\sqrt{N+a})^2} \geq \frac{4}{9+4\sqrt{5}} > 1/5.$$

Therefore, substituting constants back in we have

$$|I_l(1/N)| \leq 5\frac{\sqrt{3}34^{1/3}}{6\pi}\left(\sqrt{N}(\sqrt{N}+\sqrt{N+a})^2\right)^{-k}$$

for $k > 10$ and hence, Lemma 2 follows.

□

**Lemma 3.** *If $0 \leq l, m \leq 1$ and $N \geq 4a$ then $|p_{lm}(1/N)| \leq 1.16\left(\frac{\sqrt{N}+\sqrt{N+a})^2}{a^2N}\right)^k$.*

*Proof.* The functon $p_{lm}(x)\,(1+amx)^{1/3}$ is given by integrals $I_l(z)$ for $0 \leq l \leq 1$ with the contour in each case modified such that it encloses the integer $am$ and excludes $a(1-m)$. Hence we can write

$$p_{lm}(1/N)\left(1+\frac{am}{N}\right)^{1/3} = \frac{1}{2\pi i}\int_{\gamma_m} \frac{\left(1+\frac{z}{N}\right)^{k+1/3}}{(z-la)\,(z(z-a))^k}\,dz$$

for $0 \leq l, m \leq 1$ where $\gamma_0, \gamma_1$ are defined by the equations

$$|z| = \sqrt{N^2+aN} - N$$

and

$$|z-a| = N + a - \sqrt{N^2 + aN}$$

respectively. We set $c_0 = \sqrt{N^2+aN} - N$ and $c_1 = N + a - \sqrt{N^2+aN}$.

It follows that

$$p_{l0}(1/N) = \frac{1}{2\pi}\int_{-\pi}^{\pi}\left(\frac{c_0 e^{i\alpha}}{c_0 e^{i\alpha} - la}\right)\frac{\left(1+\frac{c_0 e^{i\alpha}}{N}\right)^{1/3}}{\left(c_0 e^{i\alpha}\left(c_0 e^{i\alpha}-a\right)\right)^k}\, d\alpha.$$

Also since

$$|c_0 e^{i\alpha} - a| \geq c_1 > c_0$$

we have that

$$p_{l1}(1/N)| \leq \left(1+\frac{c_0}{N}\right)^{1/3}\left(\frac{1+\frac{c_0}{N}}{c_0 c_1}\right)^k.$$

Similiarly,

$$|c_1 e^{i\theta} + a|^2 = (a + c_1\cos(\theta))^2 + c_1^2\sin(\theta)^2$$

so that

$$c_0 \leq |c_1 e^{i\alpha} + a| \leq c_1 + a.$$

Therefore,

$$|p_{l1}(1/N)| \leq \frac{c_1}{c_0}\left(1+\frac{c_1}{N+a}\right)^{1/3}\left(\max_{-\pi\leq\alpha\leq\pi}\left|\frac{1+\frac{c_1 e^{i\alpha}+a}{N}}{c_1(c_1 e^{i\alpha}+a)}\right|\right)^k.$$

However,

$$\max_{-\pi\leq\alpha\leq\pi}\left|\frac{1+\frac{c_1 e^{i\alpha}+a}{N}}{c_1(c_1 e^{i\alpha}+a)}\right| \leq \max_{-\pi\leq\alpha\leq\pi}\left\{\frac{1}{|c_1(c_1 e^{i\alpha}+a)|}\right\} + \frac{1}{c_1 N} \leq \frac{1}{c_0 c_1} + \frac{\frac{c_0}{N}}{c_0 c_1} = \frac{1+\frac{c_0}{N}}{c_0 c_1}.$$

We conclude that

$$|p_{l1}(1/N)| \leq \frac{c_1}{c_0}\left(1+\frac{c_1}{N+a}\right)^{1/3}\left(\frac{1+\frac{c_0}{N}}{c_0 c_1}\right)^k.$$

But

$$\frac{1+\frac{c_0}{N}}{c_0 c_1} = \frac{(\sqrt{N}+\sqrt{N+a})^2}{a^2 N}$$

and assuming we have $N \geq 4a$ we have

$$\max\left\{\left(1+\frac{c_0}{N}\right)^{1/3}, \frac{c_1}{c_0}\left(1+\frac{c_1}{N+a}\right)^{1/3}\right\} = \frac{c_1}{c_0}\left(1+\frac{c_1}{N+a}\right)^{1/3} < 1.16$$

and the result follows.

□

As we saw in a previous section, arithmetic information about our rational approximations give significant improvements in the irrationality exponent. In this section we study the bionomial coefficients occuring in $P_{lm}(1/N)$ by first defining an integer quantitiy $G(s)$ in terms of these coefficients and then using some analytic number theory to derive a lower bound on a second quantity $G_k$. Here $G_k$ is defined to be the greatest common divisor between $G(k)$ and $G(k-1)$ for integers k. This lower bound is the arithmetic information which gives us the improvement.

## 2.3 The Arithmethic Bound

For positive integers j and k, define the intervals $I_{jk}$ by $I_{jk} = [\frac{k+1}{j}, \frac{3k-4}{3j-1}]$. Also, for $0 \leq s \leq k$ we define

$$G(s) = \gcd\left\{3^{\lfloor \frac{3s}{2} \rfloor}\binom{k+\frac{1}{3}}{r}\binom{2k-r-1}{s-r} : 0 \leq r \leq s\right\}.$$

This expression comes from the binomial coefficients in our expressions for $P_{lm}(1/N)$ for example,

$$p_{11}(1/N) = a^{-2k}\sum_{r=0}^{k_{11}}(-1)^{r+k_{11}}\binom{k+1/3}{r}\binom{2k-r-1}{k_{11}-r}\left(\frac{a}{N}\right)^r\left(1+\frac{a}{N}\right)^{k-r}.$$

$G(s)$ is well defined since

$$3^{\lfloor \frac{3s}{2} \rfloor}\binom{k+\frac{1}{3}}{r} \in \mathbb{Z}$$

for any $0 \leq r \leq s$ and $k \in \mathbb{N}$ by Lemma 4.2 of [10]. Now we define $G_k = \gcd\{G(k), G(k-1)\}$. The significance of the above intervals is apparent in the following lemma which gives a lower bound on this quantity $G_k$.

**Lemma 4.** *$G_k > \frac{1}{5563}2^k$ for $k \geq 1$.*

*Proof.* Suppose that $k \geq 220000$ then from Schoenfeld [21], it follows that $\alpha(x) = \sum_{p \leq x} \log p < 1.000081x$ for $x > 0$ where the sum ranges over prime p. What we require is lowerbounds on Chebyshev's function $\alpha(x)$ and in order to do this we use Colorllary $2^*$ of [21].

We define

$$L_{l,k} = \sum_{p \in I_{l_k}} \log p.$$

It follows that,

$$L_{1,k} > 0.49584k - 1.99458,$$

$$L_{2,k} > 0.09728k - 0.79643$$

and

$$L_{3,k} > 0.03943k - 0.49706.$$

We derive similar inequalities for $L_{l,k}$ for $4 \leq k \leq 18$. The connection with $G_k$ is given by the fact that if p is a prime in $I_{j_k}$ for some positive integers j, k with $1 \leq j \leq \sqrt{k/3}$ then p divides $G_k$. This is proved in Lemma 3.1 [6] and provides the connection between $G_k$ and $L_{1,k}, L_{2,k}, L_{3,k}$. Applying this we can see that $\log G_k > L_{1,k} + L_{2,k} + L_{3,k}$. Hence, we conclude that

$$\log G_k > 0.69493k - 5.58728 > (\log 2)k$$

so that

$$G_k > 2^k$$

for $k \geq 220000$. The remaining cases are handled in Michael Bennett's paper [6] and involve directly computing $G_k$ from the definition. □

We will now present the following theorem due to Michael Bennett [6].

**Theorem 11.** *Suppose that a and N are positive integers satisfying*

$$8(\sqrt{N} + \sqrt{N+a})^2 > a^4 \kappa(a)^3$$

$$\kappa(a) = \begin{cases} 3\sqrt{3} & \textit{if } \mathrm{ord}_3(a) = 0 \\ \sqrt{3} & \textit{if } \mathrm{ord}_3(a) = 1 \\ 1 & \textit{if } \mathrm{ord}_3(a) > 1 \end{cases}$$

*and $p$ an $q$ are any positive integers, then*

$$\left| \left(1 + \frac{a}{N}\right)^{1/3} - \frac{p}{q} \right| > (4\kappa(a)N)^{-1}(10^4 q)^{-\lambda}$$

*where $\lambda$ is equal to*

$$1 + \frac{\log\left(\frac{\kappa(a)}{2}\left(\sqrt{N} + \sqrt{N+a}\right)^2\right)}{\log\left(\frac{2}{a^2\kappa(a)}\left(\sqrt{N} + \sqrt{N+a}\right)^2\right)}.$$

*Proof.* Let

$$M = \max\left\{\lfloor 3k/2 \rfloor - k ord_3(a), 0\right\}.$$

Seting

$$p_{lk} = 3^M a^{2k} N^k p_l G_k^{-1},$$

it follows that we have $p_{lmk} \in \mathbb{Z}$ for $0 \leq l, m \leq 1$. We want to multiply by the above quantities to scale $p_{lm}$ so it is an integer. The $a^{2k}N^k$ are used to eliminate the denominator in $\alpha$ to ensure it is larger than 1 as required in the lemma at the beginning. Lemma 3 and Lemma 4 then imply that

$$|p_{lmk}| \leq 6454 \left(\frac{\kappa(a)}{2}\left(\sqrt{N} + \sqrt{N+a}\right)^2\right)^k.$$

Also, Lemma 3 and Lemma 4 yield

$$\left| p_{l0k} + p_{l1k}(1 + \frac{a}{N})^{1/3} \right| \leq 5563 \left(\frac{2}{a^2\kappa(a)}(\sqrt{N} + \sqrt{N+a})^2\right)^{-k}.$$

We now apply Lemma 1 to conclude that

$$\left| \left(1 + \frac{a}{N}\right)^{1/3} - \frac{p}{q} \right| > cq^{-\lambda}$$

where the above inequality holds for all positive integers $p$ and $q$.Here $\lambda$ is the statement in Lemma 1 and

$$c^{-1} = 9681\,(8344.5)^{\lambda-1}\,\kappa(a)\left(\sqrt{N}+\sqrt{N+a}\right)^2.$$

Now, using the fact that $N \geq 4a$ we get

$$c^{-1} < 4\kappa(a)N10^{4\lambda}$$

which completes the proof.

□

The above theorem can be used to compute irrationality measures for many degree 3 algebraic irrationalities as can be seen in the table that follows. In the next section we will show how some of these irrationality measures are computed in detail.

| $\alpha$ | $\lambda(\alpha)$ | $c(\alpha)$ |
|---|---|---|
| $2^{1/3}$ | 2.47 | 0.25 |
| $3^{1/3}$ | 2.76 | 0.39 |
| $5^{1/3}$ | 2.80 | 0.29 |
| $6^{1/3}$ | 2.35 | 0.01 |
| $7^{1/3}$ | 2.70 | 0.08 |
| $10^{1/3}$ | 2.45 | 0.15 |

Table 1. Parameters from 11 computed for explicit values of $\alpha$

## 2.4 Some Computations of Irrationality Measures

We will now use Theorem 11 to compute an explicit example for $\sqrt[3]{19}$. Choosing $a = 1, N = 8^3$ we have

$$\sqrt[3]{1+1/8^3} = \frac{3}{8}\sqrt[3]{19}$$

and $\text{ord}_3(a) = 1$ so that

$$\kappa(a) = 3\sqrt{3}$$

we compute the exponent

$$\lambda = 2.2863.$$

Now using $\lambda$ to compute c as in Theorem 11 to be $2.9036e10^{-12}$. Hence we conclude that for any $p, q > 0$

$$\left|\frac{3}{8}\sqrt[3]{19} - \frac{3p}{8q}\right| > cq^{-\lambda}.$$

Writing $q^{\lambda} = q^{2.30-2.2836}q^{-2.30}$ we see that for $q > 10^{574}$

$$\left|\sqrt[3]{19} - p/q\right| > \frac{1}{50}q^{-2.30}. \tag{2.9}$$

It remains to verify $1 \leq q \leq 10^{574}$. We first note that if $p$ and $q$ fail to satisfy (2.9) then $\frac{p}{q}$ is a convergent to $\sqrt[3]{19}$ by Theorem 15 of the next section since for positive integers q, $\frac{1}{50}^{-2.30} < \frac{1}{2}q^{-2}$.

We need only consider convergents with denominators bounded above by $10^{574}$. Using Theorem 15 we see that we only need to check the first 3814 convergents, since for $k > 3814$, $q_k \geq 2^{\frac{k-1}{2}} > 10^5 74$ that is $\frac{p}{q} = \frac{p_i}{q_i}$ for some $1 \leq i \leq 3814$. Using a python program in Appendix 1 to compute continued fractions modified to deal with arbitrary precision, we see that $q_{100} > 10^{49}$. We verified this inequality for the first 100 convergents. Now we may assume that $i \geq 100$ However, using fact that

$$\left|\sqrt[3]{19} - \frac{p}{q}\right| > \frac{1}{(a_{i+1}+2)q_i^2}$$

we see that if $\frac{p}{q}$ does not satisfy (2) then

$$a_{i+1} > 50q_i^{0.30} - 2.$$

But $q_i > 10^{49}$ and we conclude that

$$a_{i+1} \geq 10^{16}.$$

Using our program we verified that

$$\max_{101 \leq i \leq 3419} a_i = 5085$$

, which is a contradiction. Hence, we conclude that (2.9) is true for all $p, q > 0$.

A more difficult example is applying Theorem 11 to the cubed root of 57. As noted in [6] this requires a more detailed analysis of the continued fraction expansion than the previous example. Theorem 11 gives

$$\left| \sqrt[3]{57} - \frac{p}{q} \right| > (2.2 * 10^{25})^{-1} q^{-2.99738}$$

for any positive integers $p$ and $q$.

The goal now is to reduce the constant to a more manageable constant between 0 and 1. First we note that for $q \leq 10^{39770}$,

$$\left| \sqrt[3]{57} - \frac{p}{q} \right| > 0.45 q^{-2.998}.$$

Now, we need to know how many convergents are less than this number. Since it is computationally expensive to compute convergents and explicitly check if each one satisfies our inequality we instead use the following fact about continued fractions which we prove as Theorem 11 in the next section

$$q_k \geq 2^{\frac{k-1}{2}}, \text{ for } k \geq 2.$$

From this we conclude that in the worst case the first 264234 convergents are less than $10^{39770}$. Computation using our python program given in Appendix 1 gives the first 10 convergents as:

$$1, 3/1, 8/3, 507/190, 515/193, 1537/576, 3589/1345, 8715/2366, 12304/4611, 11777595/441311.$$

We substitute each of these convergents for $p/q$ into our initial inequality and find that the inequality is satisfied by all except 3/1. We compute that the largest constant (to the

nearest hundreth) between 0 and 1 for which the initial inequality remains true is 0.33 and hence to show that

$$\left|\sqrt[3]{57} - \frac{p}{q}\right| > 0.33q^{-2.998}$$

it suffices to verify this inequality is true for each convergent $p_i/q_i$ for $11 \leq i \leq 264234$.

We note that $q_i \geq 10^6$ for $i \geq 11$ and arguing as in the previous example we conclude that $a_i + 1 \geq 294771$ in this range. However, using our Python program in Appendix 1 we get that the maximum partial quotient in this range is 33629, a contradiction. Thus we conclude that

$$\left|\sqrt[3]{57} - \frac{p}{q}\right| > 0.33q^{-2.998}$$

is true for all positive integers $p, q$. We have finished our discussion of irrationality measures (also called general irrationality measures) however, there is also a concept of a restricted irrationality measure and so we end this chapter with a section about this.

## 2.5 Constructing a Restricted Irrationality Measure

We will first define a restricted irrationality measure and explain how the Hypergeometric Method can be used to construct a restricted irrationality measure through the use of off-diagonal pade approximants.

**Definition 6.** *A restricted irrationality measure for an irrational number $\alpha$ is an inequality of the form*

$$\left|\frac{p}{q} - \alpha\right| \geq c\frac{1}{q^{\lambda}}$$

*where $c$ is some positive constant and $q$ is restricted to some form.*

Usually restricted irrationality measures involve $\alpha$ being an algebraic number (for example a quadratic irrational) and powers of some fixed number in the denominator and if $\alpha$ has degree n then the goal is to find an exponent $\lambda < n$ in an inequality of the above form. Suppose we want to construct a restricted irrationality measure for a quadratic irrational

$\sqrt{D}$. As in the construction of general irrationality measures, we use of Pade approximants to a bionomial function. In this particular case, the binomial function $(1-z)^{1/2}$ is of interest and the Pade approximants are derived through the use of contour integals. Bauer and Bennett [5] define

$$I_{n_1,n_2}(x) = \frac{1}{2\pi}\int_\gamma \frac{(1-zx)^{n_2}(1-zx)^{1/2}}{z^{n_1+1}(1-z)^{n_2+1}}\,dz$$

where $n_1, n_2$ are positive integers, $\gamma$ is a closed curve oriented counter clockwise and enclosing $z=0$ and $z=1$ and $|x|<1$.

Cauchy's Theorem is then applied to this contour to write

$$I_{n_1,n_2}(x) = P_{n_1,n_2}(x) - (1-x)^{1/2}Q_{n_1,n_2}$$

where $P_{n_1,n_2}(x), Q_{n_1,n_2}(x)$ are both polynomials with rational coefficients of degree $n_1$ and $n_2$ respectively. This involves a residue computation. The integrand

$$\frac{(1-zx)^{n_2}(1-zx)^{1/2}}{z^{n_1+1}(1-z)^{n_2+1}}$$

has a pole of order $n_1+1$ at $z=0$. Therefore, we need to compute the $n_1$ term in the Taylor series of $(1-zx)^{n_2+1/2}\,(1-z)^{-n_2-1}$ to find the residue.

Using the Binomial Theorem we get

$$(1-zx)^{n+1/2} = \sum_{k=0}^{\infty}(-1)^k\binom{n_2+1/2}{k}x^k z^k$$

and

$$(1-z)^{-n-1} = \sum_{k=0}^{\infty}(-1)^k\binom{-n_2-1}{k}z^k.$$

Now multiplying these series together and using Cauchy's formula for the product of two series we have

$$P_{n_1,n_2}(x) = \sum_{n=0}^{n_1}\binom{n_2+1/2}{k}\binom{n_1+n_2-k}{n_2}(-x)^k.$$

The computation for the residue at the pole $z=1$ is similar. Explicitly we have

$$P_{n_1,n_2}(x) = \sum_{n=0}^{n_2}\binom{n_2-1/2}{k}\binom{n_1+n_2-k}{n_2}(-x)^k.$$

These are called off-diagonal pade approximants. The next step is to bound $|P_{n_1,n_2}(x)|$ and $|I_{n_1,n_2}(x)|$ and consider arithmetic information about the polynomials $P_{n_1,n_2}(x)$ and $Q_{n_1,n_2}(x)$. The techniques used to find these bounds are very similar to the techniques used in deriving general irrationality measures and can be found in [5]. An explicit example of the above construction is the following theorem due to F. Beuekers [7].

**Theorem 12.** *If $p$ and $q$ are integers with $q = 2^k$ where $k$ is a nonnegative integer then*

$$\left|\sqrt{2} - \frac{p}{q}\right| > 2^{-43.9} q^{-1.8}.$$

We will use this theorem in a later chatper to show its application to the polynomial-exponential Diophantine equations.

# Chapter 3

# Continued Fractions

## 3.1 Introduction

In this chapter we define and prove some basic objects and theorems about continued fractions that we will use throughout the remainder of this document, concluding with Worley's Theorem in Diophantine Approximation. A more complete development of the theory of continued fractions can be found in Hardy [14].

## 3.2 Definitions and Basic Properties

We begin by giving the definition of a finite continued fraction. We also introduce some new notation which will simplify the representation of a finite continued fraction.

**Definition 7** (Finite Continued Fraction)**.** *Let $a_1 \in \mathbb{R}$ be any real number and $a_2, a_3, \ldots, a_n$ be any positive real numbers.*

*Then the expression:*

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

*is a finite continued fraction and is denoted $[a_1, a_2, ..., a_n]$. The $a_i$ are called partial quotients.*

Now that we have defined finite continued fractions, we are ready to introduce finite sim-

ple continued fractions. We also define infinite simple continued fractions which are usedl throughout the thesis.

**Definition 8** (Simple Finite Continued Fraction)**.** *A finite continued fraction* $[a_1, a_2, ..., a_n]$ *is said to be simple if the* $a_i$ *are positive integers. An infinite simple continued fraction is the limit of a sequence of finite simple continued fractions and is denoted by* $[a_1, a_2, \ldots]$

Given a continued fraction with $n \geq k$ partial quotients, it seems natural to consider the continued fraction formed from the first $k$ partial quotients. The resulting quantitiy is called the $k$th convergent. It is important to note that in the case of a simple continued fraction, the $k$th convergent is a rational number. This will be particularly important when we are interested in finding rational approximations to an irrational number.

**Definition 9** (Convergent)**.** *Let* $[a_1, a_2, a_3, \ldots, a_n]$ *or* $[a_1, a_2, a_3, \ldots]$ *be a continued fraction (i.e. either finite or infinite). Then the "kth convergent"* $C_k$ *of the given continued fraction is the continued fraction given by*

$$C_k = [a_1, a_2, \ldots, a_k] .$$

We also have recurrence relations which can be used to calculate the numerators and denominators of the convergents recursively. These recurrence relations are useful in some of our induction proofs so we will state and prove them.

**Theorem 13.** *The value of* $[a_1, a_2, a_3, \ldots, a_n]$ *is* $\frac{p_n}{q_n}$ *where* $p_1 = a_1, q_1 = 1, p_2 = a_1a_2+1, q_2 = a_2$ *and for any* $n \geq 3$*,*

$$p_n = a_n p_{n-1} + p_{n-2}$$

*and*

$$q_n = a_n q_{n-1} + q_{n-2}.$$

*Proof.* We will use induction on the number $n$ of partial quotients in the continued fraction expansion. That is, for any $n \in \mathbb{N}$,

$$[a_1, a_2, a_3, \ldots, a_n] = \frac{p_n}{q_n}$$

where $p_n, q_n$ are defined as in the theorem.

Clearly this is true for $n = 1$ as the result holds for any continued fraction expansion $[a_1] = \frac{a_1}{1} = \frac{p_1}{q_1}$. Likewise, for $n = 2$,

$$[a_1.a_2] = a_1 + \frac{1}{a_2} = \frac{a_1a_2 + 1}{a_2} = \frac{p_2}{q_2}$$

Suppose that $[a_1, a_2, a_3, \ldots, a_k] = \frac{p_k}{q_k}$. We need to show $[a_1, a_2, a_3, \ldots, a_k, a_{k+1}] = \frac{p_{k+1}}{q_{k+1}}$. We note that the continued fraction $[a_1, a_2, a_3, \ldots, a_k, a_{k+1}]$ can be written with one less term. That is

$$[a_1, a_2, a_3, \ldots, a_k, a_{k+1}] = \left[a_1, a_2, a_3, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right].$$

In order to simplify our notation we write $b_0 = a_0, b_1 = a_1, \ldots, b_{k-1} = a_{n-1}$ and $b_k = a_k + \frac{1}{a_{k+1}}$. We denote the convergents of $[b_1, b_2, b_3, \ldots, b_k]$ by $\frac{P_n}{Q_n}$. By our induction hypothesis we have that $P_n = b_nP_{n-1} + P_{n-2}$ and $Q_n = b_nQ_{n-1} + Q_{n-2}$ for $2 \leq n \leq k$ and therefore

$$[b_1, b_2, b_3, \ldots, b_k] = \frac{P_k}{Q_k} = \frac{nP_{n-1} + P_{n-2}}{b_nQ_{n-1} + Q_{n-2}}. \tag{3.1}$$

Now we need to relate the convergents of $[a_1, a_2, a_3, \ldots, a_k, a_{k+1}]$ and $[b_1, b_2, b_3, \ldots, b_k]$. We know that $b_n = a_n$ for all $0 \leq n \leq k-1$ and hence the $n$th convergents are the same for all $0 \leq n \leq k-1$. Thus, we can make the following substitutions into Equation 3.1. $P_{k-1} = p_{k-1}, P_{k-2} = p_{k-2}$ and $Q_{k-1} = q_{k-1}, Q_{k-2} = q_{k-2}$. Also since $[a_1, a_2, a_3, \ldots, a_k, a_{k+1}] = [b_1, b_2, b_3, \ldots, b_k]$ and $b_k = a_k + \frac{1}{a_{k-1}}$ we conclude that

$$[a_1, a_2, a_3, \ldots, a_k, a_{k+1}] = \frac{b_kP_{k-1} + P_{k-2}}{b_kQ_{k-1} + Q_{k-2}} = \frac{\left(a_k + \frac{1}{a_{k+1}}\right)p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k-1}}\right)q_{k-1} + q_{k-2}} = \frac{a_{k+1}(a_kp_{k-1} + p_{k-2}) + p_{k-2}}{a_{k+1}(a_kq_{k-1} + q_{k-2}) + q_{k-2}}. \tag{3.2}$$

Now our induction hypothesis applied to the continued fraction $[a_1, a_2, a_3, \ldots, a_k]$ tell us that the following recursion formulas hold. $p_k = a_kp_{k-1} + p_{k-2}$ and $q_k = a_kq_{k-1} + q_{k-2}$ and thus equation 3.2 simplifies to

$$[a_1, a_2, a_3, \ldots, a_k, a_{k+1}] = \frac{a_{k+1}p_k + p_{k-2}}{a_{k+1}q_k + q_{k-2}}.$$

By definition, the $k+1$st convergent is $[a_1, a_2, a_3, \ldots, a_k, a_{k+1}] = \frac{p_{k+1}}{q_{k+1}}$. Comparing these two equations we see that $p_{k+1} = a_{k+1}p_k + p_{k-1}$ and $q_{k+1} = a_{k+1}q_k + q_{k-1}$ (using the fact that both fractions are already written in lowest terms) which completes the induction.

□

We now develop some useful facts about convergents, one being an identity that comes in handy surprisingly often. We also prove that even convergents form an increasing sequence while odd convergents form a decreasing sequence. In particular, the even convergents are always less than or equal to the number that they converge to while the odd convergents are always greater than or equal to this number. The recursive formulas we just proved come in handy in this proof.

**Theorem 14.** *Let* $\frac{p_k}{q_k} = [a_0, a_1, a_2, a_3, \ldots, a_k]$ *then for* $k \geq 0$ $p_{k+1}q_k - p_kq_{k+1} = (-1)^k$. *Furthermore,* $\left\{\frac{p_{2k}}{q_{2k}}\right\}$ *is increasing and* $\left\{\frac{p_{2k+1}}{q_{2k+1}}\right\}$ *is decreasing.*

*Proof.* From Theorem 13 $p_1q_0 - p_0q_1 = 1$ and

$$p_{k+1}q_k - p_kq_{k+1} = (a_kp_k + p_{k-1})q_k - p_k(a_kq_k + q_{k-1}) = -(p_kq_{k-1} - p_{k-1}q_k). \tag{3.3}$$

Equation 3.3 gives

$$p_{k+1}q_k - p_kq_{k+1} = (-1)^k$$

so

$$\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_kq_{k+1}}$$

and

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_{k-1}q_k}.$$

Adding the above two equations together gives

$$\frac{p_{k+1}}{q_{k+1}} - \frac{p_{k-1}}{q_{k-1}} = (-1)^{k-1}\frac{q_{k+1} - q_{k-1}}{q_{k-1}q_k q_{k+1}}.$$

Since $\{q_k\}$ is an increasing sequence, the quantity on the right is positive for odd $k$ (even convergents) and negative for even $k$ (odd convergents). Therefore, $\left\{\frac{p_{2k}}{q_{2k}}\right\}$ is increasing and $\left\{\frac{p_{2k+1}}{q_{2k+1}}\right\}$ is decreasing.

□

We note that from formula $p_{k+1}q_k - p_k q_{k+1} = (-1)^k$ it is clear that $p_k$ and $q_k$ are coprime for $k \geq 0$. We now present a lower bound on $q_k$ which says that the denominators of the convergents in a simple continued fraction grow exponentially. This result is particularly useful if we combine it with the fact that $\{q_k\}$ is a strictly increasing sequence since we can use these results to estimate how many convergents there are with denominator bounded by a fixed number.

**Theorem 15.** *Let $[a_1, a_2, a_3, \ldots]$ be a continued fraction expansion and $q_1, q_2, q_3, \ldots$ denote the denominators in the convergents. Then $q_k \geq 2^{\frac{k-1}{2}}$ and furthermore, $q_{k+1} > q_k$ for $k \geq 2$.*

*Proof.* From the recurrence relations we see that

$$q_k = a_k q_{k-1} + q_{k-2} \geq q_{k-1} + q_{k-2} \geq q_{k-1} \tag{3.4}$$

since $q_{k-2} > 0$ and hence $q_k \geq q_{k-1}$. In fact,

$$q_k > q_{k-1} + q_{k-2} \geq 2q_{k-2} \geq 2^2 q_{k-4} \ldots.$$

It follows by induction that if k is odd,

$$q_k \geq 2^{\frac{k-1}{2}} q_1$$

and if k is even

$$q_k \geq 2^{\frac{k}{2}} q_0.$$

However in both cases $q_k \geq 2^{\frac{k-1}{2}}$ which completes the proof of the first proposition. We also note that $q_1 = 1, q_2 = a_2$ and $q_3 = a_3a_2 + 1$ all satisfy $1 = q_1 \leq q_2 < q_3$.

Suppose that $q_k > q_{k-1} \geq 1$ for some $k \geq 3$ Then by (3.4) can be rewritten as

$$q_k = a_k q_{k-1} + q_{k-2} \geq q_{k-1} + q_{k-2} \geq q_{k-1} + 1 > q_{k-1}.$$

Hence by induction $\{q_k\}$ is a striclty increasing sequence, with the only possible exceptions at $q_1 = q_2 = 1$.

□

A natural question would be given an irrational number how does one compute the partial quotients associated to this number. The Continued Fraction Algorithm is just such a method for finding the continued fraction expansion for any irrational number to as many partial quotients as required. We desribe the algorithm below.

Let $x_1$ be an irrational number then:

1. Set $k := 1$.

2. Set $a_k := \lfloor x_k \rfloor$.

3. Set $x_{k+1} := \dfrac{1}{x_k - a_k}$.

4. Set $k := k + 1$.

5. Go to step 2.

6. Output $x_1 = [a_1, a_2, a_3, \ldots]$.

We will prove that the algorithm is correct.

Let $x_1$ be an irrational number.

We seek $a_1, a_2, \ldots \in \mathbb{Z}$ such that $x_1 = [a_1, a_2, \ldots]$. We know from Hardy Theorem 154 [14] that $x_1$ lies strictly between any successive pair of its continued fraction convergents. So, for a start, it has to be between $C_1 = a_1$ and $C_2 = a_1 + \dfrac{1}{a_2}$. In particular, as $a_2 \geq 1$, we know that $a_1 < x_1 < a_1 + 1$. So $a_1 = \lfloor x_1 \rfloor$ where $\lfloor x_1 \rfloor$ is the floor of $x_1$. We note, in particular, that $a_1$ is therefore completely determined by $x_1$.

Now we write

$$x_1 = \lfloor x_1 \rfloor + \{x_1\}$$

where $\{x_1\}$ is the fractional part of $x_1$. Then

$$x_1 = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}} = \lfloor x_1 \rfloor + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}} = \lfloor x_1 \rfloor + \frac{1}{[a_2, a_3, a_4, \ldots]}.$$

Note that, $0 \leq \{x_1\} < 1$. But because $x_1$ is an irrational number, $\{x_1\} \neq 0$. So $0 < \{x_1\} < 1$. Hence $[a_2, a_3, a_4, \ldots] = \dfrac{1}{x_1 - \lfloor x_1 \rfloor} = \dfrac{1}{\{x_1\}}$.

Now we write $x_2 = \dfrac{1}{\{x_1\}}$. Then $x_2 = [a_2, a_3, a_4, \ldots]$. As $\{x_1\} < 1$ we have that $x_2 = \dfrac{1}{\{x_1\}} > 1$. Therefore $x_2$ is an irrational number greater than $a_2$ which is positive.

Repeating the argument gives $a_2 = \lfloor x_2 \rfloor$ and so $a_2$ is determined uniquely from $x_2$ and hence from $x_1$. Similarly, $x_3 = \dfrac{1}{\{x_2\}}$ and hence $x_3 = [a_3, a_4, a_5, \ldots]$. Therefore, the uniqueness follows by induction.

It remains to show existence, that is, $x_1 = [a_1, a_2, \ldots, ]$. We use the fact that

$$x_1 = [a_1, a_2, \ldots, a_k, x_{k+1}] = \frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}}.$$

Hence,

$$\left| x_1 - \frac{p_k}{q_k} \right| = \left| \frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k} \right| = \left| \frac{x_{k+1}p_kq_k + p_{k-1}q_k - x_{k+1}p_kq_k - p_kq_{k-1}}{(x_{k+1}q_k + q_{k-1})q_k} \right|.$$

The quantity on the right simplifies to

$$\left|\frac{p_{k-1}q_k - p_k q_{k-1}}{(x_{k+1}q_k + q_{k-1})q_k}\right| = \left|\frac{1}{(x_{k+1}q_k + q_{k-1})q_k}\right|.$$

Since $x_{k+1} > a_{k+1}$ we have $x_{k+1}q_k + q_{k-1} > a_{k+1}q_k + q_{k-1} = q_{k+1}$ and hence,

$$\left|\frac{1}{(x_{k+1}q_k + q_{k-1})q_k}\right| \leq \frac{1}{q_{k+1}q_k}.$$

But also $q_k \geq k$ and $q_{k+1} \geq k+1$ and so,

$$\left|x_1 - \frac{p_k}{q_k}\right| \leq \frac{1}{(k+1)k}.$$

Therefore by the Squeeze Theorem,

$$\lim_{k\to\infty}\left|x_1 - \frac{p_k}{q_k}\right| \leq \lim_{k\to\infty}\frac{1}{(k+1)k} = 0$$

and we conclude that

$$[a_1, a_2, \ldots,] = \lim_{k\to\infty}\frac{p_k}{q_k} = x_1$$

as required.

## 3.3 Some Approximation Results

In this section we state and prove some inequalities about the convergents of a simple continued fraction which are particularly useful in Diophantine approximation.We start with some basic inequalities which are useful for approximating irrational numbers by convergents. We then prove Legendre's Theorem which gives a criterion to decide if a rational approximation is a convergent or not. We then generalize Legendre's Theorem and consider some of its implications.

**Theorem 16.** *Let $x$ be an irrational number and $C_n$ be the nth convergent of $x$. Let $p_1, p_2, p_3, \ldots$ and $q_1, q_2, q_3, \ldots$ be the respective numerators and denominators.Then $\forall k \geq 1$,*

$$\left|x - \frac{p_{k+1}}{q_{k+1}}\right| \leq \frac{1}{q_{k+1}q_{k+2}} \leq \frac{1}{2q_k q_{k+1}} < \left|x - \frac{p_k}{q_k}\right|.$$

*Proof.* Let $x$ have a simple infinite continued fraction of

$$[a_1, a_2, a_3, \ldots].$$

The continued fraction algorithm gives the following system of equations:

$$x = [a_1 x_2] = [a_1, a_2, x_3] = [a_1, a_2, a_3, x_4] = \ldots = [a_1, a_2, ..., a_n, x_{n+1}]$$

and

$$\left| x - \frac{p_n}{q_n} \right| = \left| [a_1, a_2, \ldots, a_n, x_{n+1}] - \frac{p_n}{q_n} \right| = \left| \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} \right| = \left| \frac{p_{n-1}q_n - p_n q_{n-1}}{q_n(x_{n+1}q_n + q_{n-1})} \right|.$$

This later quantity simplifies to

$$\frac{1}{q_n(x_{n+1}q_n + q_{n+1})}.$$

by properties of convergents.

Now

$$x_{n+1} = [a_{n+1}, a_{n+2}, a_{n+3}, \ldots]$$

from the continued fraction algorithm. So $a_{n+1} < x_{n+1} < a_{n+1} + 1$ and therefore

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n \left(a_{n+1}q_n + q_{n-1}\right)} = \frac{1}{q_n q_{n+1}}.$$

We also have the inequality

$$\left| x - \frac{p_n}{q_n} \right| > \frac{1}{q_n \left(\left(a_{n+1} + 1\right) q_n + q_{n-1}\right)}.$$

Hence for $k \geq 1$,

$$\left| x - \frac{p_{k+1}}{q_{k+1}} \right| \leq \frac{1}{q_{k+1}q_{k+2}} < \left| x - \frac{p_k}{q_k} \right|.$$

For the middle inequality, note that

$$q_{k+2} = a_{k+2}q_{k+1} + q_k > q_k + q_k = 2q_k$$

so

$$\frac{1}{q_{k+1}q_{k+2}} \leq \frac{1}{2q_kq_{k+1}}.$$

□

From the above theorem we immediately get the following corollary.

**Corollary 1.** $\forall k \geq 1$,

$$\frac{1}{q_kq_{k+1}} > \left|x - \frac{p_k}{q_k}\right| > \frac{1}{2q_kq_{k+1}}$$

*and*

$$\frac{1}{(a_{n+1}+2)q_n^2} < |x - \frac{p_n}{q_n}| < \frac{1}{a_{n+1}q_n^2}$$

Before we prove Legendre's Theorem which tells us good rational approximations of irrational numbers are convergents, we first need a lemma.

**Lemma 5.** *If $x = \frac{P\zeta+R}{Q\zeta+S}$ where $\zeta > 1$ and $P, Q, R, S$ are integers such that $Q > S > 0$ and $PS - QR = \pm 1$ then $R/S$ and $P/Q$ are consecutive convergents to the simple continued fraction whose value is $x$.*

*Proof.* See Theorem 172 of [14].

□

With this in hand, we can now prove the following.

**Theorem 17** (Legendre's Theorem)**.** *If*

$$\left|\frac{p}{q} - x\right| < \frac{1}{2q^2}$$

*then $\frac{p}{q}$ is a convegent to $x$.*

*Proof.* If the conditions of the theorem are satisfied then

$$\frac{p}{q} - x = \frac{\epsilon\alpha}{q^2},$$

where $\epsilon = \pm 1$ and $0 < \alpha < \frac{1}{2}$. We write $\frac{p}{q}$ as a finite contnued fraction say $[a_0, a_1, ..., a_n]$; and since by Theorem 158 of [14] we can choose n even or odd, we may assume that $\epsilon = (-1)^{n-1}$. We write

$$x = \frac{\omega p_n + p_{n-1}}{\omega q_n + q_{n-1}},$$

where $\frac{p_n}{q_n}, \frac{p_{n-1}}{q_{n-1}}$ are the ultimate and penultimate convergents to $\frac{p}{q}$ and $\omega = \frac{1}{\alpha} - \frac{q_{n-1}}{q_n}$.

In order to see this we solve the equation $x = \frac{\omega p_n + p_{n-1}}{\omega q_n + q_{n-1}}$ for $\omega$ and find

$$\omega = \frac{q_{n-1}x - p_{n-1}}{-q_n x + p_n}.$$

Now substitute

$$x = \frac{p}{q} - \frac{\epsilon\alpha}{q^2}$$

and note that $p = p_n, q = q_n$ as well as $q_{n-1}p_n - p_{n-1}q_n = \epsilon$. This gives immediately the value for $\omega$.

It follows that

$$\frac{\epsilon}{\alpha q_n^2} = \frac{p_n}{q_n} - x = \frac{p_n q_{n-1} - p_{n-1}q_n}{q_n(\omega q_n + q_{n-1})} = \frac{(-1)^{n-1}}{q_n(\omega q_n + q_{n-1})}.$$

Hence $\frac{q_n}{\omega q_n + q_{n-1}} = \alpha$ and therefore, $\omega > 1$ since $0 < \alpha < \frac{1}{2}$. We conclude by Lemma 5 that $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_n}{q_n}$ are consecutive convergents to x. But $\frac{p_n}{q_n} = \frac{p}{q}$ which completes the proof.

□

Finally, we discuss a generalization of Legendre's Theorem known as Worley's Theorem in Diophantine approximation. Theorems like Worley's theorem are one of the main reasons for studying continued fractions since they tell us that good approxmations of irrational numbers by rational numbers are either convergents or mediants. The proof we present here is due to A. Dujella but we also give a reference to the original paper by Worley at the end of the proof.

**Theorem 18.** *Let $\alpha$ be a real number and let $a$ and $b$ be coprime nonzero integers, satisfying the inequality $|\alpha - \frac{a}{b}| < \frac{k}{b^2}$ where $k$ is a positibe real number, then $(a,b) = (rp_{m+1} + sp_m, rq_{m+1} + sq_m)$ or $(a,b) = (rp_{m+1} - sp_m, rq_{m+1} - sq_m)$ for some $m \geq 1$ and nonnegative integers $r$ and $s$ such that $rs < 2k$ We call $\frac{a}{b}$ a mediant of $\alpha$ with parameter $k$.*

*Proof.* The ideas in this proof are due to A. Dujella (see [2]). We assume that $\alpha < \frac{a}{b}$, since the other case is similar. If $\frac{a}{b} > \frac{p_1}{q_1}$ then we take $m = -1$ given that $p_{-1} = 1$ and $q_{-1} = 0$ otherwise, let m be the largest odd integer satisfying the inequality

$$\alpha < \frac{a}{b} \leq \frac{p_m}{q_m}.$$

Since

$$|p_{m+1}q_m - p_m q_{m+1}| = 1,$$

the numbers r and s defined by

$$a = rp_{m+1} + sp_m$$

$$b = rq_{m+1} + sq_m$$

are indeed integers ($[a,b]^T$is related to $[r,s]^T$ by an invertible matrix transformation). And also

$$\frac{p_{m+1}}{q_{m+1}} < \frac{a}{b} \leq \frac{p_m}{q_m}$$

by Theorem 14 and hence we have that $r \geq 0$ and $s > 0$.

Now using the maximality of m and the fact that

$$\left|\frac{a}{b} - \frac{p_{m+2}}{q_{m+2}}\right| = \frac{(a_{m+2}q_{m+1} + q_m)(rp_{m+1} + sp_m) - (a_{m+2}p_{m+1} + p_m)(rq_{m+1} + sq_m)}{bq_{m+2}}$$

we get,

$$\left|\frac{sa_{m+2} - r}{bq_{m+2}}\right| = \left|\frac{p_{m+2}}{q_{m+2}} - \frac{a}{b}\right| < \left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2},$$

where the notation $a_{m+2}$ denotes the the $m+2$ partial quotient in the simple continued fraction of $\alpha$.

Furthermore,

$$b(sa_{m+2} - r) < kq_{m+2} = \frac{k}{s}((sa_{m+2} - r)q_{m+1} + b).$$

And this implies that

$$(sa_{m+2} - r)(b - \frac{k}{s}q_{m+1}) < \frac{k}{s}b.$$

We also have that

$$\frac{1}{sa_{m+2} - r} > \frac{b - \frac{k}{s}q_{m+1}}{\frac{k}{s}b} = \frac{s}{k} - \frac{1}{r + \frac{sq_m}{q_{m+1}}} \geq \frac{s}{k} - \frac{1}{r}.$$

From this we obtain the inequality

$$r^2 - sra_{m+2} + ka_{m+2} > 0$$

which is quadratic in r.

In order to derive the condition $rs < 2k$ in the theorem, we examinine different cases. Assume first that $s^2a_{m+2} \geq 4k$ then, $s^4a_{m+2}^2 - 4ks^2a_{m+2} \geq (s^2a_{m+2} - 4c)^2$ and thus,

$$r < \frac{1}{2s}(s^2a_{m+2} - \sqrt{s^4a_{m+2}^2 - 4ks^2a_{m+2}} \leq \frac{2k}{s}$$

or

$$r > \frac{1}{2s}(s^2a_{m+2} - \sqrt{s^4a_{m+2}^2 - 4ks^2a_{m+2}} \geq \frac{1}{s}(s^2a_{m+2} - 2k).$$

The first case gives the condition that $rs < 2k$. In the second case,

$$rs > s^2a_{m+2} - 2k \tag{3.5}$$

then we define $t = sa_{m+2} - r$. We have that t is a positive integer since $\frac{p_{m+2}}{q_{m+2}} < \frac{a}{b}$ then

$$a = rp_{m+1} + sp_m = sp_{m+2} - tp_{m+1}$$

$$b = rq_{m+1} + sq_m = sq_{m+2} - tq_{m+1}$$

and hence $rt < 2k$ by (3.5). This corresponds to the negative sign in the statement of the theorem.

Finally, we consider the case where $s^2 a_{m+2} < 4c$ . Since $r < sa_{m+2}$ we have two possibilities. If $r < \frac{1}{2} sa_{m+2}$ then $rs < \frac{1}{2} s^2 a_{m+2} < 2k$ and if $r \geq \frac{1}{2} sa_{m+2}$ then $t = sa_{m+2} - r \leq \frac{1}{2} sa_{m+2}$ and thus $st \leq \frac{1}{2} s^2 a_{m+2} < 2k$

The original proof can be read in R.T. Worley's paper [25].

□

We remark that the mediants in Worley's Theorem have applications is to the Hypergeometric Method. The initial approximations used to generate the good sequences of rational approximants are usually mediants or convergents to the irrationality being approximated because all the "best rational approximations" (in the sense that any other rational approximation that is closer to $x$ must have a larger denominator) are mediants or convergents. We will conclude this section with an example of Worley's theorem for the case $k = 3$. Hence, we consider the inequality

$$\left| \alpha - \frac{a}{b} \right| < \frac{3}{b^2}.$$

Using Theorem 18 we have that

$$(a, b) = (rp_{m+1} + sp_m, rq_{m+1} + sq_m)$$

or

$$(sp_{m+2} - tp_{m+1}, sq_{m+2} - tq_{m+1}),$$

where $rs < 6$, $st < 6$, $\gcd(r, s) = 1$ and $\gcd(s, t) = 1$ (given the fraction $\frac{a}{b}$ is taken in reduced form). However, the quadratic inequalities given in the proof of Worley's Theorem show that the pairs $(r, s) = (1, 4), (1, 5)$ and $(s, t) = (4, 1), (5, 1)$ can be omitted. Therefore, following the notation given in the proof of Theorem 18 we have that either

$$(r, s) \in \{(0, 1), (1, 1), (1, 2), (1, 3), (2, 1), (3, 1), (4, 1), (5, 1)\}$$

or

$$(s, t) \in \{(1, 1), (2, 1), (3, 1), (1, 2), (1, 3), (1, 4), (1, 5)\}.$$

.

This inequality can sometimes be used to compute particular solutions. Consider the binary Thue equation $3x^3 - 2y^3 = 321$. We compute the first 5 convergents to $\left(\frac{3}{2}\right)^{1/3}$: $1/1, 7/6, 8/7, 87/76, 617/539$. We quickly check that none of these convergents are solutions to our equation. However, if we use Worley's Theorem and the first 5 convergents to compute all the mediants to $(3/2)^{1/3}$ with parameter $k = 3$ we find that $5/3$ is a mediant corresponding to $(r, s) = (9, 2)$ and convergents $7/6$ and $1/1$ and $(5, 3)$ is a solution to our equation. In the next section, we see that $k = 3$ is a good choice of parameter since either by Theorem 19, all postive integer pairs $(x, y)$ that satisfy this equation will correspond to a mediant with parameter $k = 3$ or will have $x \leq 53$. By enumerating all such values of x, we quickly check that every solution is a mediant of $\left(\frac{3}{2}\right)^{1/3}$ with parameter $k = 3$.

# Chapter 4

# Applications of the Hypergeometric Method to Some Thue Equations

In this chapter we demonstrate how irrationality measures computed using the Hypergeometric Method can be applied to solve some Thue equations, in particular the binary Thue equation. In the first section we apply theorems about simple continued fractions to the binary Thue equation. We then explicitly show how we can use irrationality measures to bound the size of the solutions to the binary Thue equation. Our analysis leads us naturally to an algorithm that can compute all solutions in positive integers (dependent on the existence of an irrationality measure). We use this algorithm to compute an upperbound on the number of solutions to the binary Thue equation. We conclude the chapter by explicitly computing upperbounds as well as all solutions in positive integers for some particular binary Thue equations.

## 4.1 Simple Continued Fractions and the Binary Thue Equation

In this section we consider when a solution $(x, y)$ to the Diophantine equation $ax^n - by^n = N$ correspond to a convergent in the simple continued fraction of $\left(\frac{a}{b}\right)^{\frac{1}{n}}$. In order to be consistent with the papers on the binary Thue equation that were discussed in Chapter 1, where the equation $|ax^n - by^n| = N$ is considered over the positive integers, we restrict x and y to positive intergers in this chapter. We have also chosen to drop the absolute value so that this equation agrees with the definition of a Thue equation, but we remark that to find all solutions to $|ax^n - by^n| = N$, we can solve both of the equations $ax^n - by^n = N$ and $bx^n - ay^n = N$ over the positive integers.

**Theorem 19.** *If $(x, y) \in \mathbb{N}^2$ satisfies $ax^n - by^n = N$ where $n \geq 3$ and $x > (\frac{2N}{b})^{\frac{1}{n-2}}$ then $\frac{y}{x}$ is an even convergent of $(\frac{a}{b})^{1/n}$. More generally, if $x > (\frac{N}{kb})^{\frac{1}{n-2}}$ then $\frac{y}{x}$ is a mediant of $(\frac{a}{b})^{1/n}$ with parameter $k$.*

*Proof.* Suppose that the above equation has a solution so that $ax^n - by^n = N$ for some positive integers $x, y$ where $a, b, N \in \mathbb{N}$ and $n \geq 3$. It follows that

$$\frac{a}{b} - \Big(\frac{y}{x}\Big)^n = \frac{N}{bx^n}.$$

But we also have the following identity,

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + ... + y^{n-2}x + y^{n-1}).$$

Hence

$$|x - y| \leq |x^n - y^n|,$$

and it follows that

$$\frac{N}{bx^n} = \Big|\frac{a}{b} - \Big(\frac{y}{x}\Big)^n\Big| \geq \Big|\Big(\frac{a}{b}\Big)^{1/n} - \frac{y}{x}\Big|.$$

Thus, if we require

$$\frac{N}{bx^n} < \frac{1}{2x^2}$$

then we have the inequality

$$\Big|\Big(\frac{a}{b}\Big)^{1/n} - \frac{y}{x}\Big| < \frac{1}{2x^2}$$

and in this case $\frac{y}{x}$ is a convergent to $(\frac{a}{b})^{1/n}$. Futhermore, by rearranging the inequality

$$\frac{N}{bx^n} < \frac{1}{2x^2}$$

we conclude that a sufficient condition for $y/x$ to be a convergent to $(\frac{a}{b})^{1/n}$ is

$$2N < bx^{n-2}$$

or equivalently,

$$\left(\frac{2N}{b}\right)^{\frac{1}{n-2}} < x.$$

Similarly, if we fix a positive real number $k$, it follows that if $x > (\frac{N}{kb})^{\frac{1}{n-2}}$ and $(x, y)$ is a solution to the equation then $\frac{y}{x}$ is a mediant with parameter $k$.

Finally, if $\frac{y}{x}$ is a convergent to $(\frac{a}{b})^{1/n}$ then since

$$ax^n - by^n = N \geq 0$$

we have

$$\left(\frac{a}{b}\right)^{\frac{1}{n}} \geq \frac{y}{x}.$$

Hence if $\frac{y}{x}$ is a convergent, it is an even convergent. A similar argument yields an analogous statement for y. In particular, if $(x, y) \in \mathbb{N}^2$ satisfies $ax^n - by^n = N$ where $n \geq 3$ and $y > (\frac{2N}{a})^{\frac{1}{n-2}}$ then $\frac{x}{y}$ is an odd convergent of $(\frac{b}{a})^{1/n}$. More generally, if $y > (\frac{N}{ka})^{\frac{1}{n-2}}$ then $\frac{x}{y}$ is a mediant of $(\frac{b}{a})^{1/n}$ with parameter $k$.

□

We remark that these computations depend only on finding the convergents of the simple continued fraction of $(\frac{a}{b})^{1/n}$. If $(x, y)$ is any other solution (where $\frac{y}{x}$ is not a mediant with parameter $k$) then we have an upperbound on $x$, namely $x \leq (\frac{N}{kb})^{\frac{1}{n-2}}$. As we will see in a later section, this is a very good upperbound on $x$. We note that the larger the $k$ that is chosen, the smaller this upperbound is. However, this is not always advantageous.

Finally, we note that solutions do not always correspond to convergents. Consider the equation $3x^3 - 2y^3 = 321$ where $(5, 3)$ is a solution but $5/3$ is not a convergent to $(\frac{3}{2})^{1/3}$. In this situation, $\frac{y}{x}$ is "close" to $(\frac{a}{b})^{1/n}$ but not "close" enough to be a convergent. This happens because of the inequality

$$\frac{N}{bx^n} \geq \left|\left(\frac{a}{b}\right)^{1/n} - \frac{y}{x}\right|.$$

Here $\frac{N}{bx^n}$ might be larger than the $\frac{1}{2x^2}$ required to be a convergent. However, since

$$\left|\left(\frac{a}{b}\right)^{1/n} - \frac{y}{x}\right| < \frac{N}{bx^n}$$

it follows that

$$\left|\left(\frac{a}{b}\right)^{1/n} - \frac{y}{x}\right| < \frac{k}{x^2},$$

where

$$k = \frac{N}{bx^{n-2}}.$$

In this case the $\frac{y}{x}$ are not convergents but are mediants given by Worley's theorem in Diophantine approximation (see Theorem 18).

We remark that Worley's theorem depends on the size of $k$ (a smaller value of k means fewer computations). In fact, if $1 \leq k \leq 12$ then tables of corresponding $(r, s)$ given in Theorem 18 are known explicitly. As an example, consider the equation

$$7x^5 - 3y^5 = 96.$$

Since $x = 1$ does not correspond to a solution to this equation and $\frac{96}{3*2^3} = 3$ we can choose $k = 4$ and compute convergents of $\sqrt[5]{\frac{7}{3}}$. Using values of $(r, s)$ corresponding to $k = 4$ to compute mediants we will eventually find a solution (if it exists). However, since there are infinitely many convergents, we will not know for certain if all of the solutions have been found. One way to solve this problem is to find an apriori upperbound on $x$. Once we have established such an upper bound on $x$, then we would know when to stop checking convergents and mediants. The Hypergeometric Method which can be applied to compute irrationality measures for specific values of $a$ and $b$, which enables us to derive an upper bound and fully solve these equations.

In particular the Hypergeometric Method may be used to derive an irrationality measure on $\left(\frac{b}{a}\right)^{\frac{1}{n}}$. If one can be found at all and it is an improvement on Liouville's approximation

theorem, then we can construct a bound that will be of the form $O\left(n^{\frac{1}{n-\omega}}\right)$ where $2 \leq \omega < n$. We will prove this in the next section.

We conclude this section by considering the equation $x^3 - 2y^3 = 2$. Applying Theorem 19 with $n = 3, a = 1, b = 2, N = 2$ we have that $x \leq (\frac{2N}{b})^{\frac{1}{n-2}} = \left(\frac{2*2}{2}\right) = 2$ or $\frac{y}{x}$ is a convergent of $(\frac{a}{b})^{1/n} = \left(\frac{1}{2}\right)^{1/3}$. We observe that $x = 0, 1, 2$ do not correspond to solutions. Therefore if a solution $(x, y) \in \mathbb{N}^2$ exists, then $\frac{y}{x}$ must be an even convergent of $\left(\frac{1}{2}\right)^{1/3}$. The first 7 even convergents are 3/4, 15/19, 23/29, 27/34, 127/160, 227/286, 504/635, none of which correspond to solutions to our equation. We will use this fact later.

## 4.2 Bounding Variables in the Binary Thue Equation

We now attempt to show explicitly that if we have an upperbound on the irrationality measure of a certain irrational number that is associated with our Thue equation then we get tight upperbounds on the size of the solutions. This observation is summarized in the following theorem.

**Theorem 20.** *If $(x, y) \in \mathbb{N}^2$ satisfies $ax^n - by^n = N$ and there exists a lower bound on the irrationality of $(\frac{b}{a})^{1/n}$, that is there exists a positive constant $C$ such that*

$$\left| \left(\frac{b}{a}\right)^{\frac{1}{n}} - \frac{p}{q} \right| > Cq^{-\omega}$$

*for all integers p,q with $q > 0$ with $\omega < n$ then $x < C_1 N^{\frac{1}{n-\omega}}$ and $y < C_2 N^{\frac{1}{n-\omega}}$. Furthermore, $C_1, C_2$ are effectively computable if $C$ is.*

*Proof.* If $ax^n - by^n = N$ divide both sides by a so

$$x^n - \frac{b}{a}y^n = \frac{N}{a} = m.$$

Letting

$$\alpha = \left(\frac{b}{a}\right)^{\frac{1}{n}},$$

then

$$x^n - \alpha^n y^n = m.$$

The left-hand side has factorization

$$|y| \left| \alpha - \frac{x}{y} \right| \left| x^{n-1} - \alpha y x^{n-2} + \alpha^2 y^2 x^{n-3} + ... + \alpha^{n-1} y^{n-1} \right|.$$

This leads us to consider the binary form of degree $n-1$,

$$F(X,Y) = X^{n-1} + YX^{n-2} + ... + Y^{n-2}X + Y^{n-1}.$$

An elementary analysis yields

$$|F(X,Y)| = |Y^{n-1} F(\frac{X}{Y}, 1)| \geq |Y|^{n-1} \tag{4.1}$$

for $\frac{X}{Y} > 0$.

Now assume we have a lower bound on the irrationality of $\alpha$, say

$$\left| \alpha - \frac{x}{y} \right| \geq \frac{C_0}{|y|^\omega}.$$

Rewriting the factorization of the left-hand side in terms of our binary form, applying (4.1) and the above lower bound we conclude that

$$m = |y| \left| \left( \alpha - \frac{x}{y} \right) \right| |F(x, \alpha y)| \geq C_0 \alpha^{n-1} |y|^n |y|^{-\omega} = C_0 \alpha^{n-1} |y|^{n-\omega}.$$

Hence,

$$y < C_2 N^{\frac{1}{n-\omega}}$$

where

$$C_2 = \left( N a^{-1} c_0^{-1} \alpha^{n-1} \right)^{\frac{1}{n-\omega}}.$$

We get an analogous bound on $x$ as follows. Our bound on $y$ gives $y^n < C_2 N^{\frac{n}{n-\omega}}$. From $ax^n = by^n + N$ we can bound N by $N^{\frac{n}{n-\omega}}$ since $\frac{n}{n-\omega} > 1$ and hence,

$$a|x^n| \leq b|y^n| + N < C_2 b N^{\frac{n}{n-\omega}} + N^{\frac{n}{n-\omega}} = (C_2 b + 1) N^{\frac{n}{n-\omega}}.$$

Therefore, $x < \left(\frac{C_2 b+1}{a}\right)^{1/n} N^{\frac{1}{n-\omega}}$ which gives $C_1 = \left(\frac{C_2 b+1}{a}\right)^{1/n}$ in the statement of the theorem.

□

This theorem agrees with Theorem 5 but our proof makes the constants in the theorem explicit. We also get the following corollary.

**Corollary 2.** *If $x$ and $y$ positive integers that satisfy the equation $|aX^n - bY^n| = N$ and we have an inequality of the form*

$$\left|\left(\frac{a}{b}\right)^{1/n} - \frac{y}{x}\right| > \frac{C_0}{x^\omega}$$

*where $C_0$ is some effectively computable constant, then*

$$x < CN^{\frac{1}{n-\omega}}$$

*where $C$ is effectively computable.*

We remark that the requirement that $(\frac{a}{b})^{\frac{1}{n}}$ be irrational can be replaced by requiring $ax^n - by^n$ be irreducible over $\mathbb{Q}[x, y]$ which is a usual restriction on Thue equations. We can see this as follows.

Suppose that $P(x, y)$ is a binary form of degree $d \geq 3$ over $\mathbb{Q}$. If $P(x, 1)$ is reducible then there exist polynomials $Q, R \in \mathbb{Q}[x]$ such that $P(x, 1) = Q(x)R(x)$. It follows that

$$P(x, y) = Y^d P(\frac{x}{y}, 1) = Y^d Q(\frac{x}{y})R(\frac{x}{y})$$

in $\mathbb{Q}(x, y)$. But $d = deg(P) = deg(R) + deg(Q)$ and so there exists $n, m \in \mathbb{N}$ such that $n + m = d$ and $Y^n Q(\frac{x}{y}) \in \mathbb{Q}[x, y]$ and $Y^m R(\frac{x}{y}) \in \mathbb{Q}[x, y]$. We conclude that $P(x, y)$ is reducible and we have shown that if $P(x, y)$ is irreducible over $\mathbb{Q}$ then $P(x, 1)$ is irreducible. In particular, if $P(x, y) = ax^n - by^n$ then $P(x, 1)$ can not have a root in $\mathbb{Q}$ so $(\frac{b}{a})^{\frac{1}{n}}$ is irrational.

Furthermore, if we can compute an irrationality exponent $\omega$ for the irrational number $(\frac{b}{a})^{\frac{1}{n}}$, it is only useful if it is an improvement of Liouville's approximation theorem, that is $2 \leq \omega < n$. Such bounds are very good and sometimes are sufficient to force at most 1

solution to the Thue equation. Since the constants in the above theorems are now explicit we can make this formal.

**Corollary 3.** *For fixed positive integers $a$ and $b$ and $n$ with $n \geq 3$ the equation $ax^n - by^n = 1$ has at most one solution in positive integers $x, y$ if there exists an effective inequality*

$$\left| \left(\frac{b}{a}\right)^{\frac{1}{n}} - \frac{x}{y} \right| > c_0 \frac{1}{y^\omega}$$

*for all positive $x$ and $y$ with*

$$c_0 > 2^{n-\omega} \alpha^{1-n} a.$$

*Proof.* From Theorem 20 we have that

$$y < \left(a^{-1} c_0^{-1} \alpha^{n-1}\right)^{\frac{1}{n-\omega}}.$$

Now, for each positive integer $y_0$ there is at most one positive integer $x_0$ such that $ax_0^n - y_0^n = 1$, so clearly the number of solutions $(x, y)$ to the equation $ax^n - by^n = 1$ in positive integers $x$,$y$ is bounded above by the number of positive integer values of $y$. Hence by our bound on $y$ it suffices to require

$$\left(a^{-1} c_0^{-1} \alpha^{n-1}\right)^{\frac{1}{n-\omega}} < 2$$

from which the corollary follows. □

Of course as we have already mentioned, Michael Bennett and Benjamin M.M. De Weger[8] proved that there is indeed at most 1 solution to this equation with only a few exceptions. We conclude this section by applying Theorem 20 to our example equation $x^3 - 2y^3 = 2$. We have already computed an irrationality measure for $2^{1/3}$ where $\omega = 2.47$ and $c = 0.25$. We know that $y < CN^{\frac{1}{n-\omega}} = C * 2^{\frac{1}{3-2.47}}$ where $C$ is equal to $\left(Na^{-1} c_0^{-1} \alpha^{n-1}\right)^{\frac{1}{n-\omega}} = (2 * 0.25^{-1} * \left(\frac{2}{1}\right)^2)^{\frac{1}{3-2.47}} < 692$. It follows that $y \leq 2558$. However, from our previous example, we know that $\frac{y}{x}$ must be an even convergent to $\left(\frac{1}{2}\right)^{1/3}$ and the even convergents with $y \leq 2258$ are 3/4, 15/19, 23/29, 27/34, 127/160, 227/286, 504/635, none of which correspond to a solution. Therefore, the equation $x^3 - 2y^3 = 2$ has no solutions in positive integers. In

the next section we will consider the related problem of bounding the number of solutions to the general equation $ax^n - by^n = N$.

## 4.3 Procedure for Computing Solutions to the Binary Thue Equation

We describe an algorithm that computes all solutions to the Binary Thue equation $ax^n - by^n = N$ in positive integers, conditional on there being an effective irrationality measure $2 \leq \omega < n$ for $\left(\frac{a}{b}\right)^{1/n}$. We will show that this algorithm is an improvement on the "naive" algorithm we get from the bounds on x and y (checking all possible pairs of solutions). The improvement comes from some of our previous observations about this equation. This algorithm requires a bound (dependent on the irrationality exponent) on $x$ and $y$ and has worst case time complexity $O\left(e^{\frac{1}{n-2}\log N}\log N^2\right)$. This is better than brute force which has worst case time complexity $O\left(e^{\frac{2}{n-\omega}}\log N^2\right)$. Here brute force means generating all pairs of positive integers $(x, y)$ that satisfy these bounds and checking if each pair is a solution to the equation. In fact assuming Roth's theorem we would expect the worst case time complexity of brute force on pairs of solutions is $O\left(e^{\frac{2}{n-2-\epsilon}}\log N^2\right)$ for any $\epsilon > 0$, so our algorithm has better complexity than this as well. Our analysis of this algorithm will also lead us to a theorem about the number of solutions to the above equation.

Suppose that we have an effective irrationality measure $\omega < n$ for $(\frac{b}{a})^{1/n}$ for fixed parameters $a, b$ and $n$ positive integers, $n \geq 3$ which gives a positive constant $C$ such that if $(x_0, y_0) \in \mathbb{N}^2$ satisfies the equation $ax^n - by^n = N$ then $x_0, y_0 < CN^{\frac{1}{n-\omega}}$ then we have the following algorithm for computing all solutions in positive integers to the equation $ax^n - by^n = N$.

1. Compute the convergents $\frac{P_k}{Q_k}$ of $(\frac{a}{b})^{1/n}$ and $(\frac{b}{a})^{1/n}$, checking to make sure that the denominator does not exceed the bound $CN^{\frac{1}{n-\omega}}$. Output a list of convergents as pairs of integers.

2. For each pair of convergents in the above list, compute $m = a\,(P_k)^n + b\,(Q_k)^n$ (if its a convergent of $(\frac{b}{a})^{1/n}$) or $m = a\,(Q_{2k})^n + b\,(P_{2k})^n$ (if it a convergent of $(\frac{a}{b})^{1/n}$) and check if $\frac{N}{m} = d^n$ for some positive integer d. This can be done via Newton's Method to some fixed precision.

3. For each $1 \leq x_0 < (\frac{2N}{b})^{\frac{1}{n-2}}$ compute $y_0 = \left(\frac{ax_0^n - N}{b}\right)^{1/n}$ and check if $ax_0^n - by_0^n = N$.

We now give a proof of correctness for the above algorithm.

**Theorem 21.** *The above algorithm is correct. Furthermore, Steps 1 and 2 of this algorithm terminate in time polynomial in* $\log N$ *and step 3 terminates in exponential time in* $\log N$. *The worst case time complexity is* $O\left(e^{\frac{1}{n-2}\log N}\log N^2\right)$ *and computes all solutions in positive integers.*

*Proof.* We will assume that $a$,$b$ and $n$ are fixed positive integers with $n \geq 3$ and an effective irrationality measure $2 \leq \omega < n$ for $\left(\frac{b}{a}\right)^{1/n}$ has been computed. If $(x_0, y_0)$ satisfies our equation then by Theorem 20 there exists $C > 0$ such that $x_0, y_0 < CN^{\frac{1}{n-\omega}}$. In step 1 we compute the convergents of $(\frac{a}{b})^{1/n}$ and $(\frac{b}{a})^{1/n}$. Consider the convergents of $(\frac{a}{b})^{1/n}$. We need to figure out how many of these convergents we need to compute. If a convergent $\frac{P_k}{Q_k}$ corresponds to a solution to our equation then $Q_k < CN^{\frac{1}{n-\omega}}$ and hence by Theorem 15 it suffices to consider the inequality $2^{(k-1)/2} > CN^{\frac{1}{n-\omega}}$ for $k \geq 2$. Taking logarithms of both sides we find that if $k > 2(n-\omega)\log N + 1 + 2\log C$ and $k \geq 2$ then $Q_k$ exceeds the bound $CN^{\frac{1}{n-\omega}}$. It follows that $k \leq \min\{2(n-\omega)\log N + 1 + 2\log C\}$. We note that the convergents of $(\frac{b}{a})^{1/n} = \frac{1}{(\frac{a}{b})^{1/n}}$ are simply the reciprocals of the convergents of $(\frac{a}{b})^{1/n}$ since if $\alpha = [a_1, a_2, a_3, \ldots]$ then $\frac{1}{\alpha} = [0, a_1, a_2, a_3, \ldots]$. Thus we have to compute at most $\lceil 2(n-\omega)\log N + 1 + 2\log C\rceil$ convergents of $(\frac{a}{b})^{1/n}$ in Step 1.

There is a fast algorithm due to Egecioglu that is used to compute the $l$th convergent of a continued fraction in time $O(l)$ [11]. Here $l$ is $\lceil 2(n-\omega)\log N + 1 + 2\log C\rceil$. Hence,

Step 1 has worst case time comlexity $O(\log N)$. We also note that Step 1 gives at most $2 * \min\{2(n-\omega)\log N + 1 + 2\log C\}$ convergents to check as possible solutions to our equation (corresponding to the convergents of $(\frac{a}{b})^{1/n}$ and $(\frac{b}{a})^{1/n}$).

Step 1 terminates because the denominators of convergents form an increasing sequence. Steps 1 and 2 then give all solutions $(x_0, y_0) \in \mathbb{N}^2$ to $ax^n - by^n = N$ where $x_0 > (\frac{2N}{b})^{\frac{1}{n-2}}$ or $y_0 > (\frac{2N}{a})^{\frac{1}{n-2}}$ by Theorem 19 and the fact that if $(x_0, y_0)$ satisfies our equation then $(x_0, y_0) = d(P_{2k}, Q_{2k})$ for some positive integer d because $\gcd(P_{2k}, Q2k) = 1$ and $\frac{P_{2k}}{Q_{2k}} = \frac{y_0}{x_0}$. Hence, $d^n(aP_{2k}^n - bQ_{2k}^n) = N$ and therefore $\frac{N}{m} = d^n$ where $m = a\,(P_{2k})^n + b\,(Q_{2k})^n$. We note that $d$ can be extracted via Newton's method (by taking the $n$th root of $\frac{N}{m}$) which converges quadratically and will not affect the resulting complexity at the end of our analysis. Since we are computing d to some fixed finite precision we should check that $\frac{N}{m} = d^n$ for the integer $d$ that was computed.

Computing m for each convergent in Step 2 requires computing 2 $n$th powers, namely, $(P_{2k})^n$ and $(Q_{2k})^n$ where the numbers $P_{2k}$ and $Q_{2k}$ are less than or equal to our bound $CN^{\frac{1}{n-\omega}}$ and hence at most size $O(\log N)$. We conclude that computing m for each convergent has worst case time complexity $O(\log N^2)$ using schoolbook multiplication. Furthermore, we know that there are at most $2 * \min\{2(n-\omega)\log N + 1 + 2\log C\}$ convergents to check as possible solutions in Step 1. We conclude that Step 2 has worst case time complexity polynomial in $\log N$.

Step 4 of the algorithm is correct since by Theorem 19 the remaining solutions $(x_0, y_0)$ satisfy $x_0 < (\frac{2N}{b})^{\frac{1}{n-2}}$ and $y_0 < (\frac{2N}{a})^{\frac{1}{n-2}}$ and for each positive integer $x_0$ there is at most one positive integer $y_0$ such that $ax_0^n - by_0^n = N$. In order to see this supppse there exists positive integers $x_1, y_1, y_2$ such that $(x_1, y_1)$ and $(x_1, y_2)$ satisfy the equation then $ax_1^n - by_1^n = ax_1^n - by_2^n$. Hence $by_2^n - by_1^n = b(y_2^n - y_1^n) = 0$. But then $y_2^n - y_1^n = (y_2 - y_1)\sum_{i=1}^n y_2^{n-i}y_1^i = 0$ and so $y_2 = y_1$.

Now for each $1 \leq x_0 < (\frac{2N}{b})^{\frac{1}{n-2}}$, we compute $y_0 = \left(\frac{ax_0^n - N}{b}\right)^{1/n}$ to some fixed precision

using Newton's Method. We need to compute $x_0^n$ to compute $y_0$. Using $x_0 < (\frac{2N}{b})^{\frac{1}{n-2}}$, the cost of computing each $y_0$ is $O(\log n \log N^2)$. Since we are computing an $n$th root to some fixed precision, we should check that our solutions satisfy the equation once they are computed. For this we need to compute $x_0^n$ and $y_0^n$ where $x_0 < (\frac{2N}{b})^{\frac{1}{n-2}}$ and $y_0 < (\frac{2N}{a})^{\frac{1}{n-2}}$. Thus for each $1 \leq x_0 < (\frac{2N}{b})^{\frac{1}{n-2}}$ we perform a computation that is $O(\log n \log N^2)$ and hence Step 4 and the entire algorithm has worst case time complexity $O\left(e^{\frac{1}{n-2}\log N} \log n \log N^2\right)$.. Since n was fixed this is $O\left(e^{\frac{1}{n-2}\log N} \log N^2\right)$.

□

We will now apply this analysis in the next section to bound the number of positive integer solutions for our equation.

## 4.4 Bounding the Number of Solutions

We use this algorithm to compute effective upperbounds on the number of solutions to the general equation $ax^n - by^n = N$ for fixed $a, b, n$ in terms of N, given an effective irrationality measure $2 \leq \omega < n$ for $\left(\frac{b}{a}\right)^{1/n}$. We first state and prove this upperbound explicitly for the number of solutions to the general equation; we will then consider some examples using effective irrationality measures that we computed explicitly using the Hypergeometric Method.

**Theorem 22.** *Denote the number of pairs $(x, y) \in \mathbb{N}^2$ satisfying $ax^n - by^n = N$ for certain fixed parameters $a, b, n \in \mathbb{N}, n \geq 3$ by $S(N)$ and suppose we have computed an effective irrationality measure $|(\frac{b}{a})^{1/n} - \frac{p}{q}| > \frac{c}{q^\omega}$ . Then $S(N) \leq \max\{2(n-\omega)\log N + 1 + 2\log C, 2\} + (\frac{2N}{b})^{\frac{1}{n-2}}$ for some constant $C$.*

*Proof.* Note that if $(x, y)$ is a solution then either $x > \left(\frac{2N}{b}\right)^{\frac{1}{n-2}}$ or $x \leq \left(\frac{2N}{b}\right)^{\frac{1}{n-2}}$. In the first case, we know that $\frac{y}{x}$ is a convergent in the simple continued fraction of $\left(\frac{a}{b}\right)^{1/n}$ by Theorem 19. Our irrationality measure gives a bound of the form $x < CN^{\frac{1}{n-\omega}}$ for some constant

$C > 0$. Hence from Theorem 21 there are at most $\max\{2(n-\omega)\log N + 1 + 2\log C, 2\}$ convergents with denominator less than this bound and therefore at most this many values of $x$. In the second case there are at most $\left(\frac{2N}{b}\right)^{\frac{1}{n-2}}$ values of $x$. Therefore, since for each positive integer $x$, there can be at most one positive integer $y$ such that the pair $(x, y)$ is a solution to the above equation, the theorem follows.

□

We remark that $n = 3$, this upperbound is $O(\log N + N)$ compared to $O\left((\frac{2N}{b})^v\right)$ where $v = \frac{1}{3-\omega} > 1$ that we would expect if we had only used the bounds on $x$ and $y$ without the algorithm. Since $\omega$ can be any positive real number less than 3, $v$ could be a very large number, so this is a significant improvement. We will now using the irrationality measure we computed in Chapter 2 for cubic irrationals to find explicit upperbounds for some particular binary Thue equations.

## 4.5 Some Explicit Examples

We illustrate the use of this theorem by computing some upperbounds on the number of positive integer solutions to our equation for varying values of $N$ given in the following two tables.

| $\alpha$ | $\lambda(\alpha)$ |
|---|---|
| $2^{1/3}$ | 2.47 |
| $3^{1/3}$ | 2.76 |
| $5^{1/3}$ | 2.80 |

Table 2. A table of restricted irrationality measures

| Equation | Upperbound |
|---|---|
| $x^3 - 2y^3 = 2$ | 4 |
| $x^3 - 3y^3 = 3$ | 4 |
| $x^3 - 5y^3 = 5$ | 4 |

Table 3. A table of equations and the corresponding upperbounds on $S(N)$

Using our previous example $x^3 - 2y^3 = 2$ and $N = 2, n = 3, \omega = 2.47, c = 0.25, a = 1, b = 2$ we have by Theorem 19 that $C = 2^{0.53}$. Plugging these values into the inequality $S(N) \leq \max\{2(n-\omega)\log N + 1 + 2\log C, 2\} + (\frac{2N}{b})^{\frac{1}{n-2}}$ from Theorem 22, we get $S(N) \leq 4$. However, we know from previous examples that this equation has no solutions.

Until this point we have been using irrationality measures to say something about Diophantine equations. In the next section we will take a different point of view and look at how Diophantine equations can be used to say something about irrationality measures.

## 4.6 Diophantine Equations to Irrationality Measures

We end the chapter by looking at a connection between Diophantine equations and Diophantine approximation. In 1909 Alan Thue proved the following theorem which shows the equivalence between certain Diophantine inequalities and refinements of Liouville's approximation theorem. We present the theorem now to illustrate this interesting connection.

**Theorem 23.** *Let $\omega > 1$ be a positive real number, and $n$ a fixed positive integer and $\alpha = \left(\frac{a}{b}\right)^{1/n}$ an irrational number for positive integers a,b then the following are equivalent.*

*(1) There exists a constant $c_1 > 0$ such that, for any $\frac{p}{q} \in \mathbb{Q}$ with $q > 0$, $|\alpha - \frac{p}{q}| > \frac{c_1}{q^\omega}$.*

*(2) There exists a constant $c_2 > 0$ such that for any $(x, y) \in \mathbb{Z}^2$, $|x^n - \alpha^n y^n| \geq c_2 |x|^{n-\omega}$.*

*Proof.* (1) $\implies$ (2) follows immediately from Theorem 20. It remains to show that (2) $\implies$ (1). Assume (2) holds and let $\frac{p}{q}$ be a rational number with $q > 0$. If $p$ is not the nearest integer to $\alpha q$ then $|\alpha q - p| > \frac{1}{2}$ and (1) follows trivially. So assume that $|\alpha q - p| \leq \frac{1}{2}$. Since

$\alpha, q > 0$ it follows that p is nonzero. Suppose that $p \geq 1$ then $\frac{1}{2}p \leq p - \frac{1}{2} \leq \alpha q \leq p + \frac{1}{2} \leq \frac{3}{2}p$ and $\frac{1}{2\alpha}p \leq q \leq \frac{3}{2\alpha}p$. Therefore, $c_3 p \leq q \leq c_4 p$ for some positive constants $c_3, c_4$ that are independent of $p$ and $q$.

Consider the factorization

$$|p^n - \alpha^n q^n| = |p - \alpha q| \left| p^{n-1} + (\alpha q)p^{n-2} + \ldots + (\alpha q)^{n-1} \right|.$$

Using the inequality $q \leq c_4 p$ in the above and applying the triangle inequality we conclude that

$$|p^n - \alpha^n q^n| \leq c_5 |p|^{n-1} |p - \alpha q|$$

for some positive constant $c_5$.

Applying (2) we get

$$c_2 |p|^{n-\omega} \leq |p^n - \alpha^n q^n| \leq c_5 |p|^{n-1} |p - \alpha q|.$$

It follows that

$$|p|^{-\omega} \leq c_5 |p|^{-1} |p - \alpha q|.$$

Finally we use the inequality $c_3 p \leq q$ in the above to get

$$|p|^{-\omega} \leq c_6 \left| \alpha - \frac{p}{q} \right|$$

for some positive constant $c_6$ and we conclude (1). In the case that $p = 0$, (1) follows since $\alpha > 0$ and we can choose $c_1$ to be any positive number less than $\alpha$.

□

In the next chapter we consider a different perspective, turning our attention away from Thue equations by studying how irrationality measures can be applied to solve some exponential Diophantine equations. We will also discuss how irrationality measures are related to simple continued fractions.

# Chapter 5

# Further Applications

In this chapter we look at two different applications of irrationality measures. The first is to badly approximable numbers which relate simple continued fractions to irrationality measures. Since simple continued fractions were used extensively throughout this thesis and the previous chapter, this relationship is of relavence to this thesis. The second is the application of restricted irrationality measures to polynomial-exponential Diophantine equations, in particular the Ramanujan-Nagell equation. This is of interest thesis because it will demonstrate how the Hypergeometric Method can be applied to solve Diophantine equations other than Thue equations.

## 5.1 Badly Approximable Numbers

It is currently not known whether any algebraic irrationality $\alpha$ has bounded partial quotients in its simple continued fraction. However, it has been conjectured (for example, by Richard Guy [13]) that for all real algebraic irrationalities of degree 3 or greater, the sequence of partial quotients in their simple continued fractions is unbounded. In this section we will show how the Hypegeometric Method can provide some justification for this conjecture. We first define what it means for a number to be "badly approximable".

**Definition 10.** *A real number $\alpha$ is said to be* ***badly approximable*** *if there exists a positive constant $C > 0$ such that for any positive integers $p, q$*

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^2}$$

**Theorem 24.** *An irrational number $\alpha$ is badly approximable if, and only if, the sequence of its partial quotients in its simple continued fraction is bounded.*

*Proof.* Assume that $\alpha$ is badly approximable, that is there exists a positive constant $C$ such that for any positive integers $p, q$,

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^2}.$$

Let $n \geq 2$ be a positive integer, then from Corollary 1 of Chapter 3 $q_n \leq \frac{q_{n-1}}{C}$. From Theorem 13 $q_n \geq a_n q_{n-1}$. It follows that $a_n \leq \frac{1}{C}$ and hence the sequence of partial quotients is bounded. Conversely, if the sequence of partial quotients is bounded by a constant $M$ then for any positive integer $n$, $a_{n+1} \leq M$. Now by Legendre's Theorem $\frac{p}{q}$ is a convergent to $\alpha$, that is, there exists a positive integer $n$ such that $\frac{p}{q} = \frac{p_n}{q_n}$ and by 1 of Chapter 3,

$$\left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{a_{n+1}q_n^2} > \frac{1}{Mq_n^2}.$$

We conclude that $\alpha$ is badly approximable.

□

We know from Roth's theorem that every algebraic irrationality has an irratonality exponent arbitrarily close to 2. However, even this theorem is not sufficient to answer the conjecture.

Still, one might wonder if the Hypergeometric Method could be used to compute a counterexample to the conjecture that every algebraic irrationality of degree at least 3 has unbouned partial quotients. In the language of irrationality measures this means finding an algebraic irrationality of degree at least 3 that has an irrationality exponent equal to 2. The numerical evidence in this thesis suggests this is unlikely. In particular, for the irrationality exponents that we have computed for degree 3 algebraic irrationalities via the Hypergeometric Method, the smallest irrationality exponent was 2.2863, corresponding to the number $19^{1/3}$.

We have seen the close relationship the Hypergeometric Method has with simple continued fractions. We conclude this chapter by considering a further application of the Hypergeometric method to Diophantine equations.

## 5.2 Appplications of Restricted Irrationality Measures

We have already seen applications of the Hypergeometric Method to equations of Thue type. In order to complete the thesis we will study some applications of the Hypergeometric Method to polynomial exponential Diophantine equations. A polynomial exponential Diophantine equation is a Diophantine equation written in terms of exponential polynomials. In this section we restrict our attention to the polynomial exponential equaton $x^2 - D = p^n$ for a prime $p$ and positive squarefree integer $D \geq 2$. This is famously known as the generalized Ramanujan-Nagell type equation.

We will first explain the relationship that exists between restricted irrationality measures and this particular polynomial exponential Diophantine equation. That is, if a restricted irrationality measure for $\sqrt{D}$, involving powers of the prime p, can be computed using the Hypergeometric Method as in Chapter 1, then we will show that this immediately leads to an upper bound on the exponent n in this equation. We state this in the following theorem.

**Theorem 25.**

$$\left| \frac{x}{p^k} - \sqrt{p} \right| \geq c \frac{1}{(p^k)^\lambda}$$

*for some positive constant $c > 0$ then the exponent $n$ in the equation $x^2 - D = p^n$ (for fixed prime $p$ and square free $D$) is bounded above.*

*Proof.* Suppose that our equation has a solution in positive integers $(x, n)$. There are two cases to consider: If n is even then we can rewrite the equation as $x^2 - p^(2n') = D$ for some integer $n'$. This is a difference of squares and hence $(x + p^{n'})(x - p^{n'}) = D$ and clearly $n$ is bounded (since $n = \log_p(D)/2$).

If n is odd then we write $n = 2k + 1$ and hence $x^2 - D = p^{2k+1}$. Dividing both sides of the equation by $p^{2k}$ yields

$$\frac{x^2}{p^{2k}} - \frac{D}{p^{2k}} = p$$

and therefore,

$$\left|\frac{x^2}{p^{2k}} - p\right| = \left|\frac{D}{p^{2k}}\right|.$$

But

$$\left|\left(\frac{x}{p^k}\right)^2 - p\right| = \left|\frac{D}{p^{2k}}\right|$$

is another difference of squares and so

$$\left|\frac{x}{p^k} - \sqrt{p}\right|\left|\frac{x}{p^k} + \sqrt{p}\right| = \left|\frac{D}{p^{2k}}\right|.$$

The above equation implies that

$$\left|\frac{x}{p^k} - \sqrt{p}\right|$$

must necessarily be "small". That is,

$$\left|\frac{x}{p^k} - \sqrt{p}\right| = \frac{|\frac{D}{p^{2k}}|}{\left|\frac{x}{p^k} + \sqrt{p}\right|}.$$

Therefore,

$$\left|\frac{x}{p^k} - \sqrt{p}\right| << \frac{1}{p^k}.$$

However, for $0 < \lambda < 2$ this contradicts the inequality

$$\left|\frac{x}{p^k} - \sqrt{p}\right| >> \frac{1}{(p^k)^\lambda},$$

for sufficiently large $k$.

Explicitly,

$$\frac{D}{p^{2k}} > \frac{|\frac{D}{p^{2k}}|}{\left|\frac{x}{p^k} + \sqrt{p}\right|} > c\frac{1}{p^{k\lambda}}.$$

Rearranging this inequality gives

$$\frac{D}{c} > p^{(2-\lambda)k}.$$

Taking logarithms of both sides we conclude that

$$\frac{\log \frac{D}{c}}{2-\lambda} > k.$$

Hence in both cases, $n$ is bounded.

□

Using Theorem 12 this theorem we have $c = 2^{-43.9}$ and $\lambda = 1.8$. From the above proof, we have for $n$ odd, $n = 2k+1 \leq 2\left(\frac{\log D + 43.9}{2-1.8}\right) + 1 \leq 20 \log D + 879$. And in the case where $n$ is even an upperbound is $\frac{\log D}{2}$. Hence, we conclude that $n < 20 \log D + 879$ for the equation $x^2 + D = 2^n$.

# Chapter 6

# Conclusion

We have discussed the Hypergeometric Method from many different angles. We began with some basic ideas about irrational numbers which were required throughout this thesis. We went on to discuss the Hypergeometric Method in great detail by constructing general irrationality measures for some degree 3 algebraic irrationalities and then used these constructions to explicitly compute irrationality measures for some specific numbers, which involved a detailed analysis of the continued fractions of these numbers.

We ended our discussion of the Hypergeometric Method by mentioning its application to the construction of restricted irrationality measures. We then developed sufficient background about continued fractions to introduce Worley's Theorem in Diophantine Approximation and apply this theorem to the binary Thue equation.

This binary Thue equation was the focus of the next chapter in which we showed how the irrationality measures we had constructed previously could be applied to equations of this form. We concluded this section by showing that the binary Thue equation $x^3 - 2y^3 = 2$ has no solutions in positive integers.

The remaining chapter looked at the Hypergeometric Method through a different lens, linking irrationality measues to an open conjecture about badly approximable numbers and also tying up some loose ends by showing the application of restricted irrationality measures to polynomial-exponential Diophantine equations. This section was also important to show the versatility of the Hypergeometric Method to Diophantine equations other than Thue equations and we accomplished this by considering the generalized Ramanujan-Nagell equation. We feel that this thesis will be of value to anyone interested in learning about Diophantine Approximation and the Hypergeometric Method.

# Bibliography


[1] Angew J. Uber rationale Annaherungswerte algebraische Zahlen, pages 284-305, 1909.

[2] Dujella A. Continued fractions and RSA with small secret exponents. *Tatra Mt. Math*, Publ. 29, pages 101-112, 2004.

[3] A. Dold, Heidelberg, B. Eckmann, E, Takens. Lecture Notes in Mathematics, pages 61-64.

[4] Baker A. George Jr., Graves-Morris, Peter. Pade Approximants. *Encyclopedia Of Mathematics and its Applications*, Vol. 13, 1981.

[5] Bauer, Mark, Bennett, Michael. Applications of the Hypergeometric Method to the generalized Ramanujan-Nagell equation. *Ramanujan Journal*, Vol. 6, pages 209-270, 2002.

[6] Bennett A. Michael. Effective Measures of Irrationality for Certain Algebraic Numbers, pages 1-15.

[7] Beukers F. On the Generalized Ramanujan-Nagell Equation I. *J. Acta Arith*, Vol. 38. pages 389-400, 1980.

[8] Bennett M.A., De Weger B. M. M. On the Diophantine Equation $|ax^n - by^n| = 1$ , *J. Mathematics of Computation*, Vol. 67, No. 221, Janurary 1998.

[9] Bennett M.A. Simultaneous Rational Approximation to Binomial Functions, *Transactions of the American Mathematical Society*, Vol. 348, No. 5, May 1996.

[10] Chudnovsky, G.V. On the Method of Thue-Siegel. *The Annals of Mathematics, Second Series*, Vol. 117, No. 2, pages 325-382, March 1983.

[11] Egecioglu Omer, Coma C. K. K. J. Fast Computation of Continued Fractions. *Computers Math, Applic.*, Vol. 21, No. 2-3, pages 167-169, 1999.

[12] Evertse J.-H. Upper Bounds for the Numbers of Solutions of Diophantine Equations, PhD Thesis, Leiden, 1983.

[13] Guy, R. K. Unsolved Problems in Number Theory, 2nd ed. New York: Springer-Verlag, pages 259, 1994.

[14] Hardy G.H., E.M. Wright E. M. An Introduction to the Theory of Numbers, pages 165-184.

[15] Hurwitz, A. Ueber die angenherte Darstellung der Irrationalzahlen durch rationale Brche (On the approximation of irrational numbers by rational numbers). *Mathematische Annalen*, Vol. 39 No. 2, pages 279-284, 1891.

[16] Ljunggren W. Einige Eigenschaften der Einheitenreeller quadratischer und rein biquadratischer Zahlkorper mit Anwendung auf die Losung einer Klasse von bestimmter Gleichungen vierten Grades, *Det Norske Vidensk. Akad. Oslo Skrifter I, No. 12*, pages 1-73, 1936.

[17] Nagell T. Solution complete de quelques equations cubiques a deux indeterminees. *J. de Math.*, Vol. 9, No. 4, pages 209-270, 1925.

[18] Nesterenko Yuri. Linear Forms in Logarithms of Rational Numbers. *Lecture Notes in Mathematics*, Vol. 18, pages 53-106, 2003.

[19] Niven Ivan. Irrational Numbers. *Cambridge University Press*, 2005.

[20] Rickert J.H. Simultaneous rational approximations and related diophantine equations. *Proc. Cambridge Philos. Soc.*, Vol 113, pages 461-472, 1993.

[21] Schoenfeld L. Sharper bounds for the Chebyshev functions. *Math. Comp. 30*, pages 337-360, 1976.

[22] Siegel Carl. Approximation algebraischer Zahlen. *Mat. Zeit.*, Vol. 10, pages 284-305, 1921.

[23] Siegel Carl, Gleichung Die. $ax^n - by^n = c$, *Math. Ann.*, Vol. 144, pages 57-68, 1937.

[24] Thue A., Uber Annaherungenswerte algebraischen Zahlen. *J. Reine Angew. Math.*, Vol. 135, pages 284-305, 1909.

[25] Worley R. T. Estimating $\left|\alpha - \frac{p}{q}\right|$. *J. Austral. Math. Soc.*, Ser. A 31, pages 202-206, 1981.

## .1 Appendix

```
from decimal import *
from random import randrange

def contfrac_float(x):
    cf = []
    temp = [(Decimal(0),Decimal(1)), (Decimal(1),Decimal(0))]
    i= x
    while True:
        y = int(x)
        cf.append(y)
        n = len(cf)-1
        pn = cf[n]*temp[n+1][0] + temp[n][0]
        qn = cf[n]*temp[n+1][1] + temp[n][1]
        temp.append((pn, qn))
        x -= y
        if abs(Decimal(i) - Decimal(pn)/Decimal(qn)) == 0:
            del temp[0]; del temp[0]
            return cf, temp
        x = 1/x

def contfrac(x):
    count=0
    cf = []
```

```
    while True:
        y = int(x)
        cf.append(y)
        n = len(cf)-1
        x -= y
        count=count+1
        if count > 3419:
      return max(cf)
        x = 1/x


getcontext().prec = 10
print contfrac_float(19**(Decimal("1.0")/3))
print contfrac(19**(Decimal("1.0")/3))
```