Chapter 4

Rational Approximation

1. Introduction

Every point on the real line corresponds, as we know, to a real number, and in every interval on the line, no matter how small, there are points corresponding to rational numbers. Mathematically, this situation is described by saying that "the rational points are dense on the line." It follows that every real number α can be approximated by a rational number to any degree of accuracy whatsoever. That is, given a real point α on the line, we can find a rational point as close as we please to α.

The process of approximating a real number by rational numbers is an approach to understanding the real numbers that gives surprising insight. By placing certain constraints on the rational numbers used in the approximation, properties of a real number α can be observed that classify it as either a rational or irrational number or as an algebraic or transcendental number.

For example, a fact we observe very quickly, first by simple experiment and then by proof, is that, as rational numbers approach a fixed real number, their denominators grow arbitrarily large. A useful and interesting way to quantify this is to study how closely real numbers can be approximated by rational numbers that have a fixed bound on the growth of their denominators. This is the focus of our presentation.

We give a brief description of the sections of the chapter as well as an indication of the level of difficulty. Familiarity with the basic properties of rational and irrational numbers is assumed. Sections 2 and 3 present an

introduction to approximation theory. Several simple, appealing ideas are discussed. For example, if we try to approximate a real number α only by rational numbers $\frac{p}{q}$ satisfying $q \leq \eta$, for a fixed positive real number η, then there are many consequences. One is that there is an open interval around α in which no such $\frac{p}{q}$ exists. Section 2 is elementary and depends only on a basic understanding of the arithmetic of real and rational numbers on the line. Familiarity with inequalities involving absolute values, and decimal expansion of real numbers is assumed. Most of the material in this section is suitable for highschool students. Some introductory number theory and simple facts about bounded sets of positive integers are needed in Section 3.

In contrast to the result mentioned above on the existence of an interval around α in which no rational numbers $\frac{p}{q}$ exist with $q \leq \eta$, Dirichlet's theorem, proved in Section 5, shows that if we let the bound depend on the variable denominator, then it is possible to find a rational number $\frac{p}{q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

The proof is an application of the pigeonhole principle. It follows from Dirichlet's theorem that the rationality or irrationality of a real number can be determined by means of rational approximation.

In Sections 8 and 9, we explore how bounds for rational approximations $\frac{p}{q}$ of the form $\frac{1}{q^t}$ motivated some of the most important and difficult research in number theory in the twentieth century, namely, the Thue-Siegel-Roth theorem. Section 8 describes Liouville's theorem, the result that was the impetus for the work of Thue, Siegel and Roth. Beginning with this section, the mathematics is more advanced, but is suitable for students with strong mathematical backgrounds. Algebraic and transcendental numbers appear in Section 8. A rather surprising fact emerges along the way in Sections 7 and 8, namely, that it is, in general, the transcendental numbers that are best approximated by rational numbers, and that some more "ordinary" numbers, such as $\sqrt{2}$, earn the name "badly approximable." Although Section 7 is quite technical, no new tools are needed other than the discriminant of a quadratic equation with integer coefficients.

Section 9 gives an overview of some of the ideas involved in the work of Thue, Siegel and Roth. The level of difficulty of the proofs of their theorems, not given here, is dramatically higher than that of the proofs we have presented in this book, but it is hoped that our discussion will be a helpful introduction and motivation for further reading. The work of Thue, Siegel and Roth is applied in Section 10 to an examination of the approximation exponent.

Rational approximation is sometimes called "Diophantine approximation" in honor of the Greek mathematician Diophantus who studied integer and rational solutions to polynomial equations over $\mathbb{Z}$, often called Diophantine equations. An application of Thue's theorem to Diophantine equations is presented in Section 12. The chapter closes with a short discussion, in Section 13, of rational approximations to transcendental numbers.

In Sections 4, 6 and 11, we track the implications of approximation theory with regard to the continuity and differentiability of an interesting family of functions. The only prerequisite for reading these sections is differential and integral calculus of one variable.

2. Introduction to Approximation Theory

When we use a fraction to represent a rational number r, unless specifically stated otherwise, *we will always choose the fraction $\frac{a}{b}$ in the class of r that is reduced to lowest terms and has positive denominator.* We write $r = \frac{a}{b}$, and, if convenient, we write "the rational number $\frac{a}{b}$." We say that a is the *numerator of* r and that b is the *denominator of* r. (We can find a fraction in the class of r with denominator as large as we like. However, there is always a fraction with least positive denominator in the class, and it is the denominator of our chosen representative.) Observe that if the rational number r is an integer, then it has denominator 1.

Suppose that α is a fixed real number, $\frac{p}{q}$ is a rational number and ϵ is a positive real number. As a reminder, we note that the inequality

$$\left|\alpha - \frac{p}{q}\right| < \epsilon, \tag{31}$$

means that the distance between $\frac{p}{q}$ and α is less than ϵ. Equivalent statements are: $\frac{p}{q} - \epsilon < \alpha < \frac{p}{q} + \epsilon$ and $\alpha - \epsilon < \frac{p}{q} < \alpha + \epsilon$. The two-fold inequality

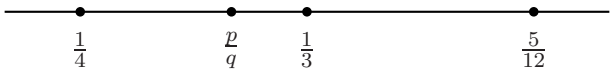
$$0 < \left|\alpha - \frac{p}{q}\right| < \epsilon, \tag{32}$$

means $\frac{p}{q} \neq \alpha$ in addition to everything implied by (31). Inequalities of this form appear with great frequency in this chapter.

We begin with an example where the fixed real number α is a rational number, say $\frac{1}{3}$. We observe the behavior of rational numbers close to $\frac{1}{3}$. To do this, we take an open interval on the real line centered at $\frac{1}{3}$, and we examine what happens as we shrink the interval squeezing in on $\frac{1}{3}$. Look first at the open interval I defined by

$$I = \left(\frac{1}{4}, \frac{5}{12}\right) = \left\{x \in \mathbb{R} \,|\, \frac{1}{4} < x < \frac{5}{12}\right\}.$$

The interval I has length $|\frac{5}{12} - \frac{1}{4}| = \frac{1}{6}$, and, as $|\frac{5}{12} - \frac{1}{3}| = |\frac{1}{4} - \frac{1}{3}| = \frac{1}{12}$, the rational number $\frac{1}{3}$ is in I and equidistant from the endpoints $\frac{1}{4}$ and $\frac{5}{12}$.



Let $\frac{p}{q}$ be a rational number in I different from $\frac{1}{3}$. We have $\frac{1}{4} < \frac{p}{q} < \frac{5}{12}$, so

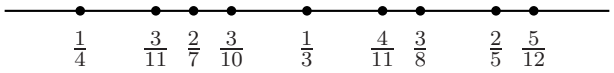
$$\frac{1}{3} - \frac{1}{12} < \frac{p}{q} < \frac{1}{3} + \frac{1}{12}.$$

Consequently,

$$0 < \left|\frac{1}{3} - \frac{p}{q}\right| < \frac{1}{12},$$

and we have the inequality (32) above with $\alpha = \frac{1}{3}$, and $\epsilon = \frac{1}{12}$.

Consider the possibilities for q. The rational numbers $\frac{1}{2}$ and $\frac{2}{3}$ are greater than $\frac{5}{12}$ and so are not in the interval I. Consequently, the denominator q must be greater than 4. A short calculation comparing fractions, shows that $\frac{2}{5}, \frac{2}{7}, \frac{3}{8}, \frac{3}{10}, \frac{3}{11}$ and $\frac{4}{11}$ are in I. A little more checking shows that q cannot be 6 or 9.



Thus, the possible denominators q that are less than 12 for $\frac{p}{q}$ are $5, 7, 8, 10$ and 11. We also observe that 11 is the smallest denominator for which there are two rational numbers with that denominator in I. Thus, even though there are infinitely many rational numbers in I, our calculations show that there are few that have denominators less than 12.
In summary: *if the rational number* $\frac{p}{q}$ *satisfies*

$$0 < \left|\frac{1}{3} - \frac{p}{q}\right| < \frac{1}{12}, \text{ then } q > 4.$$

Also, *if* $q < 12$, *there are only* 6 *rational numbers* $\frac{p}{q}$ *in* I *which are distinct from* $\frac{1}{3}$.

Next, we shrink the open interval I so that it has endpoints $\frac{24}{75}$ and $\frac{26}{75}$.

Exercise 2.1. If I is the open interval with endpoints $\frac{24}{75}$ and $\frac{26}{75}$, how large must the denominator q of a rational number $\frac{p}{q}$ be so that $\frac{p}{q}$ lies in I and is distinct from $\frac{1}{3}$? How many rational numbers $\frac{p}{q}$ with $q < 75$ are there in I? Symbolically, the first question reads: if

$$0 < \left|\frac{1}{3} - \frac{p}{q}\right| < \frac{1}{75},$$

how large is q?

This exercise illustrates one of the fundamental questions in this investigation of rational approximation. Namely, if α is a fixed real number, then what do the rational numbers $\frac{p}{q}$ close to α look like? In other words, if ϵ is a small positive real number, what does the inequality

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

imply about $\frac{p}{q}$?

Specifically, the example illustrates the case where α is a rational number $\frac{a}{b}$, and $\epsilon = \frac{1}{mb}$ has denominator a multiple of b. We looked at the case $\alpha = \frac{1}{3}$, $m = 4$ and then, in the exercise, the case $m = 25$, but m may be taken to be an arbitrarily large positive integer. What we observed for $m = 4$ and $m = 25$ may be formulated generally as follows.

Proposition 2.2. *If $\frac{a}{b}$ is a fixed rational number and $\frac{p}{q}$ is a rational number such that*

$$0 < \left|\frac{a}{b} - \frac{p}{q}\right| < \frac{1}{mb}$$

then

$$q > m.$$

Proof. From

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} < \frac{1}{mb},$$

we deduce that

$$|aq - bp|m < q.$$

Since $|aq - bp|$ is a positive integer, we have $q > m$. ■

We have established that the denominators of all rational numbers $\frac{p}{q}$, distinct from $\frac{a}{b}$, whose distance from $\frac{a}{b}$ is less than $\frac{1}{mb}$ are greater than m. Thus, as we shrink the length of the interval around $\frac{a}{b}$, the denominators of the rational numbers in the interval get arbitrarily large.

We have focused on the denominators of the rational numbers $\frac{p}{q}$ approximating a real number α (as opposed to the numerators) because, as we shall see in Section 3, any rational number close to α with small denominator has small numerator. Also, it is often possible to make use of the greatest integer function, to be defined below, to reduce problems to the situation where $0 < \alpha < 1$.

What happens to q as $\frac{p}{q}$ gets close to an *irrational* number α? The fact that the rational numbers are dense in the set of real numbers implies that we can find a rational number $\frac{a}{b}$ as close as we please to α. It follows that if $\frac{a}{b}$ is a rational number very close to α, then the rational numbers $\frac{p}{q}$ close to α are close to $\frac{a}{b}$. Thus, the denominators q get arbitrarily large.

Remark. The decimal expansion of a real number α provides rational numbers approximating α. If, for example, α is a positive real number less than 1, with decimal expansion

$$\alpha = .a_1a_2a_3...a_n...,$$

where the a_i are integers satisfying $0 \leq a_i \leq 9$, then $\alpha = \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + ... + \frac{a_n}{10^n} + ...$ It follows that

$$\left| \alpha - \left(\frac{10^{n-1}a_1 + 10^{n-2}a_2 + 10^{n-3}a_3 + ... + a_n}{10^n} \right) \right| = \frac{a_{n+1}}{10^{n+1}} + ... \leq \frac{1}{10^n},$$

for positive integers $n \geq 1$. Thus, after reducing to lowest terms, the decimal expansion provides, for each n, rational approximations

$$\left(\frac{10^{n-1}a_1 + 10^{n-2}a_2 + 10^{n-3}a_3 + ... + a_n}{10^n} \right)$$

to α with accuracy increasing with n.

Any positive real number α may be written, $\alpha = N.a_1a_2a_3...a_n...$, where N is a nonnegative integer and the a_i are integers satisfying $0 \leq a_i \leq 9$. It is frequently helpful to strip away the integer part N and concentrate on the more complicated decimal part $.a_1a_2a_3...a_n....$ This can be done for any real number α without recourse to decimal expansions.

For any real number α, we set

$$[\alpha] = \text{the largest integer less than or equal to } \alpha.$$

The function from $\mathbb{R}$ to $\mathbb{Z}$ that assigns $[\alpha]$ to the real number α is called the *greatest integer function.*
For examples and properties of this function, see Chapter 2, Section 4.1.

In the remaining sections of this chapter, we will use rational approximation to reveal previously unsuspected properties of various familiar and not so familiar subsets of the real numbers.

Exercise 2.3. Show that a real number α, $0 \leq \alpha < 1$, has a terminating decimal expansion if and only if α is rational and can be written $\alpha = \frac{r}{s}$, where $0 \leq r < s$ and the prime factors of s are a subset of $\{2, 5\}$.

Exercise 2.4. Show that if $\frac{a}{b}$ and $\frac{p}{q}$ are rational numbers with

$$\left|\frac{a}{b} - \frac{p}{q}\right| < \frac{1}{bq},$$

then $\frac{a}{b} = \frac{p}{q}$.

3. Properties of Rational Numbers Close to a Real Number

Our experimental observations in Section 2 prompt numerous questions that will be considered in the next several sections.

Let α be a fixed but arbitrary real number. Our objective is to examine the rational numbers $\frac{p}{q}$ within δ distance of α, where δ is a positive real number. To say that an integer m is *bounded above* by a real number η means that $m \leq \eta$. (So $m \leq [\eta]$.) Similarly, m is *bounded below* by a real number β means that $\beta \leq m$. Note that if $\beta \leq \eta$ are real numbers, then there are only a finite number of integers n between β and $\eta : \beta \leq m \leq \eta$.

We begin by noting that if the rational number $\frac{p}{q}$ is close to α and if the denominator q is small, then the numerator p is also small.

Lemma 3.1. *Let α be a real number. Let δ and η be positive real numbers. If the rational number $\frac{p}{q}$ satisfies $q \leq \eta$, and if*

$$\left|\alpha - \frac{p}{q}\right| \leq \delta,$$

then $|p| \leq \eta(\delta + |\alpha|)$.

Proof. By the triangle inequality,

$$|p| \leq |p - q\alpha| + |q\alpha| \leq q\delta + q|\alpha| \leq \eta(\delta + |\alpha|).$$

■

Next, we deduce that the set of all such $\frac{p}{q}$ is finite.

Corollary 3.2. *Let α be a real number, and let δ and η be positive real numbers. There exist only finitely many rational numbers $\frac{p}{q}$ with $q \leq \eta$ satisfying*

$$\left|\alpha - \frac{p}{q}\right| \leq \delta.$$

Proof. There are only a finite number of positive integers $q \leq \eta$. We show that for each such q, there are only a finite number of rational numbers $\frac{p}{q}$ in the interval $(\alpha - \delta, \alpha + \delta)$. For $\alpha - \delta \leq \frac{p}{q} \leq \alpha + \delta$ implies that $q(\alpha - \delta) \leq p \leq q(\alpha + \delta)$. So there are only a finite number of such p. Thus, for each q,

there are only a finite number of fractions $\frac{p}{q}$ in lowest terms, i.e., rational numbers, with denominator q and satisfying

$$\left|\alpha - \frac{p}{q}\right| \leq \delta.$$

The conclusion of the corollary follows immediately. ■

If δ is no longer constant but is equal to $\frac{1}{q^t}$ for some fixed positive real number t, we have the same results. Note the distinct difference here between the bound on the size of the interval of the form $\frac{1}{q^t}$ depending on the denominator of $\frac{p}{q}$, and the bound $\frac{1}{mb}$ depending on $\alpha = \frac{a}{b}$ in Section 2.

Lemma 3.3. *Let α be a real number, and let t be a positive real number. Given a positive real number η, there exists a positive real number μ_η so that, if the rational number $\frac{p}{q}$ satisfies*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^t},$$

and if the denominator q is bounded above by η, then the numerator p is bounded above by μ_η.

Proof. If $\frac{p}{q}$ is as stated and $q \leq \eta$, for some positive real number η, then

$$|p| \leq |p - q\alpha| + |q\alpha| \leq \frac{1}{q^{t-1}} + \eta|\alpha|.$$

If $t \leq 1$, then we may take $\mu_\eta = \frac{1}{\eta^{t-1}} + \eta|\alpha|$. If $t > 1$, then we may take $\mu_\eta = 1 + \eta|\alpha|$. ■

Corollary 3.4. *Let α be a real number, and let η and t be positive real numbers. There exist only finitely many rational numbers $\frac{p}{q}$ with $q \leq \eta$ satisfying*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^t}.$$

Proof. We have seen that every rational number $\frac{p}{q}$ satisfying the hypothesis of the corollary has bounded numerator and denominator. Thus there are only finitely many of them. ■

Remark. Corollary 3.4 may be derived immediately from Corollary 3.2 by taking $\delta = 1$.

Corollary 3.5. *Let α be a real number, and let η be a positive real number. Then there is a real number $\epsilon > 0$, such that the interval $(\alpha - \epsilon, \alpha + \epsilon)$ contains no rational number, distinct from α, with denominator $\leq \eta$.*

Proof. Let δ be any positive real number. By Corollary 3.2, there are only finitely many rational numbers $\frac{p}{q}$, distinct from α, with $q \leq \eta$ in the interval $(\alpha - \delta, \alpha + \delta)$. Of these, let $\frac{p'}{q'}$ be closest to α and set $\epsilon = \left|\alpha - \frac{p'}{q'}\right|$. If no such $\frac{p'}{q'}$ exists, then set $\epsilon = \delta$. The interval $(\alpha - \epsilon, \alpha + \epsilon)$ contains no rational number with denominator $\leq \eta$. ■

Since the rational numbers are dense in the real numbers, the notion of which rational number $\frac{p}{q}$ is the "best" approximation of a real number α makes no sense if by "best" we mean "closest to." In Corollary 3.4, we measured closeness of $\frac{p}{q}$ to α in terms of a positive power of $\frac{1}{q}$. As we shall see, this approach leads to substantive information about the real numbers. We will consider distances of the form $\frac{1}{q^t}$, where t is a positive real number possibly dependent on α but not on $\frac{p}{q}$. For α in various subsets of $\mathbb{R}$, we will prove several kinds of results which, taken together, give a range for the degree of accuracy with which α may be approximated.

The results take the following form. Given a real number α,
(1). positive real numbers $c(\alpha)$ and t exist so that there are infinitely many rational numbers $\frac{p}{q}$ with $\left|\alpha - \frac{p}{q}\right| \leq \frac{c(\alpha)}{q^t}$;
(2). positive real numbers $c(\alpha)$ and t exist so that there are only finitely many rational numbers $\frac{p}{q}$ with $\left|\alpha - \frac{p}{q}\right| \leq \frac{c(\alpha)}{q^t}$;
(3). for $\delta > 0$, there exist $c(\alpha, \delta)$ and t so that $\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha,\delta)}{q^{t+\delta}}$, for all rational numbers $\frac{p}{q}$.

We begin with the case where α itself is rational. For a rational number $\alpha = \frac{a}{b}$, we will find that there are infinitely many rational numbers $\frac{p}{q}$ within $\frac{1}{q}$ of $\frac{a}{b}$. This is not too surprising since the bound $\frac{1}{q}$ is not very small. However, the search for rational numbers $\frac{p}{q}$ within $\frac{1}{q^2}$ of $\frac{a}{b}$ will result in the discovery that there are only finitely many of them.

To prove these statements on approximation of rational numbers by rationals, we call on a result on linear Diophantine equations.

Lemma 3.6. *Let a and b be relatively prime integers. The linear Diophantine equation $ax - by = 1$ has infinitely many solutions (q, p).*

Proof. Since $\gcd(a, b) = 1$, there exist integers x_0 and y_0 such that $ax_0 + by_0 = 1$. Set $q_0 = x_0$ and $p_0 = -y_0$, then $aq_0 - bp_0 = 1$. Moreover, for every $n \in \mathbb{Z}$, the integers $q_n = q_0 + bn, p_n = p_0 + an$ also satisfy $aq_n - bp_n = 1$. ■

Note that the solutions (q, p) are relatively prime.

Proposition 3.7. *If $\alpha = \frac{a}{b}$ is a fixed rational number, there are infinitely many rational numbers $\frac{p}{q}$ such that*

$$\left|\frac{a}{b} - \frac{p}{q}\right| \leq \frac{1}{q}.$$

Proof. Suppose that $b \neq 1$. The linear Diophantine equation $ax - by = 1$ has infinitely many relatively prime solutions (q, p). Note that $q \neq 0$, since $b \neq 1$. For each of these solutions, form the rational number $\frac{p}{q}$, multiplying (q, p) by -1, if necessary, to obtain $q > 0$. Each of these rational numbers satisfies

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} = \frac{1}{bq} < \frac{1}{q}.$$

If $b = 1$, then, for $n > 0$, the rational numbers $\frac{an-1}{n}$ satisfy the equality

$$\left|a - \frac{an - 1}{n}\right| = \frac{1}{n}.$$

■

Proposition 3.8. *Let $\alpha = \frac{a}{b}$ be a fixed rational number, and let r be a real number > 1. There are only finitely many rational numbers $\frac{p}{q}$ satisfying*

$$\left|\frac{a}{b} - \frac{p}{q}\right| \leq \frac{1}{q^r}.$$

Proof. If, on the contrary, there exist infinitely many rational numbers $\frac{p}{q}$ satisfying the inequality, then, by Corollary 3.4, q is not bounded. Consequently, there is a rational number $\frac{p}{q}$ satisfying

$$0 < \left|\frac{a}{b} - \frac{p}{q}\right| \leq \frac{1}{q^r}$$

with $q^{r-1} > b$. It follows that

$$0 < |aq - bp| \leq \frac{b}{q^{r-1}} < 1,$$

contradicting the fact that $|aq - bp|$ is a positive integer. ■

4. An Interesting Example, Part I

Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \begin{cases} \frac{1}{q} & \text{if } x \text{ is a nonzero rational number } \frac{p}{q}, \\ \\ 0 & \text{if x = 0 or } x \text{ is irrational} \end{cases}$$

For which real numbers x is the function f continuous? Recall that a function $f : \mathbb{R} \to \mathbb{R}$ is continuous at a real number α if given a real number $\epsilon > 0$, there exists a real number $\delta > 0$, such that if $x \in \mathbb{R}$ and $|x - \alpha| < \delta$, then $|f(x) - f(\alpha)| < \epsilon$. We leave it to the reader to show that a function $f : \mathbb{R} \to \mathbb{R}$ is continuous if and only if for any sequence $\{x_n\}$ of real numbers converging to α, the sequence $\{f(x_n)\}$ converges to $f(\alpha)$.

Proposition 4.1. *The function f defined above is continuous at 0 and at irrational numbers α, but f is not continuous at any nonzero rational number $\frac{p}{q}$.*

Proof. For any real number α, there is a sequence of irrational numbers $\{x_n\}$ converging to α. The sequence $\{f(x_n)\}$ is the zero sequence since $f(x_n) = 0$, for all n. Thus, if $\alpha = \frac{p}{q}$ is a nonzero rational number then $f(\alpha) = \frac{1}{q} \neq 0$, so f is not continuous at α.

Suppose that $\alpha = 0$, or α is irrational. Let $\epsilon > 0$ be a real number. There exists a positive integer n with $\frac{1}{n} < \epsilon$. By Corollary 3.5, there is a positive real number δ such that every rational number $\frac{p}{q}$ in the interval $(\alpha - \delta, \alpha + \delta)$ has $q > n$. It follows for x in this interval that

$$|f(x) - f(\alpha)| = |f(x)| < \frac{1}{n} < \epsilon.$$

Thus, f is continuous at α if and only if $\alpha = 0$ or is α is irrational. ■

Since f is not continuous at any nonzero rational number α, it is not differentiable at α. There is the possibility that f is differentiable at 0 or at an irrational number. During the course of this chapter, we will return to the function f and its powers to study the differentiability of f by applying results in rational approximation.

5. Dirichlet's Theorem

The next question is whether there exist *any* rational numbers $\frac{p}{q}$ satisfying the inequality

$$\left|\frac{a}{b} - \frac{p}{q}\right| < \frac{1}{q^2}.$$

The affirmative answer follows from a fundamental result due to Dirichlet on rational approximation of, not just rational numbers $\frac{a}{b}$, but any real number.

Recall that the pigeonhole principle, or Dirichlet box principle, states that if more than n objects are placed in n boxes, then one box will contain at least two objects. Recall that the notation $[a]$ denotes the greatest integer less than or equal to the real number a.

Theorem 5.1 (Dirichlet)**.** *Let α be a real number and n a positive integer. Then there is a rational number $\frac{p}{q}$ with $0 < q \leq n$, satisfying*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{(n+1)q}.$$

Proof. If $n = 1$, then $\frac{p}{q} = \frac{[\alpha]}{1}$ or $\frac{p}{q} = \frac{[\alpha]+1}{1}$ satisfies

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

Suppose that $n \geq 2$. Consider the $n+2$ numbers

$$0, \alpha - [\alpha], 2\alpha - [2\alpha], ..., n\alpha - [n\alpha], 1$$

in the interval $[0, 1]$. Assume first that these numbers are distinct as they will be when α is irrational. Since the interval $[0, 1]$ can be subdivided into $n+1$ subintervals of length $\frac{1}{n+1}$, the pigeonhole principle guarantees that two of these numbers differ in absolute value by at most $\frac{1}{n+1}$. If one of the numbers is 0 and the other is $i\alpha - [i\alpha]$, then $i \leq n$, $|i\alpha - [i\alpha]| \leq \frac{1}{n+1}$, and

$$\left|\alpha - \frac{[i\alpha]}{i}\right| \leq \frac{1}{(n+1)i}.$$

After $\frac{[i\alpha]}{i}$ is reduced to lowest terms $\frac{p}{q}$, the rational number $\frac{p}{q}$ satisfies the required inequality. Similarly, if the two numbers are $j\alpha - [j\alpha]$ and 1, then $j \leq n$ and reducing $\frac{[j\alpha]+1}{j}$ to lowest terms $\frac{p}{q}$, we have $\frac{p}{q}$ satisfies the required inequality. Finally, if the two numbers are $i\alpha - [i\alpha]$, and $j\alpha - [j\alpha]$, where $i < j$, then

$$|j\alpha - [j\alpha] - (i\alpha - [i\alpha])| = |(j-i)\alpha - ([j\alpha] - [i\alpha])| \leq \frac{1}{n+1}.$$

Consequently, $j - i < n$, and

$$\left|\alpha - \frac{([j\alpha] - [i\alpha])}{j-i}\right| \leq \frac{1}{(n+1)(j-i)}.$$

Thus, after $\frac{[j\alpha]-[i\alpha]}{j-i}$ is reduced to lowest terms $\frac{p}{q}$, the rational number $\frac{p}{q}$ satisfies the required inequality.

In the event that the $n+2$ numbers are not distinct, then α itself is a rational number with denominator at most n. For, in this case, there exist $i < j$ so that α is equal to one of the two following fractions:

$$\frac{[i\alpha]}{i}, \quad \frac{[j\alpha] - [i\alpha]}{j-i}$$

reduced to lowest terms. Thus, if the numbers are not distinct, the required inequality is trivially satisfied by α itself. ■

An alternate proof of Theorem 5.1 using Farey sequences can be found in Section 6.2 of Chapter 3. Also, for a proof of Theorem 5.1 using Minkowski's theorem, see Exercise 9.4 in Chapter 3.

Corollary 5.2. *Given any real number α, there exists a rational number $\frac{p}{q}$ such that*

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

Proof. This follows immediately from Theorem 5.1 since the $\frac{p}{q}$ found in that theorem has $q \leq n$. ■

Recall, from Proposition 3.8, that if α is rational, then there are only a finite number of $\frac{p}{q}$ as in the corollary. The next result delineates markedly different behavior if α is irrational.

Proposition 5.3. *If α is irrational, then there are infinitely many rational numbers $\frac{p}{q}$ such that*

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

Proof. Suppose there are only a finite number of rational numbers $\frac{p_1}{q_1}, \frac{p_2}{q_2}, ..., \frac{p_k}{q_k}$ satisfying the inequality. Then,

$$\left|\alpha - \frac{p_i}{q_i}\right| > 0,$$

for $1 \leq i \leq k$. Consequently, since α is irrational, there is a positive integer n such that the strict inequality

$$\left|\alpha - \frac{p_i}{q_i}\right| > \frac{1}{n+1}$$

holds for $1 \leq i \leq k$. However, this contradicts Theorem 5.1 which asserts that, for this n, there is a rational number $\frac{p}{q}$ with $q \leq n$ and

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{(n+1)q} < \frac{1}{q^2}.$$

■

The rather surprising fact that rational numbers and irrational numbers can be characterized in terms of rational approximation follows immediately from Propositions 3.8 and 5.3.

Corollary 5.4. *A real number α is irrational if and only if there are infinitely many rational numbers $\frac{p}{q}$ satisfying $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$.*

Exercise 5.5. Suppose that S is a set of $n+1$ not necessarily distinct numbers contained in the set $\{1, 2, 3, ..., 2n-1, 2n\}$. Show that there are two numbers in S such that one divides the other.

6. An Interesting Example, Part II

We return to the function f defined in Section 4. We will apply Theorem 5.1 to answer the question of whether f is differentiable at any irrational number.

Proposition 6.1. *If $f : \mathbb{R} \to \mathbb{R}$ is defined by*

$$f(x) = \begin{cases} \frac{1}{q} & \text{if } x \text{ is a nonzero rational number } \frac{p}{q}, \\ \\ 0 & \text{if } x = 0 \text{ or } x \text{ is irrational} \end{cases}$$

then f is not differentiable at any real number.

Proof. Let α be a real number. By Proposition 4.1, if α is a nonzero rational number, then f is not continuous at α, so f is not differentiable at α.

Suppose α is equal to 0 or to an irrational number. To test whether f is differentiable at α, we must examine the difference quotient

$$\frac{f(x) - f(\alpha)}{x - \alpha}$$

and take the limit as x approaches α. As x approaches α through irrational numbers, the numerator of the difference quotient is 0, and the denominator is nonzero, so the limit is 0. It follows that if f is differentiable at α, then its derivative at α is equal to 0. Now, we will let x approach α through a specific sequence of rational numbers. If $\alpha = 0$, we consider the sequence $\left\{\frac{1}{n}\right\}$, for n a positive integer. This sequence converges to 0. The difference quotient is

$$\frac{f(x_n) - f(0)}{x_n - 0} = \frac{\frac{1}{n}}{\frac{1}{n}} = 1.$$

Thus, the difference quotient has no limit as x approaches 0, and x is not differentiable at 0.

Suppose that α is an irrational number. By Theorem 5.1, for each n, there is a rational number $\frac{p_n}{q_n}$, with $q_n \leq n$, such that

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{(n+1)q_n} \leq \frac{1}{n+1}.$$

It follows that, by increasing n, we may construct an infinite sequence of rational numbers that converge to α. We compute the difference quotient

letting x approach α by taking on the values of this sequence. We have $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$, so

$$\left|\frac{f(x) - f(\alpha)}{x - \alpha}\right| = \frac{\frac{1}{q_n}}{\left|\frac{p_n}{q_n} - \alpha\right|} > \frac{\frac{1}{{q_n}^2}}{\frac{1}{{q_n}^2}} = 1.$$

Consequently, the difference quotient does not have a limit as x approaches α, which confirms that f is not differentiable at any irrational number. ■

Sometimes it is possible to smooth out a function by looking at suitable powers. For example, consider the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = |x|$. The function g is not differentiable at 0, but the function $g^2(x) = |x|^2$ is differentiable at 0. With this in mind, we let r be any real number ≥ 1, and define the function

$$f_r(x) = \begin{cases} \frac{1}{q^r} & \text{if } x \text{ is a nonzero rational number } \frac{p}{q}, \\ \\ 0 & \text{if } x = 0 \text{ or } x \text{ is irrational} \end{cases}$$

The same proof as that of Proposition 4.1 shows that f_r is not continuous at any nonzero rational number and is continuous at 0 and at all irrational numbers. What about differentiability? The proof given for irrational numbers in Proposition 6.1 justifies the following statement.

Proposition 6.2. *If $1 \leq r \leq 2$, and α is an irrational number, then the function f_r, defined above, is not differentiable at α.*

For 0, however, we have the following result.

Proposition 6.3. *If $r > 1$, then the function f_r is differentiable at 0.*

Proof. Fix a real number $r > 1$. The same argument as that given in the proof of Proposition 6.1 shows that the derivative at 0, if it exists, must be equal to 0. Thus we must show that if $\epsilon > 0$, there is a $\delta > 0$, such that $x \in (-\delta, \delta)$ implies that

$$\left|\frac{f_r(x) - f_r(0)}{x - 0}\right| = \frac{|f_r(x)|}{|x|} < \epsilon.$$

If x is irrational then this difference quotient is equal to $0 < \epsilon$. Suppose x is a nonzero rational number. There is a positive integer n such that $\frac{1}{n^{r-1}} < \epsilon$. By Corollary 3.5, there is a $\delta > 0$, such that every nonzero rational number $\frac{p}{q}$ in the interval $(-\delta, \delta)$ has $q > n$. Thus, if $x = \frac{p}{q}$,

$$\frac{|f_r(x)|}{|x|} = \frac{\frac{1}{q^r}}{\left|\frac{p}{q}\right|} = \frac{1}{|p|q^{r-1}} < \frac{1}{|p|n^{r-1}} < \epsilon.$$

■

We discuss the differentiability of f_r, for $r > 2$, following the discussion of Roth's theorem.

7. Hurwitz's Theorem

We have seen in Corollary 5.2 and Proposition 5.3 that for any irrational number α, there exists infinitely many rational numbers $\frac{p}{q}$ satisfying

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

What is the best possible upper bound of the form $\frac{1}{Cq^2}$, with $C > 0$, such that the same statement holds with $\frac{1}{q^2}$ replaced by $\frac{1}{Cq^2}$? The answer is found in Hurwitz's theorem. Moreover, the terms of Farey sequences or their mediants provide infinitely many rational numbers that do the trick.

The theory of Farey sequences was worked out in Section 6.2 of Chapter 3. We briefly recall the few Farey sequence facts needed here. The Farey sequence of order n, F_n, is the sequence of rational numbers $\frac{h}{k}$, where $0 \le h \le k \le n$ and $\gcd(h,k) = 1$, arranged in increasing order. Two consecutive terms $\frac{h}{k}$ and $\frac{h'}{k'}$ in F_n satisfy $h'k - hk' = 1$ and $h'(k+k') - (h+h')k' = 1$. The rational number $\frac{h+h'}{k+k'}$ is called the mediant of h/k and h'/k'. For each n, the terms of F_n partition the interval $[0,1]$. Thus, for any n, if the real number α lies in $[0,1]$, then it lies in an interval determined by two successive terms of F_n.

Theorem 7.1 (Hurwitz)**.** *Let α be an irrational number.*
(i) There are infinitely many rational numbers $\frac{p}{q}$ such that

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

(ii) If $\sqrt{5}$ is replaced by $C > \sqrt{5}$, then there are irrational numbers α for which statement (i) does not hold.

We follow the presentation in [Sch80]. For clarity, we separate the proofs of parts (i) and (ii) and precede each proof by a lemma.

Lemma 7.2. *Suppose n is a positive integer. Let $\frac{h}{k}$ and $\frac{h'}{k'}$ be successive terms in F_n, and let $\frac{h+h'}{k+k'}$ be their mediant. For every real number α in $[\frac{h}{k}, \frac{h'}{k'}]$, at least one of the following inequalities holds:*

$$(i)\ \left|\alpha - \frac{h}{k}\right| < \frac{1}{\sqrt{5}k^2},\ (ii)\ \left|\alpha - \frac{h+h'}{k+k'}\right| < \frac{1}{\sqrt{5}(k+k')^2},\ (iii)\ \left|\alpha - \frac{h'}{k'}\right| < \frac{1}{\sqrt{5}k'^2}.$$

Proof. It is sufficient to prove the lemma for the case where $\alpha > \frac{h+h'}{k+k'}$. If $\alpha < \frac{h+h'}{k+k'}$, we may replace α by $1-\alpha$, $\frac{h}{k}$ by $1-\frac{h'}{k'}$, $\frac{h'}{k'}$ by $1-\frac{h}{k}$. For then $1-\frac{h'}{k'}$ and $1-\frac{h}{k}$ are consecutive terms of F_n with mediant $1-\frac{h+h'}{k+k'}$, and $1-\alpha > 1-\frac{h+h'}{k+k'}$.

We assume that $\alpha > \frac{h+h'}{k+k'}$. Since $\alpha \in [\frac{h}{k}, \frac{h'}{k'}]$, we may rewrite the inequalities (i), (ii), (iii) as

$$(i)\ \alpha - \frac{h}{k} < \frac{1}{\sqrt{5}k^2},\ (ii)\ \alpha - \frac{h+h'}{k+k'} < \frac{1}{\sqrt{5}(k+k')^2},\ (iii)\ -\frac{1}{\sqrt{5}k'^2} < \alpha - \frac{h'}{k'}.$$

If none of the inequalities $(i), (ii), (iii)$ holds, then all three of the following inequalities hold:

$$(i*)\,\alpha - \frac{h}{k} \geq \frac{1}{\sqrt{5}k^2},\ (ii*)\,\alpha - \frac{h+h'}{k+k'} \geq \frac{1}{\sqrt{5}(k+k')^2},\ (iii*)\,\frac{h'}{k'} - \alpha \geq \frac{1}{\sqrt{5}k'^2}.$$

Since $h'k - hk' = 1$, the sum of $(i*)$ and $(iii*)$ yields

$$\frac{h'}{k'} - \frac{h}{k} = \frac{1}{kk'} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{k^2} + \frac{1}{k'^2}\right) = \frac{1}{\sqrt{5}}\left(\frac{k^2+k'^2}{k^2k'^2}\right).$$

Since $h'(k+k') - (h+h')k' = 1$, the sum of $(ii*)$ and $(iii*)$, gives

$$\frac{h'}{k'} - \frac{h+h'}{k+k'} = \frac{1}{k'(k+k')} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{k'^2} + \frac{1}{(k+k')^2}\right).$$

Thus, $\sqrt{5}kk' \geq k^2 + k'^2$ and $\sqrt{5}k'(k+k') \geq k'^2 + (k+k')^2$, and so,

$$\sqrt{5}k'(2k+k') \geq k^2 + 2k'^2 + (k+k')^2.$$

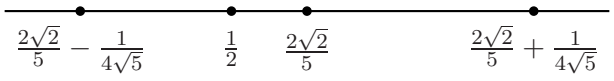
Consequently,

$$0 \geq (3-\sqrt{5})k'^2 - 2(\sqrt{5}-1)kk' + 2k^2 = \frac{1}{2}[(\sqrt{5}-1)k' - 2k]^2.$$

The only conclusion possible is the contradiction $\sqrt{5} = \frac{2k+k'}{k'}$. Hence, one of the inequalities $(i), (ii)$ or (iii) must hold. ■

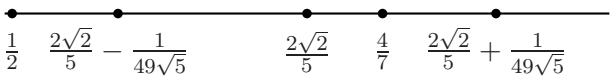
For example, if $\alpha = \frac{2\sqrt{2}}{5}$, then from the Farey sequence of order 1, F_1, we obtain the mediant $\frac{1}{2}$ satisfying

$$\left|\frac{2\sqrt{2}}{5} - \frac{1}{2}\right| < \frac{1}{\sqrt{5}\cdot 4}.$$



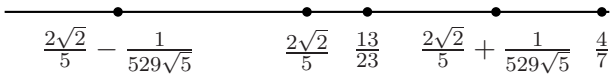
From F_5 we obtain the mediant $\frac{4}{7}$ satisfying

$$\left|\frac{2\sqrt{2}}{5}-\frac{4}{7}\right|<\frac{1}{\sqrt{5}\cdot 49}.$$



From F_{16} we obtain the mediant $\frac{13}{23}$ satisfying

$$\left|\frac{2\sqrt{2}}{5}-\frac{13}{23}\right|<\frac{1}{\sqrt{5}\cdot 529}.$$



Proof of Part (i) of Theorem 7.1. By replacing α by $\alpha-[\alpha]$, if necessary, we may assume that $0<\alpha<1$. For each positive integer n, there are successive terms $\frac{h}{k}, \frac{h'}{k'}$ in the Farey sequence F_n so that $\alpha\in[\frac{h}{k}, \frac{h'}{k'}]$. By Lemma 7.2, one of $\frac{h}{k}, \frac{h'}{k'}$ and $\frac{h+h'}{k+k'}$ satisfies the inequality in (i). Naming that rational number $\frac{p}{q}$, we have

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

Since

$$\left|\frac{h}{k}-\frac{h'}{k'}\right|=\frac{1}{kk'}\le\frac{1}{n},$$

it follows that

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

But α is irrational, so one fixed $\frac{p}{q}$ can satisfy this inequality only for small n. Thus, as $n\to\infty$, there are infinitely many solutions to the inequality in (i). ■

To show, for all irrational numbers α, that $\frac{1}{\sqrt{5}q^2}$ is the best possible upper bound for $\left|\alpha-\frac{p}{q}\right|$ of the form $\frac{1}{Cq^2}$, we need to produce an α such that

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

has only finitely many rational solutions $\frac{p}{q}$ if $C>\sqrt{5}$. The next lemma reveals exactly how to find such an α.

Lemma 7.3. *Suppose that α is a real irrational number that satisfies an equation of the form $f(X) = aX^2 + bX + c$, where $f(X)$ is a nonzero polynomial in $\mathbb{Z}[X]$. Let D be its discriminant: $D = b^2 - 4ac$. If C is a real number satisfying $C > \sqrt{D}$, then the inequality*

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

has only finitely many solutions.

Proof. Note that $f(\frac{p}{q}) \neq 0$, and, in fact, $\left|f(\frac{p}{q})\right| \geq \frac{1}{q^2}$. Suppose that $\frac{p}{q}$ satisfies

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

for some $C > \sqrt{D}$. We write $f(X) = a(X-\alpha)(X-\beta)$, and $D = a^2(\alpha-\beta)^2$. We have

$$\frac{1}{q^2} \leq \left|f\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \left|a\left(\beta - \frac{p}{q}\right)\right| < \frac{1}{Cq^2}\left|a\left(\beta - \alpha + \alpha - \frac{p}{q}\right)\right|$$

By the triangle inequality, we have that

$$\frac{1}{q^2} < \left(\frac{\sqrt{D}}{C} + \frac{|a|}{C^2q^2}\right)\frac{1}{q^2}.$$

Consequently,

$$(C - \sqrt{D})Cq^2 < |a|.$$

But $C > \sqrt{D}$, so the inequality above cannot hold for large q. Consequently, there are only a finite number of rational numbers $\frac{p}{q}$ satisfying the inequality in the statement of the lemma. ■

Proof of Part (ii) of Theorem 7.1. Set $\alpha = \frac{1}{2}(\sqrt{5}-1)$. Then α satisfies the polynomial $f(X) = X^2 + X - 1$ which has discriminant $D = 5$. Thus, by Lemma 7.3, if $C > \sqrt{5}$ the inequality

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

has only finitely many solutions. Consequently, the statement in Part (i) of the theorem is false for α if $\sqrt{5}$ is replaced by C. ■

The numbers described in Lemma 7.3 are called *quadratic irrational numbers*. The behavior described in the lemma motivates the following

definition. An irrational number α is said to be *badly approximable* if there is a real number $c(\alpha) > 0$, depending only on α, so that

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^2},$$

for all rational numbers $\frac{p}{q}$. It follows from Lemma 7.3, by adjusting the constant C, that every quadratic irrational number α, such as $\sqrt{2}$, for example, is badly approximable.

The exponent of q in Proposition 5.3 cannot be improved for badly approximable numbers.

Proposition 7.4. *If an irrational number α is badly approximable, then, for every $\epsilon > 0$, there are only finitely many rational numbers $\frac{p}{q}$ satisfying*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\epsilon}}.$$

Proof. Let $c(\alpha)$ be a positive real number with

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^2},$$

for all rational numbers $\frac{p}{q}$. Suppose, on the contrary, that there are infinitely many rational numbers $\frac{p}{q}$ such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\epsilon}}.$$

Then there exists such a rational number $\frac{p_1}{q_1}$, with

$$q_1^{\epsilon} > \frac{1}{c(\alpha)}.$$

It follows that

$$\left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{q_1^2 q_1^{\epsilon}} < \frac{c(\alpha)}{q_1^2},$$

a contradiction. ■

Since quadratic irrational numbers are badly approximable, we have the following result.

Corollary 7.5. *For quadratic irrational numbers α and any $\epsilon > 0$, there are only finitely many rational numbers $\frac{p}{q}$ satisfying*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\epsilon}}.$$

8. Liouville's Theorem

We have seen that the exponent in the upper bound $\frac{1}{q^2}$ in Dirichlet's theorem cannot be improved for real quadratic irrational numbers. This might be called a result in *reverse approximation*: the rationals are "pushed away" from quadratic irrationals. Liouville's theorem demonstrates that rational numbers can also be "pushed away" from a real number satisfying a higher degree polynomial over $\mathbb{Z}$ if the exponent is raised from 2 to its degree d.

Even more interesting, perhaps, is the fact that Liouville's theorem provides a method for constructing transcendental numbers.

Recall that a real number α is *algebraic* (over $\mathbb{Q}$) if it is a root of a polynomial with coefficients in $\mathbb{Q}$. A real number is *transcendental* if it is not algebraic. We summarize, without proof, the basic facts from field theory required in this section. (For proofs, see, for example [Art91] or [DF99].)

The *minimal polynomial of α over $\mathbb{Q}$* is the unique monic polynomial in $\mathbb{Q}[X]$ of least degree satisfied by α. Since $\mathbb{Q}$ is a field, the minimal polynomial is irreducible. The real number α is said to be an *algebraic number of degree d* if its minimal polynomial has degree d. If

$$X^d + r_{d-1}X^{d-1} + ... + r_1X + r_0,$$

is the minimal polynomial of α over $\mathbb{Q}$, then multiplication by the least common multiple of the denominators of the coefficients r_i, produces a unique polynomial with α as a root having the form

$$P(X) = a_dX^d + a_{d-1}X^{d-1} + ... + a_1X + a_0,$$

where the coefficients a_i are relatively prime integers and $a_d > 0$.

Recall that Gauss' lemma (see Chapter 11, Section 3 of [Art91] or Section 9.3 of [DF99]) implies that a nonconstant polynomial $P(X) \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$ if and only if the greatest common divisor of its coefficients is equal to 1 and $P(X)$ is irreducible in $\mathbb{Q}[X]$. Thus, it follows from Gauss' lemma that the polynomial $P(X) \in \mathbb{Z}[X]$ constructed in the previous paragraph is irreducible over $\mathbb{Z}$ (and over $\mathbb{Q}$). We call this polynomial the *minimal polynomial of α over $\mathbb{Z}$*.

For example, a real number is rational if and only if it is an algebraic number of degree 1. The algebraic number $\frac{1}{\sqrt{2}}$ has degree 2. Its minimal polynomial over $\mathbb{Q}$ is $X^2 - \frac{1}{2}$. The minimal polynomial of $\frac{1}{\sqrt{2}}$ over $\mathbb{Z}$ is $P(X) = 2X^2 - 1$. Note that if α is an algebraic number of degree greater than one, then its minimal polynomial over $\mathbb{Z}$, being irreducible over $\mathbb{Q}$, has no rational roots.

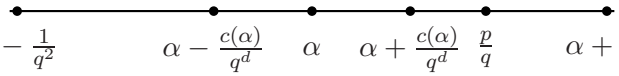
8.1. Statement and Proofs of Liouville's Theorem.

Theorem 8.1 (Liouville)**.** *Let α be a real algebraic number of degree $d \geq 2$. Then there is a constant $c(\alpha) > 0$, depending only on α, such that*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d},$$

for all rational numbers $\frac{p}{q}$.

(Note that the inequality can be made strict by replacing $c(\alpha)$ by $c(\alpha)-\epsilon$ for $\epsilon > 0$.)



We will give three proofs of Liouville's theorem.

The first proof is essentially found in [Cas57] except that we use the irreducibility of the minimal polynomial of α over $\mathbb{Z}$.

First Proof of Theorem 8.1. Let $P(X) = a_d X^d + a_{d-1}X^{d-1} + ... + a_1 X + a_0$ be the minimal polynomial of α over $\mathbb{Z}$. Let $\alpha = \alpha_1, \alpha_2, ..., \alpha_d$ be the roots of $P(X)$ and write

$$P(X) = a_d \prod_j (X - \alpha_j).$$

Let $\frac{p}{q}$ be a rational number satisfying $\left|\alpha - \frac{p}{q}\right| < 1$. Note that $\left|\alpha_j - \frac{p}{q}\right| \leq \left|\alpha - \frac{p}{q}\right| + |\alpha_j - \alpha| \leq 1 + |\alpha_j| + |\alpha|$. Consequently,

$$\begin{aligned}
\left|P\left(\frac{p}{q}\right)\right| &= |a_d| \left|\alpha - \frac{p}{q}\right| \prod_{j\geq 2} \left|a_j - \frac{p}{q}\right| \\
&\leq |a_d| \left|\alpha - \frac{p}{q}\right| \prod_{j\geq 2} (1 + |\alpha_j| + |\alpha|) \\
&= c\left|\alpha - \frac{p}{q}\right|,
\end{aligned}$$

where $c = |a_d| \prod_{j\geq 2} (1 + |\alpha_j| + |\alpha|)$ is a positive constant depending only on α.

But $P(X)$ is irreducible, so $P(\frac{p}{q}) \neq 0$. Consequently,

$$q^d P\left(\frac{p}{q}\right) = a_d p^d + a_{d-1} p^{d-1} q + ... + a_1 p q^{d-1} + a_0$$

is a nonzero integer.

From these calculations, we conclude that $\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}$ and that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{c}\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{cq^d},$$

for all $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right| < 1$.

If $\frac{p}{q}$ is a rational number with $\left|\alpha - \frac{p}{q}\right| > 1$, then certainly

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^d}.$$

So, if we set $c(\alpha) = \min\{1, \frac{1}{c}\}$, it follows that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d},$$

for all rational numbers $\frac{p}{q}$. ■

Corollary 8.2. *Let α be a real algebraic number of degree $d \geq 2$. For every $\delta > 0$, there are only finitely many rational numbers $\frac{p}{q}$ satisfying*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\delta}}.$$

Proof. For if, on the contrary, there is an $\delta > 0$ and infinitely many $\frac{p}{q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\delta}},$$

there exists one such $\frac{p_1}{q_1}$ with $q_1^\delta > \frac{1}{c(\alpha)}$. However, this implies that

$$\left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{(q_1)^{d+\delta}} < \frac{c(\alpha)}{(q_1)^d},$$

a contradiction to Theorem 8.1. ■

Remark. Liouville's result, proved in 1844, prompted a concerted effort to reduce the exponent $d + \delta$. The first significant advance was by Thue in 1908. The work culminated in Roth's theorem, proved in 1955. See Section 9.1.

The second proof of Liouville's theorem that we give is the most familiar one. It uses the Mean Value Theorem.

Second Proof of Theorem 8.1. Let $P(X)$ be the minimal polynomial for α over $\mathbb{Z}$. Define

$$M(\alpha) = \max_{x \in [\alpha-1, \alpha+1]} |P'(x)|,$$

where $P'(x)$ is the derivative of $P(x)$. Since degree $P > 0$, the number $M(\alpha) \neq 0$.

Suppose that $\left|\alpha - \frac{p}{q}\right| < 1$. By the Mean Value Theorem, we have, for some θ between α and $\frac{p}{q}$,

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

Note that $P'(\theta) \neq 0$, since $P\left(\frac{p}{q}\right) \neq 0$. It follows that

$$\left|\alpha - \frac{p}{q}\right| = \frac{\left|P\left(\frac{p}{q}\right)\right|}{|P'(\theta)|} \geq \frac{\left|P\left(\frac{p}{q}\right)\right|}{M(\alpha)} \geq \frac{1}{M(\alpha) q^d}$$

since $\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}$. Thus, setting $c(\alpha) = \frac{1}{M(\alpha)}$, we have

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d},$$

for rational numbers satisfying $\left|\alpha - \frac{p}{q}\right| < 1$. As in the first proof, $c(\alpha)$ may be adjusted to ensure that the inequality holds for all rational numbers $\frac{p}{q}$. ■

The third proof is similar to the second except that the constant $c(\alpha)$ is computed in a different manner. This proof follows [HS00] and [Sch80].

Third Proof of Theorem 8.1. Let $P(X)$ be the minimal polynomial of α over $\mathbb{Z}$. Since $P(\alpha) = 0$, when $P(X)$ is expanded in a Taylor series in powers of $(X - \alpha)$, we obtain

$$P(X) = \sum_{i=1}^{d} \frac{1}{i!} \frac{d^i P}{dX^i}(\alpha)(X - \alpha)^i. \tag{33}$$

Suppose that $\frac{p}{q}$ is a rational number satisfying $\left|\alpha - \frac{p}{q}\right| < 1$. We know that $P\left(\frac{p}{q}\right) = \frac{N}{q^d}$, where N is a nonzero integer. Computing $\left|P\left(\frac{p}{q}\right)\right|$ using (33), we have

$$\left|P\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \left|\sum_{i=1}^{d} \frac{1}{i!} \frac{d^i P}{dX^i}(\alpha) \left(\frac{p}{q} - \alpha\right)^{i-1}\right|.$$

Consequently, by the triangle inequality,

$$\left|P\left(\frac{p}{q}\right)\right| \leq \left|\alpha - \frac{p}{q}\right| \cdot \sum_{i=1}^{d} \frac{1}{i!} \left|\frac{d^i P}{dX^i}(\alpha)\right| \left|\left(\frac{p}{q} - \alpha\right)^{i-1}\right|.$$

Set $M(\alpha) = \max \frac{1}{i!} \left|\frac{d^i P}{dX^i}(\alpha)\right|$. Since degree $P > 0$, the number $M(\alpha) \neq 0$. We have

$$\left|\frac{N}{q^d}\right| = \left|P\left(\frac{p}{q}\right)\right| \leq \left|\alpha - \frac{p}{q}\right| \cdot d \cdot M(\alpha).$$

Thus,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{|N|}{d \cdot M(\alpha)} \cdot \frac{1}{q^d} = \frac{c(\alpha)}{q^d},$$

for all $\frac{p}{q}$ satisfying $\left|\alpha - \frac{p}{q}\right| < 1$. As before, $c(\alpha)$ may be adjusted to ensure that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d},$$

for all rational numbers $\frac{p}{q}$. ■

The examples in Section 2 show that the denominators of rational numbers close to a fixed real number α grow arbitrarily large. Liouville's theorem proves that this is indeed the case for real algebraic numbers α. For example, it follows from the theorem that if $\frac{p}{q}$ is within $\frac{1}{10^{10}}$ of α, then $q^d \geq 10^{10} c(\alpha)$.

Remark. In light of the discussion of rational approximation we have had so far in which the distance to α depends on q, we consider the rational number $\frac{p}{q}$ a *better* approximation to α than another rational number $\frac{p'}{q'}$ when the products of the denominator and the distance satisfy

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

The theory of continued fractions provides an efficient algorithm for constructing *best* approximations to α in this sense. The theory of continued fractions and its role in Diophantine approximations may be found, for example, in [Bur00], Exercise D18 of [HS00], and [Sch80].

8.2. Liouville's Theorem and Transcendental Numbers. The place of rational approximation in transcendental number theory is described by Gelfond in [Gel03] in this way: *All methods of proof of the transcendence of a number in either the explicit or implicit form depend upon the fact that algebraic numbers cannot be very well approximated by rational fractions....*

We give an example illustrating how Liouville's theorem may be used to construct transcendental numbers. Note that Liouville's (1844) construction of transcendental numbers in this manner predates Cantor's (1874) proof of their existence.

Example. Let

$$\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = .11000100000000000000000100.... \ .$$

The 1's appear in the 1st, 2nd, 6th, 24th, ..., $(n!)$th, ... decimal place.

For $k \geq 1$, set $q(k) = 10^{k!}$ and $p(k) = 10^{k!} \sum\limits_{n=1}^{k} \frac{1}{10^{n!}}$. Then $p(k)$ and $q(k)$ are relatively prime integers, $\frac{p(k)}{q(k)} = \sum\limits_{n=1}^{k} \frac{1}{10^{n!}}$, and

$$\left| \alpha - \frac{p(k)}{q(k)} \right| = \sum_{n=k+1}^{\infty} \frac{1}{10^{n!}}.$$

Comparing with a geometric series, we find that

$$\sum_{n=k+1}^{\infty} \frac{1}{10^{n!}} < \frac{1}{10^{(k+1)!}} \sum_{n=0}^{\infty} \frac{1}{10^{n}} = \frac{10}{9} \cdot \frac{1}{q(k)^{k+1}},$$

and that

$$\left| \alpha - \frac{p(k)}{q(k)} \right| < \frac{\frac{10}{9}}{q(k)^{k+1}}.$$

Finally, we observe that α does not satisfy Liouville's Theorem. For it follows from the calculations above that given any $c > 0$ and any $d > 0$, if we select k so that $\frac{10}{9} < c \cdot q(k)^{k+1-d}$, then

$$\left| \alpha - \frac{p(k)}{q(k)} \right| < \frac{c}{q(k)^{d}} \, ,$$

for large k. Thus α must be a transcendental number. For it follows from Theorem 8.1 that α cannot be algebraic of any degree d.

In fact, essentially the same argument as above proves the following sufficient condition for a real number to be transcendental.

Corollary 8.3. *Let α be a real number. If there is a sequence $r(k)$ of real numbers with $\lim\limits_{k\to\infty} r_k = \infty$, and a sequence $\{\frac{p(k)}{q(k)}\}$ of rational numbers with*

$q(k) \geq 2$, *satisfying*

$$0 < \left|\alpha - \frac{p(k)}{q(k)}\right| \leq \frac{1}{q(k)^{r(k)}},$$

for all k, *then* α *is transcendental.*

Real numbers α that have the property described in the corollary are called *Liouville numbers.* It is known that π, [Mah32], and e, [Per50], are not Liouville numbers. In [Mah37], Mahler puts conditions on the expansion of a real number α in base g that imply that α is a transcendental number but not a Liouville number. One such number is the decimal $\alpha = .12345678910111213141 5.....$.

Exercise 8.4. Show that there are uncountably many Liouville numbers. Hint: Refine the construction in Section 8.2.

9. The Thue-Siegel-Roth Theorem

9.1. Introduction. We proved in Corollary 5.4 that irrational numbers are distinguished from rational numbers by the fact that they can be approximated by infinitely many rational numbers $\frac{p}{q}$ to within $\frac{1}{q^2}$. This fact motivates the following definition.

For $\alpha \in \mathbb{R}$, the *approximation exponent* of α is the smallest real number $\mu(\alpha)$ such that for any real number $\epsilon > \mu(\alpha)$, the inequality

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^\epsilon}$$

is satisfied by only finitely many rational numbers $\frac{p}{q}$. If there exists no such smallest real number, then $\mu(\alpha)$ is defined to be infinite. (In the literature, the approximation exponent is also known as the *irrationality exponent.*)

We have demonstrated that $\mu(\alpha) = 1$, if α is rational (see Proposition 3.8) and that $\mu(\alpha) \geq 2$, if α is irrational (see Proposition 5.3). Liouville numbers have infinite approximation exponent.

Liouville's theorem, in the form of Corollary 8.2, establishes that $\mu(\alpha) \leq d$, if α is real algebraic of degree d. In particular, if α is algebraic of degree 2, then $\mu(\alpha) \leq 2$. In the one hundred and eleven years following Liouville's theorem in 1844, considerable effort was exerted to find the approximation exponent $\mu(\alpha)$ for α real algebraic of degree $d \geq 3$. The first significant advance was made in 1908 by Thue [Thu09] who proved that $\mu(\alpha) \leq \frac{1}{2}d + 1$ for algebraic numbers α of degree $d \geq 3$. The estimate for $\mu(\alpha)$ was further reduced to $2\sqrt{d}$ by Siegel (1921) [Sie66], and to $\sqrt{2d}$ by Dyson (1947) and by Gelfond (1947), see, for example, [HS00], [Sch80]. Siegel conjectured that $\mu(\alpha)$ should be independent of d, in fact, that it should be equal to 2.

In 1955, Roth proved Siegel's conjecture: $\mu(\alpha) = 2$. We quote from Roth's paper, [Rot55]:

Theorem. *Let α be any algebraic number, not rational. If*

$$\left|\alpha - \frac{h}{q}\right| < \frac{1}{q^\kappa},$$

has an infinity of solutions in integers h and $q\,(q > 0)$ then $\kappa \leq 2$.

We will discuss Roth's theorem in the following form.

Roth's Theorem. *Let α be a real algebraic number of degree $d \geq 2$. Then, for each $\delta > 0$, the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\delta}}$$

has only finitely many rational solutions $\frac{p}{q}$.

In addition to the original papers, the full proof of Roth's theorem can be found in [Sch80], and, in a generalized version, in [HS00]. The proof is very difficult. A special case of Thue's theorem is proved in [ST92]. We will not prove either of these results. Rather, we will give a general description illustrating that the proofs of both theorems, in outline, have the same structure as that of the third proof of Liouville's theorem in Section 8. We discuss this structure following the presentations in [HS00] and [Sch80], and in [ST92].

Steps in the Proof of Liouville's Theorem (in the form of Corollary 8.2*)*

(We use this weaker form because it most closely resembles the statements of the later results which we want to discuss.)

Let α be a real algebraic number of degree $d \geq 2$. We must show that for every $\delta > 0$, there are only finitely many rational numbers $\frac{p}{q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\delta}}.$$

Step 1. Construct a nonzero polynomial $P(X) \in \mathbb{Z}[X]$ that vanishes at α.

We take $f(X)$ to be the minimal polynomial of α over $\mathbb{Z}$, which has the extra advantage of being irreducible. Thue's theorem and Roth's theorem require polynomials of more than one variable. We shall see why this is so at the beginning of the next section. Moreover, these polynomials are not likely to be irreducible. Henceforth, we will call a polynomial constructed as in Step 1 for the purpose of improving Liouville's bound, an *auxiliary polynomial*.

Step 2. Show that if $\frac{p}{q}$ *satisfies*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\delta}},$$

and q *is sufficiently large, then* $P\left(\frac{p}{q}\right) = 0$.

With $N = q^d P\left(\frac{p}{q}\right) \in \mathbb{Z}$, using Taylor's theorem (see the third proof of Liouville's theorem in Section 8.1) we have

$$\left|P\left(\frac{p}{q}\right)\right| = \left|\frac{N}{q^d}\right| \leq \left|\alpha - \frac{p}{q}\right| \cdot d \cdot M(\alpha) \leq \frac{d \cdot M(\alpha)}{q^{d+\delta}},$$

where $M(\alpha) = \sum_{i=1}^{d} \frac{1}{i!} \left|\frac{d^i P}{dX^i}(\alpha)\right|$.
So $|N| \leq \frac{d \cdot M(\alpha)}{q^\delta}$. Thus, if $q > (d \cdot M(\alpha))^{\frac{1}{\delta}}$, then $P\left(\frac{p}{q}\right) = 0$.

Step 3. Show $P\left(\frac{p}{q}\right) \neq 0$.

The minimal polynomial $P(X)$ is irreducible and $d > 1$. (The authors of [HS00] warn of the difficulty of this step in the proof of Roth's theorem.)

Step 4 Conclusion.

If

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\delta}}$$

has infinitely many solutions, there is one such $\frac{p_1}{q_1}$ with $q_1 > (d \cdot M(\alpha))^{\frac{1}{\delta}}$. By Step 2, $P\left(\frac{p_1}{q_1}\right) = 0$. By Step 3, $P\left(\frac{p_1}{q_1}\right) \neq 0$. This contradiction completes the proof of Liouville's theorem. ■

Note that if α a real algebraic number of degree 2, then Liouville's theorem (Theorem 8.1) is stronger than Roth's theorem. Roth's theorem

gives the estimate

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha, \delta)}{q^{2+\delta}},$$

for every $\delta > 0$. Whereas Liouville's theorem states that there is a constant $c(\alpha) > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^2},$$

for all rational numbers $\frac{p}{q}$. The analogous result for real algebraic numbers α of degree ≥ 3, namely that there is a constant $c(\alpha) > 0$ so that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^2}$$

for all rational numbers $\frac{p}{q}$, is conjectured to be false for all such α. However, it is not known at the present time to be false for a single real algebraic number. See Exercise D18 in [HS00].

9.2. Thue's Theorem. It is not possible to improve Liouville's result merely by taking an auxiliary polynomial in one variable having α as a root of order greater than 1. For suppose that $P(X) \in \mathbb{Z}[X]$ is a polynomial of degree r that has α as a zero of order $h > 1$. If $\left|\alpha - \frac{p}{q}\right| < 1$, then the Taylor expansion of $P(x)$ in powers of $(X - \alpha)$ gives, as we saw earlier,

$$\left|P\left(\frac{p}{q}\right)\right| \leq C\left|\frac{p}{q} - \alpha\right|^h,$$

with C depending only on P. However, if $P(\frac{p}{q}) \neq 0$, then

$$\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^r}.$$

Consequently,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C'}{q^{\frac{r}{h}}}.$$

Since α is a zero of $P(X)$ of order h, it follows that $p(X)^h$ divides $P(X)$, where $p(X)$ is the minimal polynomial of α. Consequently, $r \geq hd$ and $\frac{r}{h} \geq d$. Thus this approach does not lead to an improvement in the bound. A new concept of auxiliary polynomial is needed.

Thue's work in 1908-1909 was a major breakthrough for the field. (The first, since Liouville's theorem in 1844.) Here is his theorem.

Theorem 9.1 (Thue)**.** *Let α be a real algebraic number of degree d. Then, for each $\delta > 0$, the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{\frac{1}{2}d+1+\delta}}.$$

has only finitely many rational solutions $\frac{p}{q}$.

The following corollary follows immediately.

Corollary 9.2. *Let α be a real algebraic number of degree d. Then, for each $\delta > 0$, there is a constant $c(\alpha, \delta) > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha,\delta)}{q^{\frac{1}{2}d+1+\delta}}$$

for all rational numbers $\frac{p}{q}$.

Since the cases $d = 1$ and $d = 2$ were already known, Thue assumed that $d > 2$. He followed the same general outline for his proof, but he had the insight to consider auxiliary polynomials in two variables $F(X, Y) \in \mathbb{Z}[X, Y]$ having a particularly nice form, namely $F(X, Y) = P(X) + YQ(X)$.

A complete proof of Thue's theorem for the case $\alpha = \sqrt[3]{b}$, where b is a positive integer that is not a perfect cube, is given in the beautiful book [ST92]. Especially enlightening is the construction of an auxiliary polynomial for $\alpha = \sqrt[3]{b}$, which illustrates, in the words of the authors, that, while appearing complicated, "the entire argument is really just an easy exercise in linear algebra."

We outline the presentation in [ST92], describing how Steps 1–4 appear in Thue's proof.

Step 1. Find a nice (nonzero) polynomial of the form $F(X, Y) = P(X) + YQ(X)$ such that $F(X, \alpha)$ has a zero of high order h at α.
"Nice" will mean "having coefficients that are not too big."

In very general terms, the argument goes as follows. Suppose $F(X, Y)$ has total degree r. For $F(X, \alpha)$ to have a zero of order h at α is equivalent to having the first h derivatives, $F(\alpha, \alpha), \frac{\partial F}{\partial X}(\alpha, \alpha), ..., \frac{\partial^{(h-1)} F}{\partial X^{h-1}}(\alpha, \alpha)$ equal to zero. This means there are h linear relations in the coefficients of $P(X)$ and $Q(X)$. Each of these relations has coefficients in $\mathbb{Q}[\alpha]$, so, since α has degree d, we have hd linear equations with rational coefficients. If $hd < 2r + 1$, the number of variables, i.e., of possible coefficients of $P(X)$ and $Q(X)$, then the system of equations has a nonzero solution. Consequently, we have a nonzero

solution if $\frac{d}{2} < \frac{r}{h} + \frac{1}{2h}$ which is suggestive of the exponent $\frac{1}{2}d+1+\delta$ in Thue's theorem. To make the coefficients of $P(X)$ and $Q(X)$, i.e., the coordinates of the solution vector, reasonably small, we make suitable adjustments to the computations above so that we are working over $\mathbb{Z}$. In that case, a lemma (Siegel's lemma) systematizes Thue's use of the pigeonhole principle to give an upper bound for the components of the solution which is small enough. (In [HS00], the authors state that results describing integer solutions to systems of linear equations are often named after Siegel because he was the first to formalize the procedure.)

Step 2. For rational numbers $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ close to α which satisfy Thue's inequality and have sufficiently large denominators, derive an upper bound for $\left|F\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)\right|$ AND the absolute value of its derivatives at $\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)$ in terms of $\left|\alpha - \frac{p_1}{q_1}\right|$ and $\left|\alpha - \frac{p_2}{q_2}\right|$ and a constant depending only on α.
Since the computations from this point on are very delicate, "normalized" derivatives, $F^{(i)}(X,Y)$, with respect to x are used. The definition is

$$F^{(i)}(X,Y) = \frac{1}{i!}\frac{\partial^i}{\partial X^i}F(X,Y) = \frac{1}{i!}\left(\frac{d^iP(X)}{dX^i} + Y\frac{d^iQ(X)}{dX^i}\right).$$

Note that $F^{(i)}(X,Y) \in \mathbb{Z}[X,Y]$, since $F(X,Y) \in \mathbb{Z}[X,Y]$. The variable Y appears only to the first power in $F(X,Y)$, so the Taylor expansion of $F(X,Y)$ around the point (α,α), using normalized derivatives, has the form

$$F(X,Y) = \sum_{i=h}^{r} F^{(i)}(\alpha,\alpha)(X-\alpha)^i + \sum_{i=0}^{r} Q^{(i)}(\alpha)(X-\alpha)^i(Y-\alpha), \tag{34}$$

where the first summation begins at $i = h$ because $F^{(i)}(\alpha,\alpha) = 0$, for $0 \le i < h$. Computation of the derivatives $F^{(i)}(X,Y)$ from the Taylor expansion (34) suggests that for rational numbers $x = \frac{p_1}{q_1}$ and $y = \frac{p_2}{q_2}$ close to α, the absolute value of $F^{(i)}(x,y)$ will be small due to the presence of factors $(x-\alpha)^{h-i}$ and $(y-\alpha)$. As indicated above, establishing this as fact requires precise and sensitive estimations.

Step 3. Show that there is an integer j depending only on α, so that the j^{th} derivative of F, $F^{(j)}(X,Y)$, is not equal to zero at $\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)$.

For, see [ST92], we are not able to prove that $F\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \neq 0$ for rational numbers $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ satisfying Thue's inequality. This is the reason that bounds on the normalized derivatives were required in Step 2. The introduction of the Wronskian determinant

$$W(P,Q) = W(X) = P(X)Q'(X) - Q(X)P'(X),$$

reduces the problem to estimating the order of W, a more tractable, one variable problem.

Step 4. Conclusion.
Suppose, contrary to the statement of the theorem, that Thue's inequality has infinitely many rational solutions. Then there exist two rational solutions, $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$, with denominators that can be chosen to exceed any specified values we desire. An auxiliary polynomial $F(X,Y)$ is constructed as in Step 1, and Steps 2 and 3 are applied to derive contradictory bounds for the absolute value of the j^{th} normalized derivative, where j is defined as in Step 3.

9.3. Roth's Theorem. We discuss Roth's theorem in the following form.

Theorem 9.3 (Roth)**.** *Let α be a real algebraic number of degree $d \geq 2$. Then, for each $\delta > 0$, the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\delta}}$$

has only finitely many rational solutions $\frac{p}{q}$.

The following corollary follows immediately.

Corollary 9.4. *Let α be a real algebraic number of degree $d \geq 2$. Then, for each $\delta > 0$, there is a constant $c(\alpha, \delta) > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha,\delta)}{q^{2+\delta}}$$

for all rational numbers $\frac{p}{q}$.

The proof of Roth's theorem is immensely more complex than those of the theorems of Liouville and of Thue, but the framework is, in essence, the same. We will make some very general remarks about the steps in the proof, but we want to make clear that each step of the proof holds only under certain conditions which must be carefully weighed to obtain the desired contradiction at the conclusion. At every step, there are constants that are dependent only on α and δ, but are not specified until later stages of the proof. The delicate balancing of these constants is the point of the proof, but is not even considered here.

It is straightforward to show that α may be assumed to be an *algebraic integer,* that is, the minimal polynomial of α over $\mathbb{Q}$ is a monic polynomial

$$P(X) = X^d + a_{d-1}X^{d-1} + ... + a_0,$$

where the coefficients a_i are integers.

Step 1. Construct a suitable auxiliary polynomial $F(X_1, X_2, ..., X_m) \in \mathbb{Z}[X_1, ..., X_m]$, *with coefficients that are small in absolute value, that vanishes to high order at* $(\alpha, \alpha, ..., \alpha)$.

For Roth's proof, auxiliary polynomials have many variables. By the end of the proof, it emerges that m, the number of variables, is at least as big as a number on the order of $\frac{4232}{\delta^2}$.

Normalized partial derivatives are used, as in the proof of Thue's theorem, but in this case, we normalize partial derivatives with respect to many variables. If $F(X_1, X_2, ..., X_m) \in \mathbb{Z}[X_1, ..., X_m]$ then the normalized partial derivatives are

$$\partial_{i_1 ... i_m} F = \frac{1}{i_1! \cdots i_m!} \frac{\partial^{i_1 + ... + i_m}}{\partial X_1^{i_1} \cdots \partial X_m^{i_m}} F.$$

If the degree of F in X_i is r_i, then the maximum of the absolute values of the integer coefficients of the normalized partial $\partial_{i_1 ... i_m} F$ is at most equal to the product of $2^{r_1 + ... + r_m}$ and the maximum of the absolute values of the integer coefficients of F. This estimate, using normalized partials, is stronger than the analogous estimate obtained with ordinary partials, a distinct advantage in critical computations.

Step 2. Show that F *has large index (defined below) at* $(\frac{p_1}{q_1}, ..., \frac{p_m}{q_m})$, *if rational numbers* $\frac{p_1}{q_1}, ..., \frac{p_m}{q_m}$ *are sufficiently close to* α *and have sufficiently large denominators.*

The index of a polynomial can be regarded as a "weighted order of vanishing." The index is defined with respect to a m-tuple $(\alpha_1, ..., \alpha_m) \in \mathbb{R}^m$ and a m-tuple of positive integers $(r_1, ..., r_m)$ (which are, in the proof, at most equal to the degree of F in X_i.) The *index of a nonzero polynomial* $P \in \mathbb{Z}[X_1, ..., X_m]$ at $(\alpha_1, ..., \alpha_m)$ with respect to $(r_1, ..., r_m)$ is the least value of

$$\frac{i_1}{r_1} + \frac{i_2}{r_2} + ... + \frac{i_m}{r_m}$$

such that

$$\partial_{i_1 ... i_m} P(\alpha_1, ..., \alpha_m) \neq 0.$$

The index of the zero polynomial is defined to be $+\infty$.
So, if $\partial_{i_1 ... i_m} P(\alpha_1, ..., \alpha_m) \neq 0$, then $\frac{i_1}{r_1} + \frac{i_2}{r_2} + ... + \frac{i_m}{r_m} \geq$ the index of P at $(\alpha_1, ..., \alpha_m)$ with respect to $(r_1, ..., r_m)$.

For example, if $P(X) \in \mathbb{Z}[X]$, then to say that the index of P at α with respect to r is equal to $\frac{i}{r}$ means that $P(X) = (X-\alpha)^i Q(X)$, where $Q(X) \in \mathbb{R}[X]$ and $Q(\alpha) \neq 0$. So if $r = 1$, then the index of P is the order of vanishing at α.

Step 3. Show that, under certain conditions, the index of F at $(\frac{p_1}{q_1}, ..., \frac{p_m}{q_m})$ with respect to $(r_1, ..., r_m)$ is small.

This is the most difficult step. In his paper [Rot55], Roth states that this step, now called Roth's lemma, is "the novel part of the proof." In very general terms, what he shows is that if the coefficients of the polynomial F are not too large, if the denominators of the rational approximations are large enough and if the r's decrease rapidly enough, then the index of P is small. Roth uses the concept of the "generalized Wronskian" of k rational functions in $\mathbb{Q}(X_1, ..., X_m)$, and its relation to linear independence of the functions over $\mathbb{Q}$.

Step 4. Conclusion.

To complete the proof, the theorem is assumed to be false. Accordingly, there exists $\delta > 0$, and infinitely many rational numbers $\frac{p}{q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\delta}}.$$

An auxiliary polynomial as in Step 1 is constructed, rational approximations $\frac{p_1}{q_1}, ..., \frac{p_m}{q_m}$ are chosen with denominators large enough and the constants arising in Steps 1–3 are specified so that both Step 2 and Step 3 are satisfied and a contradiction is obtained.

The proof of Roth's theorem is not effective, that is, as is noted in Remark D7.2 in [HS00], for a given α, the proof does not provide a method that is guaranteed to find the finitely many $\frac{p}{q}$ with

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\delta}}.$$

In other words, the proof does not give a lower bound for $c(\alpha, \delta)$. For special cases where there is information about $c(\alpha, \delta)$ see pg 117 of [Sch80], Chapters 5, 9–12 of [Sto74], and [Bak75].

Acknowledging the work of Thue and Siegel preceding that of Roth, the theorem discussed here is frequently called the Thue-Siegel-Roth theorem.

For a generalization of this theorem to a number field other than $\mathbb{Q}$, as well as references for explicit bounds on the number of solutions $\frac{p}{q}$ to

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\delta}},$$

see Part D of [HS00] and also [Sto74].

10. The Approximation Exponent

Recall that for $\alpha \in \mathbb{R}$, the *approximation exponent* of α is the smallest real number $\mu(\alpha)$ such that for any real number $\delta > \mu(\alpha)$, the inequality

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{\delta}}$$

is satisfied by only finitely many rational numbers $\frac{p}{q}$. In other words $\mu(\alpha)$ is the greatest lower bound of the set of δ for which the inequality above has only finitely many solutions. (In the literature, $\mu(\alpha)$ is sometimes called the *irrationality measure* of α.)

We know that $\mu(\alpha) = 1$ if α is rational; that $\mu(\alpha) \geq 2$ if α is irrational; and, by the Thue-Siegel-Roth theorem, that $\mu(\alpha) = 2$ if α is algebraic of degree ≥ 2. Recall that Liouville numbers have infinite approximation exponent. However, we will show next that "almost all" real numbers have approximation exponent 2. By this we mean that the set of real numbers with approximation number greater than 2 has measure zero. A set $S \subset \mathbb{R}$ has *measure zero* if, for every $\epsilon > 0$, there is a countable covering of S by open intervals having the property that the sum of their lengths is less than ϵ. The union of a countable collection of sets of measure zero has measure zero. As every point on the real line has measure zero, it follows, for example, that the set of rational numbers has measure zero. References on measure theory include [RSN90], [Sal08], [Wil62] and Appendix A.

Proposition 10.1. *The set of real numbers that have approximation exponent greater than* 2 *has measure zero.*

Proof. Since the real line is the union of a countable collection of closed intervals $[n, n+1]$ for $n \in \mathbb{Z}$, it is sufficient to show that the set of real numbers α in $[0, 1]$ having approximation exponent greater than 2 has measure zero. This set is a subset of the irrational numbers because every rational number has approximation exponent 1. Accordingly, let S be the set of irrational numbers $\alpha \in [0, 1]$ having the property that $\mu(\alpha) > 2$. We must show that S has measure zero. For $n \in \mathbb{N}$, let

$$S_n = \{\alpha \in S \,|\, \mu(\alpha) > 2 + 1/n\}.$$

Since S is the countable union of the sets S_n, it is sufficient to show that every S_n has measure zero.

Consider the countably many intervals of the form I_{pq} where $p, q \in \mathbb{Z}$ and $0 < p < q$,

$$I_{pq} = \left(\frac{p}{q} - \frac{1}{q^{2+\frac{1}{n}}},\ \frac{p}{q} + \frac{1}{q^{2+\frac{1}{n}}} \right),$$

and

$$I_{0q} = \left(0,\ \frac{1}{q^{2+\frac{1}{n}}} \right), \text{ and } I_{qq} = \left(1 - \frac{1}{q^{2+\frac{1}{n}}},\ 1 \right).$$

Each $\alpha \in S_n$ lies in countably many of the intervals I_{pq}. For a fixed q, each of the intervals I_{0q} and I_{qq} has length $\frac{1}{q^{2+\frac{1}{n}}}$, and, for $0 < p < q$, the intervals I_{pq} have length $\frac{2}{q^{2+\frac{1}{n}}}$. The sum of the lengths of all the intervals I_{pq} is

$$q \left(\frac{2}{q^{2+\frac{1}{n}}} \right) = \frac{2}{q^{1+\frac{1}{n}}}.$$

As q ranges from 1 to ∞, and p from 0 to q, the I_{pq} form a countable set of open intervals that cover S_n :

$$S_n \subset \bigcup_{q=1}^{\infty} \bigcup_{p=0}^{q} I_{pq}.$$

Moreover, since each $\alpha \in S_n$ lies in countably many of the intervals, the equation still holds if the union is taken over $q > N$, for a positive integer N. The total length of the intervals I_{pq}, for $1 \leq q < \infty$ and $1 \leq p < q$, is the sum

$$\sum_{q=1}^{\infty} \frac{2}{q^{1+\frac{1}{n}}} < \infty$$

which converges because $1 + \frac{1}{n} > 1$. This means that given any $\epsilon > 0$, there is a positive integer N such that

$$\sum_{q>N}^{\infty} \frac{2}{q^{1+\frac{1}{n}}} < \epsilon.$$

Thus, S_n has measure zero. ■

Exercise 10.2. Let f be a positive nonincreasing function such that

$$\sum_{q=1}^{\infty} f(q) < \infty.$$

Show that the set of real numbers α for which the inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{f(q)}{q}$$

has infinitely many solutions is a set of measure zero.
This exercise is part of a theorem of Khinchin [Khi64].

11. An Interesting Example, Part III

For $r \in \mathbb{R}$, with $r \geq 1$, recall that the function f_r is defined by

$$f_r(x) = \begin{cases} \frac{1}{q^r} & \text{if } x \text{ is a nonzero rational number } \frac{p}{q}, \\ \\ 0 & \text{if x =0 or } x \text{ is irrational} \end{cases}$$

We know that f_r is nowhere differentiable if $r = 1$, that f_r is differentiable at 0 for $r > 1$, and that f_r is not differentiable at any irrational number if $1 \leq r \leq 2$. In this section we examine the differentiability of f_r for $r > 2$. First, we deduce from Proposition 10.1 that the function f_r is differentiable "almost everywhere" if $r > 2$. Then we apply the Thue-Siegel-Roth theorem to establish that f_r is differentiable at all real algebraic numbers of degree at least 2.

Proposition 11.1. *Let $r > 2$. Set*

$$S = \{\alpha \in \mathbb{R} \mid \alpha \text{ is irrational and } f_r \text{ is not differentiable at } \alpha\},$$

and

$$T = \{\alpha \in \mathbb{R} \mid \mu(\alpha) > r\}.$$

Then $S \subseteq T$.

Proof. Let $S_{[0,1]} = S \cap [0,1]$ and $T_{[0,1]} = T \cap [0,1]$. It is sufficient to show that

$$S_{[0,1]} \subseteq T_{[0,1]}.$$

For each positive integer n, let S_n be the set of all irrational numbers $\alpha \in [0,1]$ such that, for every $\delta > 0$, there exists $x \in (\alpha - \delta, \alpha + \delta)$ with

$$\left|\frac{f_r(x) - f_r(\alpha)}{x - \alpha}\right| = \left|\frac{f_r(x)}{x - \alpha}\right| > \frac{1}{n}.$$

As $S_{[0,1]} = \cup_{n=1}^{\infty} S_n$, it is sufficient to show $S_n \subseteq T_{[0,1]}$, for all n. If $\alpha \in S_n$, then, it follows from the definition of f_r that, for every $\delta > 0$, there exist infinitely many rational numbers $\frac{p}{q} \in (\alpha - \delta, \alpha + \delta)$ satisfying

$$\left|\frac{f_r\left(\frac{p}{q}\right) - f_r(\alpha)}{\frac{p}{q} - \alpha}\right| = \frac{\frac{1}{q^r}}{\left|\alpha - \frac{p}{q}\right|} > \frac{1}{n}.$$

Consequently, if $\alpha \in S_n$, then there are infinitely many rational numbers $\frac{p}{q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| < \frac{n}{q^r},$$

where $r > 2$. Thus, $\mu(\alpha) > r$, and $\alpha \in T_{[0,1]}$. ■

Corollary 11.2. *Let $r > 2$. The set S of points in $\mathbb{R}$ where f_r is not differentiable has measure zero.*

Proof. Proposition 10.1 and Proposition 11.1 imply that S has measure zero. ■

Thus, for $r > 2$, the function f_r is differentiable almost everywhere. We know it is differentiable at 0. The Thue-Siegel-Roth theorem provides a countable set of real numbers where f_r is differentiable for $r > 2$.

Corollary 11.3. *For $r > 2$, the function f_r is differentiable at all real algebraic numbers of degree $d \geq 2$.*

Proof. By the Thue-Siegel-Roth theorem, $\mu(\alpha) = 2$ for all real algebraic numbers α of degree $d > 2$. It follows immediately from Proposition 11.1 that f_r is differentiable at α, for $r > 2$. ■

In Section 13, we will note, without proof, that $\mu(e) = 2$ and $\mu(\pi) \leq 8.02$. It follows that f_r is differentiable at e for $r > 2$, and that f_r is differentiable at π for $r > 8.02$. This gives rise to the question of whether, for a given transcendental number η, there is a real number r such that f_r is differentiable at η.

12. An Application to Diophantine Equations

We give an application of the Thue-Siegel-Roth theorem to Diophantine equations. The result on solutions of Diophantine equations which we will prove follows from the fact that the approximation exponent of an algebraic number α of degree $d \geq 3$ is strictly less than d. The full force of Roth's theorem is not needed. Thue's theorem is sufficient.

Theorem 12.1. *Let*

$$a_d X^d + a_{d-1} X^{d-1} + ... + a_1 X + a_0 \in \mathbb{Z}[X] \tag{35}$$

be a polynomial, irreducible over $\mathbb{Q}$, and of degree $d \geq 3$. Then, for any nonzero integer m, the Diophantine equation

$$a_d X^d + a_{d-1} X^{d-1} Y + ... + a_1 X Y^{d-1} + a_0 Y^d = m \tag{36}$$

has only finitely many integer solutions (p, q).

Proof. Let $\alpha_1, ..., \alpha_d$ be the algebraic numbers that are the roots of (35) in an algebraic closure $\overline{\mathbb{Q}}$. Write (36) in the form

$$\left(\frac{X}{Y} - \alpha_1\right)\left(\frac{X}{Y} - \alpha_2\right)\cdots\left(\frac{X}{Y} - \alpha_d\right) = \frac{m}{a_d Y^d}. \tag{37}$$

We may assume that (36) has an integer solution (p, q), with $q \neq 0$. We will show that q is bounded. Set $A = \min |\alpha_i - \alpha_j|$ for $i \neq j$. It is straightforward to check that at most one α_j satisfies

$$\left|\alpha_j - \frac{p}{q}\right| < \frac{A}{2}.$$

If such an α_j exists, then by Corollary 9.2, for a fixed δ with $0 < \delta < 1$, there is a constant $c(\alpha_j, \delta) > 0$ such that

$$\left|\alpha_j - \frac{p}{q}\right| \geq \frac{c(\alpha_j, \delta)}{|q|^{\frac{1}{2}d+1+\delta}}$$

for all rational numbers $\frac{p}{q}$. For all other roots α_i, we have $\left|\frac{p}{q} - \alpha_i\right| \geq \frac{A}{2}$. Consequently, (37) implies that

$$\frac{|m|}{|a_d||q|^d} > \left(\frac{A}{2}\right)^{d-1}\left(\frac{c(\alpha_j, \delta)}{|q|^{\frac{1}{2}d+1+\delta}}\right).$$

Thus, there is a constant $C > 0$ depending only on $\alpha_1, ..., \alpha_d$ and δ so that

$$|m| > C|q|^{\frac{1}{2}d-1-\delta},$$

which confirms that q is bounded. If no such α_j exists, we have $\left|\frac{p}{q} - \alpha_i\right| \geq \frac{A}{2}$, for $1 \leq i \leq d$. Thus (37) implies that

$$\frac{|m|}{|a_d||q|^d} > \frac{A^d}{2^d}$$

and that $|m| > C|q|^d$, where $C > 0$ depends only on the α_i, and again q is bounded. However, for any fixed q, the number of p satisfying (36) is finite. Thus there are only finitely many solutions of (36). ■

Remark. An equation of the form (36) is called a *Thue equation*.

It is interesting to note that equations of the form $X^2 - dY^2 = 1$, where d is a positive square free integer, the so called *Pell's equations*, have infinitely many integer solutions, whereas, by the theorem just proved, the equations $X^3 - dY^3 = 1$, for any integer d, have at most finitely many solutions. The exercises outline a proof that a Pell equation has infinitely many integer solutions. The following example illustrates that one integer solution, found by inspection, generates infinitely many solutions.

Example. Consider the equation

$$X^2 - 2Y^2 = 1,$$

which factors into

$$(X + \sqrt{2}Y)(X - \sqrt{2}Y) = 1.$$

As a result, a solution (x, y) of the equation yields a unit $x+y\sqrt{2}$ in the ring $\mathbb{Z}[\sqrt{2}]$ with $(x + y\sqrt{2})^{-1} = (x - y\sqrt{2})$. Since $(3, 2)$ is a solution, it follows that $u = 3 + 2\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. For each positive integer n, we have that $u^n = a_n + b_n\sqrt{2}$ is also a unit in $\mathbb{Z}[\sqrt{2}]$. Consequently, the (a_n, b_n) are solutions of $X^2 - 2Y^2 = 1$.

For other applications of the Thue-Siegel-Roth theorem to Diophantine equations see, for example, [HS00].

Exercise 12.2.

The following exercises give a proof, see [IR90], that each Pell equation has infinitely many integer solutions. This fact may also be proved by means of continued fractions, see [Bur00] or [Ros93], for example.

(i) Let d be a positive square free integer. Show that there is a constant M such that the inequality

$$|x^2 - dy^2| < M$$

has infinitely many integer solutions (x, y) with $y > 0$. Conclude that there is an integer m such that $X^2 - dY^2 = m$ has infinitely many integer solutions (x, y) with $x > 0$ and $y > 0$.

In part (ii) we use the ring $\mathbb{Z}[\sqrt{d}]$. If $\gamma = x + y\sqrt{d}$ in $\mathbb{Z}[\sqrt{d}]$, define the conjugate γ' of γ by $\gamma' = x - y\sqrt{d}$ and the norm $N(\gamma)$ by $N(\gamma) = x^2 - dy^2$. We use the multiplicative property of the norm, namely that for δ in $\mathbb{Z}[\sqrt{2}]$, $N(\gamma\delta) = N(\gamma)N(\delta)$.
$(ii.)$ Show that the equation $X^2 - dY^2 = 1$ has an integer solution (x, y) with $xy \neq 0$. Hint: Show that two integer solutions $(x_1, y_1), (x_2, y_2)$ of $X^2 - dY^2 = m$ can be found such that $x_1 \neq x_2$, and

$$x_1 \equiv x_2 (\text{mod } m),\ y_1 \equiv y_2 (\text{mod } m).$$

Set $\alpha = x_1 + y_1\sqrt{d}$, and $\beta = x_2 + y_2\sqrt{d}$. Show that $\alpha\beta' = a + b\sqrt{d}$, where a and b are integer multiples of m. Now use the norm to argue to the existence of an integer solution (u, v) with $uv \neq 0$.

(iii) Let (u, v) be an integer solution. Show that, for every integer n, if $(u + v\sqrt{d})^n = a + b\sqrt{d}$, then (a, b) is also an integer solution.

Note that $u - v\sqrt{d} = (u + v\sqrt{d})^{-1}$.

Much more is true, see [IR90]. If solutions are ordered by $(x, y) < (u, v)$ if $x + y\sqrt{d} < u + v\sqrt{d}$, then there is a smallest solution $\alpha = (x, y)$ with $x > 0, y > 0$, and every solution $\beta = (u, v)$, satisfies $u + v\sqrt{d} = (x + y\sqrt{d})^n$, for a positive integer n.

13. What About Transcendental Numbers?

In the excellent survey [FN98], Feldman and Nesterenko convincingly demonstrate that rational approximation of algebraic numbers is an important tool in transcendental number theory. The construction of Liouville numbers (Section 8.2) is evidence of this. We close this chapter with several illustrations of applications of rational approximation to the study of the "familiar" transcendental numbers, e and π. Readers are encouraged to use these examples as a starting point for a full fledged study of rational approximation in transcendental number theory. Another useful reference is Chapter 11 of [BB87]. What we present here is taken from the illuminating article [Beu00] by Beukers.

Consider e, the base of the natural logarithm. The observation below leads to a simple proof that e is irrational.

Observation 13.1. *Let α be a real number. Suppose there exists a sequence of rational numbers $\frac{p_1}{q_1}, ..., \frac{p_n}{q_n}, ...$ satisfying*

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{\epsilon_n}{q_n},$$

where $\epsilon_n \to 0$ as $n \to \infty$. Then α is irrational.

Proof. Suppose, on the contrary, that $\alpha = \frac{p}{q}$ is a rational number. For every n, the difference $\left|\alpha - \frac{p_n}{q_n}\right|$ is a positive rational number with denominator dividing qq_n, so

$$\left|\alpha - \frac{p_n}{q_n}\right| \geq \frac{1}{qq_n}.$$

Consequently, we have

$$0 < \frac{1}{qq_n} < \frac{\epsilon_n}{q_n},$$

and it follows that

$$0 < \frac{1}{q} < \epsilon_n.$$

This contradicts the fact that $\epsilon_n \to 0$ as $n \to \infty$. ■

Proposition 13.2. *e is irrational.*

Proof. We begin with the fact that

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + ... + \frac{1}{n!} + ... = \sum_{n\geq 0} \frac{1}{n!}.$$

For $n \geq 0$, set

$$\frac{p_n}{n!} = 1 + \frac{1}{1!} + ... + \frac{1}{n!}.$$

Then $e - p_n/n! = \delta_n$, where

$$\delta_n = \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + ...$$

We estimate δ_n as follows.

$$\begin{aligned} \delta_n &= \frac{1}{(n+1)!}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + ...\right) \\ &< \frac{1}{(n+1)!}\left(1 + \frac{1}{1!} + \frac{1}{2!} + ...\right) \\ &= \frac{e}{(n+1)n!}. \end{aligned}$$

Thus,

$$0 < e - \frac{p_n}{n!} < \frac{e}{(n+1)n!}.$$

We set $\epsilon_n = e/(n+1)$ and apply Observation 13.1 to conclude that e is irrational. ■

It is usually quite difficult to compute the approximation exponent of a particular transcendental number. However, the approximation exponent for e has been known for a long time. The simple continued fraction expansion (see [Old70] and [Coh06]) of e, found by Euler, provides a sequence of rational approximations of e from which its approximation exponent $\mu(e) = 2$ can be deduced. Unfortunately, the continued fraction expansion of π is not well understood. Other more intricate methods must be used. However, the underlying idea that an upper bound for $\mu(\pi)$ can be obtained from a sequence of "good quality" rational approximations to π remains the same.

The number $\mu(\pi)$ was not proved finite until 1953 when Mahler proved that $\mu(\pi) < 42$. Mahler's upper bound for $\mu(\pi)$ has gradually been lowered over the years. The most recent result that we are aware of is due to Hata. In 1993 he proved, by constructing a sequence of good quality rational approximations to π, that $\mu(\pi) \leq 8.02$. It is expected that $\mu(\pi) = 2$.

For a description of the progressive lowering of an upper bound for $\mu(\pi)$ from 42 to 8.02, see [Beu00]. Here, following [Beu00], we give an example of how an upper bound for the approximation exponent of α can be deduced

from a particular sequence of "good quality" rational approximations to α. Another example is in the exercises.

Proposition 13.3. *Let α be a real number. Suppose that there is a sequence of rational approximations*

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, ..., \frac{p_n}{q_n}, ...$$

to α and suppose there exist real numbers $\epsilon > 0$ and $Q > 1$ with the following properties:

(i) $\frac{p_n}{q_n} \neq \frac{p_{n-1}}{q_{n-1}}$, *for all* n;

(ii) $q_n < Q^n$, *for all* n;

(iii) $\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{Q^{(1+\epsilon)n}}$.

Then

$$\mu(\alpha) \leq 1 + \frac{1}{\epsilon}.$$

Proof. We must show that, for any $\delta > 0$, there are only finitely many rational numbers $\frac{p}{q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{(1+\frac{1}{\epsilon}+\delta)}}.$$

To do that, let $\frac{p}{q}$ be any rational number. Choose n such that

$$Q^{\epsilon n} \geq 2q > Q^{\epsilon(n-2)}. \tag{38}$$

If m is the least positive integer satisfying $Q^{\epsilon m} \geq 2q$, then $m+1$ and m are the two possible choices for n. Choose one that satisfies $\frac{p_n}{q_n} \neq \frac{p}{q}$. This is possible by *(i)*.

From *(iii)* we deduce

$$\frac{1}{qq_n} \leq \left|\frac{p_n}{q_n} - \frac{p}{q}\right| \leq \left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Q^{(1+\epsilon)n}} + \left|\alpha - \frac{p}{q}\right|. \tag{39}$$

Since $2q \leq Q^{\epsilon n}$, we have, by Equations 38, 39 and *(ii)*,

$$\frac{1}{qQ^n} < \frac{1}{qq_n} \leq \frac{1}{Q^n Q^{\epsilon n}} + \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2qQ^n} + \left|\alpha - \frac{p}{q}\right|. \tag{40}$$

It follows that

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{2qQ^n}. \tag{41}$$

(Note that Equations (40) and (41) show why $2q$, and not q, is needed in Equation 38.) From $2q > Q^{\epsilon(n-2)}$ we obtain

$$Q^n < (2q)^{\frac{1}{\epsilon}\left(\frac{n}{n-2}\right)}.$$

Thus, for a given $\frac{p}{q}$, there is a positive integer n so that

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{(2q)^{1+\frac{1}{\epsilon}\left(\frac{n}{n-2}\right)}}.$$

If we let $q \to \infty$, then $2q \leq Q^{\epsilon n}$ for the corresponding n, so $n \to \infty$ and $\frac{1}{n-2} \to 0$.

Suppose, contrary to the statement of the proposition, that there is a real number $\delta > 0$, and there are infinitely many rational numbers $\frac{p}{q}$ such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{1+\frac{1}{\epsilon}+\delta}}\ .$$

Then q is not bounded, and we have

$$\frac{1}{(2q)^{1+\frac{1}{\epsilon}+\frac{1}{\epsilon}\left(\frac{2}{n-2}\right)}} < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{1+\frac{1}{\epsilon}+\delta}}\ .$$

Accordingly,

$$q^{\delta} < 2^{1+\frac{1}{\epsilon}+\frac{1}{\epsilon}\left(\frac{2}{n-2}\right)}\ q^{\frac{1}{\epsilon}\left(\frac{2}{n-2}\right)}.$$

Since $q^{\delta} \to \infty$ and $n \to \infty$ with q, the inequality above is impossible for large q. This contradiction demonstrates that, for all real numbers $\delta > 0$, there are only a finite number of such approximations $\frac{p}{q}$. Consequently, $\mu(\alpha) \leq 1 + \frac{1}{\epsilon}$. ■

The difficult mathematics arises in producing such a sequence. We refer the reader to [Beu00] where Beukers describes several attempts to construct rational approximations to π satisfying the conditions of Proposition 13.3. One of these is successful; it is a variation of Hata's method.

Exercise 13.4 ([BB87])**.** Let α be a real number. Suppose that there is a sequence $\frac{p_n}{q_n}$ of rational numbers and a real number $\epsilon > 0$ such that

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{1+\epsilon}}$$

and

$$q_{n-1} < q_n < q_{n-1}^{1+\gamma_n},$$

where $\gamma_n \to 0$ as $n \to \infty$. Let $\delta > 0$ be a real number. Show that, for every rational number $\frac{p}{q}$, either

$$\frac{p}{q} = \frac{p_n}{q_n}$$

for some n, or

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{1+\frac{1}{\epsilon}+\delta}}$$

for all $\frac{p}{q}$ with q sufficiently large.

Bibliography

[Art91] M. Artin, *Algebra*, Prentice Hall, New Jersey, 1991.

[Bak75] A. Baker, *Transcendental Number Theory*, Cambridge Univ. Press, Cambridge, 1975.

[Beu00] F. Beukers, *A rational approach to* π., Nieuw Archief voor Wiskunde **5/1** (2000), no. 4, 372-379.

[BB87] J. M. Borwein and P. B. Borwein, *Pi and the ACM*, Canad. Math. Soc. Monographs and Advanced Texts, John Wiley & Sons, New York, 1987.

[Bur00] E. M. Burger, *Exploring the Number Jungle: a Journey into Diophantine Analysis*, The Student Mathematical Library, vol. 8, Math. Assoc. of America, Washington, D. C., 2000.

[Cas57] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge Tracts in Mathematics and Mathematical Physics, vol. 45, Cambridge University Press, Cambridge, 1957.

[Coh06] H. Cohn, *A short proof of the simple continued fraction expansion of e*, Amer. Math. Monthly **113** (2006), 57-62.

[DF99] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 2nd ed., John Wiley & Sons, New York, 1999.

[FN98] N. I. Feldman and Yu. V. Nesterenko, *Transcendental Numbers*: *Number Theory IV*, EMS, vol. 44, Springer, Berlin, 1998.

[Gel03] A. O. Gelfond, *Transcendental and Algebraic Numbers*, Dover Phoenix Editions, Dover, New York, 2003.

[HW98] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, Clarenden Press, Oxford, 1998.

[HS00] M. Hindry and J. H. Silverman, *Diophantine Geometry, An Introduction* **201** (2000).

[IR90] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.

[Khi64] A. Khinchin, *Continued Fractions*, University of Chicago Press, Chicago, 1964.

[Mah32] K. Mahler, *Zur approximation der exponentialfunktion und des logarithmus, I, II*, J. reine angew. Math. **166** (1932), 118-136,136-150.

[Mah37] ———, *Arithmetische Eigenschaften einer Klasse von Dezimalbruchen*, Proc. Kon. Nederlansche Akad. Wetensch. **40** (1937), 421-428.

[Old70] C. D. Olds, *The simple continued fraction expansion of e*, Amer. Math. Monthly **77** (1970), 968-974.

[Per50] O. Perron, *Die Lehre von den Kettenbrüchen*, Chelsea, New York, 1950.

[RSN90] F. Riesz and B. Sz-Nagy, *Functional Analysis*, Dover Books on Advanced Mathematics, Dover, New York, 1990.

[Ros93] K. H. Rosen, *Elementary Number Theory and Its Applications*, 3rd ed., Addison-Wesley, Reading, MA, 1993.

[Rot55] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1-20.

[Sal08] P. J. Sally Jr., *Foundations of Modern Analysis*, 2008.

[Sch80] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Math., vol. 785, Springer-Verlag, Berlin, 1980.

[Sie66] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Collected Works (1966), 209-266.

[ST92] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

[Sto74] K. B. Stolarsky, *Algebraic Numbers and Diophantine Approximation*, Pure and Applied Mathematics, vol. 26, Marcel Dekker, New York, 1974.

[Thu09] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. reine angew. Math. **135** (1909), 284-305.

[Wil62] J. H. Williamson, *Lebesgue Integration*, Holt, Rinehart and Winston, New York, 1962.