Diophantine Approximations

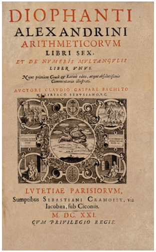
Leo Ouyang
layoouyang@gmail.com

Euler Circle

July 4, 2022

What are Diophantine Approximations?

Diophantine Approximations was named after Diophantus of Alexandria, an Alexandrian mathematician and author of *Arithmetica*. Diophantine Approximations are the approximations of real numbers using rational numbers.



Some Definitions

Definition

We say a number is **rational** if it can be written in the form $\frac{p}{q}$ for integers p and q. We say a number is **irrational** if it is not rational.

Upper Bound

Dirichlet was the first who achieved a major result for the upper bound of Diophantine Approximations.

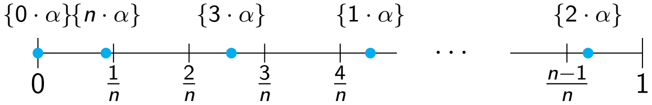
Theorem (Dirichlet's Approximation Theorem)

Let α be an irrational number. There exists a fraction p/q, where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, such that

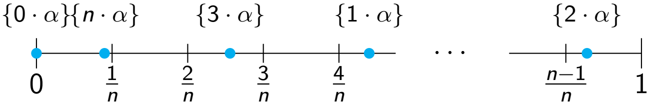
$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{0.1}$$

Proof of Dirichlet's Approximation Theorem

Let $n \geq 1$ be an integer. Let $\{x\}$ be the fractional part of x.
Consider the $n + 1$ fractional parts: $\{0 \cdot \alpha\}, \{1 \cdot \alpha\}, \ldots, \{n \cdot \alpha\}$.
Consider the n sub-intervals: $\left[0, \frac{1}{n}\right), \left[\frac{1}{n}, \frac{2}{n}\right), \ldots \left[\frac{n-1}{n}, 1\right)$.

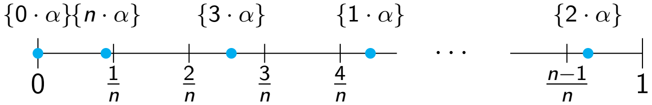


Proof of Dirichlet's Approximation Theorem Continued



By the Pigeonhole Principle, there exists two integers $0 \leq j < k \leq n$ such that $\{j \cdot \alpha\}$ and $\{k \cdot \alpha\}$ belong in the same sub-interval. That means that $|k\alpha - j\alpha|$ minus some integer p equals a number less than $\frac{1}{n}$.

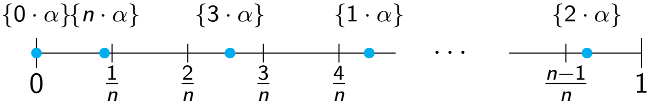
Proof of Dirichlet's Approximation Theorem Continued



By the Pigeonhole Principle, there exists two integers $0 \leq j < k \leq n$ such that $\{j \cdot \alpha\}$ and $\{k \cdot \alpha\}$ belong in the same sub-interval. That means that $|k\alpha - j\alpha|$ minus some integer p equals a number less than $\frac{1}{n}$. Thus,

$$|(k-j)\alpha - p| < \frac{1}{n}.$$

Proof of Dirichlet's Approximation Theorem Continued



By the Pigeonhole Principle, there exists two integers $0 \leq j < k \leq n$ such that $\{j \cdot \alpha\}$ and $\{k \cdot \alpha\}$ belong in the same sub-interval. That means that $|k\alpha - j\alpha|$ minus some integer p equals a number less than $\frac{1}{n}$. Thus,

$$|(k-j)\alpha - p| < \frac{1}{n}.$$

Setting $q = k - j$ and dividing by q on both sides, we get

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

Corollary of Dirichlet's Approximation Theorem

Corollary

There are infinitely many irreducible fractions p/q such that

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

Corollary of Dirichlet's Approximation Theorem

Corollary

There are infinitely many irreducible fractions p/q such that

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

Proof.

We can use the previous proof strategy to get

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Nq},$$

Corollary of Dirichlet's Approximation Theorem

Corollary

There are infinitely many irreducible fractions p/q such that

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

Proof.

We can use the previous proof strategy to get

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Nq},$$

which yields a sequence of inequalities

$$|q_n\alpha - p_n| < \frac{1}{N_n}.$$

Further work on the Upper Bound

Dirichlet's Approximation Theorem was further improved later on by Adolf Hurwitz.

Theorem (Hurwitz's Theorem)

If α is irrational, then there are infinitely many rational numbers p/q satisfying

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

Some More Definitions

Definition

We call the **degree** the highest exponent of a polynomial. (Example: 2 would be the degree of the polynomial $x^2 + 2x + 1$.)

Definition

We say $\alpha \in \mathbb{C}$ is an **algebraic number** if it is a root of a polynomial with a finite degree and integer coefficients. (Examples: 2 or $\Phi = \frac{1+\sqrt{5}}{2}$).

Definition

We say a number is **transcendental** if it is not an algebraic number.

Liouville's Theorem

Now we move onto the lower bound of Diophantine Approximations.

Theorem (Liouville's Approximation Theorem (1840))

If α is an irrational algebraic number of degree $n > 1$, there exists a constant $c(\alpha)$ such that

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

for all rationals $\frac{p}{q}$, where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$.

Proof of Liouville's Theorem

Let $f(z) = a_0 + a_1 z + \cdots + a_n z^n$ be the minimal polynomial, a polynomial with integer coefficients of smallest degree, having α as a root.

Proof of Liouville's Theorem

Let $f(z) = a_0 + a_1 z + \cdots + a_n z^n$ be the minimal polynomial, a polynomial with integer coefficients of smallest degree, having α as a root.

Then let p/q be a rational number such that $\left|\frac{p}{q} - \alpha\right| < 1$.

Proof of Liouville's Theorem

Let $f(z) = a_0 + a_1 z + \cdots + a_n z^n$ be the minimal polynomial, a polynomial with integer coefficients of smallest degree, having α as a root.

Then let p/q be a rational number such that $\left|\frac{p}{q} - \alpha\right| < 1$.

By the Mean Value Theorem,

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

where c is a real number that lies between α and p/q.

Proof of Liouville's Theorem Continued

Rearranging the previous equation we get:

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

Proof of Liouville's Theorem Continued

Rearranging the previous equation we get:

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

Let

$$M = \sup_{|z-\alpha|<1} \left| f'(z) \right|.$$

Proof of Liouville's Theorem Continued

Rearranging the previous equation we get:

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

Let

$$M = \sup_{|z-\alpha|<1} \left| f'(z) \right|.$$

Then we can say:

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

Proof of Liouville's Theorem Continued

Since $f(z)$ does not have any rational roots,

Proof of Liouville's Theorem Continued

Since $f(z)$ does not have any rational roots,

$$0 \neq f\left(\frac{p}{q}\right) = a_n \left(\frac{p}{q}\right)^n + \cdots + a_0 = \frac{a_n p^n + \cdots + a_1 p q^{n-1} + a_0 q^n}{q^n}.$$

Proof of Liouville's Theorem Continued

Since $f(z)$ does not have any rational roots,

$$0 \neq f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + \cdots + a_0 = \frac{a_n p^n + \cdots + a_1 p q^{n-1} + a_0 q^n}{q^n}.$$

The numerator has an absolute value of at least 1.

Proof of Liouville's Theorem Continued

Since $f(z)$ does not have any rational roots,

$$0 \neq f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + \cdots + a_0 = \frac{a_n p^n + \cdots + a_1 p q^{n-1} + a_0 q^n}{q^n}.$$

The numerator has an absolute value of at least 1.

Thus,

$$\left|f\left(\frac{p}{q}\right) - f(\alpha)\right| = \left|f\left(\frac{p}{q}\right)\right| = \frac{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n}{q^n} \geq \frac{1}{q^n}.$$

Proof of Liouville's Theorem Continued

Combining the two equations, we get:

$$\frac{1}{q^n} \leq M\left|\alpha - \frac{p}{q}\right| \implies \frac{1}{Mq^n} \leq \left|\alpha - \frac{p}{q}\right|.$$

Proof of Liouville's Theorem Continued

Combining the two equations, we get:

$$\frac{1}{q^n} \leq M \left| \alpha - \frac{p}{q} \right| \implies \frac{1}{Mq^n} \leq \left| \alpha - \frac{p}{q} \right|.$$

Writing $\frac{1}{c(\alpha)}$ as M, we achieve:

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

■

Liouville's Constant

This result allowed Liouville to discover the first proven example of a transcendental number, the Liouville constant.

$$\sum_{i=0}^{\infty} 10^{-i\,!} = 0.110001000000000000000001000\ldots.$$

Part of the proof also included how this transcendental number doesn't satisfy Liouville's Theorem.

Lower Bound Discoveries

A lower bound would be a result of the form:
Say α is an irrational algebraic number of degree $n \geq 2$. Then there are infinitely many rational numbers p/q that satisfy the inequality

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

where κ is some exponent.

Over time, mathematicians would improve the accuracy of Liouville's Theorem with the value of κ.

Improvements by Thue, Siegel, Dyson, and Roth

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

Improvements by Thue, Siegel, Dyson, and Roth

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

Thue (1908): $\kappa \leq \frac{1}{2}n + 1.$

Improvements by Thue, Siegel, Dyson, and Roth

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

Thue (1908): $\kappa \leq \frac{1}{2}n + 1.$

Siegel (1921): $\kappa \leq s + \frac{n}{s+1}$ for $s = 1, 2, \ldots, n-1.$

Improvements by Thue, Siegel, Dyson, and Roth

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

$$\text{Thue (1908): } \kappa \le \frac{1}{2}n + 1.$$

$$\text{Siegel (1921): } \kappa \le s + \frac{n}{s+1} \text{ for } s = 1, 2, \ldots, n-1.$$

$$\text{Dyson (1947): } \kappa \le \sqrt{2n}.$$

Improvements by Thue, Siegel, Dyson, and Roth

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

Thue (1908): $\kappa \leq \frac{1}{2}n + 1.$

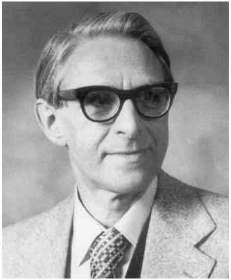
Siegel (1921): $\kappa \leq s + \frac{n}{s+1}$ for $s = 1, 2, \ldots, n-1.$

Dyson (1947): $\kappa \leq \sqrt{2n}.$

Roth (1955): $\kappa \leq 2.$

Thue-Siegel-Roth's Theorem

All of these improvements would later combine into one single theorem: the Thue-Siegel-Roth's theorem.



Theorem (Thue-Siegel-Roth's Theorem)

There exists a positive constant $c(\alpha, \epsilon)$ such that

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

holds for every rational number p/q.

Key Elements of Thue-Siegel-Roth's Theorem

Let $P(z) = a_0 + a_1 z + \cdots + a_n z^n$ be a polynomial with complex coefficients.

Then $||P|| = \max\{|a_0|, |a_1|, \ldots, |a_n|\}$. Furthermore, if α is algebraic over $\mathbb{Q}$ with its minimal polynomial $f(z)$ over $\mathbb{Q}$, we define the *height* $H(\alpha) = ||f||$.

This was used to help make numerous inequalities and properties between polynomials. Also helps when analyzing algebraic coefficients within a polynomial.

Key Elements Continued

Generalized Wronskians

$$W(z) = \begin{vmatrix} \frac{1}{0!}f_0(z) & \frac{1}{0!}f_1(z) & \cdots & \frac{1}{0!}f_{l-1}(z) \\ \frac{1}{1!}f_0'(z) & \frac{1}{1!}f_1'(z) & \cdots & \frac{1}{1!}f_{l-1}'(z) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{(l-1)!}f_0^{(l-1)}(z) & \frac{1}{(l-1)!}f_1^{(l-1)}(z) & \cdots & \frac{1}{(l-1)!}f_{l-1}^{(l-1)}(z) \end{vmatrix}$$

$$= \det\left(\frac{1}{\mu!}\frac{d^\mu}{dz^\mu}f_v(z)\right),\ \mu,\ v = 0, 1, \ldots, l-1.$$

This was used to relate the Wronskians and determinants to monomials' exponents.