Diophantine Approximation : A Chronological Survey

Li Du*
Math 336 Term Paper
(Dated: June 6, 2017)

This paper presents the development of Diophantine approximation through history, with motivation and major results from this field. This paper could be read as a survey into this particular subject, or as a compilation of elegant proofs reminding one of the minimalistic beauty of mathematics. We follow the main theme of approximating irrationals, introducing and proving beautiful results along the way. This includes Weyl's criterion for equidistribution, Dirichlet's solution to Pell's equation, Hurwitz's theorem and Minkowski's Convex Body theorem. We will use techniques from a wide range to prove these results, including continued fractions, Fourier series, and modulo arithmetic.

I. INTRODUCTION

The necessity of approximating irrational numbers arises in many context in mathematics. The Pythagorean school used to believe that the only number existed is the now-called rational numbers, until someone discovered the length of an equilateral right triangle violates this principle. The ancient Greeks then encountered the equation $x^2 - 2y^2 = 1$ when trying to understand $\sqrt{2}$ and discovered a way to construct an infinite sequence of rationals that approximates $\sqrt{2}$ better with each term ([14], Page 77). This is often introduced in introductory analysis texts to show that the rational field $\mathbb{Q}$ does not satisfy the Dedekind completeness, i.e. the Least Upper Bound property.

Another motivation for Diophantine approximation arises in solving the alleged Pell equation (wrongly attributed to Pell by Euler, see [14] page 76), which takes the form $x^2 - ny^2 = 1$ where x and y can only take on integer values. People have discovered how to construct infinitely many integer solutions to this equation given a nontrivial solution (solution not equal to $(\pm 1, 0)$) at around 600 CE, and that such sequence of solutions can approximate $\sqrt{n}$ arbitrarily close. However, the existence of such solution was not proven until Lagrange first published his proof in 1768 (see [14]). Here, we'll present a cleaner proof which is a beautiful consequence of Dirichlet's approximation theorem.

The approximation of irrational through rational numbers also inspired one of most important field of mathematics invented in 19^{th} century: the Geometry of numbers. Nowadays, the geometry of numbers is not only interesting to mathematicians, but computer scientists as well. One of most fundamental results in this fields, the Minkowski's convex body theorem, greatly reduces a problem that has trapped computer scientists for a very long time. In the last section of this paper, we will introduce and prove the Minkowski's convex body theorem and see how it relates to the mission of approximating irrationals.

* dul2@uw.edu

II. THE IRRATIONALS AND DIRICHLET'S THEOREM

The irrationals exhibit mysterious behaviours in many areas and is thus worthwhile to be studied. In this section, we present a basic theorem that sheds light on how irrationals can be approximated by rationals. We'll further explore how they interact with integers and rationals in general through several other results.

While studying the solution of Pell's equation around 1840, Dirichlet discovered an approximation theorem that becomes the starting point of Diophantine Approximation. In this interesting proof, he employed a technique that is now called the "pigeonhole principle". This principle, following from simple logic, states that when $k+1$ pigeons go into k boxes, at least one box contains at least two pigeons. In fact, this simple but useful principle was first formalized by Dirichlet (see [12]), and is widely referred to as "the Drawer Principle" in countries outside of U.S. as this is how Dirichlet called it himself. Here, we follow the version of this theorem presented in [14] with a slight generalization. Note, however, that other sources ([13], [2]) present this theorem as $|\alpha - p/q| < 1/Bq$, which is equivalent.

Theorem 1 ***(Dirichlet, 1842)*** *Let α be an irrational number and integer $B > 0$, there exists integers a, b with $0 < b < B$ such that*

$$|a - b\alpha| < \frac{1}{B}$$

Proof. Given an integer B, consider the $B-1$ numbers $\alpha, 2\alpha, \ldots, (B-1)\alpha$. We know that for any number $k\alpha$ in this sequence, we can choose an $A_k \in \mathbb{Z}$ that satisfies the strict inequality

$$0 < A_k - k\alpha < 1.$$

The strictness of the inequality follows from the choice of α being irrational. Note that the irrationality of α also implies $\forall i \neq j$, $A_i - i\alpha \neq A_j - j\alpha$. So we now have $B+1$ distinct numbers that fall into the interval $[0, 1]$:

$$0, \quad A_1 - \alpha, \quad A_2 - 2\alpha, \ldots, \quad A_{B-1} - (B-1)\alpha, \quad 1$$

We then divide this interval into B subintervals of length $1/B$. By pigeonhole principle, at least two numbers must

fall into the same subinterval. The difference between these two numbers takes the form $a - b\alpha$ where $a, b \in \mathbb{Z}$ and satisfy

$$|a - b\alpha| < \frac{1}{B}$$

□

This result admits many elaborations and strenghtenings. Here, we present one that unveils an interesting property about the irrationals [13].

Corollary 2 *For α irrational, there exists infinitely many relatively prime numbers p, q such that*

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

Proof. Suppose there are only finitely many rationals

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}$$

satisfying:

$$|\alpha - \frac{p_i}{q_i}| < \frac{1}{q_i^2}.$$

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

$$\left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{n+1}$$

holds for $1 \leq i \leq k$. However, this contradicts Dirichlet's Theorem, which asserts that, for this n, there exists a rational number p/q with $q \leq n$ such that

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

□We point out another property about the irrational numbers:

Theorem 3 *A real number α is irrational* ***if and only if*** *there are infinitely many rational numbers $\frac{p}{q}$ such that*

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

One direction in this statement follows directly from the theorem we just proved. A complete proof can be found in [11]. This theorem is interesting to note here due to its implication: it appears that irrational numbers can be distinguished from rational numbers by the fact that they can be approximated by infinitely many rational numbers p/q with an error less than $1/q^2$.

A more fascinating behaviour about the irrationals is exhibited through the equidistribution modulo $\mathbb{Z}$ of many sequences involving irrationals. Before we derive this result formally, we first introduce the notion of *equidistribution*. Below is a more intuitive definition for *equidistribution*, which is basically saying that, in its limit form, the integer multiples of an irrational number "spread out" evenly on the interval $[0, 1]$ w.r.t. its fraction part.

Definition: A real sequence $\{x_n\}_{n=1}^{\infty}$ is said to be *equidistributed modulo 1* if for every pair of real numbers $0 \leq a < b \leq 1$, we have

$$\lim_{N\to\infty} \frac{\#\{n \leq N : (x_n) \in [a, b]\}}{N} = b - a$$

Now, we present another equivalent way of stating *equidistribution*, which will be more useful to the proof. We would like to focus on the discussion of Weyl's criterion and will just assume this result. However, a proof could be found in chapter 11 in [9].

Theorem 4 *A real sequence $\{x_n\}_{n=1}^{\infty}$ is said to be equidistributed modulo 1 if and only if for every function f in $C^0[0, 1]$, we have"*

$$\lim_{n\to\infty} \frac{1}{N} \sum_{n=1} Nf(x_n) \int_0^1 f(x)dx$$

Now we use this definition to prove an elegant criteria by Weyl for determining whether a sequence is equidistributed in $[0, 1]$.

Theorem 5 ***(Weyl, 1916****, see[9]) A sequence $\{x_n\}_{n=1}^{\infty}$ is equidistributed if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i n x_n} = 0$$

Proof. Define $\psi_n(\alpha) = e^{2\pi i n\alpha}$, then for any smooth function f with integer period, it admits Fourier expansion $\sum_n \hat{f}(n)\psi_n$ converging absolutely and uniformly to f (uniform is guaranteed by our smooth assumption). So

$$\begin{aligned}
\frac{1}{N} \sum_{m=1}^{N} f(x_m) &= \frac{1}{N} \sum_{m=1}^{N} \left(\sum_n \hat{f}(n)\psi_n(x_m) \right) \\
&= \frac{1}{N} \sum_n \hat{f}(n) \left(\sum_{n=1}^{N} \psi_n(x_m) \right) \\
&= \hat{f}(0) + \frac{1}{N} \sum_{n\neq 0} \hat{f}(n) \left(\sum_{n=1}^{N} \psi_n(x_m) \right)
\end{aligned}$$

For any cut-off b for the Fourier series, noting $\hat{f}(0) =$

$\int_0^1 f(x)dx$, we have:

$$\begin{aligned}
&\frac{1}{N}\sum_1^N f(x_m) - \int_0^1 f(x)dx \\
\leq &\left|\sum_{n\neq 0} \hat{f}(n)\cdot\left(\frac{1}{N}\cdot\sum_1^N \psi_n(x_m)\right)\right| \\
\leq &\sum_{n\neq 0}|\hat{f}(n)|\cdot\left|\frac{1}{N}\sum_1^N \psi_n(x_m)\right| \\
\leq &\sum_{0<|n|\leq b}|\hat{f}(n)|\cdot\left|\frac{1}{N}\cdot\sum_1^N \psi_n(x_m)\right| + \sum_{|n|>b}|\hat{f}(n)|\cdot 1
\end{aligned}$$

Since the Fourier series converges absolutely, given $\epsilon > 0$ there is large enough b so that $\sum_{|n|>b}|\hat{f}(n)| < \epsilon$. With that b, since $\frac{1}{N}\sum_1^N \phi_n(x_m) \to 0$ for each fixed $n \neq 0$, and since there are only finitely many n with $0 < |n| \leq b$, for large enough N:

$$\sum_{0<|n|\leq b}|\hat{f}(n)|\cdot\left|\frac{1}{N}\sum_1^N \psi_n(x_m)\right| < \epsilon$$

Thus,

$$\left|\frac{1}{N}\sum_1^N f(x_m) - \hat{f}(0)\right| \leq 2\epsilon$$

That is, $1/N\cdot\sum_1^N f(x_m) \to \int_0^1 f(x)dx$, and by the equidistribution definition above, we have shown that Weyl's criterion suffices for equidistribution. □

Equipped with this powerful result, we can see that many interesting results almost follows immediately.

Corollary 6 *Given any irrational α, the sequence $\{n\alpha\}_{n=1}^{\infty}$ is equidistributed modulo 1.*

Proof. We sum over the geometric series:

$$\frac{1}{N}\sum_{l=1}^N e^{2\pi i n\cdot l\alpha} = \frac{1}{N}\cdot\frac{e^{2\pi i n\alpha} - e^{2\pi i n(N+1)\alpha}}{1 - e^{2\pi i n\alpha}}$$

The irrationality of α and $n \neq 0$ assure that the denominator does not vanish. Thus,

$$\frac{1}{N}\sum_{l=1}^N e^{2\pi i n\cdot l\alpha} \leq \frac{1}{N}\cdot\frac{2}{|1 - e^{2\pi i n\alpha}|} \to 0$$

for each fixed $n \neq 0$. By Weyl's criterion, $\{l\alpha\}$ is equidistributed modulo 1. □

Note the profound implication of this result: we can now say more than just $\lfloor n\alpha \rfloor$ is dense in $[0, 1]$. We can conclude that this sequence distributed evenly, in its limit form, among this entire interval. This is an elegant result that conforms to our intuition, and has further surprising real world implications. For example, one could see how Benford's Law could be explained with this and several other equidistribution sequences, because $\log n$ where n is not a power of 10 is irrational. For a concrete discussion of this subject, see Chapter 9 in [7].

Remark: Another interesting proof for Corollary 6 can be found in [3] chapter 23.10, which involves the continued fraction technique. We direct interested reader to this source.

III. SOLUTION TO PELL EQUATION WITH DIRICHLET'S THEOREM

Recall that **Pell Equation** refers to the equation $x^2 - ny^2 = 1$ where n is not a perfect square number. In the context of number theory, we are generally interested to find the integer solutions to this equation. So when we say *solutions to the Pell equation* in this paper, we mean integer solution. As we said in the introduction, people have long understood how to construct infinitely many solution:

Theorem 7 ***(Brahmagupta composition rule, circa 600 CE)*** *If (x_1, x_2) and (x_2, y_2) are both solutions (not necessarily different) to the Pell equation $x^2 - ny^2 = 1$, then so is*

$$(x_3, y_3) = (x_1x_2 + ny_1y_2, x_1y_2 + y_1x_2)$$

Proof. Since (x_1, y_2) and (x_2, y_2) are solutions, we have:

$$x_1^2 - ny_1^2 = 1 = x_2^2 - ny_2^2$$

Therefore

$$\begin{aligned}
1 &= (x_1^2 - ny_1^2)(x_2^2 - ny_2^2) \\
&= (x_1 - \sqrt{n}y_1)(x_1 + \sqrt{n}y_1)\cdot(x_2 - \sqrt{n}y_2)(x_2 + \sqrt{n}y_2) \\
&= (x_1 - \sqrt{n}y_1)(x_2 - \sqrt{n}y_2)\cdot(x_1 + \sqrt{n}y_1)(x_2 + \sqrt{n}y_2) \\
&= [x_1x_2 + ny_1y_2 - (x_1y_2 + y_1x_2)\sqrt{n}]\cdot \\
&\quad\ [x_1x_2 + ny_1y_2 + (x_1y_2 + y_1x_2)\sqrt{n}] \\
&= (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + y_1x_2)^2 = x_3^2 - ny_3^2
\end{aligned}$$

□

However, even though we know how to construct solutions given only one nontrivial solution, the existence of such is not obvious at all. Sometimes it is very clear there is one: $(3, 2)$ is a nontrivial solution to $x^2 - 2y^2 = 1$. But to one's surprise, the smallest nontrivial solution to $x^2 - 61y^2 = 1$ is:

$$(x, y) = (1766319049, 226153980)$$

Such mysterious behaviour of the smallest nontrivial solution naturally generates the question: does it always exist? The stunning theorem below by Dirichlet proves that its existence is guaranteed. Before proceeding, we define a few terminology that would make the proof process easier:

1. Define $\mathbb{Z}[\sqrt{n}] = \{x + y\sqrt{n} : x, y \in \mathbb{Z}\}$.
2. We call $x - y\sqrt{n}$ the conjugate of $x + y\sqrt{n}$.
3. For each member in $\mathbb{Z}[\sqrt{n}]$, we associate a norm with it:

$$\text{norm}(x + y\sqrt{n}) = (x - y\sqrt{n})(x + y\sqrt{n}) = x^2 - ny^2$$

4. It is easy to check that $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{n}]$:

$$\text{norm}(\alpha)\text{norm}(\beta) = \text{norm}(\alpha\beta)$$

Theorem 8 ***(Dirichlet, 1842)*** *Given an non-square positive integer n, the equation $x^2 - ny^2 = 1$ has an integer solution $(a, b) \neq (\pm 1, 0)$.*

Proof. We follow the following steps to construct such solution:

1. Since Dirichlet's approximation theorem holds for all $B > 0$, we can make $1/B$ arbitrarily small, thus forcing the choice of new values of a and b. Thus *there are infinitely many integer pairs (a, b) with $|a - b\sqrt{n}| < 1/B$* . Since $0 < b < B$, we have

$$|a - b\sqrt{n}| < \frac{1}{b}$$

2. It follows from step 1 that

$$|a + b\sqrt{n}| \leq |a - b\sqrt{n}| + |2b\sqrt{n}| \leq |3b\sqrt{n}|$$

and therefore

$$|a^2 - nb^2| \leq \frac{1}{b} \cdot 3b\sqrt{n} = 3\sqrt{n}$$

Hence there are infinitely many $a - b\sqrt{n}$ such that

3. We apply the infinite version of the pigeonhole principle: if infinitely many pigeons go into k boxes, then at least one box contains infinitely many pigeons. And these results follows:
   - infinitely many $a - b\sqrt{n}$ with the same norm, N say,
   - infinitely many of these with a in the smae congruence class modulo N,
   - infinitely many of these with b in the same congruence class modulo N.
4. From step 3 we get two positive numebrs, $a_1 - b_1\sqrt{n}$ and $a_2 - b_2\sqrt{n}$, with
   - the same norm N
   - $a_1 \equiv a_2 \pmod{N}$
   - $b_1 \equiv b_2 \pmod{N}$

   This uses the quotient $a - b\sqrt{n}$ of the two numbers just found. Its norm $a^2 - nb^2$ is clearly 1 by the multiplicative property of norm. It is not so clear that a and b are integers, but this now follows fro the congruence conditions in step 4.

Consider the quotient $a - b\sqrt{n}$ of the two numbers $a_1 - b_1\sqrt{n}$ and $a_2 - b_2\sqrt{n}$ found in step 4. We have

$$\begin{aligned} a - b\sqrt{n} &= \frac{a_1 - b_1\sqrt{n}}{a_2 - b_2\sqrt{n}} \\ &= \frac{(a_1 - b_1\sqrt{n})(a_2 + b_2\sqrt{n})}{a_2^2 - nb_2^2} \\ &= \frac{a_1a_2 - nb_1b_2}{N} + \frac{a_1b_2 - b_1a_2}{N} \cdot \sqrt{n} \end{aligned}$$

where $N = a_2^2 - nb_2^2$ is the common norm of $a_1 - b_1\sqrt{n}$ and $a_2 - b_2\sqrt{n}$. Since the latter numbers have equal norms, their quotient $a - b\sqrt{n} \neq \pm 1$. It remains to to show that a and b are integers. This amounts to showing that N divides $a_1a_2 - nb_1b_2$ and $a_1b_2 - b_1a_2$ or that

$$a_1a_2 - nb_1b_2 \equiv a_2b_2 - b_1a_2 \equiv 0 \pmod{N}$$

The first congruence follwos fromt he fact that $a_1^2 - nb_1^2 = N$, which implies

$$0 \equiv a_1^2 - nb_1^2 \equiv a_1a_2 - nb_1b_2 \pmod{N}$$

replacing a_1 and b_1 by their respective congruent values $a_1 \equiv a_2 \pmod{N}$ and $b_1 \equiv b_2 \pmod{N}$ found in step 4.

the second congruence follows from $a_1 \equiv a_2 \pmod{N}$ and $b_1 \equiv b_2 \pmod{N}$ by multiplying to obtain $a_1b_2 \equiv a_2b_1 \pmod{N}$, in other words, $a_1b_2 - b_1a_2 \equiv 0 \pmod{N}$. □

IV. HURWITZ'S THEOREM AND CONTINUED FRACTIONS

(Proceed with relevant definition and corollaries 1.3 in [13] to deduce the main result which is Hurwitz's theorem presented in [2] ...)

Definition: The expression $[a_0, a_1, \ldots, a_n]$ such that all $a_i \geq 1$ are integers and $a_n \geq 2$, denotes a *finite simple continued fraction*, which means the following:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \quad \text{(continued until } \frac{1}{a_n}\text{)}$$

The rational numbers:

$$\frac{p_0}{q_0} = [a_0], \quad \frac{p_1}{q_1} = [a_0, a_1], \ldots, \quad \frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$$

are called *convergents*. For convenience of notation, we further define $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$.

Given this definition, we can now prove an array of useful and interesting properties of continued fractions, all of which will eventually lead us to the development of Hurwitz's theorem.

Lemma 9 *For $n \geq 0$,*

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2}$$

Proof. Proceed with induction. Base case for $n = 0$ is obvious. We now assume

$$p_{n-1} = a_{n-1} p_{n-2} + p_{n-3}, \quad q_{n-1} = a_{n-1} q_{n-2} + q_{n-3}$$

and show the inductive case:

$$\begin{aligned}
\frac{p_n}{q_n} &= [a_0, a_1, \ldots, a_n] \\
&= [a_0, a_1, \ldots, a_{n-1} + 1/a_n] \\
&= \frac{(a_{n-1} + \frac{1}{a_n}) p_{n-1} + p_{n-2}}{(a_{n-1} + \frac{1}{a_n}) q_{n-1} + q_{n-2}} \\
&= \frac{(a_n a_{n-1} + 1) p_{n-2} + a_n p_{n-1}}{(a_n a_{n-1} + 1) q_{n-2} + a_n q_{n-1}} \\
&= \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}
\end{aligned}$$

We now simply read off the denominator and numerator to get our results. □

Corollary 10 *For $n \geq -1$,*

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n$$

Proof. Base case for $n = -1$ is $q_{-1} p_{-2} - p_{-1} q_{-2} = (-1)^{-1}$ which is established. Now, assume the claim is true for $(n-1)$, we apply Lemma 9 and get:

$$\begin{aligned}
& q_n p_{n-1} - p_n q_{n-1} \\
=& (a_n q_{n-1} + q_{n-2}) p_{n-1} - (a_n p_{n-1} + p_{n-2}) q_{n-1} \\
=& -(q_{n-1} p_{n-2} - p_{n-1} q_{n-2}) \\
=& (-1)^n
\end{aligned}$$

So the claim is true for all $n \geq -1$. □

Corollary 11 *For $n \geq 0$,*

$$q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1} a_n$$

Proof. Base case for induction is obvious. We combine Lemma 9 and Corollary 10 to get:

$$\begin{aligned}
& a_n p_{n-2} - p_n q_{n-2} \\
=& (a_n q_{n-1} + q_{n-2}) p_{n-2} - (a_n p_{n-1} + p_{n-2}) q_{n-2} \\
=& a_n (q_{n-1} p_{n-2} - p_{n-1} q_{n-2}) \\
=& (-1)^{n-1} a_n
\end{aligned}$$

□

Corollary 12 *The convergents p_k/q_k satisfies the following inequalities:*

1. $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots$
2. $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \ldots$
3. *Given any positive even n and odd m, we have:*

$$\frac{p_n}{q_n} < \frac{p_m}{q_m}$$

Proof. We divide both sides by $q_{n-2} q_n$ in Corollary 11 and get:

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1} a_n}{q_{n-2} q_n}$$

This shows that when $n \geq 2$ and n is even, we know that $(n-2)^{\text{th}}$ term is less than n^{th} term. Similarly, when $n \geq 3$ and n is odd, we know that $(n-2)^{\text{th}}$ term is larger than n^{th} term. This establishes part *1* and *2*. Note that, to show *3* is true for arbitrary pair of odd and even numbers, we can simply show $p_{m-1}/q_{m-1} < p_m/q_m$ is true for all odd m, and combine with part *1* and *2* to conclude *3*. So we only need to show:

$$\begin{aligned}
& \frac{p_{m-1}}{q_{m-1}} < \frac{p_m}{q_m} \\
\Leftrightarrow \quad & q_m p_{m-1} - p_m q_{m-1} = (-1)^m < 0
\end{aligned}$$

This establishes the third inequality. □

We can see that the inequalities in Corollary 11 is foreshadowing the existence of a limit. Indeed, such limit not only exists, but is guaranteed to be irrational!

Corollary 13 *Let a_0 be an integer and $a_1, a_2, \ldots$ be positive integers, define p_k/q_k to be the convergents of the continued fractions defined by $\{a_n\}_{n=0}^{\infty}$. Then, the limit $\lim_{n\to\infty} p_k/q_k$ exists and its value is irrational. Conversely, for α irrational, there exists a unique integer a_0 and unique positive integers $a_1, a_2, \ldots$ such that $\alpha = \lim_{n\to\infty} p_k/q_k$.*

Proof. By the results we have proven: $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_1}{q_1}$, it is clear that both limits:

$$\lim_{n \text{ even} \to \infty} \frac{p_n}{q_n} \qquad \text{and} \qquad \lim_{n \text{ odd} \to \infty} \frac{p_n}{q_n}$$

exists (both are bounded monotone sequences). And further both limits are equal by their recurrence relation. We put $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$ and compute:

$$\left| \alpha - \frac{p_n}{q_n} \right| < \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

Since p_n, q_n are relatively prime, there exist infinitely many rational numbers p/q such that $|\alpha - p/q| < 1/q^2$, so α is irrational.

Conversely, let α be irrational, $a_0 = \lfloor \alpha \rfloor$, and let $\alpha_1 := a_0 + \frac{1}{\alpha_1}$. We notice that $\alpha_1 > 1$ is irrational. For $k \geq 1$ let $a_k = \lfloor \alpha_k \rfloor$ and $\alpha_k = a_k + \frac{1}{\alpha_{k+1}}$. We observe that $a_k \geq 1$, $\alpha_{k+1} > 1$, and α_{k+1} is irrational. Our goal is to show:

$$\alpha = [a_0, a_1, a_2, \ldots]$$

Using the recurrence we've proven before with $\alpha = [a_0, a_1, a_2, \dots]$, we find:

$$\begin{aligned} q_n\alpha - p_n &= q_n \cdot \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - p_n \\ &= \frac{q_n(\alpha_{n+1}p_n + p_{n-1}) - p_n(\alpha_{n+1}q_n + q_{n-1})}{\alpha_{n+1}q_n + q_{n-1}} \\ &= \frac{(-1)^n}{\alpha_{n+1}q_n + q_{n-1}} \end{aligned}$$

Hence,

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

which implies $\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$. Finally, it remains to prove that the integers $a_0, a_1 \geq 1, a_2 \geq 2, \dots$ are uniquely determined. In view of

$$\alpha = [a_0, a_1, a_2 \dots] = a_0 + \frac{1}{[a_1, a_2, \dots]},$$

and $0 \leq \alpha - a_0 < 1$, we find $a_0 = \lfloor \alpha \rfloor$ which implies that a_0 is unique and $\alpha_1 = [a_1, a_2 \dots]$ is uniquely determined by α. Because $a_1 = \lfloor \alpha_1 \rfloor$, a_1 is unique, etc. This proves the corollary. □

Now, we have finally gathered all the tools we will need in order to develop Hurwitz's theorem. Recall from section II that we have obtained a bound $1/q^2$ for numbers takes on the form $|\alpha - p/q|$ with α irrational. Two other great mathematicians, Vahlen and Borel, successively discovered that the bound in Dirichlet's theorem can be further tightened using the technique of continued fractions. And these improvements of the bounds culminated with Hurwitz's theorem, showing that this Dirichlet-type inequality's bound cannot be improved any further. Here, we first present two improvements of the bound in chronological order:

Theorem 14 ***(Vahlen, 1895)*** *Let α be an irrational number and denote two consecutive convergent of α as p_{n-1}/q_{n-1} and p_n/q_n. Then, at least one of them satisfies the inequality*

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

Proof. We observe that:

$$\begin{aligned} \left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| &= \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| \\ &= \frac{1}{q_n q_{n-1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2}. \end{aligned}$$

Thus,

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{or} \quad \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2}$$

□

Theorem 15 ***(Borel, 1903)*** *Let α be an irrational number and denote three consecutive convergent of α as p_{n-1}/q_{n-1}, p_n/q_n and p_{n+1}/q_{n+1}. Then, at least one of them satisfies the inequality*

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

Proof. Let $\alpha = [a_0, a_1, \dots]$, $\alpha_i = [a_i, a_{i+1}, \dots]$, $\beta_i = (q_i - 2)/(q_i - 1)$, $q \geq 1$. It is not difficult to deduce that

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1}}.$$

We show that there does not exist a positive integer n satisfying

$$\alpha_i + \beta_i < \sqrt{5}$$

for $i = n-1, n, n+1$. Our reasoning is indirect. We assume that the above inequality is satisfied for $i = n-1, n$. It follows from

$$\begin{aligned} &\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}, \\ &\frac{1}{\beta_n} = \frac{q_{n-1}}{q_{n-2}} = a_{n-1} + \frac{q_{n-3}}{q_{n-2}} = \alpha_{n-1} + \beta_{n-1} \end{aligned}$$

that

$$\frac{1}{\alpha_n} + \frac{1}{\beta_n} = \alpha_{n-1} + \beta_{n-1} \leq \sqrt{5}.$$

Hence, $1 = \alpha_n \cdot \frac{1}{\alpha_n} \leq (\sqrt{5} - \beta_n)(\sqrt{5} - \frac{1}{\beta_n})$, or equivalently, $\beta_n^2 - \sqrt{5}\beta_n + 1 \leq 0$ which implies $\beta_n \geq (\sqrt{5} - 1)/2$. Now if the inequality we assumed is satisfied for $i = n, n+1$, then again $\beta_{n+1} > (\sqrt{5} - 1)/2$, so we deduce

$$\begin{aligned} 1 \leq a_n &= \frac{q_n}{q_{n-1}} - \frac{q_{n-2}}{q_{n-1}} \\ &= \frac{1}{\beta_{n+1}} - \beta_n < \frac{2}{\sqrt{5} - 1} - \frac{\sqrt{5} - 1}{2} < 1 \end{aligned}$$

Thus we have our contradiction. □

We can see that Vahlen and Borel's results are already significant departures from Dirichlet. We can push it a little further by Hurwitz's theorem. To achieve this, we first state two theorems without proof. We would like to focus on Hurwitz's theorem and direct interested reader to [12].

Theorem 16 ***(Legendre)*** *Let p, q be integers such that $q \geq 1$ and*

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

then p/q is a convergent of α.

Theorem 17 *Assume the continued fraction expansion for α is given by*

$$\alpha = [a_0, a_1, \dots, a_N, 1, 1, \dots]$$

then:

$$\lim_{n\to\infty} q_n^2 \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{\sqrt{5}}$$

Theorem 18 ***(Hurwitz, 1891**, see [4]) Let α be an irrational number,*

1. *Then there are infinitely many rational numbers $\frac{p}{q}$ such that:*

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

2. *If $\sqrt{5}$ is replaced by $C > \sqrt{5}$, then there are irrational numbers α for which statement (1) does not hold.*

Proof. Claim 1 follows directly from Borel's result, while claim 2 follows from Legendre's and the theorem 17. Namely, if α is irrational and of form :

$$\alpha = [a_0, a_1, \dots, a_N, 1, 1, \dots]$$

then according to Legendre's Theorem above, all solutions of $|\alpha - p/q| < 1/(Cq^2)$ with $C > \sqrt{5}$ can be found among the convergents to α, however, in view of theorem 18, this inequality is satisfied by ony finitely many convergents to α. □

V. MINKOWSKY'S CONVEX BODY THEOREM AND DIRICHLET REVISITED

We'll follow the strategy outlined in Chapter III from [3]. [3] gave a proof for the $\mathbb{R}^2$ case, we use the same idea of the proof to generalize the result to $\mathbb{R}^n$, which is what Minkowski originally did. A keen reader will notice that the spirit of the proof is somewhat identical to the pigeonhole argument. Before proceeding, we first define a few necessary terms:

1. A set B in $\mathbb{R}^n$ is **convex** if for any x and y in B, all points on the line segment joining x and y are also in B.

2. A set B in $\mathbb{R}^n$ is **symmetric about the origin** if for any x in B, the point $-x$ is also in B.

3. We denote the set of all points in $\mathbb{R}^n$ all of whose coordinates are integers by $\mathbb{Z}^n$.

Now, we first prove a special case of Minkowski's theorem which illustrates better the general strategy better. Once, we've established this, we will give a proof of the theorem for the general lattices

Theorem 19 ***(Minkowski's Convex Body Theorem, 1912)** Let B be a convex open set in $\mathbb{R}^n$ that is symmetric about the origin and whose volume is greater than 2^n. Then B must contains a nonzero point all of whose coordinates are integers.*

Proof. We first show the following (sometimes called *Blichfeldt's principle*, see [1]): if S is a bounded set in $\mathbb{R}^n$ whose volume is greater than 1, then there exist two points x and y in S such that $x - y$ has integer coordinates.

- Proof: The idea is essentially the same as Dirichlet's pigeonhole argument:

  For each lattice point $a = (a_1, \dots, a_n)$, let $R(a)$ be the set containing $(x_1, \dots, x_n)$ whose coordinates satisfy $a_i \le x_i < a_{i+1}$ (this is the analogue of a box in $\mathbb{R}^n$).

  If we then set $S(a) = S \cap R(a)$, we have $\sum_{a\in\mathbb{Z}^n} \text{vol}(S(a)) = \text{vol}(S)$, because each point of S lies in exactly one of the boxes $R(a)$.

  Now imagine translating the $S(a)$ by the vector $-a$: it will preserve volume, but move $S(a)$ to land inside $S(0)$. Denote this translated set by $S^*(a)$.

  Then $\sum_{a\in\mathbb{Z}^n} \text{vol}(S^*(a)) = \text{vol}(S)$.

  Now, notice that each of the sets $S^*(a)$ lies inside $S(0)$, which has volume 1, so there must be some overlap.

  Hence, there exists some distinct $x, y \in S$ and $a_1, a_2 \in \mathbb{Z}^n$ such that $x - a_1 = y - a_2$: but then $x - y = a_1 - a_2$ is a nonzero lattice point. Thus, we have shown the existence of such two points.

Now, we go back to the original statement of Minkowski. Suppose B is a convex open set symmetric about 0 whose volume is greater than 2^n, and let $\frac{1}{2}B = \{\frac{1}{2}x : x \in B\}$.

Notice that since $\text{vol}(B) > 2^n$, we have $\text{vol}(\frac{1}{2}B) > 1$. Apply Blichfeldt's principle to $\frac{1}{2}B$: we obtain distinct points $x, y \in \frac{1}{2}B$ such that $x - y$ has integer coordinates. Then $2x, 2y \in B$. Since B is symmetric about the origin, $-2y \in B$. And since B is convex, the midpoint of the line segment joining $2x$ and $-2y$ lies in B. This point is $x - y$, which is a nonzero point all of whose coordinates are integers. □

Now, we proceed to further generalize this argument. Again, we introduce a few terms first:

1. If $v_1, \dots, v_n$ are linearly independent vectors in $\mathbb{R}^n$, the set Λ of vectors of the form $c_1v_1 + \cdots + c_nv_n$, where each $c_i \in \mathbb{Z}$, is called a **lattice**.

2. A **fundament domain** for this lattice can be obtained by drawing all of the vectors $v_1, \ldots, v_n$ outward fro the origin and then filling them in to create a "skew box"

3. A basic fact from linear algebra says: the volume of the fundamental domain is equal to the determinant of the matrix whose columns are the vectors $v_1, \ldots, v_n$ expressed in terms of the standard basis of $\mathbb{R}^n$. This is one of geometric interpretations of the determinant of a matrix.

Now, we can prove the more generalized form of Minkowski's theorem:

Theorem 20 ***(Minkowski's Convex Body Theorem, 1912****, general lattice version) Let Λ be any lattice in $\mathbb{R}^n$ whose fundamental domain has volume V. If B is any open convex centrally-symmetric region in $\mathbb{R}^n$ whose volume is greater than $2^n \cdot V$, then B contains a nonzero points of Λ.*

Proof. Apply a linear transformation T sending the basis vectors of Λ to the standard basis of $\mathbb{R}^n$ (i.e., the basis consists of all unit vectors with one 1 and the rest being 0). Linear transformation preserve open sets, convex sets and central symmetry (these are easy to check using the definition of a linear mapping), so the image of B under T is still open, convex, and centrally symmetric.

$\text{vol}(T(B)) = 1/V \cdot \text{vol}(B)$ because the determinant of matrix is multiplicative and volume can be interpreted as the determinant of a matrix. So this new open convex centrally-symmetric set $T(B)$ has volume greater 2^n.

Applying the previous version of Minkowski's theorem to $T(B)$ yields that $T(B)$ contains a nonzero point all of whose coordinates are integers: then B contains a nonzero point of Λ. □

Now we apply Minkowski's theorem to give an alternative proof of a generalized form of Dirichlet's theorem:

Theorem 21 ***(Dirichlet, 1842****, simultaneous version) Let $\alpha_1, \ldots, \alpha_d$ be irrational numbers and integer $N > 0$, there exists integers $p_1, \ldots, p_d, q$ with $0 < q < N$ such that*

$$|\alpha_i - \frac{p_i}{q}| < \frac{1}{qN^{1/d}}$$

Proof. Consider the set $S = \{(x, y_1, \ldots y_d) \in \mathbb{R}^{1+d} : -N - \frac{1}{2} \leq x \leq N + \frac{1}{2}, |\alpha_i x - y_i| \leq N^{1/d}\}$. Note that $\text{vol}(S) = 2N \cdot \prod_{i=1}^{d} \frac{2}{N^{1/d}} = 2^{1+d}$. Then there exists an integer point in S by Minkowski's theorem. Let$(q, p_1, \ldots, p_n)$ be this point. This vector satisfies the condition by our definition of the set S. □

One can see the powerfulness of Minkowski's theorem through the slick proof given above. Indeed, Minkowski's theorem is not only powerful in the realm of number theory, but is proven to be crucial even outside. In a classic paper about integer programming [5], Kannan uses several concepts from Geometry of Numbers, the most curcial of them being Minkowski's convex body theorem. This elegant classical theorem turns out to be crucial in effectively reducing an n variable problem to polynomially many $(n-1)$ variable problems rather than an exponential number of them. We encourage reader who is interested in this topic to [5].

VI. CONCLUDING REMARKS

Through our journey of approximating irrationals with rationals, we can see that the results we have derived inadvertently have applications outside of the field of Diophantine Approximation, and even more, inspires and solves real world problems. Till today, this is still a vibrant research field with much more to be explored.

[1] H.F. Blichfeldt, *A new principle in the geometry of numbers, with some applications* (Amer. Math. Soc., Providence, Rhode Island, 1914).

[2] E.B. Burger, *Exploring the Number Jungle: A Journey into Diophantine Analysis* (Amer. Math. Soc., Providence, Rhode Island, 2000).

[3] G. Hardy, and E.M. Wright, *An introduction to the theory of numbers* (Oxford University Press, Oxford : New York, 1979).

[4] A. Hurwitz, in *Ueber die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche (On the approximation of irrational numbers by rational numbers)*, Mathematische Annalen (in German), Vol. 39 , 1891 pp. 279–284.

[5] R. Kannan, in *Minkowski's Convex Body Theorem and Integer Programming*, Mathematics of Operations Research, Vol. 12 , 1987 pp. 415–440.

[6] A. Klenke, *Probabiliry Theory: A Comprehensive Course* (Springer-Verlag, London, United Kingdom, 2014).

[7] S.J. Miller, and R. Takloo-Bighash, *An Invitation to Modern Number Theory* (Princeton University Press, Princeton, New Jersey, 2006).

[8] H. Minkowski, *Geometrie der Zahlen* (Leipzig, Germany: Teubner, 1912).

[9] M.R. Murty, *Problems in Analytic Number Theory* (Springer-Verlag, New York, USA, 2008).

[10] K.F. Roth, in *Rational Approximations to Algebraic Numbers*, Mathematika, Vol. 2 , 1955 pp. 1–20.

[11] J.D. Sally, and P.J. Sally Jr., *Roots to Research: A Vertical Development of Mathematical Problems* (Amer. Math. Soc., Providence, Rhode Island, 2007).

[12] P. Soberón, *Problem-Solving Methods in Combinatorics* (Birkhäuser Basel, Cham, Switzerland, 2013).

[13] J. Steuding, *Diophantine analysis : Course notes from a Summer School* (Birkhäuser Basel, Cham, Switzerland, 2016).
[14] J. Stillwell, *Elements of Number Theory* (Springer-Verlag, Berlin, Germany, 2000).