Diophantine approximation

day one

1. rational approximation

How do you approximate an irrational number? One way is to truncate the decimal approximation:

$$\pi = 3.14159265\cdots$$

From a storage perspective, this isn't very efficient. We need 8 digits to store this approximation. As a fraction, this is

$$\pi = 3 + \frac{14159265}{100000000}.$$

We can do nearly as well with a much smaller fraction:

$$\frac{355}{113} = 3.14159292\cdots \approx \pi.$$

This is a much more concise approximation!

So we will refine our question: How well can we approximate an irrational number α using rational numbers with small denominator? Here's one observation: For every $q \in \mathbb{N}$, you can pick $p \in \mathbb{N}$ so that p/q is the closest fraction to α and guarantee that

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

But this isn't such a good approximation; this is the same level of efficiency as rounding a decimal expression. The first result is that we can do much better!

Theorem 1 (Dirichlet's theorem). *Let α be a positive irrational number. For every $N > 0$, there is a pair of nonnegative integers $p, q \in \mathbb{N}$ with $q \leq N$ so that $|q\alpha - p| < 1/N$.*

What does this mean? If we divide both sides by q, we get

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

which is much better than $\frac{1}{q}$.

Proposition 2. *If α is a positive irrational number, there are infinitely many pairs of nonnegative integers $p, q \in \mathbb{N}$ so that $|\alpha - p/q| < 1/q^2$.*

Proof. Suppose that every pair has $|\alpha - p/q| > \varepsilon$. Choose $N \in \mathbb{N}$ so that $1/N < \varepsilon$. Dirichlet's theorem says that there are $p', q' \leq N$ so that $|\alpha - p'/q'| < 1/Nq' < \varepsilon$, which means that p', q' were not on the list. (So the list cannot have only finitely many pairs.) □

This is good news! It means that we have an infinite supply of pretty good rational approximations.

Definition 3. A fraction p/q is a *Diophantine approximation* for α if $|\alpha - p/q| < 1/q^2$.

But before we get ahead of ourselves, let's prove the theorem. To do that, we'll use a new function.

Definition 4. The *fractional part* of a real number x is $[\![x]\!] = x - \lfloor x \rfloor$, the difference between x and the largest integer less than it. (Or, if you prefer, the remainder of x modulo 1.) In other words, $[\![x]\!]$ is what you get by deleting everything to the left of the decimal point.

Proof of Theorem 1. Divide the interval $[0, 1)$ into N intervals of equal length $[0, 1/N)$, $[1/N, 2/N), \ldots,$ $[1 - 1/N, 1)$. If $[\![q\alpha]\!] < 1/N$ or $[\![q\alpha]\!] > (N-1)/N$, then there is an integer p for which $|q\alpha - p| < 1/N$, so we will focus on proving the first goal. For each $q \in \{0, 1, \ldots, N-1\}$, let $x_q = [\![q\alpha]\!]$. If there is some q for which $x_q \in [0, 1/N)$, then we're done. Otherwise, there are two values q, q' for which x_q and $x_{q'}$ are in the same interval. If $q < q'$, then either $x_{q'-q}$ is either in $[0, 1/N)$ or $[1 - 1/N, 1)$. In either case, there is a $p \in \mathbb{N}$ so that $|q\alpha - p| < 1/N$. □

To make things more concise, we'll use the "circle metric" to measure distance in $[0,1)$ when we're thinking modulo 1. If $x, y \in [0,1)$, their circle distance is

$$|x-y|_\circ = \min\big\{|x-y|, |y-x|\big\}.$$

This is how far you need to travel around the circle to get from x to y (or vice versa).

We can use Dirichlet's theorem to prove that the multiples of an irrational number are dense in $[0,1)$.

Proposition 5. *Let α be an irrational number. Prove that for every $\beta \in [0,1)$ and $\varepsilon > 0$, there is a positive integer n so that $|\beta - \llbracket n\alpha \rrbracket|_\circ < \varepsilon$.*

Proof. Choose a fraction p/q so that p and q are coprime, $|\alpha - p/q| < 1/q^2$, and $1/q < \varepsilon/2$. There is a number $1 \leq n \leq q$ so that $|\beta - \llbracket np/q \rrbracket| < 1/q$. Then

$$|\beta - \llbracket n\alpha \rrbracket|_\circ \leq \left|\beta - \left\llbracket \frac{np}{q} \right\rrbracket\right|_\circ + \left|\left\llbracket \frac{np}{q} \right\rrbracket - n\alpha\right|_\circ < \frac{1}{q} + \frac{n}{q^2} < \varepsilon. \qquad \square$$

Exercise 4 is a strengthening of this result: Not only does the sequence $\llbracket n\alpha \rrbracket$ get arbitrarily close to every number in $[0,1)$, it also is "equally spaced" in some precise sense.

We can also strengthen Dirichlet's theorem itself:

Theorem 6 (Simultaneous Diophantine approximation). *Suppose that $\alpha_1, \ldots, \alpha_n$ are irrational numbers. There are infinitely many positive numbers $q \in \mathbb{N}$ so that for each $1 \leq i \leq n$ there is a positive integer p_i with $|\alpha_i - p_i/q| < \frac{1}{q^{1+1/n}}$.*

2. A puzzle

Question. Suppose that a rectangle can be partitioned into finitely many squares. Is it necessarily true that the ratio of the side lengths of the rectangle is rational?

Since any rational rectangle can be easily partitioned into squares, the question is whether the converse is true. One way to prove that the converse *is* in fact true is to use linear algebra and the axiom of choice 😮. (Talk to me if you want to see how it works!) A different way is to use Dirichlet's theorem.

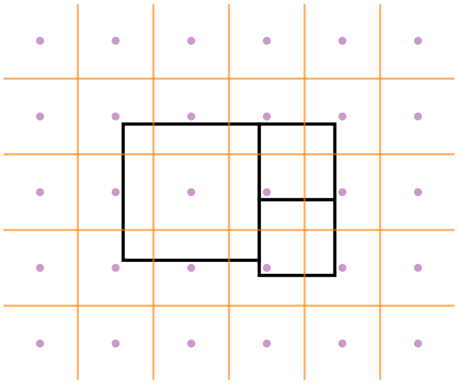
Theorem 7. *If a rectangle can be partitioned into finitely many squares, then the ratio of the side lengths of the rectangle is rational.*

Proof. Suppose that the rectangle R is divided into squares, and let $(x_1, y_1), \ldots, (x_n, y_n)$ be the vertices of these squares. By Theorem 6, there are infinitely many positive numbers q such that

$$|qx_i - p_i| < \frac{1}{q^{1/n}} \qquad \text{and} \qquad |qx_i - p_i'| < \frac{1}{q^{1/n}}$$

for some integers $p_1, \ldots, p_n, p_1', \ldots, p_n'$. Choose a value of q large enough so that $1/q^{1/n} < 1/100$ and so that the side length of each square is at least 1. Draw the vertical and horizontal lines $x = \frac{1}{2} + a$ and $y = \frac{1}{2} + b$ for every $a, b \in \mathbb{Z}$; let V and H be the total lengths of the vertical and horizontal lines that are contained inside R. Suppose the sides of the rectangle have lengths ℓ and w. If there are m vertical lines that intersect R and r horizontal lines, then $V = mw$ and $H = r\ell$.

Now, zoom in on a square. Say the side length of the square is z. Since the vertices of the square are so close to integer points, there are $\lfloor z \rceil$ vertical and horizontal lines that pass through the square. The lengths of the vertical and horizontal segments in this square are equal (because it's a square), so the sum of vertical lengths is equal to the sum of horizontal lengths. Adding up across all squares, we get that $V = H$. Using the formulas for V and H from the previous paragraph, this means that $w/\ell = r/m$, which is rational. (The following picture is a visualization of a portion of the rectangle during this process.) □



PROBLEMS

1. (a) Show that if $q > 1$, then there is at most one Diophantine approximation for α with denominator q.
   (b) Show that there are infinitely many Diophantine approximations to an irrational number where p and q have no common factors.
   (c) Show that if α is rational, then it has only finitely many Diophantine approximations.
2. Prove that e is irrational by showing that the partial sums $\sum_{k=1}^{\infty} 1/k!$ are too close to e for e to be rational. [Hint: Try something similar to problem 1(c).]
3. Prove Theorem 6.

*4. (If you're familiar with limits.) Let α be an irrational number. A sequence $(x_n) \subseteq [0,1)$ is called *equidistributed* if, for every $a, b \in [0,1)$ with $a < b$, we have

$$\lim_{n\to\infty} \frac{\#a_k \in [a,b) \text{ with } 1 \leq k \leq n}{n} \longrightarrow b - a.$$

Prove that the sequence $a_n = \llbracket n\alpha \rrbracket$ is equidistributed whenever α is an irrational number.

5. *Pell's equation* is $x^2 - ny^2 = 1$, where n is a positive integer that is not a square. There is a trivial solution $(x, y) = (\pm 1, 0)$, and the question is whether there exists any nontrivial integer solution for a given n. (If n is a square number, then there are many nontrivial solutions.)
   (a) We use $\mathbb{Z}[\sqrt{n}]$ to denote the set of numbers $a + b\sqrt{n}$ where $a, b \in \mathbb{Z}$. If $\alpha \in \mathbb{Z}[\sqrt{n}]$, its *norm* is

   $$\|\alpha\| = (a + b\sqrt{n})(a - b\sqrt{n}) = a^2 + nb^2.$$

   Show that $\|\alpha\beta\| = \|\alpha\| \, \|\beta\|$ for any $\alpha, \beta \in \mathbb{Z}[\sqrt{n}]$.
   (b) Show that if (x_1, y_1) and (x_2, y_2) are solutions to Pell's equation, then $\big(x_1x_2 + y_1y_2,\ x_1y_2 + x_2y_1\big)$ is also a solution.
   (c) Show that there are infinitely many integers $a, b \in \mathbb{Z}$ so that $|a^2 - nb^2| < 3\sqrt{n}$. [Hint: Write $|a^2 - nb^2| = |a - b\sqrt{n}||a + b\sqrt{n}|$. There are infinitely many b so that $|a - b\sqrt{n}| < \frac{1}{b}$. Then show that $|a + b\sqrt{n}| < 3b\sqrt{n}$ for these b.]
   (d) Show that there are two distinct pairs of positive integers (a_1, b_1) and (a_2, b_2) with $\|a_1 + b_1\sqrt{n}\| = \|a_2 + b_2\sqrt{n}\| = N$ and $a_1 \equiv a_2 \bmod N$ and $b_1 \equiv b_2 \bmod N$.
   (e) Show that

   $$\frac{a_1 - b_1\sqrt{n}}{a_2 - b_2\sqrt{n}} \in \mathbb{Z}[\sqrt{n}].$$

   (f) Find a nontrivial solution to Pell's equation.

Diophantine approximation

day two

3. transcendence

Now we know that we can approximate irrational numbers quadratically. Can we do better? The answer is . . .

Proposition 8. *There is no rational number p/q for which $|\sqrt{2} - p/q| < 1/4q^2$.*
Proof. If $|\sqrt{2}-p/q| < 1/2$, then $q \leq p \leq 2q$. (In the other case, the theorem is true automatically.) Therefore

$$|2q^2 - p^2| = |q\sqrt{2} - p|\,|q\sqrt{2} + p|.$$

Since $2q^2 - p^2$ is a nonzero integer, we have $|2q^2 - p^2| \geq 1$, and $|q\sqrt{2} + p| \leq (\sqrt{2} + 2)q \leq 4q$. Therefore,

$$|q\sqrt{2} - p| \geq \frac{1}{4q}. \qquad \square$$

Up to improving the constant, then, there is no stronger theorem than Dirichlet's for general approximation by rationals. As for the constant, there is the following result:

Theorem 9 (Hurwitz). *For every irrational number α, there are infinitely many nonnegative p, q so that*

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

Moreover, the theorem is not true if $\sqrt{5}$ is replaced by any larger real number.

We won't prove the first part of Hurwitz's theorem, but problem 1 asks you to prove the second part. For now, it's not the point.

This theorem applies to *all* irrational numbers—it's still plausible that certain irrationals can be approximated better than quadratically. Our next result is an extension of the previous result to any algebraic number.

Definition 10. A number is *algebraic* if it is the root of a polynomial with integer coefficients. It is *transcendental* if it is not algebraic.

Since every rational number p/q is the root of the integer polynomial $qx - p$, every rational number is algebraic.

Theorem 11. *If α is a root of an integer polynomial of degree d, then there a constant $C > 0$ such that there is no rational number p/q so that $|\alpha - p/q| < C/q^d$.*
Proof. Let f be a degree-d integer polynomial such that $f(\alpha) = 0$, and assume that $f(p/q) \neq 0$. (Otherwise, divide f by $x - p/q$ and take the resulting polynomial.) Then $f(x) = \big(x - \alpha)g(x)$ for some polynomial g (not necessarily with integer coefficients), and

$$\left|f\Big(\frac{p}{q}\Big)q^d\right| = q^d\left|\frac{p}{q} - \alpha\right|\,\left|g\Big(\frac{p}{q}\Big)\right|.$$

The left-hand side is at least 1, since it's a nonzero integer. Setting $C = \max_{\alpha-1 \leq x \leq \alpha+1} |g(x)|^{-1}$, we have

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{C}{q^d}. \qquad \square$$

This says that algebraic numbers can be approximated only so well by rational numbers. *So*, if we can construct an irrational number that is supremely well-approximated by rational numbers, we will have built a transcendental number. This is no small feat! It took nearly 100 years from the definition of a transcendental number to even prove that one existed—this is what Joseph Liouville did in 1844, and what we will soon do. In 1874, Georg Cantor proved that the set of algebraic numbers is countable while the set of transcendental numbers is uncountable. So basically every real number is transcendental—if you pick a random one, it's virtually *guaranteed* to be transcendental. And yet, proving that any specific number is transcendental is notoriously difficult, even today.[1]

Enough history, let's get to the proof!

Theorem 12 (Liouville, 1844). *The number*

$$L = \sum_{k=1}^{\infty} 2^{-k!}$$

is transcendental.

Proof. Consider the sequence of fractions

$$\frac{p_n}{q_n} = \sum_{k=1}^{n} 2^{-k!}.$$

Then $q_n \leq 2^{n!}$ and

$$\left| L - \frac{p_n}{q_n} \right| = \sum_{k=n+1}^{\infty} 2^{-k!} \leq 2^{-(n+1)!+1} \leq \left(2^{-n!}\right)^n \leq \frac{1}{q_n^n}.$$

If L were the root of a degree-d integer polynomial, there would be a constant $C > 0$ so that $|L - p_n/q_n| \geq C/q_n^d$ for every n. This would mean that

$$\frac{C}{q_n^d} \leq \frac{1}{q_n^n}$$

for every n; in other words, $q_n^{n-d} \leq 1/C$ for every n, which is impossible. So L is transcendental. □

Definition 13. A *Liouville number* is a real number α such that for every $n \in \mathbb{N}$, there is a rational number p/q such that

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

Liouville's proof that L is transcendental consists essentially of two parts: First, that L is a Liouville number, and second, that every Liouville number is transcendental.

4. Better bounds from below

In 1908, Axel Thue improved Liouville's theorem like this:

Theorem 14. *Suppose α is an irrational root of a degree-d integer polynomial. If $\gamma > d/2 + 1$, then there are only finitely many rational numbers p/q such that*

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

This leads to the idea of the *irrationality exponent* of an irrational number α, which is the smallest positive number μ such that, for every $\gamma > \mu$, there are only finitely many rational numbers p/q such that $|\alpha - p/q| < 1/q^\gamma$. Equivalently, the irrationality exponent of α is the largest value of μ for which there exist infinitely many rational numbers p/q such that $|\alpha - p/q| < 1/q^\mu$. The irrationality exponent of α is denoted $\mu(\alpha)$.

Every Liouville number α has irrationality exponent $\mu(\alpha) = \infty$ (by definition). Dirichlet's theorem says that $\mu(\alpha) \geq 2$ for every irrational number α. Liouville's theorem says that $\mu(\alpha) \leq d$ if α is algebraic, and Thue's theorem improves this to $\mu(\alpha) \leq d/2 + 1$. This was improved by Carl Siegel to $\mu(\alpha) \leq 2\sqrt{d}$ in 1921. Finally, in 1955, Karl Roth proved that $\mu(\alpha) = 2$ for every algebraic number α; this won him a Fields Medal. The astounding consequence of this is that no algebraic number can be approximated better by rational numbers than Dirichlet originally proved.[2]

[1] The Wikipedia page for transcendental numbers has a sketch of a proof that e is transcendental, for example.

[2] You might ask: Is $\mu(\alpha) > 2$ if α is transcendental? Not necessarily! We know that e is transcendental, but $\mu(e) = 2$.

5. continued fractions

We'll now turn to a new method for analyzing rational approximations, one that will allow us to prove different things and also to actually generate good approximations! This is the method of *continued fractions*.

Consider $\frac{43}{19}$. This is the same as $2 + \frac{5}{19}$, which seems is really all the reduction we can do. But if we didn't want to stop, we could invert the fraction to make the denominator is bigger than the numerator; then $\frac{19}{5} = 3 + \frac{4}{5}$. Do it again: $\frac{5}{4} = 1 + \frac{1}{4}$, and there's really nothing more we can do, since $\frac{4}{1} = 4$.

This seems, perhaps, like a ridiculous thing to do, but what we've just calculated is that

$$\frac{43}{19} = 2 + \frac{5}{19} = 2 + \frac{1}{3 + \frac{4}{5}} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}.$$

The last expression is called the *continued fraction expansion* of the rational number $\frac{43}{19}$. We usually abbreviate the nested fractions by just recording the numbers in the denominator, like this: $[2; 3, 1, 4]$.

Every rational number has a finite continued fraction expansion, because the denominator decreases at each step. In fact, the process of constructing a continued fraction is very similar to the Euclidean algorithm; problem 4 asks you to think about this.

Is the continued fraction unique? Almost, but not quite. For example:

$$\frac{43}{19} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1}}}}.$$

So $[2; 3, 1, 4] = [2; 3, 1, 3, 1]$. Problem 5 has you prove that this is the only thing that prevents uniqueness.

But enough with rational numbers; what about irrational ones? There's no reason we couldn't do the same process, separating out the integer part, inverting, and repeating. For example:

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{2 + \left(\frac{1}{\sqrt{2}} - 2\right)} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots}}}.$$

In this way, we get an *infinite* continued fraction for each irrational number. Unlike with rational numbers, each irrational number has a unique continued fraction expansion.

PROBLEMS

1. Prove one direction of Hurwitz's theorem: If $C > \sqrt{5}$, then there are only finitely many rational numbers p/q so that
$$\left|\varphi - \frac{p}{q}\right| < \frac{1}{Cq^2},$$
where $\varphi = (1 + \sqrt{5})/2$ is the golden ratio. [Hint: What polynomial is φ the root of?]
2. Construct an uncountable set of transcendental numbers.
3. Show that the number
$$\sum_{k=1}^{\infty} 2^{-3^k}$$
is transcendental. [You will need Roth's theorem.]
4. Why is constructing the continued fraction expansion of a/b similar to applying the Euclidean algorithm to a and b?
5. Prove that every rational number has exactly two different continued fraction expansions.
6. Find a formula for the continued fraction $[1; 1, 1, \dots, 1]$.
7. Prove that the continued fraction expansion of $\sqrt{2}$ is $[1; 2, 2, 2, \dots]$.

Diophantine approximation

day three

6. continued fractions, continued

Let's imagine that we have an irrational number that we've expanded into a continued fraction:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}},$$

or $\alpha = [a_0; a_1, a_2, a_3, \ldots]$ for short. The *convergents* to α are what you get by cutting off the continued fraction at some point:

$$\begin{aligned}
\frac{p_0}{q_0} &= a_0 \\
\frac{p_1}{q_1} &= a_0 + \frac{1}{a_1} \\
\frac{p_2}{p_2} &= a_0 + \cfrac{1}{a_1 + \frac{1}{a_2}} \\
\frac{p_3}{q_3} &= a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}} \\
&\vdots
\end{aligned}$$

These convergents are what we will focus on today. It would be very nice if the convergents converged to α (and a tragedy of terminology otherwise!). This is indeed the case, but we'll only prove that later. For now, we need to build up some properties.

> ⚠ For the rest of these notes, α is an irrational number with continued fraction expansion $\alpha = [a_0; a_1, a_2, a_3, \ldots]$.

It turns out that the numerator and denominator of the convergents satisfy a recurrence relation.

Proposition 15. $p_{n+1} = a_{n+1}p_n + p_{n-1}$ *and* $q_{n+1} = a_{n+1}q_n + q_{n-1}$.

Proof. You can prove by calculating that the theorem is true for $n = 1$. Assume that the relationship is true for some $n - 1$. Then

$$\begin{aligned}
\frac{p_{n+1}}{q_{n+1}} &= [a_0; a_1, a_2, \ldots, a_n, a_{n+1}] \\
&= \left[a_0; a_1, a_2, \ldots, a_n + \frac{1}{a_{n+1}}\right],
\end{aligned}$$

so by the induction hypothesis

$$\frac{p_{n+1}}{q_{n+1}} = \frac{\left(a_n + \frac{1}{a_{n+1}}\right)p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right)q_{n-1} + q_{n-2}}$$

which simplifies to

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

□

Besides a particular recurrence relation, this also tells us that p_n and q_n increase with n.

Proposition 16. $p_{n+1}q_n - q_{n+1}p_n = (-1)^n$.

Proof. Induction! You can check that the statement is true for $n = 0$. Inductively, we have

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

□

This is a simple-looking and easy-to-prove statement, but it has many consequences.

Corollary 17. *p_n and q_n have no common factors (so p_n/q_n is a fraction in reduced terms).*

Proof. If p_n and q_n shared a factor, then the right hand side of $p_{n+1}q_n - q_{n+1}p_n = (-1)^n$ would also be divisible by that factor. □

If we divide the equation in Proposition 16 by q_nq_{n+1}, we get the statement that

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_nq_{n+1}}.$$

Since we noted before that $q_{n+1} > q_n$, this means that

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

which almost looks like a Diophantine approximation, but there's no irrational number.

Moreover, this reformulation means that we can write the continued fraction as an alternating series:

$$\begin{aligned} \alpha &= \frac{p_0}{q_0} + \sum_{n=0}^{\infty}\left(\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right) \\ &= a_0 + \sum_{n=0}^{\infty}\frac{(-1)^n}{q_nq_{n+1}}. \end{aligned}$$

This means that

$$\alpha - \frac{p_n}{q_n} = \sum_{k=n}^{\infty}\frac{(-1)^k}{q_kq_{k+1}},$$

so

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

In other words, each of the convergents is a Diophantine approximation of α!

Also, the expression of α as an alternating series tells us that $p_n/q_n < \alpha$ if n is even and $p_n/q_n > \alpha$ if n is odd. Summing up:

Theorem 18. *The convergents p_n/q_n of an irrational number α are all Diophantine approximations of α that satisfy*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \alpha < \cdots \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Here, then, is how you find a magic approximation, like we did at the beginning of class. Start by evaluating the first few terms of the continued fraction. For example, $\pi = [3; 7, 15, 1, 292, 1, 1, \dots]$. The partial convergent p_n/q_n will satisfy

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \leq \frac{1}{q_nq_{n+1}}.$$

The procedure is therefore: Pick a value of n so that a_{n+1} is much larger than a_n. Then $q_{n+1} = a_{n+1}q_n + q_{n-1} > a_{n+1}q_n$ is much larger than q_n, so that $|\alpha - p_n/q_n| < 1/a_{n+1}q_n^2$. For π, this means we might choose $n = 3$, which gives

$$\frac{p_3}{q_3} = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1}}} = \frac{355}{113},$$

just like what we saw on the first day. And $p_1/q_1 = 22/7$, which is perhaps the most famous approximation to π.

Here's another example. The continued fraction expansion of e^π is $[23; 7, 9, 3, 1, 1, 591, 2, 9, \ldots]$. Compare:

$$e^\pi \approx 23.1406926327$$

$$[23;7,9,3,1,1] = 23 + \frac{65}{462} \approx 23.1406926406.$$

It's accurate to 7 decimal places!

7. Continued fractions, concluded

It turns out that the convergents are actually "best possible" approximations in a precise sense:

Definition 19. A rational number p/q is called a *best approximation* of α if $|\alpha - p/q| \leq |\alpha - a/b|$ for every fraction a/b with $1 \leq b \leq q$.

Proposition 20. *Every convergent is a best approximation to α.*

Proof. Suppose that $|\alpha - a/b| < |\alpha - p_n/q_n|$ and $1 \leq b \leq q_n$. Since $|\alpha - p_{n-1}/q_{n-1}| > |\alpha - p_n/q_n|$ and α lies between p_{n-1}/q_{n-1} and p_n/q_n, it must be that a/b also lies between p_{n-1}/q_{n-1} and p_n/q_n. First,

$$\left|\frac{a}{b} - \frac{p_{n-1}}{q_{n-1}}\right| < \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_{n-1}q_n}.$$

On the other hand,

$$\left|\frac{a}{b} - \frac{p_{n-1}}{q_{n-1}}\right| = \left|\frac{aq_{n-1} + bp_{n-1}}{bq_{n-1}}\right| \geq \frac{1}{bq_{n-1}},$$

since $a/b \neq p_{n-1}/q_{n-1}$. Therefore

$$\frac{1}{bq_{n-1}} < \frac{1}{q_{n-1}q_n}.$$

Just rearrange to get $q_n < b$, which is a contradiction, since we assumed that $b \leq q_n$. □

We'll now prove another way that convergents are the "best" approximations.

Theorem 21. *If $|\alpha - a/b| < 1/2b^2$, then a/b is one of the convergents of α.*

First, we need a stronger lemma:

Lemma 22. *If $|b\alpha - a| < |q_n\alpha - p_n|$, then $b \geq q_{n+1}$.*

We could prove it, but it's a more in-depth calculation than the one before, and not very enlightening. Let's see how to use it.

Proof of Theorem 21. Suppose that a/b is not a convergent and that nevertheless $|\alpha - a/b| < 1/2b^2$. Choose an n so that $q_n \leq b < q_{n+1}$; the lemma tells us that

$$|\alpha q_n - p_n| < |\alpha b - a| \leq \frac{1}{2b},$$

so

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

Since $a/b \neq p_n/q_n$, we have

$$\left|\frac{p_n}{q_n} - \frac{a}{b}\right| \geq \frac{1}{bq_n},$$

while the triangle inequality gives

$$\left|\frac{p_n}{q_n} - \frac{a}{b}\right| \leq \left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{a}{b}\right| < \frac{1}{2bq_n} + \frac{1}{2b^2}.$$

Comparing the two inequalities and simplifying, we get

$$\frac{1}{2bq_n} < \frac{1}{2b^2},$$

which means that $b < q_n$, a contradiction to our hypothesis that $q_n \leq b < q_{n+1}$. □

As for Hurwitz's theorem, it turns out that among every three consecutive convergents, there is at least one that satisfies $|\alpha - p_n/q_n| \leq 1/\sqrt{5}q_n^2$; this is enough to guarantee infinitely many approximations. The actual proof of this, though, is left as an exercise. Number 5, actually.

PROBLEMS

1. Why is the continued fraction expansion of an irrational number unique?
2. Show that $|\alpha - p_n/q_n| \geq 1/(2q_nq_{n+1})$.
3. A continued fraction is called *periodic* if it eventually repeats: $[a_0; a_1, a_2, \ldots, a_k, a_0, a_1, \ldots, a_k, a_0, a_1 \ldots]$. We can abbreviate this by $[\overline{a_0; a_1, a_2, \ldots, a_k}]$. A continued fraction is called *eventually periodic* if, well, it's periodic eventually: $[a_0; a_1, a_2, \ldots, \overline{a_k, a_{k+1}, \ldots, a_n}]$.
   (a) A *quadratic irrational* is a number of the form $a + b\sqrt{n}$ where a and b are rational numbers. Prove that any periodic continued fraction represents a quadratic irrational.
   (b) The set of numbers of the form $a + b\sqrt{n}$ for some fixed n with a, b rational is denoted $\mathbb{Q}[\sqrt{n}]$. Prove that the sum, product, and quotient of two numbers in $\mathbb{Q}[\sqrt{n}]$ is also in $\mathbb{Q}[\sqrt{n}]$.
   (c) Prove that any eventually periodic continued fraction represents a quadratic irrational.

   In fact, the converse is true, too: Every quadratic irrational has an eventually periodic continued fraction. This is much harder to prove.
4. Prove that at least one of every pair of consecutive convergents satisfies $|\alpha - p_n/q_n| < \frac{1}{2q_n^2}$.
5. A proof of Hurwitz's theorem:
   (a) Suppose that $x \geq 1$. Show that $x + x^{-1} < \sqrt{5}$ if and only if $x < \varphi$ and $x + x^{-1} > \sqrt{5}$ if and only if $x > \varphi$.
   $*$ (b) Prove that at least one out of every three consecutive convergents satisfies $|\alpha - p_n/q_n| < 1/\sqrt{5}q_n^2$.

SOLUTIONS

1.
2. $|\alpha - p_n/q_n| \geq \frac{1}{2}|p_n/q_n - p_{n+1}/q_{n+1}| = 1/2q_nq_{n+1}$.
3. (a) One way to prove this is to write out the expression and physically manipulate it. Another is to write

$$\alpha = [a_0; a_1, \dots, a_k, \alpha]$$

and use the recursion

$$\alpha = \frac{p_{k+1}}{q_{k+1}} = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}}.$$

This yields a quadratic equation with α as a root. The binomial theorem shows that α is a quadratic irrational.

(b) Just do it

(c) Let β be the quadratic irrational associated to the periodic part of α's continued fraction expansion, so that $\alpha = [a_0; a_1, \dots, a_k, \beta]$. Then

$$\alpha = \frac{p_{k+1}}{q_{k+1}} = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}},$$

so use part (b) to conclude that α is quadratic irrational.

4. Suppose not; then

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

Then

$$\frac{q_n^2 + q_{n+1}^2}{2q_n^2q_{n+1}^2} \leq \frac{1}{q_nq_{n+1}},$$

or $q_n^2 + q_{n+1}^2 \leq 2q_nq_{n+1}$. But this is impossible, since it's equivalent to $(q_n - q_{n+1})^2 \leq 0$.

5. (a) The only solution to $x^{-1} = \sqrt{5} + x$ with $x \geq 1$ is $x = \varphi$.

(b) Suppose that $|\alpha - p_n/q_n| \geq 1/\sqrt{5}q_n^2$ and $|\alpha - p_{n+1}/q_{n+1}| \geq 1/\sqrt{5}q_{n+1}^2$. Then

$$\frac{1}{\sqrt{5}q_n^2} + \frac{1}{\sqrt{5}q_{n+1}^2} \leq \left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{1}{q_nq_{n+1}}.$$

Simplifying, we get $q_n/q_{n+1} + q_{n+1}/q_n \leq \sqrt{5}$. Taking $q_{n+1}/q_n = x$ in part (a), we find that $q_{n+1}/q_n \leq \varphi$. Since the left side is rational and the right side is not, $q_{n+1}/q_n < \varphi$. Using the fundamental recurrence for q_n, we have

$$\varphi > \frac{q_{n+1}}{q_n} = \frac{a_{n+1}q_n + q_{n-1}}{q_n} \geq 1 + \frac{q_{n-1}}{q_n}.$$

Since $\varphi - 1 = \varphi^{-1}$, we have $\varphi^{-1} > q_{n-1}/q_n$, or $q_n/q_{n-1} > \varphi$. This is only possible if either $|\alpha - p_n/q_n| < 1/\sqrt{5}q_n^2$ or $|\alpha - p_{n-1}/q_{n-1}| < 1/\sqrt{5}q_n^2$.