154: Diophantine Equations

Nir Elber

Fall 2023

Contents

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Theme 1
Linear Equations

Think deeply of simple things

—Ross Program, [Pro22]

1.1 Modular Arithmetic and Sage

In this section, we review the elementary number theory we will use in these notes. The goal of the present chapter is to be able to solve the equation

$$ax + by = 1$$

as quickly as possible, but we will encounter Diophantine approximation in the process.

1.1.1 Local Obstructions

A theme that will reappear in this course is that of "local obstructions," so we introduce the idea now. Here are some examples.

Example 1.1. The only integer solution to the equation $x^2 + y^2 = 3z^2$ is $(x, y, z) = (0, 0, 0)$.

Solution. Of course $(0, 0, 0)$ is a solution, so the main content is showing that it is the only one. Suppose that (x, y, z) is a nonzero solution, and we suppose that (x, y, z) is minimal with respect to $|x| + |y| + |z| > 0$. If all the terms are even, then $(x/2, y/2, z/2)$ is also an integer solution with $|x/2| + |y/2| + |z/2| < |x| + |y| + |z|$, violating minimality. Thus, we may assume that at least one of the terms is odd. We have two cases; the main point is that $x^2 \equiv 0, 1 \pmod 4$ for any integer x.

- If z is odd, then we are asking for
$$x^2 + y^2 \equiv 3 \pmod 4.$$
But $x^2, y^2 \pmod 4 \in \{0, 1\}$ cannot achieve this.
- If z is even, then we are asking for
$$x^2 + y^2 \equiv 0 \pmod 4.$$
However, without loss of generality we will have x odd and so $x^2 \equiv 1 \pmod 4$. But then $x^2+y^2 \equiv 1+y^2 \pmod 4$ will never be $0 \pmod 4$.

All cases have caused contradiction, so we have finished the proof. ■

Example 1.2. There are no integer solutions to the equation $6x + 9y = 2$.

Solution. Reducing $\pmod 3$ means that any integer solution to $6x + 9y = 2$ implies $0 \equiv 2 \pmod 3$, which is a contradiction. ■

Now that we've seen some examples, let's make explicit what is going on.

Idea 1.3. Given an equation $f(x_1, \ldots, x_n) = 0$, we can check if f has solutions in $\mathbb{Z}$ by first checking if there are solutions to

$$f(x_1, \ldots, x_n) \equiv 0 \pmod m$$

for integers m.

What is useful about Idea 1.3 is that checking for solutions $\pmod m$ amounts to a finite computation where variables live in $\mathbb{Z}/m\mathbb{Z}$, and we can simply run the finite computation to check.

Of course, Idea 1.3 is not perfectly robust, but it will guide our discussion of Diophantine equations throughout this course.

Non-Example 1.4. One can show that

$$(x^2 - 2)(x^2 - 3)(x^2 - 6) = 0$$

has solutions $\pmod p$ for all primes p, but there is no integer solution.

Here is an example which is akin to Idea 1.3 but not quite the same.

Example 1.5. There are no integer solutions to $x^2 + y^2 = 2xy - 1$.

Solution. This equation is actually $(x - y)^2 = -1$, which has no solutions because $(x - y)^2 > -1$ for any real numbers $x, y \in \mathbb{R}$. ■

Example 1.6. There are no integer solutions to $x^2 + y^2 = 6$.

Solution. We see that $x \in \{0, \pm 1, \pm 2\}$ forces $y \in \{\pm\sqrt{6}, \pm\sqrt{5}, \pm\sqrt{2}\}$, none of which provide integer solutions. However, if $|x| \geq 3$, then

$$x^2 + y^2 = 9 + y^2 > 6,$$

from which we see that there are not even real solutions! ■

The above examples teach us that it is also useful to check for real-valued solutions to an equation in addition to checking $\pmod m$ for various integers m. These are also "local obstructions."

1.1.2 The Law of Linear Reciprocity

Idea 1.3 is useful for determining when a linear equation of the form $ax + by = 1$ cannot have solutions. The goal of the present section is to show that these "local obstructions" are the only obstructions. Namely, we will prove a result of the following type.

Proposition 1.7. Let a, b, and c be integers. Then there are integers $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if, for any integer m, there are integers $x_m, y_m \in \mathbb{Z}$ such that

$$ax + by \equiv c \pmod{m}.$$

In other words, it is enough to check locally. However, Proposition 1.7 is not very helpful for actually trying to determine if $ax + by = c$ has solutions: we would have to check $ax + by \equiv c \pmod{m}$ for infinitely many moduli m, which is not a finite computation! Thankfully, we have the following more effective version of Proposition 1.7.

Proposition 1.8. Let a, b, and c be integers. Then there are integers $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if there are integers $x, y \in \mathbb{Z}$ such that

$$ax + by \equiv c \pmod{b}.$$

In other words, the only modulus we have to check is $m = b$. Let's prove Proposition 1.8.

Proof of Proposition 1.8. Of course having integers x and y such that $ax + by = c$ will imply that $ax + by \equiv c \pmod{b}$. Conversely, suppose we have integers x_0 and y_0 such that

$$ax_0 + by_0 \equiv c \pmod{b}.$$

Then we know there is some integer y_1 such that

$$ax_0 + by_0 = c + by_1,$$

so $ax_0 + b(y_0 - y_1) = c$ provides an integer solution to $ax + by = c$. ■

Example 1.9. The equation $3x + 5y = 1$ has integer solutions.

Solution. By Proposition 1.8, it suffices to check $\pmod{3}$. Then we are looking for integers x and y such that

$$3x + 5y \equiv 1 \pmod{3}.$$

Well, $(x, y) = (0, 2)$ will do the trick. ■

Example 1.10. The equation $2x + 4y = 3$ has no integer solutions.

Solution. By Proposition 1.8, it suffices to check $\pmod{2}$. Then we are looking for integers x and y such that

$$2x + 4y \equiv 3 \pmod{2}.$$

But this implies $0 \equiv 3 \pmod{2}$, which is a contradiction, so there can be no integer solutions. ■

Proposition 1.8 also allows us to prove the "reciprocity" theorem. These are also a major theme in number theory, though we will not see even close to the full story in this course. What is remarkable in the following result is that we have found a way to switch the modulus of our "local obstruction" around, perhaps at the cost of adjusting the equation being considered. Such statements are in general very profitable!

Proposition 1.11 (law of linear reciprocity)**.** Let a, b, and c be integers. Then there is an integer x such that $ax \equiv c \pmod{b}$ if and only if there is an integer x such that $bx \equiv c \pmod{a}$.

Proof. There is an integer x such that $ax \equiv c \pmod{b}$ if and only if there are integers x and y such that $ax = c - by$, which is equivalent to

$$ax + by = c.$$

This condition is now symmetric in a and b, so running the above argument backwards provides equivalence to finding an integer x such that $bx \equiv c \pmod{a}$. ■

Example 1.12. The equation $93x + 35y = 1$ has integer solutions.

Solution. By Proposition 1.8, it is equivalent to check that

$$23x \equiv 93x + 35y \equiv 1 \pmod{35}$$

has integer solutions. By Proposition 1.11, this is equivalent to having integer solutions to

$$12x \equiv 35x \equiv 1 \pmod{23}.$$

Going again, by Proposition 1.11, this is equivalent to having integer solutions to

$$11x \equiv 23x \equiv 1 \pmod{12}.$$

Continuing, by Proposition 1.11, this is equivalent to having integer solutions to

$$x \equiv 12x \equiv 1 \pmod{11},$$

for which we see that $x = 1$ works. ■

Example 1.13. The equation $289x + 323y = 2$ has no integer solutions.

Solution. By Proposition 1.8, it is equivalent to check that

$$34y \equiv 289x + 323y \equiv 2 \pmod{289}$$

has integer solutions. By Proposition 1.11, this is equivalent to having integer solutions to

$$17x \equiv 289x \equiv 2 \pmod{34}.$$

One more time, Proposition 1.11 says that it is equivalent to have integer solutions to

$$0 \equiv 34x \equiv 2 \pmod{17},$$

which is false. ■

1.1.3 Bézout's Theorem

Proposition 1.11 does a good job of determining when there are integer solutions to an equation of the form $ax + by = c$, but we would like a more efficient characterization, and we would also like an efficient way to write down the solutions. We begin with the more uniform characterization.

Theorem 1.14 (Bézout)**.** Let a, b, and c be integers. Then there are integers x and y such that $ax + by = c$ if and only if $\gcd(a, b)$ divides c.

We are going to prove Theorem 1.14 multiple times, essentially to emphasize different points of view on this area of number theory. To begin, let's establish that Proposition 1.11 is in fact able to provide a proof.

Proof of Theorem 1.14 via Proposition 1.11. We imitate the previous examples. Note that $ax + by = c$ if and only if $(-a)(-x) + by = c$ and similar for other choices of signs, so we might as well assume that a and b and c are all nonnegative integers. Additionally, having solutions for $ax + by = c$ is a condition symmetric on a and b, so we might as well assume that $a \leq b$.

We induct on a. If $a = 0$, then either $b = 0$, and we have a solution if and only if $c = 0 = \gcd(a, b)$, or $b \neq 0$, and we have a solution if and only if $c = by = \gcd(a, b)y$ for some integer y. Otherwise, $a > 0$. Now, by Proposition 1.8, we have an integer solution if and only if

$$ry \equiv ax + by \equiv c \pmod{a}$$

has an integer solution, where r is chosen so that $b \equiv r \pmod{a}$ and $0 \leq r < a$. By Proposition 1.11, this is now equivalent to having an integer solution to

$$ax \equiv c \pmod{b - a},$$

which by Proposition 1.8 is equivalent to having an integer solution to $rx+ay = c$. But now we have replaced (a, b) with (r, a), where $r < a$ and $\gcd(a, b) = \gcd(r, a)$, so induction completes the argument. ■

The above argument is fairly involved, so it is rewarding to know that the following cleaner proof exists.

Proof of Theorem 1.14 via well-ordering. It suffices to show that

$$\{ax + by : x, y \in \mathbb{Z}\} = \gcd(a, b)\mathbb{Z}.$$

Quickly, if $a = b = 0$, then both sides are $\{0\}$, so there is nothing to say. Otherwise, we may assume that at least one of a or b is nonzero. Certainly $\gcd(a, b)$ divides $ax + by$ for any $x, y \in \mathbb{Z}$, so $\{ax + by : x, y \in \mathbb{Z}\} \subseteq \gcd(a, b)\mathbb{Z}$. It remains to show the other inclusion, which is equivalent to showing $\gcd(a, b) \in \{ax+by : x, y \in \mathbb{Z}\}$.

Well, we expect $\gcd(a, b)$ to be the smallest positive element of $\{ax + by : x, y \in \mathbb{Z}\}$, so we let g denote this smallest positive element, and we want to show that $g = \gcd(a, b)$. (This g exists by the well-ordering of $\mathbb{N}$. Note that $\{ax + by : x, y \in \mathbb{Z}\}$ certainly has some positive element because it contains $a^2 + b^2 > 0$.) Certainly $\gcd(a, b)$ divides g by the argument of the previous paragraph, so it suffices to show that g divides $\gcd(a, b)$, for which we will show that $g \mid a$ and $g \mid b$.

In fact, we will only show that $g \mid a$, and $g \mid b$ follows symmetrically. For this, we use the division algorithm to write

$$a = gq + r$$

for some integers $q, r \in \mathbb{Z}$ where $0 \leq r < g$. Now, $r = a - gq$ will live in $\{ax + by : x, y \in \mathbb{Z}\}$, but $r < g$ forces r to not be a positive element in this set by minimality, so we must have $r = 0$. Thus, $a = gq$, which means $g \mid a$, as needed. ■

The drawback of the above cleaner proof is that it is difficult to see how to turn it into an effective algorithm to actually compute x and y. Indeed, the argument does not even make it clear how to find $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b),$$

which is in some sense the crux of the matter because we can then multiply x and y by $c/\gcd(a, b)$. With some care, we will be able to provide an effective algorithm, but it will take some care.

1.1.4 The Extended Euclidean Algorithm

The motivation to our algorithm will begin with wanting an efficient way to compute $\gcd(a, b)$, which we need to use Theorem 1.14 anyway. The Euclidean algorithm is based on the following lemma.

Lemma 1.15. Let a and b be integers. For any integer q, we have $\gcd(a, b) = \gcd(a - bq, b)$.

Proof. Note that an integer d divides a and b implies that d divides $a - bq$ and b; the converse holds by a symmetric argument. Thus, the conclusion follows from taking the least elements of the sets

$$\{d \in \mathbb{Z}_{\geq 0} : d \mid a \text{ and } d \mid b\} = \{d \in \mathbb{Z}_{\geq 0} : d \mid a - bq \text{ and } d \mid b\},$$

finishing. ■

We are now equipped to see an example of the Euclidean algorithm.

Example 1.16. We use the "Euclidean algorithm" to compute $\gcd(93, 35)$.

Solution. To begin, we repeatedly use the division algorithm to write

$$\begin{aligned} 93 &= 2 \cdot 35 + 23 \\ 35 &= 1 \cdot 23 + 12 \\ 23 &= 1 \cdot 12 + 11 \\ 12 &= 1 \cdot 11 + 1 \\ 11 &= 11 \cdot 1 + 0. \end{aligned}$$

Thus, repeatedly applying Lemma 1.15, we see

$$\gcd(93, 35) = \gcd(35, 23) = \gcd(23, 12) = \gcd(12, 11) = \gcd(11, 1) = 1,$$

which is what we wanted. ■

Exercise 1.17. Use the Euclidean algorithm to compute $\gcd(47, 31)$.

It is somewhat technical to make a rigorous argument avoid the above process. Take a moment to read and digest the following statement.

Proposition 1.18 (Euclidean algorithm)**.** Let a_0 and a_1 be positive coprime integers. Define the integer sequences $a_2, a_3, \ldots$ and $q_0, q_1, \ldots$ recursively by

$$a_n = q_n a_{n+1} + a_{n+2} \qquad \text{where} \qquad 0 \leq a_{n+2} < a_{n+1}$$

where $q_n \coloneqq \lfloor a_n / a_{n+1} \rfloor$ if $a_{n+1} > 0$ and $(a_{n+2}, q_n) \coloneqq (0, 0)$ otherwise. Then there is a minimal N such that $a_n = 0$ for $n > N$, and $a_N = \gcd(a_0, a_1)$.

Proof. By construction of the sequence, if $a_{n+1} > 0$, then $0 \leq a_{n+2} < a_{n+1}$. Thus, if $a_{n+1} > 0$ always, then $a_1, a_2, \ldots$ is a strictly decreasing sequence of positive integers, which is impossible by the well-ordering of the positive integers.

So indeed, there is some integer N such that $a_{N+1} = 0$, and we may choose N to be minimal with this property so that $a_N \neq 0$. (Note that $a_0 \neq 0$, so there is some n with $a_n \neq 0$.) Then $a_{N+1} = 0$ by construction, and the definition of our recursion enforces $a_n = 0$ for all $n > N$.

It remains to show that $a_N = \gcd(a_0, a_1)$. The main claim is that $\gcd(a_0, a_1) = \gcd(a_n, a_{n+1})$ for any $0 \leq n \leq N$, which will complete the proof by plugging in $n = N$. We show this claim by induction: there is nothing to say for $n = 0$, and for any $n < N$ so that $a_{n+1} > 0$, we see that

$$\gcd(a_n, a_{n+1}) = \gcd(q_n a_{n+1} + a_{n+2}, a_{n+1}) = \gcd(a_{n+1}, a_{n+2}),$$

which completes the inductive step. ■

Proposition 1.18 grants us another proof of Theorem 1.14.

Proof of Theorem 1.14 via Proposition 1.18. As usual, we start off with the "easier" direction: if $ax+by=c$ for some $x, y \in \mathbb{Z}$, then we note $\gcd(a,b)$ divides $ax+by$ and so divides c.

We use Proposition 1.18 to show the harder direction. Both the condition $ax+by=c$ and $\gcd(a,b) \mid c$ remain invariant to adjusting the sign of a and b, so we may assume $a, b \geq 0$. Additionally, if $a=0$, then both conditions are equivalent to $b \mid c$; a symmetric argument works for $b=0$. Thus, we may assume that $a, b > 0$.

Now, set $a_0 \coloneqq a$ and $a_1 \coloneqq b$ and build the sequence $a_2, a_3, \ldots$ of Proposition 1.18. By induction, we see that

$$a_n \in \{a_0 x + a_1 y : x, y \in \mathbb{Z}\}.$$

Indeed, there is nothing to say for $n=0$ and $n=1$. Then for the induction, we note that $\{a_0x+a_1y : x, y \in \mathbb{Z}\}$ is closed under $\mathbb{Z}$-linear combination, so containing a_n and a_{n+1} implies containing $a_{n+2} = a_n - q_n a_{n+1}$. Thus, using Proposition 1.18, we see that $a_N = \gcd(a,b)$ takes the form $ax+by$ for $x, y \in \mathbb{Z}$, completing the proof. ■

We are finally able to read the above proof closely to have an effective algorithm to compute x and y solving $ax+by=\gcd(a,b)$. This is called the "extended Euclidean algorithm" and is best seen by example.

Example 1.19. We use the "extended Euclidean algorithm" to find integers x and y such that $93x+35y=1$.

Proof. The idea is to run the Euclidean algorithm backwards "solving" for the remainders. Indeed, using the computations of Example 1.16, we see

$$\begin{aligned} 1 &= 12 - 1 \cdot 11 \\ 11 &= 23 - 1 \cdot 12 \\ 12 &= 35 - 1 \cdot 23 \\ 23 &= 93 - 2 \cdot 35. \end{aligned}$$

We now plug in for each successive remainder, writing

$$\begin{aligned} 1 &= 12 - 1 \cdot 11 \\ &= 12 - 1 \cdot (23 - 1 \cdot 12) = 2 \cdot 12 - 1 \cdot 23 \\ &= 2 \cdot (35 - 1 \cdot 23) - 1 \cdot 23 = 2 \cdot 35 - 3 \cdot 23 \\ &= 2 \cdot 35 - 3 \cdot (93 - 2 \cdot 35) = 8 \cdot 35 - 3 \cdot 93. \end{aligned}$$

Thus, $(x,y) = (-3, 8)$ will do the trick. ■

Exercise 1.20. Use the extended Euclidean algorithm to find integers x and y such that $47x+31y=1$.

1.1.5 Problems

Do at least ten points worth of the following exercises.

Problem 1.1.1 (1 point). Let $n \equiv 3 \pmod 4$. Show that there are not two integers $x, y \in \mathbb{Z}$ such that $x^2+y^2=n$.

Problem 1.1.2 (2 points). Let $n \equiv 7 \pmod 8$. Show that there are not three integers $x, y, z \in \mathbb{Z}$ such that $x^2+y^2+z^2=n$.

Problem 1.1.3 (2 points). Let a and b be integers. Suppose that there are pairs of integers (x, y) and (x', y') such that $ax + by = ax' + by' = 1$. Show that

$$x \equiv x' \pmod{b} \qquad \text{and} \qquad y \equiv y' \pmod{a}.$$

Problem 1.1.4 (2 points). Define the Fibonacci sequence $\{F_n\}_{n=0}^{\infty}$ by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for any $n \geq 0$. Show that $\gcd(F_{n+1}, F_n) = 1$ for any $n \geq 0$.

Problem 1.1.5 (3 points). Compute $\gcd(1027, 1738)$. Then find integers x and y such that $1027x + 1738y = \gcd(1027, 1738)$.

Problem 1.1.6 (3 points). Let a, b, and c be integers with $\gcd(a, b, c) = 1$. Show that there exist integers $x, y, z \in \mathbb{Z}$ such that $ax + by + cz = 1$.

Problem 1.1.7 (5 or 6 points). Implement the extended Euclidean algorithm.

(a) For five points, write (and submit) a function in Python with takes as input two coprime positive integers a and b and outputs integers x and y such that $ax + by = 1$. Your function should implement the extended Euclidean algorithm.

(b) For an additional point, make the function work for any coprime integers a and b.

Your test case is $(a, b) = (12345678901, 10987654321)$.

1.2 Finite Continued Fractions

In this section, we begin our discussion of continued fractions with a discussion of finite continued fractions. The reward for our efforts will be a more memory-efficient version of the extended Euclidean algorithm.

1.2.1 Connection to Continued Fractions

We begin with the definition of a continued fraction.

Definition 1.21 (continued fraction). A *continued fraction* expansion is an expression of the form

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

which we will notate by $[a_0; a_1, a_2, \ldots]$. The terms $a_\bullet$ are the *continued fraction coefficients*.

In our application, the terms $a_0, a_1, a_2, \ldots$ will always be integers, and $a_1, a_2, \ldots$ will always be positive integers, but we take the moment to remark that this definition operates just fine even if these are not integers. This specialization does guarantee that we never run into division-by-zero problems, which is its principal advantage.

Remark 1.22. For the present section, our continued fractions will always be finite in length. In other words, our continued fractions will look like $[a_0; a_1, a_2, \ldots, a_n]$ for some perhaps large n. In the next section, we will allow continued fractions to have infinite length by defining

$$[a_0; a_1, a_2, \ldots] \coloneqq \lim_{n\to\infty} [a_0; a_1, a_2, \ldots, a_n],$$

but we will have to prove that this limit exists before providing this definition.

Continued fractions will be very interesting to us in the sequel, approximately speaking because they provide good rational approximations to real numbers. To start us off, suppose we have a real number α, and we would like to find coefficients $a_0, a_1, a_2, \ldots \in \mathbb{Z}$ such that $\alpha = [a_0; a_1, a_2, \ldots]$. In fact, we will be able to enforce $a_1, a_2, \ldots \in \mathbb{Z}_{\geq 0}$. To see how, note that if we want

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

then we should have $a_0 \coloneqq \lfloor \alpha \rfloor$. Once we agree what a_0 should be, we may rearrange this equation into

$$\frac{1}{\alpha - a_0} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}.$$

Now we are trying to compute the continued fraction for $(\alpha - \lfloor \alpha \rfloor)^{-1} > 1$, so we may recurse. Namely, set $a_1 \coloneqq \left\lfloor (\alpha - \lfloor \alpha \rfloor)^{-1} \right\rfloor$ and then rearrange again.

Here's an example.

Example 1.23. We express $93/35$ as a continued fraction.

Solution. We write

$$\begin{aligned}
\frac{93}{35} &= 2 + \frac{23}{35} \\
&= 2 + \frac{1}{35/23} \\
&= 2 + \frac{1}{1 + \frac{12}{23}} \\
&= 2 + \frac{1}{1 + \frac{1}{23/12}} \\
&= 2 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{11}{12}}} \\
&= 2 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{12/11}}} \\
&= 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{11}}}},
\end{aligned}$$

so $\frac{93}{35} = [2; 1, 1, 1, 11]$. ■

Exercise 1.24. Express $47/31$ as a continued fraction.

Compare Example 1.16 with Example 1.23: the coefficients $[2; 1, 1, 1, 11]$ match up exactly with the quotients appearing in the Euclidean algorithm. Rigorizing this is a little technical, but it is not too hard.

Proposition 1.25. Let a_0 and a_1 be coprime positive integers, and define integer sequences $q_0, q_1, \ldots, q_N$ and $a_0, a_1, a_2, \ldots, a_N$ recursively as in Proposition 1.18 by

$$a_n = q_n a_{n+1} + a_{n+2}$$

for any $n \geq 0$, where $0 < a_{n+2} < a_{n+1}$ and terminating once $a_N = 1$ so that $a_{N+1} = 0$. Then $\frac{a_0}{a_1} = [q_0; q_1, q_2, \ldots, q_N]$.

Proof. Recall that N exists by the Euclidean algorithm. We induct on N. If $N = 1$, then $a_1 = 1$ and

$$a_0 = q_0 a_1 + a_2$$

forces $a_2 = 0$ and $q_0 = a_0$. Thus, $a_0 = \frac{a_0}{a_1} = q_0 = [q_0]$.

Now take $N > 1$ (which implies $a_2 > 0$), and suppose the statement is true at $N - 1$. Then we see $a_0 = q_0 a_1 + a_2$ implies

$$\frac{a_0}{a_1} = q_0 + \frac{1}{a_1/a_2}.$$

Thus, running the Euclidean algorithm with the coprime positive integers a_1 and a_2, we find that $\frac{a_1}{a_2} = [q_1; q_2, \ldots, q_N]$ by the inductive hypothesis. It follows

$$\frac{a_0}{a_1} = q_0 + \frac{1}{[q_1; q_2, \ldots, q_N]} = [q_0; q_1, q_2, \ldots, q_N],$$

which is what we wanted. ∎

Remark 1.26. Proposition 1.25 also has the nice side effect of showing that any rational number is equal to some finite continued fraction. However, note this continued fraction is not unique: given integers $a_0, a_1, a_2, \ldots, a_n$ with $a_1, a_2, \ldots, a_n$ positive, one has

$$[a_0; a_1, a_2, \ldots, a_{n-1}, a_n] = [a_0; a_1, a_2, \ldots, a_{n-1}, a_n - 1, 1]$$

when $a_n > 1$, and otherwise

$$[a_0; a_1, a_2, \ldots, a_{n-1}, 1] = [a_0; a_1, a_2, \ldots, a_{n-1} + 1].$$

In particular, given any rational number q, we can find n of any parity such that there are integers $a_0, a_1, a_2, \ldots, a_n$ with $a_1, a_2, \ldots, a_n$ positive and $q = [a_0; a_1, a_2, \ldots, a_n]$.

The proof of Proposition 1.25 is fairly instructive: many of our arguments involving continued fractions are going to be inductive ones using identities like

$$q_0 + \frac{1}{[q_1; q_2, \ldots, q_N]} = [q_0; q_1, q_2, \ldots, q_N].$$

1.2.2 Continued Fraction Convergents

We mentioned at the outset that continued fractions provide good rational approximations for numbers. The way that this is done is by taking a long continued fraction $[a_0; a_1, a_2, \ldots]$ and "truncating" it at some point to produce the shorter (and notably finite) continued fraction $[a_0; a_1, a_2, \ldots, a_n]$. This truncation process is so important it has a name.

Definition 1.27 (convergent)**.** Given a continued fraction $[a_0; a_1, a_2, \ldots]$ and some $n \geq 0$, the truncation $[a_0; a_1, a_2, \ldots, a_n]$ is the *nth convergent*, often denoted

$$\frac{h_n}{k_n} \coloneqq [a_0; a_1, \ldots, a_n].$$

As usual, we begin with an example.

Example 1.28. We compute the continued fraction convergents of $93/35$.

Solution. In Example 1.23, we computed that $\frac{93}{35} = [2; 1, 1, 1, 11]$, so here are our convergents.

- The zeroth convergent is $[2] = 2$.
- The first convergent is $[2; 1] = 2 + \frac{1}{1} = 3$.
- The second convergent is $[2; 1, 1] = 2 + \frac{1}{1+1} = \frac{5}{2}$.
- The third convergent is $[2; 1, 1, 1]$ is

$$[2; 1, 1, 1] = 2 + \frac{1}{1 + \dfrac{1}{1+1}} = 2 + \frac{1}{3/2} = \frac{8}{3}.$$

- The fourth convergent is $[2; 1, 1, 1, 11] = \frac{93}{35}$. ∎

Exercise 1.29. Compute the continued fraction convergents of $47/31$.

The process outlined in Example 1.28 is rather annoying to execute by hand. We did not even compute $[2; 1, 1, 1, 11]$ by hand, but already $[2; 1, 1, 1]$ required some focus. In general, the problem with computing these convergents is that we are basically doing a totally new computation for every convergent.

However, there is a much faster way to compute these convergents: the "magic box" algorithm. For a sense of wonder, we will describe the algorithm first and then prove that it works second. We begin with the following grid.

		2	1	1	1	11
0	1					
1	0					

Explicitly, the 0s and 1s on the leftmost two columns will always be there in all computations, and the top row is made of our coefficients $[2; 1, 1, 1, 11]$. We now fill in the grid column-by-column, moving from left to right. For the next leftmost column, we multiply the coefficient 2 by the previous column and then add the column before that. In other words, we compute

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} + 2 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix},$$

so the next column in our grid is as follows.

		2	1	1	1	11
0	1	2				
1	0	1				

Indeed, $2/1$ is the zeroth convergent. We now repeat the process: multiply 1 by the previous column and then add the column before that, writing

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} + 1 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix},$$

making our grid as follows.

		2	1	1	1	11
0	1	2	3			
1	0	1	2			

Indeed, $3/1$ is the first convergent. We now fill in the rest of the grid.

		2	1	1	1	11
0	1	2	3	5	8	93
1	0	1	1	2	3	35

And indeed, we see the remaining convergents $5/2$, $8/3$, and $93/35$ appear from our grid.

Exercise 1.30. Execute this "magic box" algorithm to compute the continued fraction convergents of $47/31$.

Exercise 1.31. Compute the following 2×2 "minors" of our grid, as follows.

$$\det \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \det \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad \det \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}, \quad \det \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}, \quad \dots.$$

Do you see any patterns?

Proving that the magic box algorithm works is again somewhat technical. Perhaps the main difficulty is figuring out how to state the result, but the proof is still tricky. For now, we will settle for the following statement, but we will establish the refinement Corollary 1.36 shortly.

Proposition 1.32 (magic box)**.** Let $a_0, a_1, a_2, \dots$ be real numbers, where $a_1, a_2, \dots$ are positive. Define the sequences $\{h_n\}_{n=-2}^{\infty}$ and $\{k_n\}_{n=-2}^{\infty}$ of real numbers recursively by

$$\begin{bmatrix} h_{-2} & h_{-1} \\ k_{-2} & k_{-1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} h_{n+2} \\ k_{n+2} \end{bmatrix} = a_{n+2} \begin{bmatrix} h_{n+1} \\ k_{n+1} \end{bmatrix} + \begin{bmatrix} h_n \\ k_n \end{bmatrix}$$

for $n \geq -2$. Then

$$[a_0; a_1, \dots, a_n] = \frac{h_n}{k_n}$$

for any $n \geq 0$.

Proof. The requirement that $a_1, a_2, \dots$ be positive is entirely to avoid division by zero errors. We also take a moment to recognize that the $a_\bullet$ are being allowed to be real numbers rather than only integers. This will actually be relevant to the proof!

We induct on n. For $n = 0$, we can compute that $(h_0, k_0) = a_0(1, 0) + (0, 1) = (a_0, 1)$, so $\frac{h_0}{k_0} = a_0 = [a_0]$. For $n = 1$, we can compute that $(h_1, k_1) = a_1(a_0, 1) + (1, 0) = (a_1 a_0 + 1, a_1)$, so

$$\frac{h_1}{k_1} = \frac{a_1 a_0 + 1}{a_1} = a_0 + \frac{1}{a_1} = [a_0; a_1].$$

Now take $n \geq 2$. The trick for the inductive step is to write

$$[a_0; a_1, \dots, a_{n-2}, a_{n-1}, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} = \left[a_0; a_1, \dots, a_{n-2}, a_{n-1} + \frac{1}{a_n}\right].$$

We may now apply the inductive hypothesis to this altered continued fraction, which is legal because $a_{n-1} + 1/a_n$ is surely a positive real number. Explicitly, define the sequence $a'_0, a'_1, \ldots, a'_{n-1}$ where $a'_m := a_m$ for $m < n-1$ and $a'_{n-1} := a_{n-1} + \frac{1}{a_n}$, and then define the sequence $\{h'_m\}_{m=-2}^{n-1}$ and $\{k'_m\}_{m=-2}^{\infty}$ as in the proposition so that

$$[a_0; a_1, \ldots, a_{n-2}, a_{n-1}, a_n] = [a'_0; a'_1, \ldots, a'_{n-1}] = \frac{h'_{n-1}}{k'_{n-1}}.$$

To compute h'_{n-1} and k'_{n-1} we acknowledge that the construction of the $a'_\bullet$ implies that $h'_m = h_m$ and $k'_m = k_m$ for $m < n-1$. So we see that

$$\begin{aligned}
\begin{bmatrix} h'_{n-1} \\ k'_{n-1} \end{bmatrix} &= a'_{n-1} \begin{bmatrix} h'_{n-2} \\ k'_{n-2} \end{bmatrix} + \begin{bmatrix} h'_{n-3} \\ k'_{n-3} \end{bmatrix} \\
&= \left(a_{n-1} + \frac{1}{a_n} \right) \begin{bmatrix} h_{n-2} \\ k_{n-2} \end{bmatrix} + \begin{bmatrix} h_{n-3} \\ k_{n-3} \end{bmatrix} \\
&= \begin{bmatrix} \left(a_{n-1} + \frac{1}{a_n} \right) h_{n-2} + h_{n-3} \\ \left(a_{n-1} + \frac{1}{a_n} \right) k_{n-2} + k_{n-3} \end{bmatrix}.
\end{aligned}$$

From here, we compute

$$\begin{aligned}
\frac{h'_{n-1}}{k'_{n-1}} &= \frac{a_{n-1}a_n h_{n-2} + h_{n-2} + a_n h_{n-3}}{a_{n-1}a_n k_{n-2} + k_{n-2} + a_n k_{n-3}} \\
&= \frac{a_n(a_{n-1}h_{n-2} + h_{n-3}) + h_{n-2}}{a_n(a_{n-1}k_{n-2} + k_{n-3}) + k_{n-2}} \\
&= \frac{a_n h_{n-1} + h_{n-2}}{a_n k_{n-1} + k_{n-2}} \\
&= \frac{h_n}{k_n},
\end{aligned}$$

which completes the proof. ■

Remark 1.33. The proof of Proposition 1.32 in fact works even if we merely assume that the $a_\bullet$ are indeterminate variables.

Example 1.34. Define the Fibonacci sequence $\{F_n\}_{n=0}^{\infty}$ by $F_0 = 0$ and $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for any $n \geq 0$. Then for any $n \geq 0$,

$$\underbrace{[1; 1, \ldots, 1]}_{n+1} = \frac{F_{n+2}}{F_{n+1}}.$$

Solution. We proceed by induction on n, using Proposition 1.32. From there, we may compute that $h_0/k_0 = 1/1 = F_2/F_1$ and $h_1/k_1 = 2/1 = F_3/F_2$. For the inductive step, we note that Proposition 1.32 yields

$$h_{n+2} = h_{n+1} + h_n \qquad \text{and} \qquad k_{n+2} = k_{n+1} + k_n$$

for any $n \geq 0$, which is the recursion for the Fibonacci sequence. ■

1.2.3 More on the Magic Box Algorithm

Proposition 1.32 essentially explains why the magic box works, though perhaps there is some doubt that the fractions h_n/k_n is in reduced form. Let's show this. We begin by explaining Exercise 1.31.

Corollary 1.35. Let $a_0, a_1, a_2, \ldots$ be real numbers, where $a_1, a_2, \ldots$ are positive, and define $\{h_n\}_{n=-2}^{\infty}$ and $\{k_n\}_{n=-2}^{\infty}$ as in Proposition 1.32. Then

$$\det \begin{bmatrix} h_n & h_{n+1} \\ k_n & k_{n+1} \end{bmatrix} = (-1)^{n+1}$$

for any $n \geq -2$.

Proof. This is essentially row-reduction. We proceed by induction on n. At $n = -2$, we see that $\det \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] = -1$. For the inductive step, suppose the statement for n, and we show $n+1$. We note

$$\begin{bmatrix} h_{n+2} \\ k_{n+2} \end{bmatrix} = a_{n+2} \begin{bmatrix} h_{n+1} \\ k_{n+1} \end{bmatrix} + \begin{bmatrix} h_n \\ k_n \end{bmatrix}$$

allows us to use column operations in order to see

$$\det \begin{bmatrix} h_{n+1} & h_{n+2} \\ k_{n+1} & k_{n+2} \end{bmatrix} = \det \begin{bmatrix} h_{n+1} & h_n \\ k_{n+1} & k_n \end{bmatrix} = -\det \begin{bmatrix} h_n & h_{n+1} \\ k_n & k_{n+1} \end{bmatrix} = -(-1)^{n+1} = (-1)^{n+2},$$

which is what we wanted. ■

Corollary 1.36. Let $a_0, a_1, a_2, \ldots$ be integers, where $a_1, a_2, \ldots$ are positive, and define $\{h_n\}_{n=-2}^{\infty}$ and $\{k_n\}_{n=-2}^{\infty}$ as in Proposition 1.32. Then, for any $n \geq 0$,

$$[a_0; a_1, \ldots, a_n] = \frac{h_n}{k_n},$$

and h_n/k_n is a fraction in reduced form with $k_n \geq 1$.

Proof. The equality follows directly from Proposition 1.32. Additionally, note that h_n and k_n are integers because they are terms of a sequence defined by integer recursion. Thus, to complete the proof, we must show that $\gcd(h_n, k_n) = 1$ and that $k_n \geq 1$ for $n \geq 0$. On one hand, we see $\gcd(h_n, k_n) = 1$ is direct from Corollary 1.35. On the other hand, $k_n \geq 1$ follows from a quick induction because $k_{-1} = 0$ and $k_0 = a_1 \geq 1$ and so $k_{n+2} = a_{n+2}k_{n+1} + k_n \geq 1$ always. ■

Corollary 1.35 has in fact suggested a faster algorithm (in terms of memory) than the Extended Euclidean algorithm. Let's see this by example.

Example 1.37. We find integers x and y such that $93x + 35y = 1$.

Solution. As in Example 1.16, we begin by writing

$$\begin{aligned} 93 &= 2 \cdot 35 + 23 \\ 35 &= 1 \cdot 23 + 12 \\ 23 &= 1 \cdot 12 + 11 \\ 12 &= 1 \cdot 11 + 1 \\ 11 &= 11 \cdot 1 + 0. \end{aligned}$$

From here, we apply the magic box algorithm Proposition 1.32 to build the following grid.

		2	1	1	1	11
0	1	2	3	5	8	93
1	0	1	1	2	3	35

Tracking Corollary 1.35 through, we see that

$$35 \cdot 8 - 93 \cdot 3 = \det \begin{bmatrix} 8 & 93 \\ 3 & 25 \end{bmatrix} = 1,$$

so $(x, y) = (-3, 8)$ works. ■

Remark 1.38. Here are a few ways to "check" the magic box algorithm.

- If using the magic box algorithm to compute convergents of the fraction p/q, then the last column of the magic box grid should yield p/q.
- The magic box algorithm has 2×2 minors controlled by Corollary 1.35, so one can compute a few of these for security.

1.2.4 Problems

Do at least 10 points worth of the following exercises.

Problem 1.2.1 (1 point)**.** Find integer sequences $a_0, a_1, a_2, \ldots, a_m$ and $b_0, b_1, b_2, \ldots, b_n$ with $a_1, a_2, \ldots, a_m$ and $b_1, b_2, \ldots, b_n$ positive such that the sequences are distinct, but

$$[a_0; a_1, \ldots, a_m] = [b_0; b_1, \ldots, b_n].$$

Problem 1.2.2 (2 points)**.** Compute the continued fraction convergents of $1738/1027$.

Problem 1.2.3 (3 points)**.** Let $a_0, a_1, a_2, \ldots$ be integers, where $a_1, a_2, \ldots$ are positive, and define $\{h_n\}_{n=-2}^{\infty}$ and $\{k_n\}_{n=-2}^{\infty}$ as in Proposition 1.32. Show that

$$\left| \det \begin{bmatrix} h_n & h_{n+2} \\ k_n & k_{n+2} \end{bmatrix} \right| = 1.$$

Additionally, predict the sign as a function on n.

Problem 1.2.4 (5 or 6 points)**.** Let $a_0, a_1, a_2, \ldots, a_m$ and $b_0, b_1, b_2, \ldots, b_n$ be integers with $a_1, a_2, \ldots, a_m$ and $b_1, b_2, \ldots, b_n$ positive. Suppose

$$[a_0; a_1, a_2, \ldots, a_m] = [b_0; b_1, b_2, \ldots, b_n].$$

(a) For five points, suppose $m = n$. Show that $a_k = b_k$ for all $0 \le k \le m$.

(b) For an additional point, suppose $m < n$. Show that $m = n - 1$ and $a_k = b_k$ for $0 \le k \le m - 1$.

Problem 1.2.5 (5 points)**.** Write (and submit) a function in Python which takes as input a list of integers $[a_0, a_1, a_2, \ldots]$ with $a_1, a_2, \ldots$ positive and an index n and outputs the nth convergent $[a_0; a_1, a_2, \ldots, a_n]$. You should implement the magic box algorithm.

Your test case is $[2; 1, 2, 1, 1, 4, 1, 1, 6, 1]$.

1.3 Infinite Continued Fractions

In this section, we examine continued fractions more closely. Our main task will be to show that continued fractions provide good and in fact the best rational approximations for a given irrational number. Of course, it will be a nontrivial task in order to make sense of what "best" means in this context. To set up our intuition, we will say that a fraction h/k provides a good rational approximation for a real number α if the difference

$$\left|\alpha - \frac{h}{k}\right|$$

is smaller than one might expect it to be. Of course, for any given denominator, we know that $\lfloor k\alpha \rfloor \leq k\alpha < \lfloor k\alpha \rfloor + 1$, so

$$\left|\alpha - \frac{\lfloor k\alpha \rfloor}{k}\right| \leq \frac{1}{k},$$

so a bound of $1/k$ is not too impressive. In fact, if α is irrational, we will be able to show that there are infinitely many rational numbers h/k such that

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{\sqrt{5}k^2},$$

and we will be able to show that this bound is essentially sharp.

1.3.1 Convergence of Infinite Continued Fractions

Thus far our discussion has been focused on finite continued fractions. We would now like to extend this discussion to infinite continued fractions. As in Remark 1.22, we would like to define

$$[a_0; a_1, a_2, \ldots] \stackrel{?}{:=} \lim_{n\to\infty} [a_0; a_1, a_2, \ldots, a_n],$$

but we should begin by showing that this limit in fact exists. The idea is to show that the infinite continued fraction is an infinite series, and then we can use known results on infinite series to complete the proof. As such, we begin by turning $[a_0; a_1, a_2, \ldots]$ into a series.

Lemma 1.39. Let $a_0, a_1, a_2, \ldots$ be real numbers, where $a_1, a_2, \ldots$ are positive, and let $\{h_n/k_n\}_{n=0}^{\infty}$ denote the continued fraction convergents $h_n/k_n := [a_0; a_1, a_2, \ldots, a_n]$ where $k_n \geq 1$ and $\gcd(h_n, k_n) = 1$. Then

$$\frac{h_n}{k_n} - \frac{h_{n+1}}{k_{n+1}} = \frac{(-1)^{n+1}}{k_n k_{n+1}}.$$

Thus,

$$\frac{h_n}{k_n} = \frac{h_0}{k_0} + \sum_{m=0}^{n-1} \frac{(-1)^m}{k_m k_{m+1}}.$$

Proof. Note that $\{h_n\}_{n=0}^{\infty}$ and $\{k_n\}_{n=0}^{\infty}$ are the sequences constructed in Proposition 1.32 by Corollary 1.36. As such, the first claim follows directly from Corollary 1.35. The second claim now follows from writing

$$\frac{h_n}{k_n} = \frac{h_0}{k_0} + \sum_{m=0}^{n-1} \left(\frac{h_{m+1}}{k_{m+1}} - \frac{h_m}{k_m}\right) = \frac{h_0}{k_0} + \sum_{m=0}^{n-1} \frac{(-1)^m}{k_m k_{m+1}},$$

which is what we wanted. ∎

Proposition 1.40. Let $a_0, a_1, a_2, \ldots$ be integers, where $a_1, a_2, \ldots$ are positive, and let $\{h_n/k_n\}_{n=0}^{\infty}$ denote the continued fraction convergents $h_n/k_n \coloneqq [a_0; a_1, \ldots, a_n]$ where $k_n \geq 1$ and $\gcd(h_n, k_n) = 1$. Then

$$\alpha \coloneqq \lim_{n\to\infty} [a_0; a_1, a_2, \ldots, a_n]$$

converges, and

$$\frac{1}{k_n(k_{n+1}+k_n)} < \left|\alpha - \frac{h_n}{k_n}\right| < \frac{1}{k_n k_{n+1}}$$

for each $n \geq 0$.

Proof. As usual, note that $\{h_n\}_{n=0}^{\infty}$ and $\{k_n\}_{n=0}^{\infty}$ are the sequences constructed in Proposition 1.32 by Corollary 1.36. To begin, we compute the limit as

$$\alpha = \lim_{n\to\infty} \frac{h_n}{k_n} = \frac{h_0}{k_0} + \sum_{n=0}^{\infty} \frac{(-1)^n}{k_n k_{n+1}},$$

where we have used Lemma 1.39 in the last equality. Now, the sequence $\{k_n\}_{n=0}^{\infty}$ is strictly increasing by Proposition 1.32 because $a_1, a_2, \ldots$ are all positive integers. Thus, the summation above absolute converges: an induction shows $k_n \geq n+1$, so

$$\frac{h_0}{k_0} + \sum_{n=0}^{\infty} \left|\frac{(-1)^n}{k_n k_{n+1}}\right| \leq \frac{h_0}{k_0} + \sum_{n=0}^{\infty} \frac{1}{(n+1)(n+2)} < \infty.$$

As such, the limit does in fact converge.

To compute the error term, we use the error bound for alternating series. To begin the computation, note that the above work allows us to write

$$\left|\alpha - \frac{h_n}{k_n}\right| = \left|\frac{h_0}{k_0} + \sum_{m=0}^{\infty} \frac{(-1)^m}{k_m k_{m+1}} - \frac{h_0}{k_0} - \sum_{m=0}^{n-1} \frac{(-1)^m}{k_m k_{m+1}}\right| = \left|\sum_{m=n}^{\infty} \frac{(-1)^m}{k_m k_{m+1}}\right|.$$

Because the sequence $\{k_m\}_{m=0}^{\infty}$ is strictly increasing, the terms in the sum are monotonously decreasing in magnitude to zero, so the error bound for alternating series forces $|\alpha - h_n/k_n| < 1/(k_n k_{n+1})$, which proves the upper bound for our error.

To prove the lower bound of the error, we adjust for signs and note that the sum is

$$\begin{aligned}
\left|\alpha - \frac{h_n}{k_n}\right| &= \left|\sum_{m=0}^{\infty} \frac{(-1)^m}{k_{m+n}k_{m+n+1}}\right| \\
&= \left|\sum_{m=0}^{\infty} \left(\frac{1}{k_{2m+n}k_{2m+n+1}} - \frac{1}{k_{2m+n+1}k_{2m+n+2}}\right)\right| \\
&= \left|\sum_{m=0}^{\infty} \frac{1}{k_{2m+n+1}} \cdot \frac{k_{2m+n+2} - k_{2m+n}}{k_{2m+n}k_{2m+n+2}}\right|.
\end{aligned}$$

Because $\{k_n\}_{n=0}^{\infty}$ is a strictly increasing sequence, all the terms of the sum are positive, so we may remove the absolute signs to see

$$\left|\alpha - \frac{h_n}{k_n}\right| > \frac{1}{k_{n+1}} \cdot \frac{k_{n+2} - k_n}{k_n k_{n+2}}.$$

Thus, to prove the desired lower bound, we must show $k_{n+1}k_{n+2} < (k_{n+1}+k_n)(k_{n+2}-k_n)$. This rearranges to $k_n^2 < k_n(k_{n+1}+k_{n+2})$, which is true. ∎

Remark 1.41. Proposition 1.40 tells us that h_n/k_n will be a "better" rational approximation for α when k_{n+1} is particularly large. For example, $\pi = [3; 7, 15, 1, 292, 1, 1, 1]$, so we would guess that

$$[3; 7, 15, 1] = \frac{355}{113} = 3.14159292035\ldots$$

is a particularly good rational approximation of π, and indeed it is. Notably, $[3; 7] = 22/7$ is also a remarkable rational approximation.

As such, we may make the following definition.

Definition 1.42 (infinite continued fraction)**.** Let $a_0, a_1, a_2, \ldots$ be integers, where $a_1, a_2, \ldots$ are positive. Then we define the *infinite continued fraction*

$$[a_0; a_1, a_2, \ldots] \coloneqq \lim_{n\to\infty} [a_0; a_1, a_2, \ldots, a_n].$$

Example 1.43. We have

$$\varphi \coloneqq \frac{1+\sqrt{5}}{2} = [1; 1, 1, \ldots].$$

Solution. By Proposition 1.40, we know that $[1; 1, 1, \ldots]$ converges to some real number α. Further,

$$\alpha = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}} = 1 + \frac{1}{\alpha},$$

which rearranges to $\alpha^2 - \alpha - 1 = 0$, so

$$\alpha \in \left\{ \frac{1 \pm \sqrt{5}}{2} \right\}.$$

However, we claim that $\alpha > 0$. With the tools we have, this is somewhat annoying to show, but we remark that Lemma 1.57 makes this relatively easy. Anyway, let $\{h_n/k_n\}_{n=0}^{\infty}$ denote the continued fraction convergents. Proposition 1.32 implies that $h_0/k_0 = 1/1$ and $h_1/k_1 = 2/1$, so

$$|\alpha - 1| = \left|\alpha - \frac{h_0}{k_0}\right| < \frac{1}{k_0 k_1} = 1,$$

so $\alpha > 0$. Thus, $\alpha = \varphi$. ∎

Exercise 1.44. Compute $[2; 2, 2, \ldots]$.

The above examples have the amusing feature that $[a_0; a_1, a_2, \ldots]$ is irrational. This is not a coincidence. The following result is perhaps our first "Diophantine approximation" result.

Proposition 1.45. Let α be a real number, and let $C > 0$. Then α is irrational if there is a sequence of rational numbers $\{h_n/k_n\}_{n=0}^{\infty}$ such that

$$\left|\alpha - \frac{h_n}{k_n}\right| < \frac{C}{k_n^2}$$

for each $n \geq 0$.

Proof. We show the contrapositive. Suppose that $\alpha = p/q$ is rational with $q \geq 1$ and $\gcd(p,q) = 1$, and we show that there are only finitely many rational numbers h/k such that $|\alpha - h/k| < C/k^2$; we may assume that $k \geq 1$ and that $\gcd(h,k) = 1$ in our fractions h/k. Now, for any given k, we note that our inequality rearranges to

$$|h - k\alpha| < \frac{C}{k},$$

so there are only finitely many integers h in our interval. Thus, it suffices to upper-bound k. Well, plugging in $\alpha = p/q$ and clearing fractions reveals that we want

$$|qh - pk| < \frac{Cp}{k}.$$

Now, we claim that $k \leq \max\{Cp, q\}$, which completes the proof. Well, suppose that $k > Cp$, and we will show $k = q$. Indeed, $qh - pk$ is an integer with magnitude less than 1, so it follows that $qh - pk = 0$, so in fact

$$qh = pk.$$

By the uniqueness of our representation of rational numbers, it follows that $k = q$. Explicitly, $q \mid pk$, but $\gcd(q,p) = 1$, so $q \mid k$. A symmetric argument shows $k \mid q$, so $k, q \geq 1$ establishes $k = q$. ■

Remark 1.46. Proposition 1.45 is fairly surprising result! Approximately speaking, it says that having "too many" good rational approximations of a given real number actually forces the real number to be irrational! We will prove a converse shortly in Corollary 1.53.

Remark 1.47. Here is a way to intuit Proposition 1.45: there is a sense in which rational numbers cannot be "too close to each other" simply because

$$\left|\frac{a}{b} - \frac{c}{d}\right| \geq \frac{1}{|bd|}.$$

Thus, we should not be able to use rational numbers to provide good rational approximations of rational numbers.

Corollary 1.48. Let $a_0, a_1, a_2, \ldots$ be integers, where $a_1, a_2, \ldots$ are positive. Then $[a_0; a_1, a_2, \ldots]$ is irrational.

Proof. Let $\{h_n/k_n\}_{n=0}^{\infty}$ denote the continued fraction convergents $h_n/k_n := [a_0; a_1, \ldots, a_n]$ where $k_n \geq 1$ and $\gcd(h_n, k_n) = 1$. Then Proposition 1.40 establishes that

$$\left|[a_0; a_1, a_2, \ldots] - \frac{h_n}{k_n}\right| < \frac{1}{k_n k_{n+1}} < \frac{1}{k_n^2}$$

for each $n \geq 0$, where the last inequality follows because $\{k_n\}_{n=0}^{\infty}$ is strictly increasing. Proposition 1.45 completes the proof. ■

1.3.2 Building Infinite Continued Fractions

Given an irrational real number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, we would like to construct a sequence of integers $a_0, a_1, a_2, \ldots$ with $a_1, a_2, \ldots$ positive and $\alpha = [a_0; a_1, a_2, \ldots]$. We did this by hand for φ in Example 1.43, but this is not a general algorithm.

Let's describe what the algorithm should be. Suppose we could write $\alpha = [a_0; a_1, a_2, \ldots]$. Then

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

forces $a_0 = \lfloor \alpha \rfloor$. From here, define $\alpha_1 \coloneqq (\alpha - a_0)^{-1}$, and we see

$$\alpha_1 = a_1 + \cfrac{1}{a_2 + \ddots}.$$

Then we can see that we must have $a_1 = \lfloor \alpha_1 \rfloor$, and we go on to define $\alpha_2 = (\alpha_1 - a_1)^{-1}$ and continue the process. This suggests the following result.

Proposition 1.49. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be an irrational number. Define the sequence of real numbers $\{\alpha_n\}_{n=0}^{\infty}$ and integers $\{a_n\}_{n=0}^{\infty}$ by $\alpha_0 \coloneqq \alpha$ and

$$a_n \coloneqq \lfloor \alpha_n \rfloor \qquad \text{and} \qquad \alpha_{n+1} \coloneqq \frac{1}{\alpha_n - a_n}$$

Then $a_0, a_1, a_2, \ldots$ are integers, and $a_1, a_2, \ldots$ are positive, and $\alpha = [a_0; a_1, a_2, \ldots]$.

Proof. Quickly, we note that there are no division by zero problems: by construction, the $a_\bullet$ are all integers, and the recursion implies that α_{n+1} is irrational if and only if α_n is irrational, so induction implies that all the $\alpha_\bullet$ are irrational. Next up, we note that $a_n < \alpha_n < a_n + 1$ for each $n \geq 0$ (recall α_n is irrational for each n), so $0 < \alpha_n - a_n < 1$ for each $n \geq 0$, so $a_{n+1} \geq 1$ for each $n \geq 0$, so $a_1, a_2, \ldots$ are in fact positive integers.

It remains to show $\alpha = [a_0; a_1, a_2, \ldots]$. This is somewhat technical. The main claim is that

$$\alpha \overset{?}{=} [a_0; a_1, \ldots, a_n, \alpha_{n+1}]$$

for each $n \geq 0$. We show this by induction. For $n = -1$, there is nothing to say because $\alpha = \alpha_0$. For the induction, we write

$$\begin{aligned}
\alpha &= [a_0; a_1, \ldots, a_n, \alpha_{n+1}] \\
&= [a_0; a_1, \ldots, a_n, \lfloor \alpha_{n+1} \rfloor + \{\alpha_{n+1}\}] \\
&= \left[a_0; a_1, \ldots, a_n, a_{n+1} + \frac{1}{\alpha_{n+2}}\right] \\
&= [a_0; a_1, \ldots, a_n, a_{n+1}, a_{n+2}],
\end{aligned}$$

which completes the induction.

We now finish the proof that $\alpha = [a_0; a_1, a_2, \ldots]$. For each $n \geq 0$, set $h_n/k_n \coloneqq [a_0; a_1, \ldots, a_n]$ and $h'_{n+1}/k'_{n+1} \coloneqq [a_0; a_1, a_2, \ldots, a_n, \alpha_{n+1}]$ as constructed in Proposition 1.32. Then applying Lemma 1.39 implies

$$\begin{aligned}
\alpha - [a_0; a_1, a_2, \ldots, a_n] &= [a_0; a_1, \ldots, a_n, \alpha_{n+1}] - [a_0; a_1, a_2, \ldots, a_n] \\
&= \frac{h_0}{k_0} + \sum_{m=0}^{n-1} \frac{(-1)^m}{k_m k_{m+1}} - \frac{h_0}{k_0} - \sum_{m=0}^{n-1} \frac{(-1)^m}{k_m k_{m+1}} - \frac{(-1)^n}{k_n k'_{n+1}} \\
&= \frac{(-1)^n}{k_n k'_{n+1}}.
\end{aligned}$$

Thus,

$$|\alpha - [a_0; a_1, a_2, \ldots, a_n]| \leq \frac{1}{k_n^2},$$

where we have used the fact that $k'_{n+1} = \alpha_{n+1} k_n + k_{n-1} \geq k_n$. Sending $n \to \infty$ makes $k_n \to \infty$, so we conclude $[a_0; a_1, \ldots, a_n] \to \alpha$ as $n \to \infty$. ∎

Exercise 1.50. Use Proposition 1.49 (and Sage) to compute the first 10 continued fraction coefficients of π.

Remark 1.51. In contrast to Remark 1.26, the continued fraction attached to irrational $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ is unique. The proof is approximately along the lines as the argument at the start of the subsection. Namely, suppose we have integers $a_0, a_1, a_2, \ldots$ and $b_0, b_1, b_2, \ldots$ with $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ positive, and suppose

$$[a_0; a_1, a_2, \ldots] = [b_0; b_1, b_2, \ldots].$$

We want to show $a_n = b_n$ for all n. Because $[a_0; a_1, a_2, \ldots] = a_0 + [a_1; a_2, \ldots]^{-1}$, it suffices by induction to show that $a_0 = b_0$. Well, $a_1, b_1 \geq 1$ implies $[a_1; a_2, \ldots], [b_1, b_2, \ldots] > 1$, so

$$a_0 = \left\lfloor a_0 + \frac{1}{[a_1; a_2, \ldots]} \right\rfloor = \lfloor [a_0; a_1, a_2, \ldots] \rfloor = \lfloor [b_0; b_1, b_2, \ldots] \rfloor = b_0.$$

Proposition 1.49 allows us to make the following terminology.

Definition 1.52 (convergent)**.** Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be an irrational number. By Proposition 1.49, we may find integers $a_0, a_1, a_2, \ldots$ where $a_1, a_2, \ldots$ are positive and $\alpha = [a_0; a_1, a_2, \ldots]$. Then the *$n$th continued fraction convergent of α* is $[a_0; a_1, a_2, \ldots, a_n]$.

Corollary 1.53. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be an irrational number. Then there is a sequence of rational numbers $\{h_n/k_n\}_{n=0}^{\infty}$ such that

$$\left| \alpha - \frac{h_n}{k_n} \right| < \frac{1}{k_n^2}$$

for each $n \geq 0$.

Proof. We use continued fraction convergents. Let $\{h_n/k_n\}_{n=0}^{\infty}$ be the sequence of continued fraction convergents of α. Then Proposition 1.40 implies

$$\left| \alpha - \frac{h_n}{k_n} \right| < \frac{1}{k_n k_{n+1}}.$$

Because $k_{n+1} > k_n$ by the recursion, the conclusion follows. ∎

1.3.3 Convergents Are Good Rational Approximations

As before, let $a_0, a_1, a_2, \ldots$ be integers, where $a_1, a_2, \ldots$ are positive, and let $\{h_n/k_n\}_{n=0}^{\infty}$ denote the continued fraction convergents $h_n/k_n := [a_0; a_1, \ldots, a_n]$ where $k_n \geq 1$ and $\gcd(h_n, k_n) = 1$. Proposition 1.40 immediately implies that

$$\left| \alpha - \frac{h_n}{k_n} \right| \leq \frac{1}{k_n^2},$$

but we can improve this result somewhat. The goal of the present section is to show that there are infinitely many n for which

$$\left| \alpha - \frac{h_n}{k_n} \right| \leq \frac{1}{\sqrt{5} k_n^2},$$

and the following example explains that the constant $\sqrt{5}$ is the best possible.

Example 1.54. Let $\varphi = \frac{1+\sqrt{5}}{2} = [1; 1, 1, \ldots]$ as in Example 1.43. By Example 1.34, the nth continued fraction convergent is F_{n+2}/F_{n+1}. For any $c > \sqrt{5}$, we have

$$\left| \varphi - \frac{F_{n+2}}{F_{n+1}} \right| < \frac{1}{c F_{n+1}^2}$$

for only finitely many n.

Solution. Set $\overline{\varphi} := \frac{1-\sqrt{5}}{2}$, which is the negative solution of $x^2 = x+1$; note $\varphi + \overline{\varphi} = 1$ and $\varphi\overline{\varphi} = -1$. An induction n proves Binet's formula

$$F_n \stackrel{?}{=} \frac{\varphi^n - \overline{\varphi}^n}{\sqrt{5}}.$$

Indeed, the above equality holds at $n = 0$ and $n = 1$ by a direct computation, and taking a linear combination of the relations $\varphi^{n+2} = \varphi^{n+1} + \varphi^n$ and $\overline{\varphi}^{n+2} = \overline{\varphi}^{n+1} + \overline{\varphi}^n$ proves the inductive step.

We now carefully study the error. For any $n \geq 0$, we see

$$\begin{aligned} 5\left(\varphi F_{n+1}^2 - F_{n+2}F_{n+1}\right) &= \varphi\left(\varphi^{n+1} - \overline{\varphi}^{n+1}\right)^2 - \left(\varphi^{n+2} - \overline{\varphi}^{n+2}\right)\left(\varphi^{n+1} - \overline{\varphi}^{n+1}\right) \\ &= \varphi\left(\varphi^{2n+2} + \overline{\varphi}^{2n+2} - 2(\varphi\overline{\varphi})^{n+1}\right) - \left(\varphi^{2n+3} + \overline{\varphi}^{2n+3} - (\varphi\overline{\varphi})^{n+1}(\varphi + \overline{\varphi})\right) \\ &= (-1)^n(2\varphi - 1) + \overline{\varphi}^{2n+2}(\varphi - \overline{\varphi}) \\ &= (-1)^n\sqrt{5} + \overline{\varphi}^{2n+2}\sqrt{5}. \end{aligned}$$

Thus,

$$cF_{n+1}^2\left|\varphi - \frac{F_{n+2}}{F_{n+1}}\right| = \frac{c}{\sqrt{5}}\left|(-1)^n + \overline{\varphi}^{2n+2}\right|. \tag{1.1}$$

As $n \to \infty$, we see $\overline{\varphi}^{2n+2} \to 0$, so the error above approaches $c/\sqrt{5} > 1$. Thus, only finitely many n have the above quantity less than 1, which is what we wanted. ■

Remark 1.55. Carefully tracking through Example 1.54 tells us that

$$\left|\varphi - \frac{F_{n+2}}{F_{n+1}}\right| < \frac{1}{\sqrt{5}F_{n+1}^2}$$

exactly for the even n. Indeed, this follows from (1.1) upon noting $-\overline{\varphi}^{2n+2} < 0$. Compare this result with the statement and proof of Theorem 1.59.

Exercise 1.56. Set $\alpha := \sqrt{2}$, and let $\{h_n/k_n\}_{n=0}^{\infty}$ be the continued fraction convergents of α. Find the largest real number $c > 0$ for which there exist infinitely many integers $n \geq 0$ such that

$$\left|\alpha - \frac{h_n}{k_n}\right| < \frac{1}{ck_n^2}.$$

As should be somewhat evident by the $\sqrt{5}$ in our bounds and in the above proof, the arguments here are going to be somewhat ad-hoc. The following result starts us off.

Lemma 1.57. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be irrational, and let $\{h_n/k_n\}_{n=0}^{\infty}$ be the sequence of continued fraction convergents of α. For any $n \geq 0$, we have

$$\frac{h_{2n}}{k_{2n}} < \frac{h_{2n+2}}{k_{2n+2}} < \frac{h_{2n+3}}{k_{2n+3}} < \frac{h_{2n+1}}{k_{2n+1}}.$$

Proof. Applying Lemma 1.39, we are trying to show

$$\frac{h_{2n}}{k_{2n}} \stackrel{?}{<} \frac{h_{2n}}{k_{2n}} + \frac{1}{k_{2n}k_{2n+1}} - \frac{1}{k_{2n+1}k_{2n+2}} \stackrel{?}{<} \frac{h_{2n}}{k_{2n}} + \frac{1}{k_{2n}k_{2n+1}} - \frac{1}{k_{2n+1}k_{2n+2}} + \frac{1}{k_{2n+2}k_{2n+3}} \stackrel{?}{<} \frac{h_{2n}}{k_{2n}} + \frac{1}{k_{2n}k_{2n+1}}.$$

Simplifying, we want to show

$$0 \stackrel{?}{<} \frac{1}{k_{2n}k_{2n+1}} - \frac{1}{k_{2n+1}k_{2n+2}} \stackrel{?}{<} \frac{1}{k_{2n}k_{2n+1}} - \frac{1}{k_{2n+1}k_{2n+2}} + \frac{1}{k_{2n+2}k_{2n+3}} \stackrel{?}{<} \frac{1}{k_{2n}k_{2n+1}}.$$

The leftmost inequality is equivalent to $k_{2n} < k_{2n+2}$, which is true. The middle inequality is equivalent to $0 < 1/(k_{2n+2}k_{2n+3})$, which is true. Lastly, the rightmost inequality is equivalent to $k_{2n+1} < k_{2n+3}$, which is true. ■

Proposition 1.58. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be irrational, and let $\{h_n/k_n\}_{n=0}^{\infty}$ be the sequence of continued fraction convergents of α. For any $m \geq 0$, there exists $n \in \{2m, 2m+1\}$ such that

$$\left|\alpha - \frac{h_n}{k_n}\right| < \frac{1}{2k_n^2}.$$

Proof. The point is that one of h_{2m}/k_{2m} or h_{2m+1}/k_{2m+1} is going to be "closer" to α. By Lemma 1.57, we see that $\{h_{2m}/k_{2m}\}_{m=0}^{\infty}$ is a strictly ascending sequence of rational numbers, which converges to α by definition of α. Analogously, $\{h_{2m+1}/k_{2m+1}\}_{m=0}^{\infty}$ is a strictly descending sequence of rational numbers which also converges to α. Thus,

$$\frac{h_{2m}}{k_{2m}} < \alpha < \frac{h_{2m+1}}{k_{2m+1}}.$$

By Lemma 1.39, the length of this interval is $1/(k_{2m}k_{2m+1})$.

Now, suppose for contradiction that

$$\left|\alpha - \frac{h_n}{k_n}\right| \geq \frac{1}{2k_n^2}$$

for $n \in \{2m, 2m+1\}$. Then we must have

$$\frac{h_{2m}}{k_{2m}} + \frac{1}{2k_{2m}^2} \leq \alpha \leq \frac{h_{2m+1}}{k_{2m+1}} - \frac{1}{2k_{2m+1}^2}.$$

This rearranges to

$$\frac{1}{2k_{2m}^2} + \frac{1}{2k_{2m+1}^2} \leq \frac{1}{k_{2m}k_{2m+1}}$$

by Lemma 1.39, but this is equivalent to $(k_{2m} - k_{2m+1})^2 \leq 0$, or $k_{2m} = k_{2m+1}$. This is a contradiction because the sequence $\{k_n\}_{n=0}^{\infty}$ is strictly increasing. ■

With a little more care in the last half of the argument, we can achieve the desired result.

Theorem 1.59 (Hurwitz)**.** Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be irrational, and let $\{h_n/k_n\}_{n=0}^{\infty}$ be the sequence of continued fraction convergents of α. For any $m \geq 0$, there exists $n \in \{3m, 3m+1, 3m+2\}$ such that

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

Proof. The proof is along the same lines as Proposition 1.58. Without loss of generality, we work with even m in order to make our inequalities better-behaved; the argument for odd m is analogous but requires reversing a few inequalities. Anyway, if m is even, Lemma 1.57 implies

$$\frac{h_{3m}}{k_{3m}} < \frac{h_{3m+2}}{k_{3m+2}} < \alpha < \frac{h_{3m+1}}{k_{3m+1}}.$$

(The location of α adjusts in the case where m is odd.) Now, suppose for the sake of contradiction that

$$\left|\alpha - \frac{h_n}{k_n}\right| \geq \frac{1}{\sqrt{5}k_n^2}$$

for each $n \in \{3m, 3m+1, 3m+2\}$. Removing the absolute values, we receive the inequalities

$$\frac{h_{3m}}{k_{3m}} + \frac{1}{\sqrt{5}k_{3m}^2} \leq \alpha, \quad \alpha \leq \frac{h_{3m+1}}{k_{3m+1}} - \frac{1}{\sqrt{5}k_{3m+1}^2}, \quad \text{and} \quad \frac{h_{3m+2}}{k_{3m+2}} + \frac{1}{\sqrt{5}k_{3m+2}^2} \leq \alpha,$$

which imply

$$\frac{h_{3m}}{k_{3m}} + \frac{1}{\sqrt{5}k_{3m}^2} \leq \frac{h_{3m+1}}{k_{3m+1}} - \frac{1}{\sqrt{5}k_{3m+1}^2}, \quad \text{and} \quad \frac{h_{3m+2}}{k_{3m+2}} + \frac{1}{\sqrt{5}k_{3m+2}^2} \leq \frac{h_{3m+1}}{k_{3m+1}} - \frac{1}{\sqrt{5}k_{3m+1}^2}.$$

By Lemma 1.39, these rearrange into

$$\frac{1}{k_{3m}^2} + \frac{1}{k_{3m+1}^2} \leq \frac{\sqrt{5}}{k_{3m}k_{3m+1}}, \quad \text{and} \quad \frac{1}{k_{3m+1}^2} + \frac{1}{k_{3m+2}^2} \leq \frac{\sqrt{5}}{k_{3m+1}k_{3m+2}}.$$

By Proposition 1.32, we see that $k_{3m} + k_{3m+1} \leq k_{3m+2}$, so our inequalities read

$$\frac{1}{k_{3m}^2} + \frac{1}{k_{3m+1}^2} \leq \frac{\sqrt{5}}{k_{3m}k_{3m+1}}, \quad \text{and} \quad \frac{1}{k_{3m+1}^2} + \frac{1}{(k_{3m}+k_{3m+1})^2} \leq \frac{\sqrt{5}}{k_{3m+1}(k_{3m}+k_{3m+1})}.$$

Now, we set $q \coloneqq k_{3m+1}/k_{3m}$ to homogenize the inequalities. This gives

$$q^2 + 1 \leq \sqrt{5}q, \quad \text{and} \quad (q+1)^2 + 1 \leq \sqrt{5}(q+1).$$

In other words, we are asking for $\{q, q+1\} \subseteq \{x \in \mathbb{R} : x^2 + 1 \leq \sqrt{5}x\}$. To solve for q, we note $x^2 - \sqrt{5}x + 1 = 0$ exactly when $x = \frac{\sqrt{5}\pm 1}{2}$, so $\{x \in \mathbb{R} : x^2 + 1 \leq \sqrt{5}x\}$ is the closed interval from $\frac{\sqrt{5}-1}{2}$ up to $\frac{\sqrt{5}+1}{2}$. Thus, we must have $q = \frac{\sqrt{5}-1}{2}$, which is a contradiction because q is rational while $\frac{\sqrt{5}-1}{2}$ is irrational! ■

1.3.4 Convergents Are Best Rational Approximations

Now that we are somewhat acquainted with what it means to be a "good" rational approximation, we are ready to state and prove our main result on continued fractions. It is a converse to Proposition 1.58.

Theorem 1.60. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be irrational, and let $\{h_n/k_n\}_{n=0}^{\infty}$ be the sequence of continued fraction convergents of α. Given a rational number h/k with $\gcd(h,k) = 1$ and $k \geq 1$, if

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{2k^2},$$

then $(h,k) = (h_n, k_n)$ for some n.

Approximately speaking, Theorem 1.60 tells us that the best rational approximations of a real number are all continued fraction convergents.

It will be helpful to have a criterion to check that a fraction is a convergent. This is the content of the following lemma.

Lemma 1.61. Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be irrational, and let $\{h_n/k_n\}_{n=0}^{\infty}$ be the sequence of continued fraction convergents of α. Suppose we have rational numbers h/k and h'/k' with $k > k' > 0$ and $|hk' - h'k| = 1$ and

$$\alpha = \frac{h\beta + h'}{k\beta + k'}$$

for some $\beta > 1$. Then there is $n \geq 1$ such that $(h', k') = (h_{n-1}, k_{n-1})$ and $(h,k) = (h_n, k_n)$.

Proof. By Remark 1.26, we may write

$$\frac{h}{k} = [a_0; a_1, a_2, \dots, a_n]$$

with a_n with parity chosen so that $h'k - hk' = (-1)^{n+1}$. (This is what we expect from Corollary 1.35.) Quickly, we let $\{p_n/q_n\}_{m=0}^n$ denote the convergents of $[a_0; a_1, a_2, \dots, a_n]$. We know $(h, k) = (p_n, q_n)$. From here, the proof has two steps.

1. We show $(h', k') = (p_{n-1}, q_{n-1})$. By Corollary 1.35, we know

   $$p_{n-1}q_n - p_n q_{n-1} = (-1)^n = h'k - hk' = h'q_n - p_n k'.$$

   Reducing $\pmod{q_n}$, we see that $-p_n q_{n-1} \equiv -p_n k'$, so $q_{n-1} \equiv k'$, but $0 < k', q_{n-1} < q_n$, so $k' = q_{n-1}$. Plugging this in and simplifying then forces $p_{n-1} = h'$, which is what we wanted.

2. We show that $[a_0; a_1, a_2, \dots, a_n]$ is the beginning of the continued fraction of α. Well, Proposition 1.49 allows us to write

   $$\beta = [a_{n+1}; a_{n+2}, a_{n+3}, \dots]$$

   for integers $a_{n+1}, a_{n+2}, a_{n+3}, \dots$ with $a_{n+2}, a_{n+3}, \dots$ positive. In fact, $a_{n+1} = \lfloor \beta \rfloor \geq 1$ is positive by construction. Now, Proposition 1.32 implies

   $$\alpha = \frac{h\beta + h'}{k\beta + k'} = \frac{p_n\beta + p_{n-1}}{q_n\beta + q_{n-1}} = [a_0; a_1, a_2, \dots, a_n, \beta] = [a_0; a_1, a_2, \dots, a_n, a_{n+1}, a_{n+2}, \dots].$$

   (Note we have implicitly used the uniqueness of the continued fraction, shown in Remark 1.51.) Thus, we see $(p_m, q_m) = (h_m, k_m)$ for $0 \leq m \leq n$, from which $(h', k') = (p_{n-1}, q_{n-1}) = (h_{n-1}, k_{n-1})$ and $(h, k) = (p_n, q_n) = (h_n, k_n)$ follows. ∎

We are now ready to prove Theorem 1.60.

Proof of Theorem 1.60. We use Lemma 1.61. To choose h' and k', we use Remark 1.26 to write

$$\frac{h}{k} = [a_0; a_1, a_2, \dots, a_n]$$

with a_n with parity chosen so that n is even if and only if $\alpha > h/k$. (This is what we expect from Lemma 1.57.) Then let $\{p_m/q_m\}_{m=0}^n$ be the continued fraction convergents; for example, $(h, k) = (p_n, q_n)$, and we set $(h', k') \coloneqq (p_{n-1}, q_{n-1})$. The construction gives $k > k' > 0$, and $|hk' - h'k| = 1$ by Corollary 1.35.

Now, we know that we can certainly find some $\beta \in \mathbb{R}$ such that

$$\alpha = \frac{h\beta + h'}{k\beta + k'}$$

by rearranging. (Explicitly, we need to know that $\alpha k - h \neq 0$ to set $\beta \coloneqq (h' - \alpha k')/(\alpha k - h)$, which is true because α is irrational.) Our goal is to show $\beta > 1$, which will complete the proof by Lemma 1.61. Well, comparing with our error, we see

$$\alpha - \frac{h}{k} = \frac{h\beta + h'}{k\beta + k'} - \frac{h}{k} = \frac{h'k - hk'}{(k\beta + k')k} = \frac{(-1)^n}{(k\beta + k')k},$$

where we applied Corollary 1.35 in the last equality. We arranged the parity n so that the left-hand side is positive if and only if $(-1)^n = 1$, so we may now write

$$1 > 2k^2 \left| \alpha - \frac{h}{k} \right| = \frac{2k}{k\beta + k'},$$

so $\beta > 2 - k'/k$, which is bigger than 1 because $k' < k$. This completes the proof. ∎

1.3.5 Problems

Do at least ten points worth of the following exercises.

Problem 1.3.1 (2 points)**.** Work Exercise 1.44.

Problem 1.3.2 (3 points)**.** Work Exercise 1.56.

Problem 1.3.3 (3 points)**.** Let $a_0, a_1, a_2, \ldots$ be integers with $a_1, a_2, \ldots$ positive. Suppose that there exists an integer m such that $a_n = a_{n+m}$ for all n. Show that $[a_0; a_1, a_2, \ldots]$ is the root of a polynomial with integer coefficients and of degree two.

Problem 1.3.4 (4 points)**.** Find an irrational number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and integers h and k such that

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{k^2},$$

but h/k is not a continued fraction convergent of α.

Problem 1.3.5 (5 points)**.** Write (and submit) a Python program which takes as input an irrational number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and an index n and then outputs the nth coefficient a_n of the corresponding continued fraction $[a_0; a_1, a_2, \ldots]$ equal to α.

Problem 1.3.6 (8 points)**.** Let $\alpha \in \mathbb{R}$ be irrational and $[a_0; a_1, a_2, \ldots]$ its continued fraction expansion. Fix N sufficiently large. Suppose that among the first $1000N$ digits of the decimal expansion of α, the last $999N$ of them are all zeroes or all nines. Then there exists some $n \leq 5N$ so that $a_n > 10^{100N}$.

Problem 1.3.7 (2 points)**.** Use Problem 1.3.6 to conclude that for any sufficiently large N, the last $999N$ digits of the first $1000N$ decimal digits in the decimal expansion of $\sqrt{5}$ cannot be all zeroes or all nines.

1.4 Diophantine Approximation

Theme 2

Quadratic Equations

Theme 3

Intermission: Other Fields

Theme 4
Cubic Equations

Every person believes that he knows what a curve is until he has learned so much mathematics that the countless possible abnormalities confuse him.

—Felix Klein, [Kle16]

BIBLIOGRAPHY

[Kle16] Felix Klein. *Elementary Mathematics from a Higher Standpoint*. Trans. by Gert Schubring. Vol. II. Springer Berlin, Heidelberg, 2016.

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

[Pro22] Ross Mathematics Program. *Students*. 2022. URL: https://rossprogram.org/students/.

List of Definitions