7
Continued Fractions

A *continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

which may or may not go on indefinitely. We denote the value of this continued fraction by

$$[a_0, a_1, a_2, \ldots].$$

The a_n are called the *partial quotients* of the continued fraction (we will see why at the end of this section). Thus, e.g.,

$$[1, 2] = 1 + \frac{1}{2} = \frac{3}{2},$$

and

$$\frac{172}{51} = [3, 2, 1, 2, 6] = 3 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}}}.$$

Continued fractions have many applications, from the abstract to the concrete. They give good rational approximations to irrational numbers, and the have been used to understand why you can't tune a piano perfectly (see [Dun]).

Continued fractions also suggest a sense in which e appears to be "less transcendental" than π (see Example 7.2.4).

There are many places to read about continued fractions, including [HW79, Ch. X], [Bur89, §13.3], [Dav99, Ch. IV], and [Khi63]. This chapter was most influenced by Hardy and Wright, which I find to be the clearest of the above references.

7.1 Finite Continued Fractions

Definition 7.1.1. A *finite continued fraction* is an expression

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_m}}},$$

where each a_n is a real number and $a_n > 0$ for all $n \geq 1$. If the a_n are integers, we say that the continued fraction is *integral*.

To get a feeling for continued fractions, observe that

$$\begin{aligned}
[a_0] &= a_0, \\
[a_0, a_1] &= a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}, \\
[a_0, a_1, a_2] &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}.
\end{aligned}$$

Also,

$$\begin{aligned}
[a_0, a_1, \ldots, a_{m-1}, a_m] &= [a_0, a_1, \ldots, a_{m-2}, a_{m-1} + \frac{1}{a_m}] \\
&= a_0 + \frac{1}{[a_1, \ldots, a_m]} \\
&= [a_0, [a_1, \ldots, a_m]].
\end{aligned}$$

7.1.1 Partial Convergents

Fix a continued fraction $[a_0, \ldots, a_m]$.

Definition 7.1.2. For $0 \leq n \leq m$, the nth *convergent* of the continued fraction $[a_0, \ldots, a_m]$ is $[a_0, \ldots, a_n]$.

For each $n \geq -1$, define real numbers p_n and q_n as follows:[1] 1

[1]Also define $p_{-2} = 0$ and $q_{-2} = 1$.

$$\begin{array}{llll} p_{-1}=1, & p_0=a_0, & p_1=a_1p_0+p_{-1}=a_1a_0+1, & p_n=a_np_{n-1}+p_{n-2}, \\ q_{-1}=0, & q_0=1, & q_1=a_1q_0+q_{-1}=a_1, & q_n=a_nq_{n-1}+q_{n-2}. \end{array}$$

Proposition 7.1.3. $[a_0,\ldots,a_n]=\dfrac{p_n}{q_n}$

Proof. We use induction. We already verified the assertion when $n=0,1$. Suppose the proposition is true for all continued fractions of length $n-1$. Then

$$\begin{aligned} [a_0,\ldots,a_n] &= [a_0,\ldots,a_{n-2},a_{n-1}+\frac{1}{a_n}] \\ &= \frac{\left(a_{n-1}+\frac{1}{a_n}\right)p_{n-2}+p_{n-3}}{\left(a_{n-1}+\frac{1}{a_n}\right)q_{n-2}+q_{n-3}} \\ &= \frac{(a_{n-1}a_n+1)p_{n-2}+a_np_{n-3}}{(a_{n-1}a_n+1)q_{n-2}+a_nq_{n-3}} \\ &= \frac{a_n(a_{n-1}p_{n-2}+p_{n-3})+p_{n-2}}{a_n(a_{n-1}q_{n-2}+q_{n-3})+q_{n-2}} \\ &= \frac{a_np_{n-1}+p_{n-2}}{a_nq_{n-1}+q_{n-2}}=\frac{p_n}{q_n}. \end{aligned}$$

□

Proposition 7.1.4. *Suppose $n\le m$.*

1. *The determinant of* $\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1}\end{pmatrix}$ *is* $(-1)^{n-1}$*; equivalently,*

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

2. *The determinant of* $\begin{pmatrix} p_n & p_{n-2} \\ q_n & q_{n-2}\end{pmatrix}$ *is* $(-1)^n a_n$*; equivalently,*

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

Proof. For the first statement, we proceed by induction. The case $n=0$ holds because the determinant of $\begin{pmatrix} a_0 & 1 \\ 1 & 0\end{pmatrix}$ is $-1=(-1)^{-1}$. Suppose the statement is true for $n-1$. Then

$$\begin{aligned} p_nq_{n-1}-q_np_{n-1} &= (a_np_{n-1}+p_{n-2})q_{n-1}-(a_nq_{n-1}+q_{n-2})p_{n-1} \\ &= p_{n-2}q_{n-1}-q_{n-2}p_{n-1} \\ &= -(p_{n-1}q_{n-2}-p_{n-2}q_{n-1}) \\ &= -(-1)^{n-2}=(-1)^{n-1}. \end{aligned}$$

This completes the proof of the first statement. For the second statement,

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

□

Corollary 7.1.5. *The fraction* $\dfrac{p_n}{q_n}$ *is in lowest terms.*

Proof. If $p \mid p_n$ and $p \mid q_n$ then $p \mid (-1)^{n-1}$. □

7.1.2 How the Convergents Converge

Let $[a_0, \ldots, a_m]$ be a continued fraction and for $n \leq m$ let

$$c_n = [a_0, \ldots, a_n] = \frac{p_n}{q_n}$$

denote the nth convergent.

Proposition 7.1.6. *The even convergents c_{2n} increase strictly with n, and the odd convergents c_{2n+1} decrease strictly with n. Moreover, the odd convergents c_{2n+1} are greater than all of the even convergents.*

Proof. For $n \geq 1$ the a_n are positive, so the q_n are all positive. By Proposition 7.1.4, for $n \geq 2$,

$$c_n - c_{n-2} = (-1)^n \cdot \frac{a_n}{q_n q_{n-2}},$$

which proves the first claim.

Next, Proposition 7.1.4 implies that for $n \geq 1$,

$$c_n - c_{n-1} = (-1)^{n-1} \cdot \frac{1}{q_n q_{n-1}}$$

has the sign of $(-1)^{n-1}$, so that $c_{2n+1} > c_{2n}$. Thus if there exists r, n such that $c_{2n+1} < c_{2r}$, then $r \neq n$. If $r < n$, then $c_{2n+1} < c_{2r} < c_{2n}$, a contradiction. If $r > n$, then $c_{2r+1} < c_{2n+1} < c_{2r}$, also a contradiction. □

7.1.3 Every Rational Number is Represented

Proposition 7.1.7. *Every rational number is represented by a continued fraction.*

Proof. Let a/b, where $b > 0$, be any rational number. Euclid's algorithm gives:

$$\begin{aligned}
a &= b \cdot a_0 + r_1, & 0 < r_1 < b\\
b &= r_1 \cdot a_1 + r_2, & 0 < r_2 < r_1\\
&\cdots\\
r_{n-2} &= r_{n-1} \cdot a_{n-1} + r_n, & 0 < r_n < r_{n-1}\\
r_{n-1} &= r_n \cdot a_n + 0.
\end{aligned}$$

Note that $a_i > 0$ for $i > 0$. Rewrite the equations as follows:

$$\begin{aligned}
a/b &= a_0 + r_1/b = a_0 + 1/(b/r_1),\\
b/r_1 &= a_1 + r_2/r_1 = a_1 + 1/(r_1/r_2),\\
r_1/r_2 &= a_2 + r_3/r_2 = a_2 + 1/(r_2/r_3),\\
&\cdots\\
r_{n-1}/r_n &= a_n.
\end{aligned}$$

It follows that

$$\frac{a}{b} = [a_0, a_1, \ldots a_n].$$

□

7.2 Infinite Continued Fractions

7.2.1 The Continued Fraction Algorithm

Let $x \in \mathbb{R}$ and write

$$x = a_0 + t_0$$

with $a_0 \in \mathbb{Z}$ and $0 \leq t_0 < 1$. If $t_0 \neq 0$, write

$$\frac{1}{t_0} = a_1 + t_1$$

with $a_1 \in \mathbb{N}$ and $0 \leq t_1 < 1$. Thus $t_0 = \frac{1}{a_1+t_1} = [0, a_1 + t_1]$, which is a (nonintegral) continued fraction expansion of t_0. Continue in this manner so long as $t_n \neq 0$ writing

$$\frac{1}{t_n} = a_{n+1} + t_{n+1}$$

with $a_{n+1} \in \mathbb{N}$ and $0 \leq t_{n+1} < 1$. This process, which associates to a real number x the sequence of integers $a_0, a_1, a_2, \ldots$, is called the *continued fraction algorithm.*

Example 7.2.1. Let $x = \frac{8}{3}$. Then $x = 2 + \frac{2}{3}$, so $a_0 = 2$ and $t_0 = \frac{2}{3}$. Then $\frac{1}{t_0} = \frac{3}{2} = 1 + \frac{1}{2}$, so $a_1 = 1$ and $t_1 = \frac{1}{2}$. Then $\frac{1}{t_1} = 2$, so $a_2 = 2$, $t_2 = 0$, and the sequence terminates. Notice that

$$\frac{8}{3} = [2, 1, 2],$$

so the continued fraction algorithm produces the continued fraction of $\frac{8}{3}$.

Proposition 7.2.2. *For every n such that a_n is defined, we have*

$$x = [a_0, a_1, \ldots, a_n + t_n],$$

and if $t_n \neq 0$ then $x = [a_0, a_1, \ldots, a_n, \frac{1}{t_n}]$.

Proof. Use induction. The statements are both true when $n = 0$. If the second statement is true for $n - 1$, then

$$\begin{aligned} x &= [a_0, a_1, \ldots, a_{n-1}, \frac{1}{t_{n-1}}] \\ &= [a_0, a_1, \ldots, a_{n-1}, a_n + t_n] \\ &= [a_0, a_1, \ldots, a_{n-1}, a_n, \frac{1}{t_n}]. \end{aligned}$$

Similarly, the first statement is true for n if it is true for $n - 1$. $\square$

Example 7.2.3. Let $x = \frac{1+\sqrt{5}}{2}$. Then

$$x = 1 + \frac{-1 + \sqrt{5}}{2},$$

so $a_0 = 1$ and $t_0 = \frac{-1+\sqrt{5}}{2}$. We have

$$\frac{1}{t_0} = \frac{2}{-1 + \sqrt{5}} = \frac{-2 - 2\sqrt{5}}{-4} = \frac{1 + \sqrt{5}}{2}$$

so again $a_1 = 1$ and $t_1 = \frac{-1+\sqrt{5}}{2}$. Likewise, $a_n = 1$ for all n. As we will see below, the following crazy-looking equality makes sense.

$$\frac{1 + \sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}}$$

Example 7.2.4. Suppose $x = e = 2.71828182\ldots$. Applying the continued fraction algorithm, we have

$$a_0, a_1, a_2, \ldots = 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots$$

We have

$$[a_0, a_1, a_2, a_3, a_4, a_5] = \frac{87}{32} = 2.71875$$

which is a good rational approximation to e.

Let's do the same thing with $\pi = 3.14159265358979\ldots$: We have

$$a_0, a_1, a_2, \ldots = 3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, \ldots$$

The first few partial convergents are

$$3, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \frac{103993}{33102}, \cdots$$

These are all good rational approximations to π; for example,

$$\frac{103993}{33102} = 3.14159265301\ldots.$$

Notice that the continued fraction of e exhibits a nice pattern (see .??..), whereas the continued fraction of π appears to be fairly random. In some vague sense, this suggests that π is "more transcendental" than e.

7.2.2 Infinite Continued Fractions

Theorem 7.2.5. *Let $a_0, a_1, a_2, \ldots$ be a sequence of integers such that $a_n > 0$ for all $n \geq 1$, and for each $n \geq 0$, set $c_n = [a_0, a_1, \ldots a_n]$. Then $\lim\limits_{n\to\infty} c_n$ exists.*

Proof. For any $m \geq n$, the number c_n is a partial convergent of $[a_0, \ldots, a_m]$. By Proposition 7.1.6 the even convergents c_{2n} form a strictly *increasing* sequence and the odd convergents c_{2n+1} form a strictly *decreasing* sequence. Moreover, the even convergents are all $\leq c_1$ and the odd convergents are all $\geq c_0$. Hence $\alpha_0 = \lim_{n\to\infty} c_{2n}$ and $\alpha_1 = \lim_{n\to\infty} c_{2n+1}$ both exist and $\alpha_0 \leq \alpha_1$. Finally, by Proposition 7.1.4

$$|c_{2n} - c_{2n-1}| = \frac{1}{q_{2n} \cdot q_{2n-1}} \leq \frac{1}{2n(2n-1)} \to 0,$$

so $\alpha_0 = \alpha_1$. □

We define

$$[a_0, a_1, \ldots] = \lim_{n\to\infty} c_n.$$

Example 7.2.6. We illustrate the theorem with $x = \pi$. As in the proof of Theorem 7.2.5, let c_n be the nth partial convergent to π. The c_n with n odd converge down to π

$$c_1 = 3.1428571\ldots,\ c_3 = 3.1415929\ldots,\ c_5 = 3.1415926\ldots$$

whereas the c_n with n even converge up to π

$$c_2 = 3.1415094\ldots,\ c_4 = 3.1415926\ldots,\ c_6 = 3.1415926\ldots.$$

Theorem 7.2.7. *Let $x \in \mathbb{R}$ be a real number. Then*

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

where $a_0, a_1, a_2, \ldots$ is the sequence produced by the continued fraction algorithm.

Proof. If the sequence is finite then some $t_n = 0$ and the result follows by Proposition 7.2.2. Suppose the sequence is infinite. By Proposition 7.2.2,

$$x = [a_0, a_1, \ldots, a_n, \frac{1}{t_n}].$$

By Proposition 7.1.3 (which we apply in a case when the partial quotients of the continued fraction are not integers!), we have

$$x = \frac{\dfrac{1}{t_n} \cdot p_n + p_{n-1}}{\dfrac{1}{t_n} \cdot q_n + q_{n-1}}.$$

Thus if $c_n = [a_0, a_1, \ldots, a_n]$, then

$$\begin{aligned}
x - c_n &= x - \frac{p_n}{q_n} \\
&= \frac{\frac{1}{t_n} p_n q_n + p_{n-1} q_n - \frac{1}{t_n} p_n q_n - p_n q_{n-1}}{q_n \left(\frac{1}{t_n} q_n + q_{n-1}\right)}. \\
&= \frac{p_{n-1} q_n - p_n q_{n-1}}{q_n \left(\frac{1}{t_n} q_n + q_{n-1}\right)} \\
&= \frac{(-1)^n}{q_n \left(\frac{1}{t_n} q_n + q_{n-1}\right)}.
\end{aligned}$$

Thus

$$\begin{aligned}
|x - c_n| &= \frac{1}{q_n \left(\frac{1}{t_n} q_n + q_{n-1}\right)} \\
&< \frac{1}{q_n (a_{n+1} q_n + q_{n-1})} \\
&= \frac{1}{q_n \cdot q_{n+1}} \leq \frac{1}{n(n+1)} \to 0.
\end{aligned}$$

(In the inequality we use that a_{n+1} is the integer part of $\frac{1}{t_n}$, and is hence $\leq \frac{1}{t_n}$.)

$\square$

Proposition 7.2.8. *If x is a rational number then the sequence $a_0, a_1, a_2, \ldots$ terminates (at n say) and*

$$x = [a_0, a_1, a_2, \ldots, a_n].$$

Proof. Let $[b_0, b_1, \ldots, b_m]$ be the continued fraction representation of x that we obtain using the Euclidean algorithm. Then

$$x = b_0 + 1/[b_1, \ldots, b_m].$$

If $[b_1, \ldots, b_m] = 1$ then $m = 1$ and $b_1 = 1$, which would never happen using the Euclidean algorithm since x is expressed in lowest terms. Thus $[b_1, \ldots, b_m] > 1$, so in the continued fraction algorithm we choose $a_0 = b_0$ and $t_0 = 1/[b_1, \ldots, b_m]$. Repeating this argument enough times proves the claim. □

7.3 Quadratic Irrationals

In this lecture we prove that the continued fraction expansion of a number is periodic if and only if the number is a quadratic irrational.

7.3.1 Quadratic Irrationals

Definition 7.3.1. An element $\alpha \in \mathbb{R}$ is a *quadratic irrational* if it is irrational and satisfies a quadratic polynomial.

Thus, e.g., $(1+\sqrt{5})/2$ is a quadratic irrational. Recall that

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

The continued fraction of $\sqrt{2}$ is $[1, 2, 2, 2, 2, 2, \ldots]$, and the continued fraction of $\sqrt{389}$ is

$$[19, 1, 2, 1, 1, 1, 1, 2, 1, 38, 1, 2, 1, 1, 1, 1, 2, 1, 38, \ldots].$$

Does the $[1, 2, 1, 1, 1, 1, 2, 1, 38]$ pattern repeat over and over again??

7.3.2 Periodic Continued Fractions

Definition 7.3.2. A *periodic continued fraction* is a continued fraction $[a_0, a_1, \ldots, a_n, \ldots]$ such that

$$a_n = a_{n+h}$$

for a fixed positive integer h and all sufficiently large n. We call h the *period* of the continued fraction.

Example 7.3.3. Consider the periodic continued fraction $[1, 2, 1, 2, \ldots] = [\overline{1, 2}]$. What does it converge to?

$$[\overline{1,2}] = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cdots}}}},$$

so if $\alpha = [\overline{1,2}]$ then

$$\alpha = 1 + \frac{1}{2 + \alpha}.$$

Thus $2\alpha + \alpha^2 = 2 + \alpha + 1$, so

$$\alpha^2 + \alpha - 3 = 0 \quad \text{and} \quad \alpha = \frac{-1 + \sqrt{7}}{2}.$$

Theorem 7.3.4. *An infinite integral continued fraction is periodic if and only if it represents a quadratic irrational.*

Proof. ($\Longrightarrow$) First suppose that

$$[a_0, a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+h}}]$$

is a periodic continued fraction. Set $\alpha = [a_{n+1}, a_{n+2}, \ldots]$. Then

$$\alpha = [a_{n+1}, \ldots, a_{n+h}, \alpha],$$

so

$$\alpha = \frac{\alpha p_{n+h} + p_{n+h-1}}{\alpha q_{n+h} + q_{n+h-1}}.$$

(We use that α is the last partial convergent.) Thus α satisfies a quadratic equation. Since the a_i are all integers, the number

$$\begin{aligned}[a_0, a_1, \ldots] &= [a_0, a_1, \ldots, a_n, \alpha] \\ &= a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots + \alpha}}\end{aligned}$$

can be expressed as a polynomial in α with rational coefficients, so $[a_0, a_1, \ldots]$ also satisfies a quadratic polynomial. Finally, $\alpha \notin \mathbb{Q}$ because periodic continued fractions have infinitely many terms.

($\Longleftarrow$) This direction was first proved by Lagrange. The proof is much more exciting! Suppose $\alpha \in \mathbb{R}$ satisfies a quadratic equation

$$a\alpha^2 + b\alpha + c = 0$$

with $a, b, c \in \mathbb{Z}$. Let $[a_0, a_1, \ldots]$ be the expansion of α. For each n, let

$$r_n = [a_n, a_{n+1}, \ldots],$$

so that

$$\alpha = [a_0, a_1, \ldots, a_{n-1}, r_n].$$

We have

$$\alpha = \frac{r_n p_n + p_{n-1}}{r_n q_n + q_{n-1}}.$$

Substituting this expression for α into the quadratic equation for α, we see that

$$A_n r_n^2 + B_n r_n + C_n = 0,$$

where

$$\begin{aligned} A_n &= a p_{n-1}^2 + b p_{n-1} q_{n-1} + c q_{n-1}^2, \\ B_n &= 2a p_{n-1} p_{n-2} + b(p_{n-1} q_{n-2} + p_{n-2} q_{n-1}) + 2c q_{n-1} q_{n-2}, \\ C_n &= a p_{n-2}^2 + b p_{n-2} q_{n-2} + c p_{n-2}^2. \end{aligned}$$

Note that $A_n, B_n, C_n \in \mathbb{Z}$, that $C_n = A_{n-1}$, and that

$$B^2 - 4A_n C_n = (b^2 - 4ac)(p_{n-1} q_{n-2} - q_{n-1} p_{n-2})^2 = b^2 - 4ac.$$

Recall from the proof of Theorem 2.3 of the previous lecture that

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

Thus

$$|\alpha q_{n-1} - p_{n-1}| < \frac{1}{q_n} < \frac{1}{q_{n+1}},$$

so

$$p_{n-1} = \alpha q_{n-1} + \frac{\delta}{q_{n-1}} \qquad \text{with } |\delta| < 1.$$

Hence

$$\begin{aligned} A_n &= a \left(\alpha q_{n-1} + \frac{\delta}{q_{n-1}} \right)^2 + b \left(\alpha q_{n-1} + \frac{\delta}{q_{n-1}} \right) q_{n-1} + c q_{n-1}^2 \\ &= (a\alpha^2 + b\alpha + c) q_{n-1}^2 + 2a\alpha\delta + a\frac{\delta^2}{q_{n-1}^2} + b\delta \\ &= 2a\alpha\delta + a\frac{\delta^2}{q_{n-1}^2} + b\delta. \end{aligned}$$

Thus

$$|A_n| = \left| 2a\alpha\delta + a\frac{\delta^2}{q_{n-1}^2} + b\delta \right| < 2|a\alpha| + |a| + |b|.$$

Thus there are only finitely many possibilities for the integer A_n. Also,

$$|C_n| = |A_{n-1}| \quad \text{and} \quad |B_n| = \sqrt{b^2 - 4(ac - A_n C_n)},$$

so there are only finitely many triples (A_n, B_n, C_n), and hence only finitely many possibilities for r_n as n varies. Thus for some $h > 0$,

$$r_n = r_{n+h}.$$

This shows that the continued fraction for α is periodic. □

7.3.3 What About Higher Degree?

Definition 7.3.5. An *algebraic number* is a root of a polynomial $f \in \mathbb{Q}[x]$.

Open Problem 7.3.6. *Give a simple description of the complete continued fraction expansion of the algebraic number* $\sqrt[3]{2}$. *It begins*

$$[1, 3, 1, 5, 1, 1, 4, 1, 1, 8, 1, 14, 1, 10, 2, 1, 4, 12, 2, 3, 2, 1, 3, 4, 1, 1, 2, 14,$$
$$3, 12, 1, 15, 3, 1, 4, 534, 1, 1, 5, 1, 1, \ldots]$$

I don't see a pattern, and that 534 reduces my confidence that I will. One could at least try to analyze the first few terms of the continued fraction statistically (see [LT72] which suggests that $\sqrt[3]{2}$ has an "unusual" continued fraction, and [LT74] that suggests that maybe it doesn't.)

Khintchine (1963), page 59:

> No properties of the representing continued fractions, analogous to those which have just been proved, are known for algebraic numbers of higher degree. [...] It is of interest to point out that up till the present time no continued fraction development of an algebraic number of higher degree than the second is known. It is not even known if such a development has bounded elements. Generally speaking the problems associated with the continued fraction expansion of algebraic numbers of degree higher than the second are extremely difficult and virtually unstudied.

Richard Guy (see [Guy94, pg. 260])

> Is there an algebraic number of degree greater than two whose simple continued fraction has unbounded partial quotients? Does *every* such number have unbounded partial quotients?

7.4 Applications

In this lecture we will learn about two applications of continued fractions. The first is a solution to the computational problem of recognizing a rational number using a computer. The second application is to the solution of "Pell's Equation": Given a positive nonsquare integer d, find *integers* x and y such that $x^2 - dy^2 = 1$.

7.4.1 Recognizing Rational Numbers

Suppose that you can compute approximations to a rational number using a computer, and desparately want to know what the rational number is. Henri Cohen gives a superb explaination in [Coh93] of how continued fraction are helpful in recognizing rational numbers.

> Consider the following apparently simple problem. Let $x \in \mathbb{R}$ be given by an approximation (for example a decimal or binary one). Decide if x is a rational number or not. Of course, this question as posed does not really make sense, since an approximation is usually itself a rational number. In practice however the question does make a lot of sense in many different contexts, and we can make it algorithmically more precise. For example, assume that one has an algorithm which allows us to compute x to as many decimal places as one likes (this is usually the case). Then, if one claims that x is (approximately) equal to a rational number p/q, this means that p/q should still be extremely close to x whatever the number of decimals asked for, p and q being fixed. This is still not completely rigorous, but it comes quite close to actual practice, so we will be content with this notion.
>
> Now how does one find p and q if x is indeed a rational number? The standard (and algorithmically excellent) answer is to compute the continued fraction expansion $[a_0, a_1, \ldots]$ of x. The number x is rational if and only if its continued fraction expansion is finite, i.e., if and only if one of the a_i is *infinite*. Since x is only given with the finite precision, x we be considered rational if x has a *very* large partial quotient a_i in its continued fraction expansion.

The following example illustrates Cohen's remarks:

Example 7.4.1. Let

$$x = 9495/3847 = 2.46815700545879906420587470756433584611385\ldots.$$

The continued fraction of the truncation 2.468157005458799064 is

$$[2, 2, 7, 2, 1, 5, 1, 1, 1, 1, 1, 1, 328210621945, 2, 1, 1, 1, \ldots]$$

We have

$$[2, 2, 7, 2, 1, 5, 1, 1, 1, 1, 1, 1] = \frac{9495}{3847}.$$

Notice that no repeating is evident in the digits of x giving above, though we know that the decimal expansion of x must be eventually periodic, since all decimal expansions of fractions are eventually periodic. In fact, the length of the period of the decimal expansion of $1/3847$ is 3846 (the order of 10 modulo 3847)!

7.4.2 Pell's Equation

In February of 1657, Pierre Fermat issued the following challenge:

> Given a positive integer d, give a systematic way to find a positive integer y such that $dy^2 + 1$ is a perfect square.

In other words, find a solution to $x^2 - dy^2 = 1$ with $y \in \mathbb{N}$.

Note Fermat's emphasis on *integer* solutions. It is easy to find rational solutions to the equation $x^2 - dy^2 = 1$. Simply divide the relation

$$(r^2 + d)^2 - d(2r)^2 = (r^2 - d)^2$$

by $(r^2 - d)^2$ to arrive at

$$x = \frac{r^2 + d}{r^2 - d}, \qquad y = \frac{2r}{r^2 - d}.$$

Fermat said: "Solutions in fractions, which can be given at once from the merest elements of arithmetic, do not satisfy me."

The equation $x^2 - dy^2 = 1$ is called **Pell's equation**. This is because Euler (in about 1759) accidently called it "Pell's equation" and the name stuck, though Pell (1611–1685) had nothing to do with it. (Hendrik Lenstra jokes that Pell was named after the equation.)

If d is a perfect square, $d = n^2$, then

$$(x + ny)(x - ny) = x^2 - dy^2 = 1$$

which implies that $x + ny = x - ny = 1$, so

$$x = \frac{x + ny + x - ny}{2} = \frac{1+1}{2} = 1.$$

We will thus always assume that d is not a perfect square. Pell's equation is best understood in terms of units in real quadratic fields.

7.4.3 Units in Real Quadratic Fields

Let d be a nonsquare positive integer, and set

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$$
$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

Then $\mathbb{Q}(\sqrt{d})$ is a *real quadratic field* and $\mathbb{Z}[\sqrt{d}]$ is a ring. There is a homomorphism called norm:

$$N : \mathbb{Q}(\sqrt{d})^\times \to \mathbb{Q}^\times, \qquad N\left(a+b\sqrt{d}\right) = \left(a+b\sqrt{d}\right)\left(a-b\sqrt{d}\right) = a^2-b^2d.$$

Definition 7.4.2. An element $x \in R$ is a *unit* if there exists $y \in R$ such that $xy = 1$.

Proposition 7.4.3. *The units of $\mathbb{Z}[\sqrt{d}]$ are exactly the elements of norm ± 1 in $\mathbb{Z}[\sqrt{d}]$.*

Proof. Suppose $u \in \mathbb{Z}[\sqrt{d}]$ is a unit. Then

$$1 = N(1) = N(uu^{-1}) = N(u) \cdot N(u^{-1}).$$

Since $N(u), N(u^{-1}) \in \mathbb{Z}$, we have $N(u) = N(u^{-1}) = \pm 1$ $\square$

Thus Fermat's challenge amounts to determing the group U^+ of units in $\mathbb{Z}[\sqrt{d}]$ of the form $a + b\sqrt{d}$ with $a, b \geq 0$.

Theorem 7.4.4. *The group U^+ is an infinite cyclic group. It is generated by $p_m + q_m\sqrt{d}$, where $\frac{p_m}{q_m}$ is one of the partial convergents of the continued fraction expansion of $\sqrt{d}$. (In fact, if m is the period of the continued fraction of $\sqrt{d}$ then $n = m - 1$ when m is even and $2n - 1$ when m is odd.)*

The theorem implies that *Pell's equation always has a solution*! Warning: the smallest solution is typically shockingly large. For example, the value of x in the smallest solution to $x^2 - 1000099y^2 = 1$ has **1118 digits**. For more on how to deal with huge solutions, see Lenstra's beautiful article [Len02].

The following example illustrates how to use Theorem 7.4.4 to solve Pell's equation when $d = 61$, where the simplest solution is already quite large.

Example 7.4.5. Suppose $d = 61$. Then

$$\sqrt{d} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}],$$

which has odd period $n = 11$. Thus the group U^+ is generated by

$$x = p_{21} = 1766319049$$
$$y = q_{21} = 226153980.$$

That is, we have

$$U^+ = \langle u \rangle = \langle 1766319049 + 226153980\sqrt{61} \rangle,$$

and $x = 1766319049$, $y = 226153980$ gives a solution to $x^2 - dy^2 = 1$. All the other solutions arise from u^n for some n. For example,

$$u^2 = 6239765965720528801 + 798920165762330040\sqrt{61}$$

leads to another solution.

Remark 7.4.6. To help with your homework, note that if the equation

$$x^2 - dy^2 = n$$

has at least one (nonzero) solution $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$, then it must have infinitely many solutions. This is because if $x_0^2 - dy_0^2 = n$ and u is a generator of the cyclic group U^+, then for any integer i,

$$N(u^i(x_0 + y_0\sqrt{d})) = N(u^i) \cdot N(x_0 + y_0\sqrt{d}) = 1 \cdot n = n,$$

so

$$x_1 + y_1\sqrt{d} = u^i(x_0 + y_0\sqrt{d})$$

provides another solution to $x^2 + dy^2 = n$.

7.4.4 Some Proofs

The rest of this lecture is devoted to proving most of Theorem 7.4.4. We will prove that partial convergents to continued fractions contribute infinitely many solutions to Pell's equation. We will not prove that every solution to Pell's equation is a partial convergent, though this is true (see, e.g., [Bur89, §13.5]).

Fix a positive nonsquare integer d.

Definition 7.4.7. A quadratic irrational $\alpha = a + b\sqrt{d}$ is *reduced* if $\alpha > 1$ and if the conjugate of α, denoted by α', satisfies $-1 < \alpha' < 0$.

For example, the number $\alpha = 1 + \sqrt{2}$ is reduced.

Definition 7.4.8. A continued fraction is *purely periodic* if it is of the form $[\overline{a_0, a_1, \ldots, a_n}]$.

The continued fraction $[\overline{2}]$ of $1 + \sqrt{2}$ is purely periodic.

Lemma 7.4.9. *If α is a reduced quadratic irrational, then the continued fraction expansion of α is purely periodic. (The converse is also true, and is easy to prove.)*

Lemma 7.4.10. *The continued fraction expansion of $\sqrt{d}$ is of the form*

$$[a_0, \overline{a_1, \ldots, a_{n-1}, 2a_0}].$$

Proof. Let a_0 be the floor of $\sqrt{d}$. Then $\alpha = \sqrt{d} + a_0$ is reduced because $\alpha > 1$ and $\alpha' = -\sqrt{d} + a_0$ satisfies $-1 < \alpha' < 0$. Let $[a_0, a_1, a_2, \ldots]$ be the continued fraction expansion of $\sqrt{d}$. Then the continued fraction expansion of $\sqrt{d} + a_0$ is $[2a_0, a_1, a_2, \ldots]$. By Lemma 7.4.9, the continued fraction expansion of $\sqrt{d} + a_0$ is purely periodic, so

$$[2a_0, a_1, a_2, \ldots] = [\overline{2a_0, a_1, a_2, \ldots, a_{n-1}}],$$

where n is the period. It follows that $a_n = 2a_0$, as claimed. $\square$

The following proposition shows that there are infinitely many solutions to Pell's equation that arise from continued fractions.

Proposition 7.4.11. *Let p_k/q_k be the partial convergents of the continued fraction expansion of $\sqrt{d}$, and let n be the period of the expansion of $\sqrt{d}$. Then*

$$p_{kn-1}^2 - dq_{kn-1}^2 = (-1)^{kn}$$

for $k = 1, 2, 3, \ldots$.

Proof. (This proof is taken from [Bur89, §13.5].) By Lemma 7.4.10, for $k \geq 1$, the continued fraction of $\sqrt{d}$ can be written in the form

$$\sqrt{d} = [a_0, a_1, a_2, \ldots, a_{kn-1}, r_{kn}]$$

where

$$r_{kn} = [2a_0, \overline{a_1, a_2, \ldots, a_n}] = a_0 + \sqrt{d}.$$

Because $\sqrt{d}$ is the last partial convergent of the continued fraction above, we have

$$\sqrt{d} = \frac{r_{kn}p_{kn-1} + p_{kn-2}}{r_{kn}q_{kn-1} + q_{kn-2}}.$$

Upon substituting $r_{kn} = a_0 + \sqrt{d}$ and simplifying, this reduces to

$$\sqrt{d}(a_0a_{kn-1} + q_{kn-2} - p_{kn-1}) = a_0p_{kn-1} + p_{kn-2} - dq_{kn-1}.$$

Because the right-hand side is rational and $\sqrt{d}$ is irrational,

$$a_0a_{kn-1} + q_{kn-2} = p_{kn-1}, \quad \text{and} \quad a_0p_{kn-1} + p_{kn-2} = dq_{kn-1}.$$

Multiplying the first of these equations by p_{kn-1} and the second by $-q_{kn-1}$, and then adding them, gives

$$p_{kn-1}^2 - dq_{kn-1}^2 = p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2}.$$

But

$$p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2} = (-1)^{kn-2} = (-1)^{kn},$$

which proves the proposition. □

Exercises

7.1 Compute the p_n and q_n for the continued fractions $[-3, 1, 1, 1, 1, 3]$ and $[0, 2, 4, 1, 8, 2]$. Observe that the propositions in Section 7.1.1.

7.2 If $c_n = p_n/q_n$ is the nth convergent of the continued fraction $[a_0, a_1, \ldots, a_n]$ and $a_0 > 0$, show that

$$[a_n, a_{n-1}, \ldots, a_1, a_0] = \frac{p_n}{p_{n-1}}$$

and

$$[a_n, a_{n-1}, \ldots, a_2, a_1] = \frac{q_n}{q_{n-1}}.$$

(Hint: In the first case, notice that $\frac{p_n}{p_{n-1}} = a_n + \frac{p_{n-2}}{p_{n-1}} = a_n + \frac{1}{\frac{p_{n-1}}{p_{n-2}}}$.)

7.3 Evaluate each of the following infinite continued fractions:

(a) $[\overline{2,3}]$
(b) $[2,\overline{1,2,1}]$
(c) $[0,\overline{1,2,3}]$

7.4 Determine the infinite continued fraction of each of the following numbers:

(a) $\sqrt{5}$
(b) $\dfrac{1+\sqrt{13}}{2}$
(c) $\dfrac{5+\sqrt{37}}{4}$

7.5 (a) For any positive integer n, prove that $\sqrt{n^2+1} = [n, \overline{2n}]$.
(b) Find a convergent to $\sqrt{5}$ that approximates $\sqrt{5}$ to within four decimal places.

7.6 A theorem of Hurwitz (1891) asserts that for any irrational number x, there exists infinitely many rational numbers a/b such that

$$\left| x - \frac{a}{b} \right| < \frac{1}{\sqrt{5}b^2}.$$

Take $x = e$, and obtain four rational numbers that satisfy this inequality.

7.7 The continued fraction expansion of e is

$$[2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, \ldots].$$

It is a theorem that the obvious pattern continues indefinitely. Do you think that the continued fraction expansion of e^2 also exhibits a nice pattern? If so, what do you think it is?

7.8 (a) Show that there are infinitely many even integers n with the property that both $n+1$ and $\frac{n}{2}+1$ are perfect squares.
(b) Exhibit two such integers that are greater than 389.

7.9 A primitive Pythagorean triple is a triple x, y, z of integers such that $x^2 + y^2 = z^2$. Prove that there exists infinitely many primitive Pythagorean triples x, y, z in which x and y are consecutive integers.

References

[ACD+99] K. Aardal, S. Cavallar, B. Dodson, A. Lenstra, W. Lioen, P. L. Montgomery, B. Murphy, J. Gilchrist, G. Guillerm, P. Leyland, J. Marchand, F. Morain, A. Muffett, C.&C. Putnam, and P. Zimmermann, *Factorization of a 512-bit RSA key using the Number Field Sieve*, `http://www.loria.fr/~zimmerma/records/RSA155` (1999).

[AKS02] M. Agrawal, N. Kayal, and N. Saxena, *Primes is in p*, `http://www.cse.iitk.ac.in/users/manindra/` (2002).

[Ber] D. J. Bernstein, *An Exposition of the Agrawal-Kayal-Saxena Primality-Proving Theorem*, `http://cr.yp.to/papers/aks.ps`.

[Bur89] David M. Burton, *Elementary number theory*, second ed., W. C. Brown Publishers, Dubuque, IA, 1989. MR 90e:11001

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 94i:11105

[Dav99] H. Davenport, *The higher arithmetic*, seventh ed., Cambridge University Press, Cambridge, 1999, An introduction to the theory of numbers, Chapter VIII by J. H. Davenport. MR 2000k:11002

[Dun] Edward G. Dunne, *Pianos and Continued Fractions*, `http://www.research.att.com/~njas/sequences/DUNNE/TEMPERAMENT.HTML`.

[GS02] X. Gourdon and P. Sebah, *The pi(x) project*, `http://numbers.computation.free.fr/Constants/Primes/Pix/pixproject.html` (2002).

[Guy94] R.K. Guy, *Unsolved problems in number theory*, second ed., Springer-Verlag, New York, 1994, Unsolved Problems in Intuitive Mathematics, I. MR 96e:11002

[Hoo67] Christopher Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR 34 #7445

[HW79] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979. MR 81i:10002

[IBM01] IBM, *IBM's Test-Tube Quantum Computer Makes History*, `http://www.research.ibm.com/resources/news/20011219_quantum.shtml` (2001).

[IR90] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Springer-Verlag, New York, 1990. MR 92e:11001

[Khi63] A. Ya. Khintchine, *Continued fractions*, Translated by Peter Wynn, P. Noordhoff Ltd., Groningen, 1963. MR 28 #5038

[Leh14] D.N. Lehmer, *List of primes numbers from* 1 *to* 10,006,721, Carnegie Institution Washington, D.C. (1914).

[Lem] F. Lemmermeyer, *Proofs of the Quadratic Reciprocity Law*, `http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`.

[Len02] H.W. Lenstra, Jr., *Solving the Pell equation*, Notices Amer. Math. Soc. **49** (2002), no. 2, 182–192. MR 2002i:11028

[LT72] S. Lang and H. Trotter, *Continued fractions for some algebraic numbers*, J. Reine Angew. Math. **255** (1972), 112–134; addendum, ibid. **267** (1974), 219–220; MR **50** #2086. MR 46 #5258

[LT74] ———, *Addendum to: "Continued fractions for some algebraic numbers" (J. Reine Angew. Math.* **255** *(1972), 112–134)*, J. Reine Angew. Math. **267** (1974), 219–220. MR 50 #2086

[Mat] Matsucom, *The on*hand *PC Watch*, `http://www.pconhand.com/`.

[Mor93] Pieter Moree, *A note on Artin's conjecture*, Simon Stevin **67** (1993), no. 3-4, 255–257. MR 95e:11106

[RSA] RSA, *The New RSA Factoring Challenge*, `http://www.rsasecurity.com/rsalabs/challenges/factoring`.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), no. 2, 120–126. MR 83m:94003

[Sho97] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26** (1997), no. 5, 1484–1509. MR 98i:11108

[Sin99] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Doubleday, 1999.