An Introduction to Continued Fractions, Part 2 of 2

Abstract

In this session, we shall continue our exploration of *continued fractions* and their applications. Our approach is modeled on that of The Ross Mathematics Program (formerly The Ross Young Scholars Program), as well as more traditional texts such as [3] and [4]. An approach to Pell's Equation via continued fractions is in [1] and especially [2].

0 Review: Basic Concepts and Notation about Continued Fractions

Let us review some of the basic notions regarding continued fractions.

Definition 0.1. A *finite simple continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}},$$

where a_0 is an integer, and $a_1, a_2, \ldots, a_n$ are all positive integers. To simplify this notation we let

$$[a_0; a_1, a_2, \ldots, a_n]$$

denote the above expression.

Definition 0.2. An *infinite simple continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n + \cfrac{1}{\ddots}}}}}},$$

where a_0 is an integer, and $a_1, a_2, \ldots, a_n, \ldots$ are all positive integers. As in Definition 0.1, we let

$$[a_0; a_1, a_2, \ldots, a_n, \ldots]$$

denote the above infinite simple continued fraction.

The "simple" in "simple continued fraction" refers to the fact that all the numerators in this expression are equal to 1. Since we shall be considering *only* simple continued fractions, we consider "simple" to be implicit in the discussion below.

Definition 0.3. Let $\alpha := [a_0; a_1, a_2, \ldots, a_n, \ldots]$ be an infinite simple continued fraction. We say that α is *periodic* if the sequence eventually repeats. That is, α is periodic if and only if it is of the form

$$[a_0; a_1, \ldots, a_k, a_{k+1}, \ldots, a_m, a_{k+1}, \ldots, a_m, \ldots].$$

We denote a periodic infinite continued fraction as above by

$$[a_0; a_1, \ldots, a_k, \dot{a}_{k+1}, \ldots, \dot{a}_m]$$

or

$$[a_0; a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_m}].$$

Definition 0.4. Let α be either a simple finite continued fraction or an infinite simple continued fraction as in Definitions 0.1 and 0.2. Further, let k be an integer with $0 \le k \le n$. Then the kth *convergent* to α is the finite continued fraction

$$\alpha_k := [a_0; a_1, \ldots, a_k].$$

Definition 0.5. Let α be either a finite or infinite simple continued fraction as above. Then the *magic table* for α is an array of the form

		a_0	a_1	a_2	a_3	a_4	a_5	$\cdots$
0	1	P_0	P_1	P_2	P_3	P_4	P_5	$\cdots$
1	0	Q_0	Q_1	Q_2	Q_3	Q_4	Q_5	$\cdots$

The P_j and Q_j are integers defined by the following recurrence relations:

$$\begin{aligned} P_{-2} &:= 0 & Q_{-2} &:= 1 \\ P_{-1} &:= 1 & Q_{-1} &:= 0 \\ P_0 &:= a_0 & Q_0 &:= 1 \\ P_k &:= a_k P_{k-1} + P_{k-2} & Q_k &:= a_k Q_{k-1} + Q_{k-2}. \end{aligned}$$

Explicitly, we have

		a_0	a_1	a_2	a_3	a_4	a_5	$\cdots$
0	1	a_0	a_1P_0+1	$a_2P_1+P_0$	$a_3P_2+P_1$	$a_4P_3+P_2$	$a_5P_4+P_3$	$\cdots$
1	0	1	a_1	$a_2Q_1+Q_0$	$a_3Q_2+Q_1$	$a_4Q_3+Q_2$	$a_5Q_4+Q_3$	$\cdots$

Example 0.6. Let $\alpha := [3; 1, 2, 4]$. Then the magic table for α is

		3	1	2	4
0	1	3	4	11	48
1	0	1	1	3	13

1 Recapitulation: Continued Fractions and the Magic Table

The magic table allows us to compute convergents, as well as having other interesting properties. These appeared as exercises in Section 2 of the previous worksheet, and we repeat them here as a list of propositions which will be useful later. (Many can be proven using mathematical induction, a proof technique explained in the accompanying supplement.)

Note: Feel free to try to prove these exercises, of course! But for this session, the priority is to understand these results enough to use them in proving other results.

Proposition 1.1. *Prove that for any continued fraction* $[a_0; a_1, a_2, \ldots, a_n]$*, we have* $Q_0 \geq 1$*,* $Q_1 \geq 1$*,* $Q_2 \geq 2$*,* $Q_3 \geq 3$*,* $Q_4 \geq 5$*, and in general,* $Q_n > Q_{n-1}$ *and* $Q_n > n+1$ *for all* $n \geq 3$*. (Can you provide an even better lower bound for* Q_k*?)*

Proposition 1.2. *Let* $[a_0; a_1, a_2, \ldots, a_n]$ *be a continued fraction. Prove that for each integer* k *with* $1 \leq k \leq n$*, we have*

$$\det \begin{bmatrix} P_{k-1} & P_k \\ Q_{k-1} & Q_k \end{bmatrix} := P_{k-1}Q_k - Q_{k-1}P_k = (-1)^k. \tag{1}$$

Proposition 1.3. *Let* $[a_0; a_1, a_2, \ldots, a_n]$ *be a continued fraction. Prove that for each integer* k *with* $1 \leq k \leq n$*, we have*

$$\det \begin{bmatrix} P_{k-2} & P_k \\ Q_{k-2} & Q_k \end{bmatrix} := P_{k-2}Q_k - Q_{k-2}P_k = (-1)^{k-1}a_k. \tag{2}$$

Proposition 1.4. *Let* $\alpha := [a_0; a_1, \ldots, a_n]$ *be a continued fraction. Prove that* $\alpha = \frac{P_n}{Q_n}$*; that is, prove that the continued fraction* α *is recovered as the quotient entries under index* n *in the magic table. Moreover, prove that* $\frac{P_n}{Q_n}$ *is already in lowest terms.*

Proposition 1.5. *Prove that for all* k *for which the quantity makes sense,*

$$\left| \frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}} \right| = \frac{1}{Q_k Q_{k+1}} \leq \frac{1}{Q_k^2}. \tag{3}$$

Proposition 1.6. *Let* $\alpha := [a_0; a_1, \ldots, a_n]$ *be a finite continued fraction. Prove that for each* k *with* $0 \leq k \leq n$ *and* $\alpha_k := [a_0; a_1, \ldots, a_k]$*, we have*

$$\alpha_0 < \alpha_2 < \alpha_4 < \cdots < \alpha < \cdots < \alpha_5 < \alpha_3 < \alpha_1. \tag{4}$$

We also computed certain real numbers, given their infinite continued fractions. Conversely, given real numbers of the form $\sqrt{d}$, where d is a positive integer that is not a perfect square, we computed their infinite continued fractions. For the latter, we noted certain interesting properties of the associated magic table.

Example 1.7. Assuming convergence, compute the value for the infinite continued fraction $\alpha := [1;1,1,\dots] = [1;\dot{1}]$. Construct the magic table, and compute the first few entries.
Solution: Note that $\alpha = [1;1,1,\dots] = [1;\alpha]$, so we have $\alpha = 1 + \frac{1}{\alpha}$. Solving for α, we obtain the quadratic equation $\alpha^2 - \alpha - 1 = 0$. By the quadratic equation, this has the two roots $\frac{1\pm\sqrt{5}}{2}$. Since $\alpha > 0$, we must choose the positive root, whence $\underline{\alpha = \frac{1+\sqrt{5}}{2}}$. □

Example 1.8. Compute the infinite continued fraction expansion for $\sqrt{41}$. For the first few columns of its magic table, compute the values $P_k^2 - 41Q_k^2$.
Solution: Following the usual algorithm, we obtain $\sqrt{41} = [6;\dot{2},2,\dot{12}]$. Our associated magic table is thus

		6	2	2	12	2	2	12	⋯
0	1	6	13	32	397	826	2049	25414	⋯
1	0	1	2	5	62	129	320	3969	⋯
$P_k^2 - 41Q_k^2$		−5	5	−1	5	−5	1	−5	⋯

Note that although the values of P_k and Q_k grow large very rapidly, the values of $P_k^2 - 41Q_k^2$ remain bounded. □

2 Linear Diophantine Equations

Using some of the results from Section 0, we can show how to use continued fractions to solve certain Diophantine equations. These are equations where admissible solutions are either all integers or (depending on context) all rational numbers.

We repeat the following exercises, which appeared in Section 2 of the previous session's worksheet.

2.1 Let a, b be positive integers. If $\gcd(a,b) = 1$, describe a method guaranteed to produce integers x, y such that $ax + by = 1$. More generally, if $\gcd(a,b) = d$, how can we produce integers x, y such that $ax + by = d$?

2.2 Let a, b be positive integers. If $d := \gcd(a,b)$, then describe a method to find integers x and y such that $ax + by = d$.

2.3 Let a, b, and c be arbitrarily given integers. Provide, with justification, a set of criteria for which the equation

$$ax + by = c$$

has a solution such that x and y are both integers.

2.4 Let a and m be integers, with $m > 1$. We say that x is the *multiplicative inverse of a modulo m* if and only if x is an integer and $ax \equiv 1 \pmod{m}$. (For those unfamiliar with modular arithmetic: this means that $ax - 1$ is divisible by m.) *Important:* note that x must itself be an integer!

Fix an integer $m > 1$. Give a complete characterization of all integers a such that a has a multiplicative inverse modulo m. For those a admitting a multiplicative inverse modulo m, provide a method for computing such a multiplicative inverse.

2.5 Compute, if possible, the following multiplicative inverses modulo m for a:

(a) $a := 4$, $m := 17$

(b) $a := 43$, $m := 257$

(c) $a := 17$, $m := 119$

2.6 Let $a_1, \dots, a_k, c$ be integers. When can we solve the Diophantine equation

$$a_1 x_1 + a_2 x_2 + \cdots a_k x_k = c$$

for integers $x_1, \dots, x_k$? For those cases where a solution exists, describe an algorithm for producing at least one solution.

3 Rational Approximations

One nice property of continued fractions is that their convergents provide very good rational approximations to given real numbers. This is useful in its own right. Moreover, using these properties, we will show that another family of Diophantine equations can be solved using continued fractions.

3.1 Let α be an irrational real number. Then for all nonnegative integers n, we have

$$\left|\alpha - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n^2}.$$

Note: A priori, we could expect that

$$\left|\alpha - \frac{P_n}{Q_n}\right| \leq \frac{1}{2Q_n}.$$

Being able to approximate α to within the *square* of the denominator of the convergent is a considerable improvement over this initial worst-case scenario.

3.2 Let α be a real number, and let $\frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n}$ be consecutive convergents to α. Then

$$\left|\alpha - \frac{P_n}{Q_n}\right| < \left|\alpha - \frac{P_{n-1}}{Q_{n-1}}\right|.$$

That is, as n increases, the convergents $\frac{P_n}{Q_n}$ get closer to α.

3.3 Here, we shall build up to a basic result establishing another sense in which the convergents to α are "good" rational approximations to α. First, we state the following without proof:

Theorem 3.1 (Pick's Theorem)**.** *Let P be a simple polygon in the plane, each of whose vertices is a lattice point. (That is, for each vertex V on the boundary of P, both the x- and y-coordinates of V are integers.) Let I denote the number of lattice points in the interior of P, and let B denote the number of lattice points on the boundary. (I.e., B counts the number of lattice points that lie on the edges of the boundary of P.) Then the area A of P is given by the formula*

$$A = I + \frac{B}{2} - 1.$$

(a) Let (a,b) and (c,d) be points in the plane. Consider the parallelogram P whose vertices are $(0,0)$, (a,b), (c,d), and $(a+c,b+d)$. Then

$$\text{Area}(P) = \left|\det\begin{bmatrix} a & c \\ b & d \end{bmatrix}\right| = |ad = bc|.$$

(b) Let α be a real number, and let $\frac{P_k}{Q_k}$ be a convergent to α. If $\frac{P}{Q}$ is any rational number with $P, Q \in \mathbb{Z}$, $Q > 0$, and $Q < Q_k$, then

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \left|\alpha - \frac{P}{Q}\right|.$$

That is, we cannot find a better rational approximation to α than $\frac{P_k}{Q_k}$ using a smaller denominator.

3.4 Let α be an irrational number. Prove that for infinitely many convergents $\frac{P_n}{Q_n}$, we have

$$\left|\frac{P_n}{Q_n} - \alpha\right| < \frac{1}{2Q_n^2}.$$

Hint: Prove that for any two consecutive convergents, at least one must satisfy this stronger condition.

Note: In general, the best possible result we can obtain is that there are infinitely many convergents such that

$$\left|\frac{P_n}{Q_n} - \alpha\right| < \frac{1}{\sqrt{5}Q_n^2};$$

the constant $\sqrt{5}$ is optimal if and only if α is of the form $\alpha = [a_0; a_1, \ldots, a_n, \dot{1}]$. Otherwise, $\sqrt{8}$ is the optimal constant if and only if $\alpha = [a_0; a_1, \ldots, a_n, \dot{2}]$. There are a number of other refinements possible.

3.5 Let $\alpha \in \mathbb{R}$, $P, Q \in \mathbb{Z}$ with $Q \neq 0$. If

$$\left|\alpha - \frac{P}{Q}\right| < \frac{1}{2Q^2},$$

then $\frac{P}{Q}$ is a convergent to α. (This is a partial converse to Exercise #3.4

4 Pell's Equation

Let d be a positive integer that is not a perfect square. Then $\sqrt{d}$ is an irrational number, so it must have an infinite continued fraction representation. Using this continued fraction $sqrt d = [a_0; a_1, a_2, \ldots]$, we shall solve another Diophantine equation: *Pell's Equation*, which seeks integer solutions (x, y) to the equation $x^2 - dy^2 = 1$.

4.1 Let $\frac{P_n}{Q_n}$ be a convergent to $\sqrt{d}$. Then

$$\left|P_n^2 - dQ_n^2\right| < 1 + 2\sqrt{d}.$$

4.2 Let d be a positive, nonsquare integer. Then there exists some integer M such that for infinitely many convergents $\frac{P_n}{Q_n}$ to $\sqrt{d}$,

$$P_n^2 - dQ_n^2 = M.$$

4.3 Let d and M be as in Exercise #4.2. Then there exist infinitely many convergents $\frac{P_n}{Q_n}$ to $\sqrt{d}$ such that

$$P_n^2 - dQ_n^2 = M$$

and we have simultaneously

$$P_j \equiv P_k \pmod{M} \text{ and } Q_j \equiv Q_k \pmod{M}.$$

4.4 Let d be a positive, nonsquare integer. Then there are infinitely many solutions (x, y) over the integers such that

$$x^2 - dy^2 = 1.$$

4.5 If d is as above, and P, Q are integers such that $P^2 - dQ^2 = 1$, then

$$\left|\frac{P}{Q} - \sqrt{d}\right| < \frac{1}{2Q^2}.$$

4.6 Let d be as above, and assume P, Q are integers such that $P^2 - dQ^2 = 1$. Then $\frac{P}{Q}$ is a convergent to $\sqrt{d}$.

References

[1] Keith Conrad. Pell's equation, i. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn1.pdf. online: retrieved October 16, 2021.

[2] Keith Conrad. Pell's equation, ii. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn2.pdf. online: retrieved October 16, 2021.

[3] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Walton Street, Oxford OX2 6DP, fifth edition, 1979.

[4] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.