CONTINUED FRACTIONS: THE PAST AND THE MODERN

MING-LUN HSIEH

1. Basic properties of continued fractions

For any sequence $\{a_0, a_1, a_2, \dots\}$ of positive numbers and a non-negative integer n, we define the real number

$$[a_0, a_1, \dots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_n}}}}.$$

For example,

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

We introduce two sequences $\{p_n\}_{n=0,1,2,\dots}$ and $\{q_n\}_{n=0,1,2,\dots}$ to study the sequence

$$[a_0], \quad [a_0, a_1], \quad [a_0, a_1, a_2], \dots.$$

Definition 1.1. For the sequence $\{a_0, a_1, \dots\}$, we define the sequences $\{p_n\}$ and $\{q_n\}$ by

$$\begin{array}{lllll} p_0 = a_0, & p_1 = a_0 a_1 + 1, & p_2 = a_2 p_1 + p_0, & p_3 = a_3 p_2 + p_1, & \dots \\ q_0 = 1, & q_1 = a_1, & q_2 = a_2 q_1 + q_0, & q_3 = a_3 q_2 + q_1, & \dots \end{array}$$

For $n \geq 2$, we have

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

In terms of the equation between matrices, we have

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix},$$

Lemma 1.2. *For any sequence $\{a_0, a_1, \dots\}$ and $n \geq 0$, we have*

$$[a_0, a_1, \dots, a_n] = \frac{p_n}{q_n}. \tag{1.1}$$

Proof. We shall prove by induction. It is easy to see the above identity holds for $n = 0$ and $n = 1$. Assume for *any* sequence $\{a_0, a_1, \dots,\}$, the equation (1.1) holds for $k = 0, 1, \dots, n$. Applying the induction hypothesis to the new sequence

$$\left\{a_0, a_1, \dots a_{n-1}, a_n + \frac{1}{a_{n+1}}, \dots\right\},$$

we obtain

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

This proves the lemma by induction. □

Lemma 1.3. *For any positive integer n, we have*

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

Proof. When $n = 1$ it is obvious that $p_1 q_0 - p_0 q_1 = 1$. Note that

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

The lemma easily follows from the induction. □

Indeed, if a real number x is not an integer , we can write uniquely

$$x = \lfloor x \rfloor + \frac{1}{x_1}, \quad x_1 > 1.$$

Repeating this process, we obtain

$$\begin{aligned}x &= \lfloor x \rfloor + \frac{1}{x_1} = [\lfloor x \rfloor, x_1] \\ &= \lfloor x \rfloor + \frac{1}{\lfloor x_1 \rfloor + \frac{1}{x_2}} = [\lfloor x \rfloor, \lfloor x_1 \rfloor, x_2] = \ldots.\end{aligned}$$

This shows that any real number α can be written as

$$\alpha = [a_0, \alpha_1] = [a_0, a_1, \alpha_2] = \cdots = [a_0, a_1, a_2, \ldots, a_n, \alpha_{n+1}] = \ldots,$$

where $a_1, a_2, \ldots a_n, \ldots$ are positive integers and $\alpha_n \geq 1$. We call $[a_0, a_1, \ldots, a_n, \ldots]$ the continued fraction expansion of α.

For example, we let $\alpha = \sqrt{2}$:

$$\begin{aligned}\sqrt{2} = 1 + \sqrt{2} - 1 &= 1 + \frac{1}{\sqrt{2}+1} = [1, \sqrt{2}+1] \\ &= 1 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}} = [1, 2, \sqrt{2}+1] \\ &= [1, 2, 2, 2, \ldots] = [1, \overline{2}].\end{aligned}$$

Let $\alpha = \sqrt{7}$:

$$\begin{aligned}\sqrt{7} = 2 + \sqrt{7} - 2 &= [2, \frac{2+\sqrt{7}}{3}] \\ &= 2 + \frac{1}{1 + \frac{-1+\sqrt{7}}{3}} = [2, 1, \frac{1+\sqrt{7}}{2}] \\ &= 2 + \frac{1}{1 + \frac{1}{1+\frac{-1+\sqrt{7}}{2}}} = [2, 1, 1, \frac{1+\sqrt{7}}{3}] \\ &= [2, 1, 1, 1, 2+\sqrt{7}] = [2, 1, 1, 1, 4, \frac{2+\sqrt{7}}{3}] = [2, \overline{1, 1, 1, 4}].\end{aligned}$$

In the above examples, α is irrational number, so the length of the continued fraction expansion of α is finite. If α is a rational number, then the length of the continued fraction expansion of α is finite. For example,

$$\frac{13}{11} = [1, 5, 2] = [1, 5, 1, 1]; \quad \frac{30}{13} = [2, 3, 4] = [2, 3, 3, 1].$$

We find that there are two different continued fraction expansions of a rational number, but the continued fraction expansion of an irrational number is unique.

2. Rational approximation of irrational numbers

Let $\alpha \in \mathbf{R}_+$ with the continued fraction expansion $[a_0, a_1, a_2, \dots]$. Since a_i are positive integers, the sequences $\{p_n\}$ and $\{q_n\}$ consist of positive integers with

$$p_1 < p_2 < \cdots < p_n; \quad q_1 < q_2 < \cdots < q_n.$$

On the other hand, by Lemma 1.3, we see that for any k, the positive integers p_k and q_k are **coprime**. The theorem below shows that any positive number α can be approximated by p_n/q_n.

Theorem 2.1. *Let $\alpha = [a_0, a_1, a_2, \dots]$ be the continued fraction expansion of α. For any positive integer n, we have*

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

If α is irrational, then we have infinitely many n such that

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

Proof. We can write

$$\alpha = [a_0, a_1, \dots, a_n, b], \quad b \geq 1.$$

Then

$$\alpha = \frac{bp_n + p_{n-1}}{bq_n + q_{n-1}}$$

and

$$\begin{aligned}\alpha - \frac{p_n}{q_n} =& \frac{(bp_n + p_{n-1})q_n - p_n(bq_n + q_{n-1})}{q_n(bq_n + q_{n-1})} \\ =& \frac{(-1)^{n+1}}{q_n(bq_n + q_{n-1})} \quad (\textit{Lemma } 1.3).\end{aligned}$$

Since $\alpha_n \geq 1$ and $q_n \geq q_{n-1} > 0$, we find that

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

Now assume α is an irrational number, so the continued fraction expansion $[a_0, a_1, a_2, \dots]$ of α has infinite length. Write

$$\alpha = [a_0, a_1, \dots, a_n, b] = [a_0, a_1, \dots, a_n, a_{n+1}, c] \text{ for some } b,\, c > 1.$$

Then the above computation shows that

$$\left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| + \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(bq_n + q_{n-1})} + \frac{1}{q_{n+1}(cq_{n+1} + q_n)}.$$

By definition, we have $b = a_{n+1} + \frac{1}{c}$, so

$$\frac{1}{q_n(bq_n + q_{n-1})} + \frac{1}{q_{n+1}(cq_{n+1} + q_n)} = \frac{1}{cq_{n+1} + q_n}(\frac{c}{q_n} + \frac{1}{q_{n+1}}) = \frac{1}{q_n q_{n+1}}$$

and hence

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

This implies that we must have

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

for $(p, q) =$ either (p_n, q_n) or (p_{n+1}, q_{n+1}). □

It follows from Theorem 2.1 that

$$\alpha = \lim_{m\to\infty} \frac{p_n}{q_n}.$$

Remark 2.2. The famous Roth's theorem asserts that if α is an irrational algebraic number, then for any $\rho > 2$, there are only finitely many rational numbers p/q such that

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

Therefore $1/q^2$ in the right hand side of the inequality in Theorem 2.1 is optimal. Roth was awarded Fields Medal in 1958 for this achievement.

3. Integral solutions to the Pell equation $x^2 - dy^2 = 1$

We have seen the integral solutions to the linear equation $ax + by = 1$ with $a, b \in \mathbf{Z}$ and $(a, b) = 1$ can be found by Euclid's algorithm. Let d be a non-square positive integer. We next explain how to use continued fractions to obtain integral solutions to the quadratic equation $x^2 - dy^2 = 1$ (the Pell equation). Obviously $(x, y) = (\pm 1, 0)$ is an integral solution, so we seek for integral solutions other than $(\pm 1, 0)$, which are called non-trivial integral solutions. Sometimes simple equation can have very complicated solutions.

Example 3.1. A smallest solution to the equation $x^2 - 61y^2 = 1$ is given by $(1766319049, 226153980)$.

Let us prepare some notation. Let K be the set

$$K := \left\{x + y\sqrt{d} \mid x, y \in \mathbf{Q}\right\} \subset \mathbf{R}.$$

One verifies that if $x, y \in K$, then

- $x \pm y$ and $x \cdot y$ belong to K.
- if $x \neq 0 \in K$, then $x^{-1} \in K$.

In other words, we can do four arithmetic operations in the set K. In mathematics, any set like this is called a field. On the other hand, we define the subset

$$R := \left\{x + y\sqrt{d} \in K \mid x, y \in \mathbf{Z}\right\} \subset K.$$

Note that we can do addition/substraction/multiplication except for the division! This is because for non-zero $x \in R$, x^{-1} may not belong to R.

Given $a = x + y\sqrt{d} \in K$, define the conjugate $\overline{x}$ of x by

$$\overline{a} := x - y\sqrt{d},$$

and the norm $\mathrm{N}(a)$ of a is defined by

$$\mathrm{N}(a) := a\overline{a} = x^2 - dy^2.$$

To find an integral solution to $x^2 - dy^2 = 1$ is equivalent to finding $a \in R$ such that $\mathrm{N}(a) = 1$. By definition if $b = x' + y'\sqrt{d}$, then

$$\overline{a} \cdot \overline{b} = (x - y\sqrt{d})(x' - y'\sqrt{d}) = xx' + yy'd - (xy' + x'y)\sqrt{d} = \overline{a \cdot b}.$$

We obtain the multiplicative property of the norm map

$$\mathrm{N}(a \cdot b) = \mathrm{N}(a) \cdot \mathrm{N}(b). \tag{3.1}$$

Theorem 3.2. *There exists a non-trivial integral solution to the Pell equation* $x^2 - dy^2 = 1$.

PROOF. By Theorem 2.1, we find that there are infinitely many p/q with $(p, q) = 1$ such that

$$\begin{aligned} \left|\mathrm{N}(a + q\sqrt{d})\right| &= \left|p^2 - dq^2\right| \\ &= \left|(p + q\sqrt{d})(p - q\sqrt{d})\right| < \frac{p + q\sqrt{d}}{q} = \sqrt{d} + \frac{p}{q} < 2\sqrt{d} + 1. \end{aligned}$$

This implies that there exist infinitely many p/q such that

$$\mathrm{N}(p + q\sqrt{d}) = p^2 - dq^2 = M$$

for some integer M with $|M| < 2\sqrt{d} + 1$ by the pigeon hole principle. By the pigeonhole principle again, we can find distinct (p, q) and (p', q') such that

- $(p, q) \neq (\pm p', \pm q')$,
- $p \equiv p' \pmod{M}$, $q \equiv q' \pmod{M}$, and
- $\mathrm{N}(p + q\sqrt{d}) = \mathrm{N}(p' + q'\sqrt{d}) = M$.

Since d is not a perfect square, M is non-zero. We set

$$\beta := \frac{p + q\sqrt{d}}{p' + q'\sqrt{d}} \in K.$$

Then $\beta \neq \pm 1$ and by (3.1),

$$\mathrm{N}(\beta) = \frac{\mathrm{N}(p + q\sqrt{d})}{\mathrm{N}(p' + q'\sqrt{d})} = 1.$$

On the other hand, we note that

$$\beta = \frac{(pp' - dqq') + (p'q - pq')\sqrt{d}}{M} \in R.$$

We thus proved that

$$\left(\frac{pp' - dqq'}{M}, \frac{p'q - pq'}{M}\right) \neq (\pm 1, 0)$$

is an integral solution to $x^2 - dy^2 = 1$. □

Next we proceed to explain how to find a non-trivial integral solution to the Pell equation.

Definition 3.3. Let α be a real number with the continued fraction expansion $\alpha = [a_0, a_1, a_2, \ldots]$. The n-th convergent of α is defined by

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

Theorem 3.4. *Let α be a positive real number. If p and q are co-prime positive integers such that*

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

then the rational number $\frac{p}{q}$ must be a convergent of α.

Proof. By the assumption, we can write

$$\alpha = \frac{p}{q} + \frac{\delta}{2q^2} \text{ with } |\delta| < 1.$$

Since p/q is a rational number, we can express the continued fraction expansion of p/q as

$$\frac{p}{q} = [a_0, a_1, \ldots, a_n] \text{ such that } (-1)^n\delta > 0.$$

Now consider the following equation with variable x:

$$\alpha = [a_0, a_1, \ldots, a_n, x]. \tag{3.2}$$

If we can solve x with $x > 1$, then $\frac{p}{q}$ would be the n-th convergent of x. According to (3.2), we obtain

$$\alpha = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}, \quad p_n = p,\ q_n = q.$$

It follows that

$$\begin{aligned} & x(q_n\alpha - p_n) = p_{n-1} - \alpha q_{n-1} \\ \iff & \frac{x\delta}{2q_n} = p_{n-1} - \alpha q_{n-1} \\ \iff & \frac{x\delta}{2} = (-1)^n - \frac{q_{n-1}\delta}{2q_n}. \end{aligned}$$

We thus find that

$$x = \frac{2}{\delta(-1)^n} - \frac{q_{n-1}}{q_n} > 2 - 1 = 1.$$

□

Corollary 3.5. *If $0 < m < \sqrt{d}$, and (x, y) are co-prime positive integers with $x^2 - dy^2 = m$, then x/y is a convergent of $\sqrt{d}$.*

Proof. Since $(x + y\sqrt{d})(x - y\sqrt{d}) = m$ and x, y are coprime positive integers, we find that $x > y\sqrt{d}$ and that

$$\left|\frac{x}{y} - \sqrt{d}\right| = \frac{m}{y^2(\frac{x}{y} + \sqrt{d})} < \frac{m}{2\sqrt{d}y^2} < \frac{1}{2y^2}.$$

Therefore by Theorem 3.4, we see that $\frac{x}{y}$ is a convergent of $\sqrt{d}$, and □

Example 3.6. Consider the Pell equation $x^2 - 7y^2 = 1$. We have $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$.

a_n	2	1	1	1	4	1	...
p_n	2	3	5	8	37	45	...
q_n	1	1	2	3	14	17	...

.

We find that $(x, y) = (8, 3)$ is a non-trivial integral solution.

4. Generalized Pell equation $x^2 - dy^2 = m$

The generalized Pell equation $x^2 - dy^2 = m$ for $m \in \mathbf{Z}$ may not have integral solution in general. For example, there are no integral solutions to the equation $x^2 - 3y^2 = 5$, and if p is a prime with $p \equiv 3 \pmod 4$, then there is no integral solution to $x^2 - py^2 = -1$.

We give a general method to solve $x^2 - dy^2 = m$ for the integral solutions. First we choose a non-trivial solution $(a, b) \in \mathbf{Z}^2_{>0}$ with $x^2 - dy^2 = 1$ and put

$$u := a + b\sqrt{d} \in R.$$

Then we have $\mathrm{N}(u) = u\overline{u} = a^2 - db^2 = 1$. In particular, $u > 1$ and $0 < \overline{u} < 1$.

Theorem 4.1. *Suppose that $x^2 - dy^2 = m$ has an integral solution, Then there exists an integral solution (x_0, y_0) satisfying*

$$|x_0| \le \frac{|m|}{2}(\sqrt{u} + \frac{1}{\sqrt{u}}), \quad |y_0| \le \frac{|m|}{2\sqrt{d}}(\sqrt{u} + \frac{1}{\sqrt{u}}).$$

Proof. Let (x_1, y_1) be an integral solution to $x^2 - dy^2 = m$. We may assume x_1 and y_1 are positive integers. Let $\beta := x_1 + y_1\sqrt{d}$. We write

$$\log|\beta| = \frac{|m|}{2} + c_1 \log u \text{ for some } c_1 \in \mathbf{R}.$$

Since $\mathrm{N}(\beta) = \beta\overline{\beta} = x_1^2 - dy_1^2 = m$ and $u\overline{u} = 1$, it follows that

$$\log\left|\overline{\beta}\right| = \frac{|m|}{2} - c_1 \log u.$$

We may write $c_1 = k + \delta$, where $k \in \mathbf{Z}$ and $|\delta| < 1/2$. Put

$$\gamma := \beta u^{-k} = \beta\overline{u}^k \in R.$$

Then $\mathrm{N}(\gamma) = \mathrm{N}(\beta) = m$ and

$$\log|\gamma| = \log\sqrt{|m|} + \delta \log u.$$

So we find that

$$|\gamma| = \sqrt{|m|} \cdot u^{\delta} \quad |\overline{\gamma}| = \sqrt{|m|} \cdot u^{-\delta}, \quad |\delta| < 1/2.$$

Write $\gamma = x_0 + y_0\sqrt{d} \in R$. Then $x_0^2 - dy_0^2 = m$ and

$$|x_0| = \left|\frac{\gamma + \overline{\gamma}}{2}\right| \leq \frac{|\gamma| + |\overline{\gamma}|}{2} < \frac{\sqrt{|m|}}{2}\left(u^{\delta} + u^{-\delta}\right) < \frac{\sqrt{|m|}}{2}\left(\sqrt{u} + \sqrt{u}^{-1}\right).$$

Likewise

$$|y_0| = \left|\frac{\gamma - \overline{\gamma}}{2\sqrt{d}}\right| \leq \frac{|\gamma| + |\overline{\gamma}|}{2\sqrt{d}} < \frac{\sqrt{|m|}}{2\sqrt{d}}\left(\sqrt{u} + \sqrt{u}^{-1}\right).$$

□

Example 4.2. Consider the equation $x^2 - 7y^2 = 11$. Put

$$u := 8 + 3\sqrt{7}.$$

Note that

$$\frac{11}{2\sqrt{7}}(\sqrt{u} + \sqrt{u}^{-1}) < 8.84.$$

One verifies that $|y_0| \leq 8$, $7y_0^2 + 11$ is not a square, so there is no integral solution to $x^2 - 7y^2 = 11$ by Theorem 3.4.

Homework 1 (Due date: 09/12)

Exercise 1. (5pts) Find the continued fraction expansion of $\frac{157}{68}$. Use this expansion to find a solution of $157x - 68y = 3$.

(Use Lemma 1.3).

Exercise 2. (5pts)Use the continued fraction expansion of $\sqrt{19}$ to find a non-trivial integral solution of $x^2 - 19y^2 = 1$.

Exercise 3. (10pts) Use the continued fraction expansion of $\sqrt{61}$ to find the solution to $x^2 - 61y^2 = 1$ in Example 3.1.

(You may use a calculator).

Exercise 4. (10pts)Let p be a prime such that $p \equiv 1 \pmod 4$. Let $(x_0, y_0) \in \mathbf{Z}^2_{>0}$ be a non-trivial integral solution to $x^2 - py^2 = 1$ such that y_0 is minimal.

(1) Prove that x_0 is odd and y_0 is even.
(2) Prove $x_0 + 1$ is divisible by p.
(3) Show that $x^2 - py^2 = -1$ has an integral solution.

Exercise 5. (10pts)Let d be a positive integer that is not a square. Suppose that $x^2 - dy^2 = -1$ has an integral solution. Let $(\alpha, \beta) \in \mathbf{Z}^2_{>0}$ be the minimal solution to $x^2 - dy^2 = 1$, i.e. $\alpha + \beta\sqrt{d}$ is minimal. Prove that there exist $(a, b) \in \mathbf{Z}^2_{>0}$ such that $\alpha = 2a^2 + 1$ and $\beta = 2ab$.