Number theory and Cryptography June 4, 2024

Lecture 9 : Continued Fractions

Instructor: Chao Qin *Notes written by: Wenhao Tong and Yingshu Wang*

A continued fraction continued fraction is an expression of the form

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

We denote the continued fraction displayed above by

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

For example,

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

$$\begin{aligned}[3,7,15,1,292] &= 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292}}}} \\ &= \frac{103993}{33102} = 3.14159265301190260407\ldots,\end{aligned}$$

and

$$[2,1,2,1,1,4,1,1,6] = 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6}}}}}}}}$$
$$= \frac{1264}{465}$$
$$= 2.718279569892473118279569 8\ldots$$

1 Finite Continued Fractions

Definition (Finite Continued Fraction)**.** *A* finite continued fraction *is an expression*

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\cdots+\frac{1}{a_n}}}}$$

where each a_m is a real number and $a_m > 0$ for all $m \geq 1$.

Definition (Simple Continued Fraction)**.** *A* simple continued fraction *is a finite or infinite continued fraction in which the a_i are all integers.*

To get a feeling for continued fractions, observe that

$$[a_0] = a_0,$$
$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0a_1+1}{a_1},$$
$$[a_0, a_1, a_2] = a_0 + \cfrac{1}{a_1+\cfrac{1}{a_2}} = \frac{a_0a_1a_2+a_0+a_2}{a_1a_2+1}.$$

Also,

$$\begin{aligned}[a_0, a_1, \ldots, a_{n-1}, a_n] &= \left[a_0, a_1, \ldots, a_{n-2}, a_{n-1} + \frac{1}{a_n}\right] \\ &= a_0 + \frac{1}{[a_1, \ldots, a_n]} \\ &= [a_0, [a_1, \ldots, a_n]].\end{aligned}$$

1.1 Partial Convergent

Definition (Partial Convergents)**.** *For* $0 \le n \le m$*, the nth* convergent *of the continued fraction* $[a_0, \ldots, a_m]$ *is* $[a_0, \ldots, a_n]$*. These convergents for* $n < m$ *are also called* partial convergents.

Proposition (Partial Convergents)**.** *For* $n \ge 0$ *with* $n \le m$ *we have*

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

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

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

□

Proposition. *For* $n \ge 0$ *with* $n \le m$ *we have*

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

and

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

Equivalently,

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

and

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

Proof. The case for $n = 0$ is obvious from the definitions. Now suppose $n > 0$ and the statement is true for $n - 1$. Then

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

This completes the proof of Simple Continued Fraction. □

Theorem. *If $[a_0, a_1, \ldots, a_m]$ is a simple continued fraction, so each a_i is an integer, then the p_n and q_n are integers and the fraction p_n/q_n is in lowest terms.*

Proof. It is clear that the p_n and q_n are integers, from the formula that defines them. If d is a positive divisor of both p_n and q_n, then $d \mid (-1)^{n-1}$, so $d = 1$. □

1.2 The Sequence of Partial Convergents

Proposition (How Convergents Converge)**.** *The even indexed convergents c_{2n} increase strictly with n, and the odd indexed convergents c_{2n+1} decrease strictly with n. Also, the odd indexed convergents c_{2n+1} are greater than all of the even indexed convergents c_{2m}.*

Proof. The a_n are positive for $n \geq 1$, so the q_n are positive. By proposition, 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.

Suppose for the sake of contradiction that there exist integers r and m such that $c_{2m+1} < c_{2r}$. From the previous proposition implies that for $n \geq 1$,

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

has sign $(-1)^{n-1}$, so for all $s \geq 0$ we have $c_{2s+1} > c_{2s}$. Thus it is impossible that $r = m$. If $r < m$, then by what we proved in the first paragraph, $c_{2m+1} < c_{2r} < c_{2m}$, a contradiction (with $s = m$). If $r > m$, then $c_{2r+1} < c_{2m+1} < c_{2r}$, which is also a contradiction (with $s = r$). □

1.3 Every Rational Number is Represented

Proposition (Rational Continued Fractions)**.** *Every nonzero rational number can be represented by a simple continued fraction.*

Proof. Without loss of generality, we may assume that the rational number is a/b, with $b \geq 1$ and $\gcd(a, b) = 1$.

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

Note that $a_i > 0$ for $i > 0$ (also $r_n = 1$, since $\gcd(a, b) = 1$). 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

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

□

2 Infinite Continued Fractions

2.1 The Continued Fraction Procedur

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

$$x = a_0 + t_0$$

with $a_0 \in \mathbb{Z}$ and $0 \le t_0 < 1$. We call the number a_0 the *floor* of x, and we also sometimes write $a_0 = \lfloor x \rfloor$. If $t_0 \neq 0$, write

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

with $a_1 \in \mathbb{N}$ and $0 \le t_1 < 1$. Thus $t_0 = \frac{1}{a_1+t_1} = [0, a_1+t_1]$, which is a continued fraction expansion of t_0, which need not be simple. 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 $0 \le t_{n+1} < 1$. We call this procedure, which associates to a real number x the sequence of integers $a_0, a_1, a_2, \ldots$, the continued fraction process.

Example 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 procedure produces the continued fraction of $\frac{8}{3}$.

Example 2. *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 $a_1 = 1$ and $t_1 = \frac{-1+\sqrt{5}}{2}$. Likewise, $a_n = 1$ for all n. As we will see below, the following exciting 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 3. *Suppose $x = e = 2.71828182\ldots$. Using the continued fraction procedure, we find that*

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

For example, $a_0 = 2$ is the floor of 2. Subtracting 2 and inverting, we obtain $1/0.718\ldots = 1.3922\ldots$, so $a_1 = 1$. Subtracting 1 and inverting yields $1/0.3922\ldots = 2.5496\ldots$, so $a_2 = 2$.

The 5th partial convergent of the continued fraction of e is

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

which is a good rational approximation to e, in the sense that

$$\left|\frac{87}{32} - e\right| = 0.000468\ldots.$$

Note that $0.000468\ldots < 1/32^2 = 0.000976\ldots$, which illustrates the bound in Theorem.

Let's do the same thing with $\pi = 3.14159265358979\ldots$. Applying the continued fraction procedure, we find that the continued fraction of π is

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

The first few partial convergents are

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

These are good rational approximations to π; for example,

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

2.2 Convergence of Infinite Continued Fract

Lemma. *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. We use induction. The statements are both true when $n = 0$. If the second statement is true for $n - 1$, then

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

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

Theorem (Continued Fraction Limit)**.** *Let $a_0, a_1, \ldots$ 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 $\lim_{n\to\infty} c_n$ exists.*

Proof. For any $m \geq n$, the number c_n is a partial convergent of $[a_0, \ldots, a_m]$. 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 $\alpha_0 \leq \alpha_1$.

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

so $\alpha_0 = \alpha_1$. □

We define

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

Example 4. *We illustrate the theorem with $x = \pi$.*

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. *Let $a_0, a_1, a_2, \ldots$ be a sequence of real numbers 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 $\lim_{n\to\infty} c_n$ exists if and only if the sum $\sum_{n=0}^{\infty} a_n$ diverges.*

Example 5. *Let $a_n = \frac{1}{n\log(n)}$ for $n \geq 2$ and $a_0 = a_1 = 0$. By the integral test, $\sum a_n$ diverges, the continued fraction $[a_0, a_1, a_2, \ldots]$ converges. This convergence is very slow, since, e.g.*

$$[a_0, a_1, \ldots, a_{9999}] = 0.5750039671012225425930\ldots$$

yet

$$[a_0, a_1, \ldots, a_{10000}] = 0.7169153932917378550424\ldots.$$

Theorem. *Let $x \in \mathbb{R}$ be a real number. Then x is the value of the (possibly infinite) simple continued fraction $[a_0, a_1, a_2, \ldots]$ produced by the continued fraction procedure.*

Theorem (Convergence of continued fraction)**.** *Let $a_0, a_1, \ldots$ define a simple continued fraction, and let $x = [a_0, a_1, \ldots] \in \mathbb{R}$ be its value. Then for all m,*

$$\left| x - \frac{p_m}{q_m} \right| < \frac{1}{q_m \cdot q_{m+1}}.$$