Continued Fractions

Tristan Liu

November 2019

1 Basics

Definition: A simple continued fraction is an expression like

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

with infinite or finitely many terms (when we say terms we refer to the a_i's), where a_i are all integers, and (except for a_0) are all positive. This is alternatively written as $[a_0; a_1, a_2, a_3, \cdots]$ for compactness. If there are finitely many terms, say n terms, we write it as $[a_0; a_1, a_2, a_3, \cdots, a_n]$.

Definition: The m^{th} convergent of the continued fraction $[a_0; a_1, a_2, a_3, \cdots]$ is the continued fraction $[a_0; a_1, a_2, a_3, \cdots, a_m]$.

You may be slightly worried about the infinite continued fraction, but we can define it to be the limit of the convergents (which as we will see does exist).

Example: We compute the continued fraction $[1; 1, 1, 1]$. Convergent 0 is just 1. The next convergent is then $1 + \frac{1}{1} = \frac{2}{1}$. The next convergent is $1 + \frac{1}{1+\frac{1}{1}} = 1 + \frac{1}{2} = \frac{3}{2}$. Convergent 3 is $\frac{5}{3}$ and is the value of our continued fraction.

Theorem 1. *A simple continued fraction is finite iff it is a rational number.*

Proof sketch: For any finite continued fraction, we can inductively evaluate it, yielding a fraction at each stage, and thus when we finish the evaluation in a finite number of steps, we will have a rational value. For any rational with denominator 1, we can trivially find a continued fraction. Suppose we can find a finite continued fraction for any rational with denominator less than b. For a rational $\frac{a}{b}$, let $a_0 = \lfloor \frac{a}{b} \rfloor$, and let c be such that $a_0 + \frac{c}{b} = \frac{a}{b}$. Then $\frac{a}{b} = a_0 + \frac{1}{\frac{b}{c}}$. However, note that $c < b$, and thus we can find a continued fraction for b/c by our inductive hypothesis, say $[a_1; a_2, a_3, \cdots, a_i]$. Then $\frac{a}{b} = [a_0; a_1, a_2, \cdots, a_i]$. This can be adapted easily into an algorithm for computing a finite (or even an infinite) continued fraction, and is in fact related to the Euclidean Algorithm. This algorithm can be shown to give a more or less unique continued fractions with some slight subleties.

Definition: Let p_n and q_n to be the unique positive numbers such that $\frac{p_n}{q_n}$ is equal to the nth convergent of α and p_n and q_n are relatively prime integers.

Theorem 2. *For* $\alpha = [a_0; a_1, a_2, \cdots]$ *and integer* n*, we have* $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$ *and that* $\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_{n-2} q_n}$.

Proof: We have that p_n and q_n of $[a_0; a_1, a_2, \cdots]$ satisfy the recursion $p_n = a_n p_{n-1} + p_{n-2}$ and $q_n = a_n q_{n-1} + q_{n-2}$, which can be shown fairly easily by inducting on n, and is left as an exercise.

We now show that $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$. We can induct on n again. The base case is trivial We have that

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

. By induction, we then have that $p_n q_{n-1} - p_{n-1} q_n$ equals $(-1)^{n-1}$. Since $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_n q_{n-1} - p_{n-1} q_n}{q_{n-1} q_n}$, we have $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$.

Then

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

.

Corollary: The even convergents $p_0/q_0, p_2/q_2, \cdots$ is a increasing sequence while the odd convergents form a decreasing sequence.

Corollary: The convergents converge, and the value they converge to is greater than all the even convergents and smaller than all the odd convergents.

Corollary: $|\frac{p_n}{q_n} - \alpha| < \frac{1}{q_n^2}$ (ie convergents are very good approximations for α)

Theorem 3. *: If* $|p/q - \beta| < \frac{1}{2q^2}$ *then* p/q *is a convergent of* β.

We refer readers to [10] for a proof.

2 Irrationality

Historically, one of the main uses of continued fractions was to prove irrationality. The first proofs of irrationality were through use of continued fractions.

Theorem 4. ***(Euler)*** $\frac{e-1}{2} = [0; 1, 6, 10, 14, 18, 22, 26, 30, \cdots]$.

Euler showed this using a differential equation: the Ricatti equation, $ady + y^2 dx = x^{\frac{-4n}{2n+1}} dx$. How Euler did it is further elaborated in [3]. Euler also showed that $e - 1 = [1; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \cdots]$.

Corollary: e is irrational

Theorem 5. ***(Lambert)*** $\tan(x) = \frac{x}{1 - \frac{x^2}{3 - \frac{x^2}{5 - \frac{x^2}{\cdots}}}}$*, and furthermore, for any rational* $x \neq 0$*, the right hand side is irrational.*

We begin with

$$\tan(x) = \frac{x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots}{1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdot} = \frac{x}{\frac{1-\frac{x^2}{2!}+\frac{x^4}{4!}-\cdot}{1-\frac{x^2}{3!}+\frac{x^4}{5!}-\cdots}} = \frac{x}{1 - x^2 \frac{1/3-\frac{x^2}{3!5}+\frac{x^4}{5!7}-\cdots}{1-\frac{x^2}{3!}+\frac{x^4}{5!}-\cdots}}$$

. Repeating the process yields the equation $\frac{x}{1-\frac{x^2}{3-\frac{x^2}{5-\cdots}}}$ (feel free to repeat this process a few more times to get the beginning of the continued fraction). This isn't entirely rigorous, since we need to show the convergents of this fraction do in fact converge to $\tan(x)$, but that is in fact true, and we thus have an expression for $\tan(x)$. Showing it is irrational is a little more difficult, and those interested may consider [5] or [11].

Corollary: π is irrational. If π were rational, then $\tan(\frac{\pi}{4})$ would be irrational by the above theorem, but this is not the case since $\tan(\frac{\pi}{4})$ is 1.

3 Factoring

Let $n > 1$ be an odd composite number. We consider the continued fraction of $\sqrt{n}$. Consider the ith convergent. Let $Q_i = a_i^2 - b_i^2 n$. Then $Q_i \equiv a_i^2 \pmod{n}$. These Q_i when reduced modulo n have that $-2\sqrt{n} < Q_i < 2\sqrt{n}$ We can factor these Q_i and try to find a subset which multiplies to a square, and thus, as in the Quadratic Sieve factoring method, construct two squares which are non trivially equal.

Consider RSA encryption. Suppose $p < q < 2p$, which should be somewhat reasonable since the two primes should be around the same size, with $n = pq$ public. Say the encryption key is e and the decryption key is d. Suppose by chance $d < \sqrt[4]{n}$, in which case we have an attack. Let $ed - 1 = k\phi(n)$. Since $e < \phi(n)$, $d > k$. We also have that $3\sqrt{n} > p + q$. Thus $|\frac{e}{n} - \frac{k}{d}| = \frac{|k\phi(n)+1-nk|}{nd} = \frac{k(p+q-1)+1}{nd} \leq \frac{3k}{d\sqrt{n}} < \frac{1}{3d^2}$. This implies that $\frac{k}{d}$ is a convergent of $\frac{e}{n}$. Thus computing the convergents of $\frac{e}{n}$ and checking them all (note that there are relatively few convergents of $\frac{e}{n}$) will yield k and d. This then completely breaks the encryption, since, if these are the correct k, d, we can find $\phi(n)$ and thus obtain a factorization quickly.

Example: Consider $n = 7119477283$. Let $e = 525410191$. Checking $\frac{e}{n}$'s convergents yields $20/271$ and $d = 271$.

4 Various Neat Things Which We State Without Proof

4.1 Sums of Two Squares

Let p be a prime congruent to 1 modulo 4. Suppose $0 < w < \frac{p}{2}$ and $w^2 \equiv -1 \pmod{p}$. Compute the continued fraction of p/w. It will be of the form

$[a_0 a_1, a_2, \cdots a_m, a_m, \cdots, a_2, a_1, a_0]$. Then compute the $m-1^{th}$ convergent and the m^{th} convergent: $\frac{p_{m-1}}{q_{m-1}}$ and $\frac{p_m}{q_m}$. Then $p_{m-1}^2 + p_m^2 = p$. This is further considered in [8] and [10]

Example: take 601. Suppose we find that $125^2 \equiv 1 \pmod{601}$. We compute $\frac{601}{125} = [4; 1, 4, 4, 1, 4]$. The second convergent is $\frac{5}{1}$ and the third convergent is $\frac{24}{5}$, and $5^2 + 24^2 = 601$.

4.2 On the Terms of Continued Fractions

For almost all real α, the probability a_n is equal to some given k is about $\frac{\log(1+\frac{1}{k(k+2)})}{log(2)}$. This can be used to show that for almost all real α, the geometric mean of the terms of the continued fraction of α is Khinchin's constant which is about 2.68545, though the arithmetic mean is unbounded.

It is unknown if Khinchin's constant is irrational or not.

4.3 Various Miscellaneous Continued Fractions

$$\frac{1}{1+\frac{e^{-2\pi}}{1+\frac{e^{-4\pi}}{1+\frac{e^{-6\pi}}{1+e^{-8\pi}}}}} = \left(\sqrt{\frac{5+\sqrt{5}}{2}} - \frac{\sqrt{5}+1}{2}\right)e^{2\pi/5}.$$

$$\sqrt{\frac{2}{e\pi}}\frac{1}{\operatorname{erfc}(\frac{1}{\sqrt{2}})} = 1 + \frac{1}{1+\frac{2}{1+\frac{3}{1+\frac{4}{1+\frac{5}{1+\frac{6}{\cdots}}}}}}.$$

4.4 Pell Equations

If $(p, q) \in \mathbb{Z}^2$ is a solution to the Pell equation for a nonsquare d, $x^2 - dy^2 = \pm 1$, then $\frac{p}{q}$ is a convergent of $\sqrt{d}$. Since

$$|p - \sqrt{d}q| = \frac{1}{p + \sqrt{d}q} < \frac{1}{(1+\sqrt{d})q} < \frac{1}{2q}$$

and thus $|\frac{p}{q} - \sqrt{d}| < \frac{1}{2q^2}$, and thus $\frac{p}{q}$ is a convergent of $\sqrt{d}$.

Furthermore, let $\sqrt{d} = [a_0; \overline{a_1, a_2, \cdots a_m}]$, where m is the smallest period. (p_n, q_n) is a solution to the Pell Equation iff $m|n+1$. This topic is further discussed in [8] and [10].

5 Problems

1. What are the convergents of $[1, 1, 1, \cdots]$, and what does it converge to?
2. When is a continued fraction periodic?
3. What are the convergents of $\sqrt{2}$.

4. Transform the Wallis Product $\frac{4}{\pi} = \frac{3\cdot3\cdot5\cdot5\cdot7\cdots}{2\cdot4\cdot4\cdot6\cdot6\cdots}$ into the continued fraction

$$1 + \cfrac{1^2}{2 + \frac{3^2}{2 + \frac{5^2}{2 + \cdots}}}$$

5. Use the Wallis product to find $\pi = 3 + \frac{1^2}{6 + \frac{3^2}{6 + \frac{5^2}{6 + \cdots}}}$.

6. What is $[1; 3, 5, 7, 9, \cdots]$.

7. Show e^2 is irrational. More generally, show e^u for $u \in \mathbb{Q}$ is irrational.

5.1 Sources

[1]http://www.maths.surrey.ac.uk/hosted-sites/R.Knott/Fibonacci/cfINTRO.html
[2]http://pi.math.cornell.edu/ gautam/ContinuedFractions.pdf
[3]http://eulerarchive.maa.org/hedi/HEDI-2006-02.pdf
[4]https://www.jstor.org/stable/2974737?seq=1#page_scan_tab_contents
[5]http://www.bibnum.education.fr/sites/default/files/24-lambert-analysis.pdf
[6]https://www.ams.org/journals/mcom/1975-29-129/S0025-5718-1975-0371800-5/
[7]http://www.ams.org/notices/199612/pomerance.pdf
[8]https://www.math.ru.nl/ bosma/Students/CF.pdf
[9]http://www.math.hawaii.edu/ pavel/contfrac.pdf
[10]https://www.math.arizona.edu/ jeremybooher/expos/continued_fractions.pdf
[11]https://youtu.be/Lk_QF_hcM8A
[12]http://mathworld.wolfram.com/KhinchinsConstant.html