Continued Fractions and the Euclidean Algorithm

November 13, 2017

Continued Fractions

(Finite) continued fraction A

finite continued fraction in the variables $x_1, x_2, \ldots, x_n$ is an expression of the form:

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \ddots + \cfrac{1}{x_N}}}$$

Notation: $/x_0, x_1, \ldots, x_N/$

Examples:

$$/x_0, x_1/ = x_0 + \frac{1}{x_1} = \frac{x_0 x_1 + 1}{x_1}$$

$$/x_0, x_1, x_2/ = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2}} = \frac{x_0 x_1 x_2 + x_2 + x_0}{x_2 x_1}.$$

Q-polynomials

Definition

For $n \geq 0$:

$$\begin{aligned} Q_0 &= 1 \\ Q_1(x_1) &= x_1 \\ Q_n(x_1, x_2, \ldots, x_n) &= x_1 Q_{n-1}(x_2, \ldots, x_n) + Q_{n-2}(x_3, \ldots, x_n) \end{aligned}$$

Q-polynomials

Definition

For $n \geq 0$:

$$\begin{aligned} Q_0 &= 1 \\ Q_1(x_1) &= x_1 \\ Q_n(x_1, x_2, \ldots, x_n) &= x_1 Q_{n-1}(x_2, \ldots, x_n) + Q_{n-2}(x_3, \ldots, x_n) \end{aligned}$$

In this way we get

$$\begin{aligned} Q_1(x_1) &= x_1 \\ Q_2(x_1, x_2) &= x_1 x_2 + 1 \\ Q_3(x_1, x_2, x_3) &= x_1 x_2 x_3 + x_1 + x_3 \\ Q_4(x_1, x_2, x_3, x_4) &= x_1 x_2 x_3 x_4 + x_1 x_4 + x_3 x_4 + x_1 x_2 + 1. \end{aligned}$$

Theorem (L. Euler)

The polynomial $Q_n(x_1, x_2, \ldots, x_n)$ is the sum of all terms produced by starting with the product:

$$1 \cdot x_1 \cdot x_2 \cdots x_n$$

and omitting zero or more nonoverlapping pairs of consecutive variables $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 + x_3x_4 + x_1x_4 + x_1x_2 + 1.$$

Theorem (L. Euler)

The polynomial $Q_n(x_1, x_2, \ldots, x_n)$ is the sum of all terms produced by starting with the product:

$$1 \cdot x_1 \cdot x_2 \cdots x_n$$

and omitting zero or more nonoverlapping pairs of consecutive variables $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 + x_3x_4 + x_1x_4 + x_1x_2 + 1.$$

Theorem (L. Euler)

The polynomial $Q_n(x_1, x_2, \ldots, x_n)$ is the sum of all terms produced by starting with the product:

$$1 \cdot x_1 \cdot x_2 \cdots x_n$$

and omitting zero or more nonoverlapping pairs of consecutive variables $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 + x_3x_4 + x_1x_4 + x_1x_2 + 1.$$

Theorem (L. Euler)

The polynomial $Q_n(x_1, x_2, \ldots, x_n)$ is the sum of all terms produced by starting with the product:

$$1 \cdot x_1 \cdot x_2 \cdots x_n$$

and omitting zero or more nonoverlapping pairs of consecutive variables $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 + x_3x_4 + x_1x_4 + x_1x_2 + 1.$$

Theorem (L. Euler)

The polynomial $Q_n(x_1, x_2, \ldots, x_n)$ is the sum of all terms produced by starting with the product:

$$1 \cdot x_1 \cdot x_2 \cdots x_n$$

and omitting zero or more nonoverlapping pairs of consecutive variables $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 + x_3x_4 + x_1x_4 + x_1x_2 + 1.$$

Fibbonacci numbers an Q-polynomials

Definition

We define the sequence $(F_n)_{n\in\mathbb{N}}$ of the Fibonacci numbers as follows:

$$F_0 = 0, \quad F_1 = 1$$
$$F_{n+2} = F_{n+1} + F_n, \quad \text{for} \quad n \geq 0.$$

$1, 1, 2, 3, 5, 8, 13, 21, \ldots$

Theorem

The number of summands appearing in the polynomial $Q_n(x_1, x_2, \ldots, x_n)$ *is equal to the Fibonacci number* F_{n+1}.

Proof.

This is obvious for $n = 0, 1$ and inductively, the number of summands that appears in $Q_n(x_1, x_2, \ldots, x_n)$ is

$$\begin{aligned} Q_n(1, 1, \ldots, 1) &= 1 \cdot Q_{n-1}(1, \ldots, 1) + Q_{n-2}(1, \ldots, 1) \\ &= 1 \cdot F_n + F_{n-1} (\text{ind. hyp.}) \\ &= F_{n+1}. \quad \text{Def.of Fib.} \end{aligned}$$

□

Greatest common divisor

GCD

$gcd(a, b) =$ the largest natural number that's a divisor (factor) of both a and b Example

$$594 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 11$$

$$924 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 11$$

$$gcd(594, 924) = 2 \cdot 3 \cdot 11$$

Two integers are relatively prime to each other if the integer 1 is their only common positive divisor. E.g.
$gcd(8, 17) = 1, gcd(3, 2) = 1, gcd(10, 9) = 1$

Q-polynomials and continued fractions

Theorem

We have

$$/x_0, x_1, \ldots, x_n/ = \frac{Q_{n+1}(x_0, x_1, \ldots, x_n)}{Q_n(x_1, x_2, \ldots, x_n)},$$

moreover it holds that

$$\gcd(Q_{n+1}(x_0, x_1, \ldots, x_n), Q_n(x_1, x_2, \ldots, x_n)) = 1.$$

Continued Fractions a a way to represent numbers

The continued fraction representations of some familiar numbers

$$\frac{423}{720} = /1, 1, 2, 2, 1, 4/,$$
$$\pi = /3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, \ldots/,$$
$$e = /2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, 1, \ldots/,$$

$$\phi = /1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \ldots/,$$

where $\phi = \frac{1+\sqrt{5}}{2}$ is the Golden Ratio.

Continued fractions are a way of representing the real numbers.
Other representations are:

- decimal numbers
- binary numbers
- prime factorization (only for numbers in $\mathbb{N}$)

Infinite Continued Fractions

Definition

The continued fraction $/a_0, a_1, \ldots, a_n/$ is simple if $a_0 \geq 0, a_1 > 0, a_2 > 0, \ldots$ $a_0, a_1, a_2, \ldots \in \mathbb{N}$

Definition

Let $a_0, a_1, a_2, \ldots$ be an infinite sequence of integers with $a_0 \geq 0, a_1 > 0, a_2 > 0, \ldots$. Let $x_n = /a_0, a_1, \ldots, a_n/$. If

$$\lim_{n \to \infty} x_n = x$$

then we will say that the infinite simple continued fraction $/a_0, a_1, a_2, \ldots/$ converges to the value x and we will write $x = /a_0, a_1, a_2, \ldots/$.

Theorem

All infinite simple continued fractions converge.

Theorem (Division theorem for natural numbers)

For $x \geq y > 0$, $x, y \in \mathbb{N}$, there exist unique natural numbers q (quotient) and r (remainder) such that $q \in \mathbb{N}$ and $\upsilon \in \mathbb{N}$ such that

$$x = yq + \upsilon \quad \textit{and} \quad 0 \leq \upsilon < y.$$

e.g. divide 59 by 7 $59 = 78 + 3$ and $r = 3 < 7$ and $q = 8$

Theorem (Division theorem for natural numbers)

For $x \geq y > 0$, $x, y \in \mathbb{N}$, there exist unique natural numbers q (quotient) and r (remainder) such that $q \in \mathbb{N}$ and $\upsilon \in \mathbb{N}$ such that

$$x = yq + \upsilon \quad \textit{and} \quad 0 \leq \upsilon < y.$$

e.g. divide 59 by 7 $59 = 78 + 3$ and $r = 3 < 7$ and $q = 8$

Theorem (Division theorem for real numbers $q \in \mathbb{N}$)

For $x \geq y > 0$ and $x, y \in \mathbb{R}$, there exist unique natural numbers q (quotient) and r (remainder) such that $q \in \mathbb{N}$ and $r \in \mathbb{R}$ such that

$$x = y \cdot q + r \quad \textit{and} \quad 0 \leq r < y.$$

e.g. $5.6 = 1.1 \cdot 5 + 0.1$ *Moreover,*

$$q = \left\lfloor \frac{x}{y} \right\rfloor.$$

Continued Fraction Expansion

$$\frac{8}{3} = 2 + \frac{2}{3} = 2 + \frac{1}{\frac{3}{2}} = 2 + \frac{1}{1 + \frac{1}{2}}$$

$$\varphi = 1 + \frac{1}{\varphi} = 1 + \frac{1}{1 + \frac{1}{\varphi}}$$

By substituting each time φ from:

$$\varphi = 1 + \frac{1}{\varphi}$$

Let

$$\varphi = \frac{\sqrt{5}+1}{2}$$

then

$$1-\varphi = \frac{\sqrt{5}-1}{2}$$

$$1+\frac{1}{\varphi} = \varphi$$

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

now observe that:

$$\frac{\sqrt{5}-1}{2} = \frac{(\sqrt{5}-1)(\sqrt{5}+1)}{2(\sqrt{5}+1)} = \frac{(\sqrt{5}^2-1)}{2(\sqrt{5}+1)}$$

$$= \frac{4}{2(\sqrt{5}+1)} = \frac{2}{(\sqrt{5}+1)}$$

$$\frac{\sqrt{5}-1}{2} = \frac{(\sqrt{5}+1)}{2}$$

Continued fraction algorithm

To each real number x we assign two finite or infinite sequences $a_0, a_1, \ldots \in \mathbb{N}$ and $\xi_0, \xi_1, \ldots \in \mathbb{R}$ of reals as follows:

1. Let $a_0 = \lfloor x \rfloor, \quad \xi_0 = x - a_0$.
2. If $a_0, \ldots, a_n, \xi_0, \ldots, \xi_n$, are defined and $\xi_n \neq 0$, then let

$$a_{n+1} = \lfloor \frac{1}{\xi_n} \rfloor, \qquad \xi_{n+1} = \frac{1}{\xi_n} - a_{n+1}$$

3. If $\xi_n = 0$ then the algorithm terminates and returns $a_0, a_1, \ldots, a_n$ and $\xi_0, \ldots, \xi_n$.

That is

$$x = a_0 + \xi_0 = a_0 + \frac{1}{a_1 + \xi_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \xi_2}} = \ldots$$

$$= /a_0, \ldots, a_n + \xi_n/.$$

Theorem (Correctness of the continued fraction algorithm)

For the sequence $a_0, a_1, \ldots, a_n$ assigned to x by the continued fraction algorithm, we have that:

(a) *If x is rational then the algorithm terminates with $\xi_N = 0$ for some $N \geq 0$, and $x = /a_0, \ldots, a_N/$, (with $a_N > 1$ if $N \neq 0$).*

(b) *If x is irrational, then $\xi_n \neq 0$ for all n, thus the algorithm does not terminate, and*

$$x = \lim_{n \to \infty} /a_0, a_1, \ldots, a_n/.$$

Modular Arithmetic

Definition

Let m be an integer. We say that two integers a and b are **congruent** modulo m if m divides $a - b$ and write $a \equiv b \bmod m$. That is

$$a \equiv b \bmod m \Leftrightarrow m \mid a - b.$$

E.g., $4 \bmod 1 = 0$ (1 divides 4 so the remainder is 0)
$4 \bmod 2 = 0$ as $4 = 21 + 0$
$4 \bmod 3 = 1$ as $4 = 31 + 1$ and 1 is the remainder
$14 \bmod 3 = 2$ as $13 = 34 + 2$ and 2 is the remainder

The following statements are equivalent:

$a \equiv b(\mod n)$

$(a \mod n) \equiv (b \mod n)$

a is congruent to b*modulo*n

n divides $a - b$

$a = b + nd$ for some integer n

Examples of practical use

Hourly arithmetic on a 12 hour clock uses a modulus 12
"Minute arithmetic uses mod 60
all students with odd numbers solve problem A all students with even numbers solve problem B

Congruency is an equivalence relationship

Definition

A relation $\sim$ in a nonempty set A is called an equivalence relation in A if
1) $(\forall a \in A)[a \sim a]$
2) $a \sim b \Rightarrow b \sim a$
3) $[a \sim b \ \& \ b \sim c] \Rightarrow a \sim c$. For each $a \in A$ we define the equivalence class of a,

$$[a] = \{x \in A | x \sim a\}.$$

Clearly $a \sim b$ if and only if $[a] = [b]$.
It is easy to check that the relation $\sim$ defined by

$$a \sim b \Leftrightarrow a \equiv b \bmod m$$

is an equivalence relation.

Congruency is an equivalence relationship

Definition

If $x \equiv a \bmod m$ then a is called a **residue** of x modulo m. If $0 \leq a \leq m-1$, then a is **the least non-negative residue** of x modulo m.

The equivalence class of $a \in \mathbb{Z}$ is

$$\begin{aligned} [a] &= \{x \in \mathbb{Z} |\, x \equiv a \bmod m\} \\ &= \{x \in \mathbb{Z} |\, m \mid x-a\} \\ &= \{x \in \mathbb{Z} |\, x-a = km, \text{ for some } k \in \mathbb{Z}\}. \end{aligned}$$

Definition

We denote by $\mathbb{Z}_m$ the set of all equivalence classes defined by (1.1). A **complete set of (incongruent) residues mod** m is any set X of natural numbers which contains exactly one member of each equivalence class $[a] \in \mathbb{Z}_m$, for example the set $\{0, 1, 2, \ldots, m-1\}$.

Subtructive Euclidean Algorithm

"keep subtracting the smaller from the bigger number:"

$\{18, 42\}$

1. If $u = 1$ or $v = 1$ then $\gcd(u, v) = 1$.
2. If $u = v$, then $\gcd(u, v) = u$.
3. If $u > v$ then let $u \leftarrow u - v$ and goto 1.
4. If $u < v$ then let $v \leftarrow v - u$ and goto 1.

Subtructive Euclidean Algorithm

"keep subtracting the smaller from the bigger number:"

$$\{18, 42\} \to \{18, 42 - 18 = 24\}$$

1. If $u = 1$ or $v = 1$ then $\gcd(u, v) = 1$.
2. If $u = v$, then $\gcd(u, v) = u$.
3. If $u > v$ then let $u \leftarrow u - v$ and goto 1.
4. If $u < v$ then let $v \leftarrow v - u$ and goto 1.

Subtructive Euclidean Algorithm

"keep subtracting the smaller from the bigger number:"

$$\{18, 42\} \to \{18, 42 - 18 = 24\} \to \{18, 24 - 18 = 6\}$$

1. If $u = 1$ or $v = 1$ then $\gcd(u, v) = 1$.
2. If $u = v$, then $\gcd(u, v) = u$.
3. If $u > v$ then let $u \leftarrow u - v$ and goto 1.
4. If $u < v$ then let $v \leftarrow v - u$ and goto 1.

Subtructive Euclidean Algorithm

"keep subtracting the smaller from the bigger number:"

$$\{18, 42\} \to \{18, 42 - 18 = 24\} \to \{18, 24 - 18 = 6\}$$
$$\to \{18 - 6 = 12, 6\}$$

1. If $u = 1$ or $v = 1$ then $\gcd(u, v) = 1$.
2. If $u = v$, then $\gcd(u, v) = u$.
3. If $u > v$ then let $u \leftarrow u - v$ and goto 1.
4. If $u < v$ then let $v \leftarrow v - u$ and goto 1.

Subtructive Euclidean Algorithm

"keep subtracting the smaller from the bigger number:"

$$\{18, 42\} \to \{18, 42 - 18 = 24\} \to \{18, 24 - 18 = 6\}$$
$$\to \{18 - 6 = 12, 6\} \to \{12 - 6 = 6, 6\}.$$

1. If $u = 1$ or $v = 1$ then $\gcd(u, v) = 1$.
2. If $u = v$, then $\gcd(u, v) = u$.
3. If $u > v$ then let $u \leftarrow u - v$ and goto 1.
4. If $u < v$ then let $v \leftarrow v - u$ and goto 1.

Euclidean algorithm with division:

$$\begin{aligned} 42 &= 18 \cdot 2 + 6 \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

expand $\frac{18}{42}$ as a continued fraction:

$$\frac{18}{42} = 0 + \cfrac{1}{2 + \cfrac{1}{3}} = /0, 2, 3/$$

I:

Implementation of division with consecutive subtructions:
Number of subtractive steps: 2+3=5.

Euclidean algorithm with division:

$$\begin{aligned} 42 &= 18 \cdot 2 + 6 \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

expand $\frac{18}{42}$ as a continued fraction:

$$\frac{18}{42} = 0 + \cfrac{1}{2 + \cfrac{1}{3}} = /0, 2, 3/$$

I:

Implementation of division with consecutive subtructions:
Number of subtractive steps: 2+3=5.

It is the Subtractive Euclidean Algorithm.

If $1 \leq m \leq n$, then

$$\frac{m}{n} = /0, q_1, q_2, \ldots, q_r, 1/.$$

For $1 \leq i < r$,
q_i are the quotients from the divisions of the Euclidean algorithm:

$$\begin{aligned} n &= mq_1 + r_1, \quad 0 < r_1 < m \\ m &= r_1 q_2 + r_3, \quad 0 < r_2 < r_1 \\ &\ldots \end{aligned}$$

Number of steps of the Subtractive Euclidean algorithm$= q_1 + q_2 + \ldots + q_r$.

Modular arithmetic

The Euclidean algorithm for the pair $\{x, y\}$ is as follows:

$$
\begin{aligned}
x &= ya_1 + v_1 && 0 < v_1 < y \\
y &= v_1 a_2 + v_2 && 0 < v_2 < v_1 \\
v_1 &= v_2 a_3 + v_3 && 0 < v_3 < v_2 \\
&\vdots && \vdots \\
v_{n-3} &= v_{n-2} a_{n-1} + v_{n-1} && 0 < v_{n-1} < v_{n-2} \\
v_{n-2} &= v_{n-1} a_n && v_n = 0.
\end{aligned}
$$

Euclidean algorithm

To each pair of real numbers $\{x, y\}$ such that $x \geq y > 0$ we assign two finite or infinite sequences $a_1, a_2, a_3, \ldots$ and $v_{-1}, v_0, v_1, v_2, \ldots$ as follows:

1. Let $v_{-1} = x$, $v_0 = y$
2. If $v_{-1}, \ldots, v_i, a_1, \ldots, a_i$ are defined and $v_i \neq 0$ then, by the division Theorem, choose v_{i+1}, a_{i+1} such that

$$v_{i-1} = v_i a_{i+1} + v_{i+1} \qquad 0 \leq v_{i+1} < v_i.$$

3. If $v_i = 0$ then the algorithm terminates and returns $v_{-1}, v_0, \ldots, v_{i-1}$ and $a_1, \ldots, a_i$.

Correspondance of the Euclidean algorithm with the continued fraction expansion algorithm

Theorem

(a) *If we implement the euclidean algorithm for the pair* $\{x, 1\}$ *and*

$a_0, \ldots, a_n, \ldots$: *are the quotients that appear then*

$x = /a_1, \ldots, a_n, \ldots/$.

(b) *IF* $x = \dfrac{h}{k} \in \mathbb{Q}$, $h \geq k$,

then implementing again the euclidean algorithm for the pair $\{h, k\}$.

taking again the quotionents $a_0, \ldots, a_n, \ldots$ *we get:*

$x = /a_1, \ldots, a_n, \ldots/$

$$\frac{h}{k} = \frac{a_1 k + v_1}{k} = a_1 + \frac{1}{\frac{k}{v_1}} = a_1 + \frac{1}{\frac{v_1 a_2 + v_2}{v_1}} = a_1 + \frac{1}{a_2 + \frac{1}{\frac{v_1}{v_2}}}$$

Problems

1) Compute the Q-polynomial Q_5 (closed form).
2) Which is the $gcd(F_n, F_{n+1})$?.
3) Use the Euclidean algorithm to find gcd$(1287, 403)$ How many steps does the subtractive Euclidean algorithm do? Find the continued fraction expansion of $\frac{403}{1287}$.
4) a) Give a definition of the greatest common divisor of three integers a, b, c. Prove that gcd(a, b, c) = gcd(gcd(a, b), c) for any integers a, b, c.
5) Use the Euclidean algorithm to find the gcd$(2322, 654)$

$$2322 = 654 \cdot 3 + 360 \qquad \gcd(2322, 654) = \gcd(654, 360)$$
$$654 = 360 \cdot 1 + 294 \qquad \gcd(654, 360) = \gcd(360, 294)$$
$$360 = 294 \cdot 1 + 66 \qquad \gcd(360, 294) = \gcd(294, 66)$$
$$294 = 66 \cdot 4 + 30 \qquad \gcd(294, 66) = \gcd(66, 30)$$
$$66 = 30 \cdot 2 + 6 \qquad \gcd(66, 30) = \gcd(30, 6)$$
$$30 = 6 \cdot 5 \qquad \gcd(30, 6) = 6$$

$$\frac{2322}{654} = \frac{654 \cdot 3 + 360}{654} = 3 + \frac{360}{654} = 3 + \frac{1}{\frac{654}{360}} = 3 + \frac{1}{\frac{360 \cdot 1 + 294}{360}}$$

$$= 3 + \frac{1}{1 + \frac{294}{360}} = \ldots = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{2 + \frac{1}{5}}}}}$$

Proof of 4) First part: We will show that $\gcd(gcd(a, b), c)$ divides $\gcd(a, b, c)$.
$\gcd(gcd(a, b), c)$ divides $gcd(a, b), c$ so it also divides a, b, c
(Because by the definition of the greatest common divisor if d dividies $\gcd(a, b)$ then d dividies a, b) consequently
$\gcd(gcd(a, b), c)$ divides $\gcd(a, b, c)$
Second part: We will show that $\gcd(a, b, c)$ divides $\gcd(\gcd(a, b), c)$.
$\gcd(a, b, c)$ divides a, b, c so it also divides $\gcd(a, b), c$ so it also divides $\gcd(\gcd(a, b), c)$. (Every other common divisor of two numbers divides their gcd)