Euclidean Algorithm

- Anglin-Lambek, Part II, Chap. 14, pp. 227-230.
- Stillwell 3.3 (the Euclidean Algorithm), 3.4 (Pell's Equation)
- Wei Lu's Notes: pp.50-53.

Theorem (Division Algorithm, Euclid, Book VII, Prop.2.)

$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, b > 0$ *there exists unique* $q, r \in \mathbb{Z}$ *such that* $a = qb + r$, *where* $0 \leq r < b$. *Here,* q *is the quotient and* r *is the remainder.*

Recall, $gcd(a, c)$ (the greatest common divisor of a and c) is a number m satisfying:

(i) $m|a$ and $m|c$ (i.e. m is a common divisor of a and c).

(ii) $\forall d(d|a \& d|c \Rightarrow d|m)$ (i.e. any common divisor of a and c must divide m).

Euclid's Algorithm 2

Let's calculate $gcd(502, 1604)$.

$$\begin{array}{r|r} & 3 \\ \hline 502 & 1604 \\ & 1506 \\ \hline & 98 \end{array} \qquad \begin{array}{r|r} & 5 \\ \hline 98 & 502 \\ & 490 \\ \hline & 12 \end{array} \qquad \begin{array}{r|r} & 8 \\ \hline 12 & 98 \\ & 96 \\ \hline & \boxed{2} \end{array} \qquad \begin{array}{r|r} & 6 \\ \hline 2 & 12 \\ & 12 \\ \hline & 0 \end{array}$$

And the other is to use a series of equations:

$$\begin{aligned} 1604 &= 3 \cdot 502 + 98 \\ 502 &= 5 \cdot 98 + 12 \\ 98 &= 8 \cdot 12 + \boxed{2} \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

So, in both cases, $gcd(502, 1604) = 2$.

Euclidean Algorithm 3

Corollary

$\forall a, b \in \mathbb{Z}$, *there exist* $s, t \in \mathbb{Z}$ *such that* $gcd(a, b) = s \cdot a + t \cdot b$.

This is obtained by "back-substitution" as shown in class; in the above example:

$$\begin{aligned} 2 &= 98 - 8 \cdot 12 \\ &= 98 - 8 \cdot (502 - 5 \cdot 98) \\ &= (1604 - 3 \cdot 502) - 8 \cdot (502 - 5 \cdot (1604 - 3 \cdot 502)) \end{aligned}$$

Do the arithmetic above to find $s, t \in \mathbb{Z}$ such that $2 = gcd(502, 1604) = s \cdot 502 + t \cdot 1604$.

Euclidean Algorithm 4

In class we show:

Corollary

If $gcd(p, a) = 1$ and $p|ab$ then $p|b$. In particular, if p is a prime and $p \not| a$ and $p|ab$ then $p|b$.

Proof (Added): Suppose $gcd(p, a) = 1$ and $p|ab$. This means there exists integers s, t such that $sp + ta = 1$. Multiplying through by b, we get $spb + tab = b$. But we know p divides the LHS, since p divides each summand. Hence p must divide the RHS, that is: $p|b$.

The case when p is a prime is a special case of the above (why?)

According to Fowler's book *The Mathematics of Plato's Academy*, continued fractions were already known to the ancient Greeks. See History at bottom of Wikipedia link to Continued Fractions.

Rewriting $gcd(502, 1604)$ we get the following:

$$\frac{1604}{502} = 3 + \frac{98}{502} = 3 + \frac{1}{\frac{502}{98}} = 3 + \frac{1}{5 + \frac{12}{98}}$$

$$= 3 + \frac{1}{5 + \frac{1}{\frac{98}{12}}} = 3 + \frac{1}{5 + \frac{1}{8 + \frac{2}{12}}} = 3 + \frac{1}{5 + \frac{1}{8 + \frac{1}{6}}}$$

which we denote $(3, 5, 8, 6)$ and call it a *simple continued fraction*.

Another example is $(5, 1, 1, 1, 3)$, written:

$$5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}}$$

Another notation for a continued fraction (a_0, a_1, a_2) is $a_0 + \frac{1}{a_1^+}\frac{1}{a_2}$

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = \quad a_0 + \frac{1}{a_1^+}\frac{1}{a_2}$$

.

Continued Fractions 3

$$(a_0, a_1, a_2, a_3) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}} = a_0 + \frac{1}{a_1^+}\frac{1}{a_2^+}\frac{1}{a_3}$$

More generally, the continued fraction

$$(a_0, a_1, a_2, a_3, \cdots, a_n) = a_0 + \frac{1}{a_1^+}\frac{1}{a_2^+}\cdots\frac{1}{a_{n-1}^+}\frac{1}{a_n}$$

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

Continued Fractions 4

We can even look at infinite continued fractions $(a_0, a_1, a_2, \cdots)$. When the number of quotients $a_1, a_2, \cdots$ is finite, we call it a *terminating continued fraction*. Otherwise, it is an *infinite continued fraction*.

Theorem

Every terminating continued fraction can be converted to an ordinary rational. Conversely, every rational can be represented in precisely 2 different ways as a finite continued fraction.

The idea: to convert $\frac{m}{n}$ to a continued fraction, just divide n into m, getting remainder r_0. Hence

$$\frac{m}{n} = a_0 + \frac{r_0}{n} = a_0 + \frac{1}{\frac{n}{r_0}}$$

Now continue the procedure, by dividing n by r_0, getting $n = a_1 r_0 + r_1$, hence

$$\frac{m}{n} = a_0 + \frac{r_0}{n} = a_0 + \frac{1}{\frac{n}{r_0}} = a_0 + \frac{1}{a_1 + \frac{r_1}{r_0}}$$

Continue the process.

$$\begin{aligned} m &= a_0 n + r_0 \\ n &= a_1 r_0 + r_1 \\ r_0 &= a_2 r_1 + r_2 \\ r_1 &= a_3 r_2 + r_3 \\ &\vdots \end{aligned}$$

So $\frac{m}{n} = a_0 + \frac{1}{a_1^+}\frac{1}{a_2^+} \cdots \frac{1}{a_{k-1}^+}\frac{1}{a_k}$, i.e. we will get a finite continued fraction $(a_0, a_1, \cdots, a_k)$, for some k. Why? The sequence of remainders $r_i \to 0$.

But notice $(2, 2, 2) = (2, 2, 1, 1)$. Why?

Infinite Continued Fractions 1

We can even look at infinite continued fractions $(a_0, a_1, a_2, \cdots)$. When the number of quotients $a_1, a_2, \cdots$ is finite, we call it a *terminating continued fraction*. Otherwise, it is an *infinite continued fraction*.

Theorem

Every terminating continued fraction can be converted to an ordinary rational. Conversely, every rational can be represented in precisely 2 different ways as a finite continued fraction.

In the infinite case, we need some notion of convergence of sequences to make this precise. We shall argue "informally" in what follows (although it can be made rigorous).

Infinite Continued Fractions 2

Consider the continued fraction $X = (1, 1, 1, \ldots)$. Then

$$(1, 1, 1, \ldots) = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}$$

Notice, symbolically, this says:

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

Rearranging, $X^2 - X - 1 = 0$. Solve, to get a version of the Golden Ratio.

Infinite Continued Fractions 3

Consider the continued fraction $X = (2, 2, 2, \ldots)$. Then

$$X = (2, 2, 2, \ldots) \quad = \quad 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}$$

Notice, symbolically, this says:

$$X = 2 + \frac{1}{X}$$

Rearranging, $X^2 - 2X - 1 = 0$. Solve, to get $X = 1 + \sqrt{2}$ (Only allowed positive solutions: why?).

Infinite Continued Fractions: technicalities

The process of applying the Euclidean algorithm to line segments was called *anthyphairesis* and used in understanding the irrationals. Let $a = (a_0, a_1, a_2, \cdots)$. We get *approximations* to a which are given by finite initial prefixes of a:
$c_0 = a_0,\ c_1 = (a_0, a_1),\ c_2 = (a_0, a_1, a_2)$, etc. A finite initial prefix c_i is called a *convergent*. Consider $a_n > 0$, except possibly for a_0. To simplify, suppose $a_i \in \mathbb{Q}$, although later we only consider $a_i \in \mathbb{Z}$. Observe:

$$c_0 = a_0,\ c_1 = (a_0, a_1) = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}, \cdots .$$

To calculate c_n we introduce two sequences of rationals (which ultimately are integers):
$p_0 = a_0, p_1 = a_0 a_1 + 1, \cdots,\ p_n = a_n p_{n-1} + p_{n-2}$, if $n > 1$.
$q_0 = 1, q_1 = a_1, \cdots,\ q_n = a_n q_{n-1} + q_{n-2}$, if $n > 1$.

Infinite Continued Fractions: Anglin-Lambek 2

Theorem

Using the above definitions, if $a_0 \in \mathbb{N}$ *and* $0 < a_n \in \mathbb{N}$ *for* $n > 0$, *then the convergents satisfy:* $c_n = \frac{p_n}{q_n}$.

The proof is by induction (Exercise).

Theorem

Let p_n, q_n *be defined as above. Then* $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$.

Corollary

(i) $gcd(p_n, q_n) = 1$.

(ii) $\forall n > 0 \quad c_n - c_{n-1} = \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$

Infinite Continued Fractions: Anglin-Lambek 3

It can be shown: for *odd* n, $c_n - c_{n-2} < 0$ and for *even* n, $c_n - c_{n-2} > 0$. For example for the first one, for n odd,:

$$c_n - c_{n-2} = \frac{1}{q_n q_{n-1}} - \frac{1}{q_{n-2} q_{n-1}} < 0$$

Hence we have two sequences:

- $c_1 > c_3 > c_5 > \cdots$
- $c_0 < c_2 < c_4 < \cdots$

The difference of these two sequences tends to 0 by the above corollary, so they have a common limit, which we write as $a = (a_0, a_1, a_2, \cdots)$. Hence: **Infinite Continued Fractions exist!**

Continued Fractions: anthyphairesis

The following algorithm seems to be much closer to the underlying Greek notions of anthyphairesis (see the very scholarly paper on Virtual Campus by D. H. Fowler: *Anthyphairetic Ratio and Eudoxan Proportion*). See also Stillwell, pp. 41-48.
To find $gcd(a, b)$, calculate the following:

$$a_1 = max(a, b) - min(a, b)$$
$$b_1 = min(a, b)$$

$$a_2 = max(a_1, b_1) - min(a_1, b_1)$$
$$b_1 = min(a_1, b_1)$$

$$\vdots$$

$$a_{n+1} = max(a_n, b_n) - min(a_n, b_n)$$
$$b_{n+1} = min(a_n, b_n)$$

The algorithm terminates when $a_k = b_k$ for some k. This common value, say a_k, is then the greatest common divisor.

In class, we shall show how this may have been used by the Pythagoreans to show $\sqrt{2}$ is irrational, as well as how it seems to have other appearances in recurrence solutions to certain Diophantine equations.