Math 4400

Week 2 - Thursday

Continued fractions, the Euclidean algorithm, and uniqueness of prime factorization.

Notation For continued Fractions:

① For $a_0 \in \mathbb{Z}$ and $a_1, a_2, \dots, a_n$ positive integers,

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

② For $a_0 \in \mathbb{Z}$ and $a_1, a_2, \dots$ a sequence of positive integers,

$$[a_0; a_1, a_2, a_3, \dots] := \lim_{n \to \infty} [a_0; a_1, a_2, \dots, a_n]$$

↑ "n-th partial convergent"

Theorem: this converges to a real number!

$$r = "a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \frac{1}{\ddots}}}".$$

Examples:

① (Tuesday in class) $\frac{60}{22} = [2; 1, 2, 1, 2]$

② (Tuesday in class) $\sqrt{2} = [1; 2, 2, 2, 2, \ldots]$

③ $17 = [17;]$

④ $\pi = [3; 7, 15, 1, 292, 1, \ldots]$ (A001203 in OEIS).

Note: $[3; 7, 15, 1] = \frac{355}{113} = 3.1415929\ldots$

$(\pi = 3.1415926\ldots)$.

Theorem (Continued fraction algorithm):

Any $\alpha \in \mathbb{R}$ has a unique continued fraction expansion. It is finite if and only if $\alpha \in \mathbb{Q}$. To compute it, follow this algorithm:

Let $\alpha_0 = \alpha$.

① Let $a_i = \lfloor \alpha_i \rfloor$ and $B_i = \alpha_i - \lfloor \alpha_i \rfloor$ (fractional part).

② If $B_i = 0$, stop. Otherwise, set $\alpha_{i+1} = \frac{1}{B_i}$, and go to ① for $i+1$.

$\alpha = [a_0; a_1, a_2, \ldots, a_n]$ if you stop, i.e. if $\alpha \in \mathbb{Q}$; $[a_0; a_1, a_2, \ldots]$ otherwise.

Example:

① $\sqrt{2} = [1; 2, 2, 2, \ldots]$ is not rational. (this gives another proof)

② $\alpha = \alpha_0 = \frac{60}{22}$

i	$a_i = \lfloor \alpha_i \rfloor$	$B_i = \alpha_i - \lfloor \alpha_i \rfloor$	$\alpha_{i+1} = \frac{1}{B_i}$
0	2	$\frac{16}{22}$	$\frac{22}{16}$
1	1	$\frac{6}{16}$	$\frac{16}{6}$
2	2	$\frac{4}{6}$	$\frac{6}{4}$
3	1	$\frac{2}{4}$	$\frac{4}{2}$

4	2	0	STOP

$\frac{60}{22} = [2; 1, 2, 1, 2]$.

Recall: gcd(60, 22) by Euclidean algorithm:

$$60 = 2 \cdot 22 + 16$$
$$22 = 1 \cdot 16 + 6$$
$$16 = 2 \cdot 6 + 4$$
$$6 = 1 \cdot 4 + 2$$
$$4 = 2 \cdot 2 + 0.$$

In our computations in class Tuesday, we saw that for $\alpha = \frac{a}{b}$ $a, b \in \mathbb{Z}$, $b > 0$ (i.e. α rational),

Euclidean algorithm

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$
$$r_{m-1} = q_m r_m + 0.$$

Continued fraction

$$\alpha = \frac{a}{b} = [q_1; q_2, q_3, q_4, \ldots q_m]$$
$$= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \frac{1}{q_m}}}}.$$

Back to unique factorization...

Theorem (Fundamental Theorem of Arithmetic in book)

If a and b are two positive integers, then there exist integers x and y such that

$$ax + by = \gcd(a, b).$$

Example / Proof idea: $\gcd(60, 22) = 2$.

($a = 60$, $b = 22$)

Euclidean Algorithm.

$60 = 2 \cdot 22 + 16$

$22 = 1 \cdot 16 + 6$

$16 = 2 \cdot 6 + 4$

$6 = 1 \cdot 4 + 2$

$4 = 2 \cdot 2 + 0.$

$$\begin{aligned} 2 &= 1 \cdot 6 - 1 \cdot 4 \\ &= 1 \cdot 6 - 1 \cdot (16 - 2 \cdot 6) \\ &= 3 \cdot 6 + (-1) \cdot 16 \\ &= 3(1 \cdot 22 - 1 \cdot 16) + (-1 \cdot 16) \\ &= 3 \cdot 22 - 4 \cdot 16. \\ &= 3 \cdot 22 - 4(1 \cdot 60 - 2 \cdot 22) \\ &= -4 \cdot 60 + 11 \cdot 22. \end{aligned}$$

x y x y.

$60 \cdot (-4) + 22 \cdot (11) = 2$

Note: $\frac{60}{22} = [2; 1, 2, 1, 2]$.

$[2;] = 2$ — 1st partial convergent

$[2; 1] = 2 + \frac{1}{1} = 3$ — 2nd "

$[2; 1, 2] = 2 + \frac{1}{1 + \frac{1}{2}} = \frac{8}{3}$ — 3rd "

$[2; 1, 2, 1] = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1}}} = \frac{11}{4}$ — 4th "

$[2; 1, 2, 1, 2] = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}}} = \frac{60}{22}$ — 5th "

!! Numerator and negative of denominator of 2nd to last partial convergent give a solution! !!

Lemma: Let p be prime and let a and b be two integers such that $p \mid ab$. Then p divides a or p divides b.

More generally, if $p \mid a_1 \cdot a_2 \cdots a_n$, then $p \mid a_i$ for some i.

Proof: Since $p \mid ab$, $ab = qp$.

Suppose $p \nmid a$. Then I need to show $p \mid b$.

Implies $\gcd(p, a) = 1$ (only divisors of p are 1 and p).

FTA: $\exists\ x, y \in \mathbb{Z}$ s.t. $px + ay = 1$

Multiply by b $\rightsquigarrow$

$$pxb + aby = b$$

$$p(xb + qy) = b \quad \text{so} \quad p \mid b. \checkmark$$

Proof of uniqueness of prime factorizations

Let n be a positive integer, and suppose

$$p_1 p_2 \cdots p_r = n = q_1 q_2 \cdots q_s$$

Write $12 = 2^2 \cdot 3$ as $12 = 2 \cdot 2 \cdot 3$.

for primes $p_1 \leq p_2 \leq p_3 \cdots \leq p_r$, $q_1 \leq q_2 \leq \cdots \leq q_s$

WTS: $r = s$ and $p_i = q_i \quad \forall\ i$.

Assume $p_1 \leq q_1$. $\quad p_1 \mid n = q_1 q_2 \cdots q_s$.

Lemma $\Rightarrow$ $p_1 \mid q_i$ for some i.

so $p_1 \mid q_1$ (by inequalities).

$p_1 \neq 1$ so $p_1 = q_1$.

Then cancel $p_1 = q_1$ and get

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

Repeat! Done. $\ddot{\smile}$.