MATH 113: DISCRETE STRUCTURES
WEDNESDAY WEEK 11 HANDOUT

The *greatest common divisor* $d = \gcd(a, b)$ of integers a, b is the largest positive integer such that $d \mid a$ and $d \mid b$. We say that a and b are *relatively prime* when they share no divisors larger than 1, and this is equivalent to $\gcd(a, b) = 1$.

Problem 1. Draw a divisor diagram for 84 and 105. Where does the $\gcd$ appear in partially ordered set of divisors?

If we know the prime factorizations of a and b, this number is easy to determine. Let $\{p_1, p_2, \ldots, p_k\}$ be the set of distinct prime divisors of a and b. Then we may write

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$
$$b = p_1^{b_1} p_2^{b_2} \cdots p_k^{a_k}$$

for nonnegative integers a_i, b_i and

$$\gcd(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \cdots p_k^{\min\{a_k, b_k\}}.$$

It is frequently the case, though, that we do not have access to the prime factorizations of integers. In this case, the *Euclidean algorithm* allows us to determine the greatest common divisor. Let's execute the algorithm with $a = 81$, $b = 57$:

$$\begin{aligned} 81 &= 1 \cdot 57 + 24 \\ 57 &= 2 \cdot 24 + 9 \\ 24 &= 2 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

We conclude that the final nonzero remainder, 3, is the $\gcd$ of 81 and 57. Indeed, $81 = 3^4$ and $57 = 3 \cdot 19$, so this agrees with our first method for determining $\gcd$'s.

The Euclidean algorithm can be described formally as follows:

1. Assume $a > b$ are integers (if $a < b$, swap them).
2. Perform long division to express to express $a = qb + r$ where $0 \leq r \leq b - 1$.
3. Replace a with b and b with r.
4. If $r \neq 0$, return to step 2; else
5. if $r = 0$, conclude that the final nonzero remainder is $\gcd(a, b)$.

A generic run of the algorithm then looks like

$$\begin{aligned} a &= q_0 b + r_1 \\ b &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

where $1 \le r_k \le r_{k-1}$ and we conclude that $r_n = \gcd(a,b)$ (since $r_{n+1} = 0$).

Problem 2. Suppose an integer x divides integers y and z. Show that for any $k, \ell \in \mathbb{Z}$, $x \mid ky + \ell z$.

Problem 3. Why does the Euclidean algorithm work? Start at the end of the algorithm and check that $r_n \mid r_{n-1}$, then inductively check that $r_k \mid r_{k-1}$ for $-1 \le k \le n$ where we write $r_0 = b$ and $r_{-1} = a$ for notational convenience. Conclude that r_n divides a and b. Use a similar argument starting at the beginning of the algorithm to show that $\gcd(a,b)$ divides r_k for $-1 \le k \le n$. Why does this prove that the algorithm produces the $\gcd$.

Problem 4. The Euclidean algorithm gives us a way to dissect a rectangle with integer sides into squares. Run the Euclidean algorithm to find $\gcd(23, 13)$. Interpret the first step $(23 = 1 \cdot 13 + 10)$ as telling you that $q_0 = 1$-many 10×10 squares fit inside a 23×13 rectangle. Figure out what instructions the rest of the algorithm is giving you and draw a corresponding picture. At the end, your 23×13 rectangle should be partitioned into squares! What is special about this procedure if you start with consecutive Fibonacci numbers $a = F_{n+1}$, $b = F_n$?

Problem 5. Run the Euclidean algorithm when $a = 45$, $b = 16$. How is it related to the expression

$$\frac{45}{16} = 2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{3}}}?$$

Come up with a general procedure by which the Euclidean algorithm produces *continued fraction* expressions for rational numbers of the form

$$\frac{a}{b} = x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{x_4 + \cdots}}}$$

where the x_i are integers.