PROBLEM 1. Suppose that $a = p_1^{a_1} \cdots p_k^{a_k}$ and $b = p_1^{b_1} \cdots p_k^{b_k}$ for $p_1, \ldots, p_k$ distinct prime numbers and $a_i, b_i \in \mathbb{N}$ for $1 \leq i \leq k$. Prove that

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

and

$$\operatorname{lcm}(a,b) = p_1^{\max\{a_1,b_1\}} \cdots p_k^{\max\{a_k,b_k\}}.$$

SOLUTION: Let

$$d = p_1^{\min\{a_1,b_1\}} \cdots p_k^{\min\{a_k,b_k\}}.$$

Recall that e divides a if and only if it is of the form $e = p_1^{e_1} \cdots p_k^{e_k}$ with $0 \leq e_i \leq a_i$ for $1 \leq i \leq k$. Since $\min\{a_i, b_i\} \leq a_i$, it follows that d divides a, and similarly, it divides b. In addition, if e divides both a and b, we have that $e = p_1^{e_1} \cdots p_k^{e_k}$ with $e_i \leq a_i$ and $e_i \leq b_i$. Thus $e_i \leq \min\{a_i, b_i\}$, and hence e divides d, thus showing d is the gcd of a and b.

The proof for the lcm is similar and left for you to complete.

PROBLEM 2. Use the Euclidean algorithm to compute $\gcd(270, 192)$. Back-solve for $\gcd(270, 192)$ as an integer linear combination of 270 and 192, *i.e.*, find $s, t \in \mathbb{Z}$ such that

$$\gcd(270, 192) = 270s + 192t.$$

SOLUTION: We compute

$$\begin{aligned} 270 &= 1 \cdot 192 + 78 \\ 192 &= 2 \cdot 78 + 36 \\ 78 &= 2 \cdot 36 + 6 \\ 36 &= 6 \cdot 6 + 0. \end{aligned}$$

As such,

$$6 = \gcd(270, 192).$$

Back-solving for 6 gives

$$\begin{aligned} 6 &= 78 - 2 \cdot 36 \\ &= 78 - 2 \cdot (192 - 2 \cdot 78) \\ &= 5 \cdot 78 - 2 \cdot 192 \\ &= 5 \cdot (270 - 192) - 2 \cdot 192 \\ &= 5 \cdot 270 - 7 \cdot 192. \end{aligned}$$

PROBLEM 3. 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.

SOLUTION: The Euclidean algorithm runs as follows:

$$\begin{aligned} 45 &= 2 \cdot 16 + 13 \\ 16 &= 1 \cdot 13 + 3 \\ 13 &= 4 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Note the numbers in blue and their relation to the continued fraction for $\frac{45}{16}$. Working backwards, we see

$$\frac{13}{3} = 4 + \frac{1}{3},$$

then

$$\frac{16}{13} = 1 + \frac{3}{13} = 1 + \frac{1}{13/3} = 1 + \frac{1}{4 + \frac{1}{3}},$$

and, finally,

$$\begin{aligned} \frac{45}{16} &= 2 + \frac{13}{16} \\ &= 2 + \frac{1}{\frac{16}{13}} \\ &= 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{3}}}. \end{aligned}$$

In general, we have $x_k = q_{k-1}$.

PROBLEM 4. The "rectangular" visualization of the Euclidean algorithm is a technique from ancient Greece known as *anthyphairesis*. It gives us a visual test for when the quotient of two real numbers x/y is a rational number.

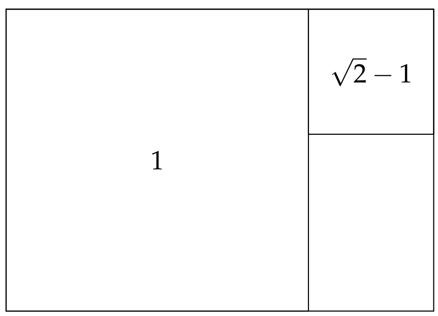
(a) Thinking in terms of similar rectangles, argue that for x and y positive real numbers, $x/y = a/b$ for some $a, b \in \mathbb{N}$ if and only if the *anthyphairetic* dissection of an $x \times y$ rectangle terminates in a finite number of steps.

(b) Use (a) to show that $\sqrt{2}/1$ is not a rational number.

SOLUTION:

(a) If x/y is rational, then we can scale the rectangle to be $a \times b$ for $a, b \in \mathbb{N}$ and then apply the Euclidean algorithm until we tile the rectangle with finitely many squares. Conversely, assume the $x \times y$ rectangle is *anthyphairetically* tiled by finitely many squares where the smallest is $z \times z$. Then we may scale by $1/z$ to get a similar rectangle with integers sides and side ratio x/y.

(b) Consider the start of the *anthyphairetic* dissection of $R(\sqrt{2}, 1)$:



The remaining rectangle has dimensions $(\sqrt{2}-1) \times (2-\sqrt{2})$, and thus its side ratio is

$$\frac{2-\sqrt{2}}{\sqrt{2}-1}.$$

Since $1 = (\sqrt{2}-1)(\sqrt{2}+1)$, we know that $1/(\sqrt{2}-1) = \sqrt{2}+1$, so the above expression simplifies to

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

We thus see that *anthyphairetic* subdivision will continue forever, replicating similar rectangles and never terminating. We conclude that $\sqrt{2}$ is not rational.