## Math 406 Section 3.4: The Eucliden Algorithm

1. **Introduction:** Given $a$ and $b$ we have two computationally interesting questions:
   - How can we find $\gcd(a, b)$?
   - How can we find $\alpha, \beta$ so that $\gcd(a, b) = \alpha a + \beta b$?

2. **Theorem (The Euclidean Algorithm):** Given integers $a$ and $b$ with $a > b$ we know that subtracting multiples of one from the other does not change the gcd. It follows that we can write $a = qb + r$ with $0 \leq r < b$ and then $\gcd(a, b) = \gcd(qb + r, b) = \gcd(r, b)$. What this means is that when calculating a gcd we can replace the larger number by the remainer when we divide it by the smaller number. Let's see what happens if we do this:

   **Example:** Let's calculate $\gcd(252, 198)$:

   $$\begin{aligned} 252 &= (1)198 + 54 & \gcd(252,198) &= \gcd(198,54) \\ 198 &= (3)54 + 36 & \gcd(198,54) &= \gcd(54,36) \\ 54 &= (1)36 + 18 & \gcd(54,36) &= \gcd(36,18) \\ 36 &= (2)18 + 0 & \gcd(36,18) &= \gcd(18,0) \end{aligned}$$

   At this point we know that $\gcd(18, 0) = 18$ which was in fact the last nonzero remainder.

   **Example:** Let's calculate $\gcd(97, 44)$:

   $$\begin{aligned} 97 &= (2)44 + 9 \\ 44 &= (4)9 + 8 \\ 9 &= (1)8 + 1 \\ 8 &= (8)1 + 0 \end{aligned}$$

   So we find $\gcd(97, 44) = 1$.

3. **Discovering the Linear Combination:** The Euclidean Algorithm also gives us a way of discoving the linear combination. We solve for the gcd in the last line with nonzero remainder. We then use the lines above that line to replace each remainder with the expression it equals. If we tidy thing up as we go, and keep track of remainders, this isn't so bad.

   **Example:** We have:

   $$\begin{aligned} 1 &= (1)9 - (1)8 \\ 1 &= (1)9 - (1)(44 - (4)9) \\ 1 &= (5)9 - (1)44 \\ 1 &= (5)(97 - (2)44) - (1)44 \\ 1 &= (5)97 - (11)44 \end{aligned}$$