Lesson Six

Math 6080 (for the Masters Teaching Program), Summer 2020

A Mathematical Interlude. The math behind Euclid's algorithm is this:

Lemma. If n and m are integers, let $r = n\%m$ (in Pythonese). Then:
All common divisors of n and m are common divisors of m and r and vice versa.

Proof. Let $q = n//m$ (in Pythonese), so that:

$$n = mq + r$$

If d is a common divisor of n and m then d also divides $r = n - mq$, therefore d is a common divisor of m and r. Conversely, if d is a common divisor of m and r, then d is also a divisor of $n = mq + r$, so d is a common divisor of n and m. $\square$

In particular, the **greatest** common divisors are the same:

$$\gcd(n, m) = \gcd(m, r)$$

which is the basis for the Euclidean algorithm

Remark. This Lemma is only applicable when $m \neq 0$. When $r = 0$, the Euclidean algorithm terminates, because m divides n, and thus m is the gcd of n and m.

Enhanced Lemma. In the Lemma above, suppose that x and y are integers, and:

$$ax + by = n \text{ and } cx + dy = m$$

Then

$$(a - cq)x + (b - dq)y = n - mq = r$$

Remark. If you prefer, we can think of this in terms of matrices. If:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} n \\ m \end{bmatrix}$$

then:

$$\begin{bmatrix} c & d \\ (a - cq) & (b - dq) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} m \\ r \end{bmatrix}$$

This gives rise to a strategy for solving the equation:

$$an + bm = \gcd(n, m)$$

Enhanced Euclid's Algorithm.

Step 1. Set $x, y = n, m$ (storing away the values of n and m).

Step 2. Initialize the variables $a, b, c, d = 1, 0, 0, 1$ so that:

$$ax + by = x = n \text{ and } cx + dy = y = m$$

Step 3 (to repeat until $m = 0$). Replace:

$$a, b, c, d = c, d, a - c * (n//m), b - d * (n//m)$$

$$n, m = m, n\%m \text{ and}$$

(it is important to do them in this order!) and repeat until $m = 0$, at which point:

(1) n is the gcd, and (2) $ax + by = n = \gcd(x, y)$ is the desired expression.

Now write the Python code to do this....