Problem Set 7

The Euclidean Algorithm. If $a = qb + r$, where q and r are the quotient and remainder when b is divided into a, then either

- $\gcd(a, b) = b$ if $r = 0$ or
- $\gcd(a, b) = \gcd(b, r)$ if $r \neq 0$.

In class on November 16th, I "proved" this in the case of $a = 2175$ and $b = 555$ and argued that the same reasoning works for any two integers. I also used the algorithm to find the gcd of 2175 and 555, which turned out to be 15.

1. Use the Euclidean Algorithm to find the gcd of 4025 and 1242. *(You'll need to do this by hand to get credit here, although you're welcome to check your work using Wolfram|Alpha.)*

2. Use your work from Question 1 to find numbers s and t such that $4025s + 1242t = \gcd(4025, 1242)$. *(You'll need to do this by hand to get credit here, although you're welcome to check your work using Wolfram|Alpha.)*

3. Suppose you're given a piece of ciphertext known to have been enciphered using pre-World War Two cryptography techniques. (For instance, this one.) We've discussed a variety of ciphers and ways to break them during this course. Create a cryptanalysis flowchart that summarizes the steps you might take to cryptanalyze a ciphertext of unknown origin. *(What do I mean by a flowchart? Here are some examples: tech support, legal immigration, Christopher Nolan movies, social search sites. Your flowchart can be simple and hand-drawn, like the tech support flowcart.)*