Homework 1, Introduction to Number Theory, Due Thursday, February 5th in class
On this homework, do not use congruences.

1. Show all steps of the Euclidean Algorithm in finding the following greatest common divisors
   (a) \((12378, 3054)\)
   (b) \((225, 139)\)
   (c) \((589, 465)\)

2. Show all steps in using the Euclidean Algorithm (or reversing the Euclidean Algorithm) to derive
   constants \(x\) and \(y\) such that \(ax + by = (a, b)\) where
   (a) \(a = 12378, b = 3054\)
   (b) \(a = 589, b = 465\)

3. Suppose that \(a, b, c\) are positive integers. Show that \(a\mid bc\) if and only if \(a\mid c(a, b)\)


5. Apostol, problem 16, page 22. HINT: First show that for \(x > 1\) that
   \[a^x - 1 = (a - 1)(1 + a + a^2 + \ldots + a^{x-1})\]
   by expanding the right hand side of the equation.
   NOTE: Primes of the form \(2^n - 1\) are known as Mersenne Primes. The largest known primes are
   Mersenne primes due to a specialized primality testing algorithm for numbers in this form. The
   currently largest known prime is a Mersenne Prime: \(2^{57,885,161} - 1\). This was found as part of
   the Great Internet Mersenne Prime Search (GIMPS).

6. Apostol, problem 17, page 22. HINT: First show that for \(x \geq 3\) where \(x\) is odd that
   \[a^x + 1 = (a + 1)(1 - a + a^2 - \ldots + a^{x-1})\]
   by expanding the right hand side of the equation.
   NOTE: Primes of the form \(2^{(2^k)}\) are called Fermat Primes.

7. Suppose \(b \geq 2\). Show that for every positive integer \(n\) there exists unique integers \(a_0, a_1, a_2\) such that
   (a) \(n = a_0 + a_1 \cdot b + a_2 \cdot b^2\)
   (b) \(0 \leq a_0 < b\)
   (c) \(0 \leq a_1 < b\)
   (In some sense, this is an extension algorithm the division algorithm.)