You should read Chapter 1-6 of A Friendly Introduction to Number Theory to make sure you are familiar with the basic definitions before you start working on this assignment.

1: GCD, (10 pts)

In the lecture I did not give a complete proof of the following fact:

$$Let n = qm + r, \text{ where } 0 \leq r \leq m-1, \text{ then} \gcd(n, m) = \gcd(m, r)$$

2: Extended Euclidean GCD Algorithm (10 pts)

Please do some research online to find an implemention the Euclidean Algorithm. For each pair (n, m) of the following numbers, apply your algorithm to calculate $\gcd(n, m)$.

You will also need to submit your source code on Canvas.

(a) (35, 15).

(b) (154878552455, 98871521).

(c) (9784515182034984165, 3164547984351248).

(d) (54321, 9876).

(e) (12345, 67890).

3: Linear Combination of Multiple(10 pts)

Show that if $d|n$ and $d|m$, then for any $s, t \in \mathbb{Z}$,

$$d|(sn + tm).$$

4: Divisibility and GCD, (Friendly) Exercise 7.1 and 7.2. (20 pts, 10 each,)

Hint: use extended GCD algorithm to get a fancy way of writing one!

(a) Suppose that $\gcd(a, b) = 1$, and suppose further that a divides the product bc. Show that a must divide c.

(b) Suppose that $\gcd(a, b) = 1$, and suppose further that a divides c and b divides c. Show that the product ab must divide c.