Math 11200/20 homework 5
Due date: Friday, October 28, 2016

Note: You shouldn't need to use a calculator for these problems.

Please present your solutions clearly and in an organized way. Think of it this way: if you show it to another student in this class, he/she should be able to understand it without needing to ask you questions.

Problem 5.1. In Problem 4.6 of last week's assignment, you had to calculate $(1001, 105)$ and $(55, 34)$ by repeatedly applying the division algorithm. (This method of finding GCDs is called the "Euclidean algorithm." If it's not clear how this works, see the Example on page 94 of the textbook.)

When calculating $(55, 34)$ in this way, the procedure might have seemed long, because every time you divided, the quotient was 1. Can you find other positive integers a, b with this property? (That is, when you apply the Euclidean algorithm to find (a, b), the quotient is always 1?)

Hint 1: Study the calculations for $(55, 34)$ carefully.

Hint 2: Try working backwards.

Hint 3: I'll write out the calculations for $(55, 34)$ here:

$$\begin{aligned} 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

As observed, the quotient is always 1 (except for the last one). If I asked you to do the calculations for $(34, 21)$ you don't have to start over. You can just start from the second row above. What is special about all the numbers that appear? Can you extend these calculations "upwards"? (i.e., add more rows above the first one?)

Problem 5.2. Exercise 4.6 from the textbook.

Problem 5.3. Exercise 4.9 from the textbook. For part (c), $b = 997$. You can use a calculator for this problem, but try to do (a) and (b) without one.

Problem 5.4. Exercise 4.10 from the textbook. (This is a real world application of the extended Euclidean algorithm, I guess?)

Problem 5.5. Exercise 4.11 from the textbook.

Problem 5.6. Use your answers to Problem 5.3 to determine the following. (First, divide out by the GCD, like we did in class on 10/26.) You can use a calculator. (a^{-1} denotes the multiplicative inverse of a.)

(a) 5^{-1} in $\mathbb{Z}_{13}$ and 3^{-1} in $\mathbb{Z}_5$
(b) 37^{-1} in $\mathbb{Z}_{59}$ and 22^{-1} in $\mathbb{Z}_{37}$
(c) 881^{-1} in $\mathbb{Z}_{997}$ and 116^{-1} in $\mathbb{Z}_{881}$
(d) 2387^{-1} in $\mathbb{Z}_{3158}$ and 771^{-1} in $\mathbb{Z}_{2387}$.
(e) 59^{-1} in $\mathbb{Z}_{301}$ and 6^{-1} in $\mathbb{Z}_{59}$.