WORKSHEET #4 – MATH 2200
SPRING 2018

DUE FRIDAY, MARCH 16TH

You may work in groups of up to 4 people. Only one assignment needs to be turned in per group, but make sure everyone's name is on it.

The first part of this worksheet will describe the *extended* Euclidean algorithm. In other words, given integers a, b, at least one nonzero, this finds integers s and t so that

$$sa + tb = \gcd(a, b).$$

1. Suppose that $a = b$. What s and t can you pick so that

$$sa + tb = \gcd(a, b)?$$

2. Suppose that $b \mid a$. What s and t can you pick so that

$$sa + tb = \gcd(a, b)?$$

Recall that when doing the Euclidean Algorithm, we repeatedly use the fact that if $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

3. With notation as above, suppose we already found integers s', t' so that $s'b + t'r = \gcd(b, r)$. Derive formulas for s and t so that $sa + tb = \gcd(a, b)$.

$s =$

$t =$

4. Compute gcd of 675 and 210 by running the Euclidean Algorithm. In this problem, fill in the columns labeled a, b and then fill in the gcd column. I've even done the first line for you. In particular I computed $675 = 3 \cdot 210 + 45$. Note you are going to fill out the first two columns before you figure out the gcd. Ignore the s, t column for now.

a	b	$\gcd(a, b)$	s	t	check
675	210				
210	45				

5. Starting at the bottom line in the above table, find s and t so that $sa + tb$ is the gcd. Fill out the s and t in the table. Make sure to use your formulas from **3.** to find the s and t based on the values of the previous line. Check your work at each step (to make sure the s and t give you the gcd) and put a checkmark in the corresponding column when you have done so.

6. Use any method you like (guess and check is ok) to find s and t so that $sa + tb = \gcd(a, b)$ for the given values of a and b.

(i) 5, 7

(ii) 9, 16

(iii) 15, 49

(iv) 10, 37

7. Write down a careful proof that if $sa + tb = 1$, the $sa \equiv_b 1$ (remember, $\equiv_b$ means equivalent mod b). The number s is called an *inverse of a mod b.*

8. Compute the inverses of the following integers a mod the integer b. Check your answer carefully in each case. (*Hint:* Don't forget the work you did in **5.**)

(i) a = 5, b = 7

(ii) a = 9, b = 16

(iii) a = 15, b = 49

(iv) a = 10, b = 37

9. Solve the following congruences for x using what you did in **8.**

(i) $5x \equiv_7 4$

(ii) $5x \equiv_{16} 3 - 4x$

(iii) $15x \equiv_{49} -1$

(iv) $-9x \equiv_{37} 1 + x$