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

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

Solution: Since the gcd $= a = b$, you can pick $s = 1$ and $t = 0$, or many other things ($s = -3, t = 4...$)

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

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

Solution: Since the gcd $= b$, you can choose $s = 0, t = 1$.

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

$s =$

$t =$

Solution: We have two equations $a = bq + r$ and $s'b + t'r = \gcd(b, r)$. Solving the first equation for r we get $r = a - bq$. Plugging this into the second equation we get

$$\gcd(b, r) = s'b + t'(a - bq) = t'a + (s' - t'q)b.$$

But $\gcd(a, b) = \gcd(b, r)$ and so we can take $s = t'$ and $t = s' - t'q$.

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
$q = 3$	675	210	15	5	$-16 = (-1) - (5 \cdot 3)$	✓
$q = 4$	210	45	15	-1	$5 = 1 - (-1 \cdot 4)$	✓
$q = 1$	45	30	15	1	$-1 = 0 - (1 \cdot 1)$	✓
$q = 2$	30	15	15	0	1	✓

Solution: Filled in above

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.

Solution: One solution is filled in above. Notice that if you start in the s and t line with a different pair of values, the s and t at the top will be different.

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

Solution: For (i), one set of valid values is $s = 3, t = -2$ since $(3 \cdot 5) + ((-2) \cdot 7) = 1$.
For (ii), one set of valid values is $s = -7, t = 4$ since $((-7) \cdot 9) + (4 \cdot 16) = 1$.
For (iii) one set of valid values is $s = -13, t = 4$ since $((-13) \cdot 15) + (4 \cdot 49) = 1$.
For (iv), one set of values values is $s = 26, t = -7$ since $(26 \cdot 10) + (7 \cdot 37) = 1$.

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

Solution: Suppose $sa + tb = 1$. Note that $(sa + tb) \equiv_b sa + 0 = sa$ using a result from the text in Section 4.1 (it is also correct to argue that tb has zero remainder modulo b and so $sa + tb$ has the same remainder as sa). Hence

$$1 \equiv_b sa + tb \equiv_b sa.$$

This completes the proof.

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

Solution: For (i), $s = 3 \equiv_7 -4$.
For (ii), $s = -7 \equiv_{16} 9$.
For (iii) $s = -13 \equiv_{49} 36$.
For (iv) $s = 26 \equiv_{37} -11$.

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

Solution: For the (i), multiplying both sides by 3 we get $x \equiv_7 12 \equiv_7 5$.

For the (ii), moving the xs to the same side, we get that $9x \equiv_{16} 3$. Multiplying both sides by -7 we get $x \equiv_{16} -21 \equiv_{16} -5 \equiv_{16} 11$.

For (iii), multiplying both sides by (-13) we get $x \equiv_{49} 13$.

For (iv), we first move the xs to the same side to obtain that $-1 \equiv_{37} 10x$. Multiplying both sides by (-11) we obtain that $11 \equiv_{37} = x$.