Math 2110 # Homework #11 **Due: Fri., Nov. 20^{th}, 2020**

Handwritten solutions are fine. ☺

#1 Extended Euclidean Exhaustion: For each of the following pairs of numbers, $a, b \in \mathbb{Z}$, compute their greatest common divisor, $d = \gcd(a, b)$, using the Euclidean algorithm. Then use your work to write the gcd as an integral linear combination of your pair of numbers (i.e., find $x, y \in \mathbb{Z}$ such that $ax + by = d$).

Note: Obviously my Sage Interact found at...

`https://billcookmath.com/sage/algebra`

will compute the end result. But I want you to do this by hand and *show your work*! [Then go use the interact to check your answers.]

(a) $a = 555$ and $b = 95$.

(b) $a = 9999$ and $b = 122$.

#2 What does this get me? Suppose that $a, b, x, y \in \mathbb{Z}$ and we have $ax + by = 10$. What can we say about $\gcd(a, b)$? What must be true if $ax + by = 1$?

#3 Modulo Inverses Fix some positive integer n.

It turns out that the set of equivalence classes mod n, $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$, has the structure of something called a "commutative ring with 1". This means that we can add and multiply elements of $\mathbb{Z}_n$ much like we add and multiply integers. However, some things are weird. In particular, multiplicative inverses and cancellation properties don't quite work as one might initially expect.

(a) We say $[a]$ is a *unit* of $\mathbb{Z}_n$ if there is some $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$.
Explain why $[a]$ is a unit if and only if $\gcd(a, n) = 1$.

(b) Let $\mathbb{Z}_n^\times = \{[k] \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$ (this is the set of units).
Find the elements of $\mathbb{Z}_7^\times$ along with their inverses. Do the same for $\mathbb{Z}_8^\times$.
For example, $\mathbb{Z}_6 = \{[0], [1], \ldots, [5]\}$ but $\mathbb{Z}_6^\times = \{[1], [5]\}$. Notice that $[1][1] = [1 \cdot 1] = [1]$ and $[5][5] = [5 \cdot 5] = [25] = [1]$ (working mod 6). Thus $[1]^{-1} = [1]$ and $[5]^{-1} = [5]$.

(c) Show that cancellation does not work in $\mathbb{Z}_6$. Specifically, find some $[a], [b], [c] \in \mathbb{Z}_6$ such that $[a] \neq [0]$ and $[a][b] = [a][c]$ but $[b] \neq [c]$.
Note: This doesn't happen in $\mathbb{Z}$. If $a, b, c \in \mathbb{Z}$ and $a \neq 0$. Then $ab = ac$ implies $b = c$. It is also interesting to note that this failure of cancellation can only happen because 6 is composite. Cancellation laws do hold in $\mathbb{Z}_p$ for any prime p.

#4 Calculatin' Modulo Compute $5^{-2} \cdot (4 - 10) \cdot 13^{9999} + 11 \pmod{14}$. Give a "good manners" answer (i.e., simplify so your answer is between 0 and 13).

Please keep in mind that 5^{-2} means $(5^{-1})^2$ where 5^{-1} is the multiplicative inverse of 5 modulo 14. Let me emphasize that 5^{-1} is not the same thing as the fraction $1/5$.