Math 2110-410 **Homework #6** **Due: Fri., Apr. 17th, 2020**

#1 Casting Out Nines: In our "childhood" we are taught that a number is divisible by 9 if its digits add up to 9. Well, not quite – if its digits add up to a number bigger than 9, we need to repeat the process. For example, 63 is divisible by 9 because $6+3=9$. Also, 99 is divisible by 9 because $9+9=18$ and $1+8=9$. Here's a big example: $19,008,675$ is divisible by 9 because $1+9+0+0+8+6+7+5=36$ and $3+6=9$. On the other hand, $123,454,321$ is not divisible by 9 because $1+2+3+4+5+4+3+2+1=25$ and $2+5=7\neq 9$.

Why does this work? Well, it rests on **the fact** that if $n = d_\ell \times 10^\ell + \cdots d_2 \times 10^2 + d_1 \times 10 + d_0$ where $d_j \in \{0,1,\ldots 9\}$ for all $j=0,\ldots,\ell$ then $9 \,\big|\, n$ if and only if $9 \,\big|\, (d_\ell + \cdots + d_1 + d_0)$. [This says that a number is divisible by 9 if and only if its digits sum to a number divisible by 9. By repeatedly summing digits we will eventually end up with a number between 0 and 9. So n is divisible by 9 if and only if this process terminates with a "9".]

Prove the fact. [Make sure your argument shows "if and only if".]

Hint: Translate this statment into congruences mod 9 and consider the value of 10 mod 9, 10^2 mod 9, etc.

#2 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 $b=122$.

#3 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 $ax+by=1$?

#4 Rationalizing Away Our Problems: At the end of the third video about Divisiblity and the Extended Euclidean Algorithm, I gave an example showing how to use the extended Euclidean algorithm applied to polynomials to rationalize a fraction involving a cube root. Use my Sage Interact for polynomial gcds to compute a gcd of appropriate polynomials and then use the result of that computation to rationalize:

$$\frac{1}{2-3^{1/4}-3\cdot 3^{1/2}+3^{3/4}} = ??? + ??? \cdot 3^{1/4} + ??? \cdot 3^{1/2} + ??? \cdot 3^{3/4}$$

where the ??? coefficients are rational numbers.

#5 A Modern Algebra Problem The set $\mathbb{Z}_n=\{0,1,\ldots,n-1\}$ forms an Abelian group under addition (mod n). This means that adding (mod n) elements in $\mathbb{Z}_n$ will give back an element in $\mathbb{Z}_n$, this addition is associative, there is an identity element 0 where $0+k=0=k+0$, each element has an additive inverse (for example: $1+(n-1)=0$ mod n so the additive inverse of 1 is $-1=n-1$), and addition is commutative.

Notice that $\mathbb{Z}_n$ is **cyclic**. By this we mean that there is an element that generates all of the rest of the elements. In particular: 1, $1+1=2$, ..., $1+\cdots+1=n-1$, $1+\cdots+1=n=0$. Thus 1 is a generator for $\mathbb{Z}_n$.

Now $\mathbb{Z}_n$ is not an Abelian group under multiplication (mod n). This is because we fail to have multiplicative inverses for everyone. In particular, 0^{-1} never exists. In fact, one can show that the elements which have multiplicative inverses mod n are exactly the elements relatively prime to n. We call this collection $\mathbb{Z}_n^\times$ or sometimes $U(n)$. In particular, $\mathbb{Z}_n^\times=\{k\in\mathbb{Z}_n \mid \text{any representative of } k \text{ and } n \text{ are relatively prime}\}$.

It is the case that the collection $\mathbb{Z}_n^\times$ forms an Abelian group under multiplication mod n. However, sometimes it is cyclic and sometimes it is not.

For example: $\mathbb{Z}_6=\{0,1,2,3,4,5\}$ is a group under addition mod 6 whereas $\mathbb{Z}_6^\times=\{k\in\mathbb{Z}_6 \mid \gcd(k,6)=1\}=\{1,5\}$ is a group under multiplication mod 6. Notice that $1\cdot 1=1$ so $1^{-1}=1$ and $5\cdot 5=1$ so $5^{-1}=5$. Also, $\mathbb{Z}_6^\times$ is cyclic since 5 generates this group: $5^1=5$ and $5^2=25=1$.

FINALLY, your problems:

(a) Find the elements of $\mathbb{Z}_7^\times$ and $\mathbb{Z}_8^\times$.

(b) Compute the multiplicative inverse of each of the elements of $\mathbb{Z}_7^\times$ and again for $\mathbb{Z}_8^\times$.

(c) Show that $\mathbb{Z}_7^\times$ is cyclic. In fact, it is generated by 3. Does it have any other generators? Then show that $\mathbb{Z}_8^\times$ is not cyclic (none of its elements generate the whole group).