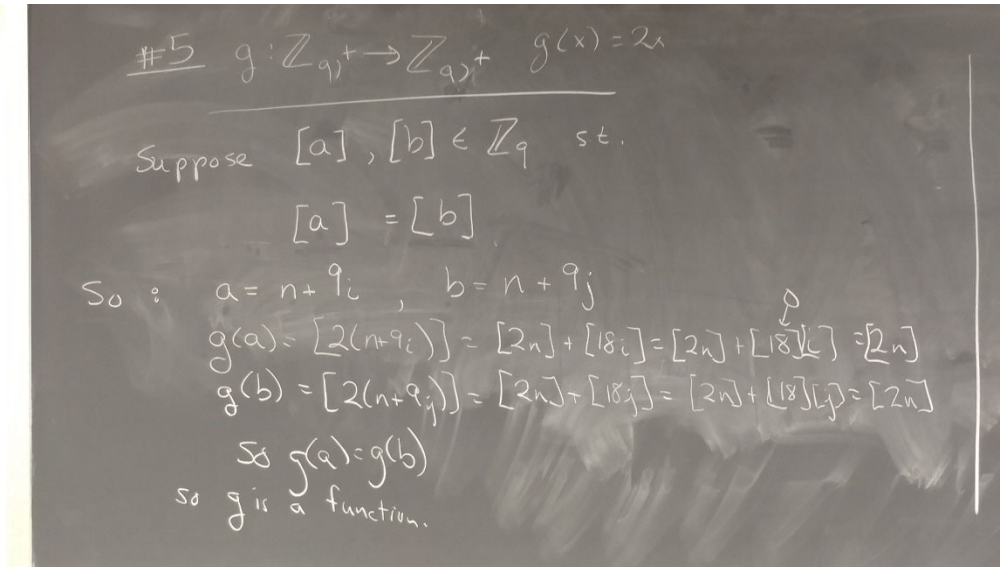
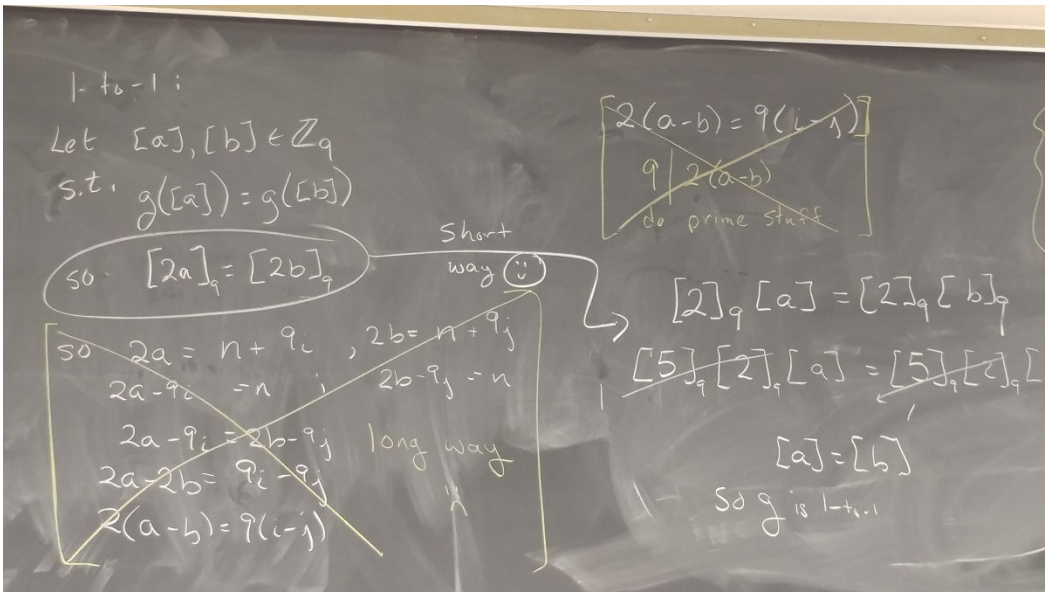
We started today by asking about the first homework problem. Here was our in-class solution.

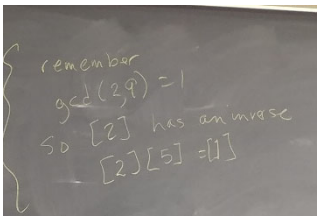
First, we proved g is a function:



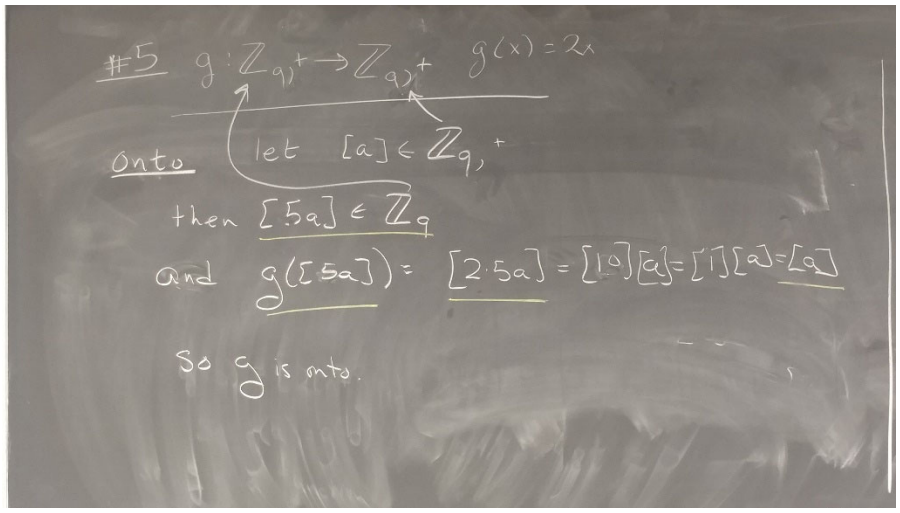
Next we proved it was one-to-one. You can see that at first I started doing things that were more complicated than necessary. Then Blake and Emily made some great suggestions that got us to the answer in a way that was much faster: Yay—this is clearly the "right" thing to do.



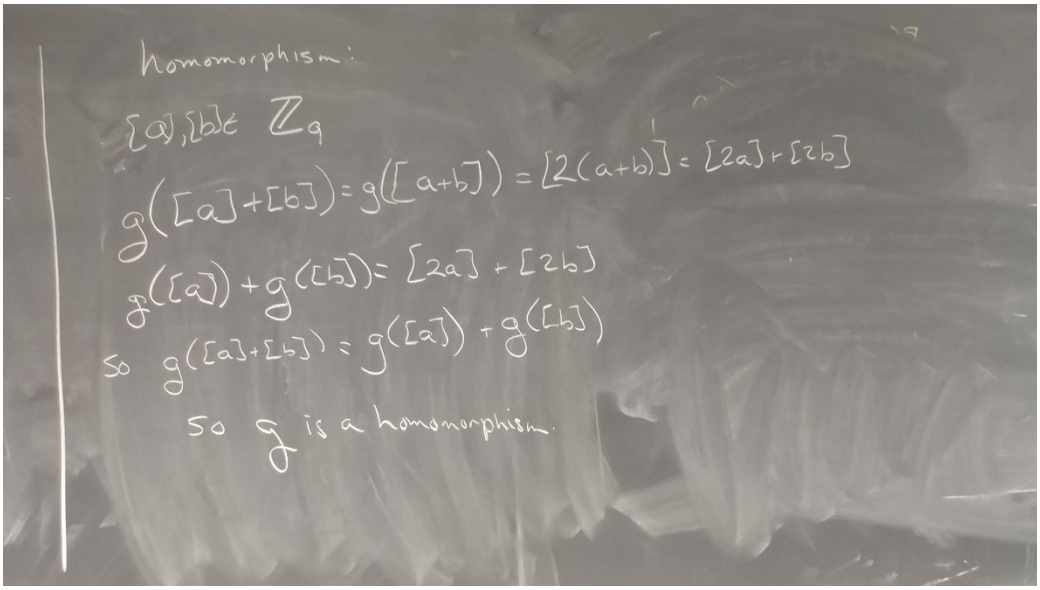
Notice that the way we know we can find a nice inverse for [5] is because gcd(5,9)=1



That same multiplicative inverse is what lets us show easily that the function is onto:



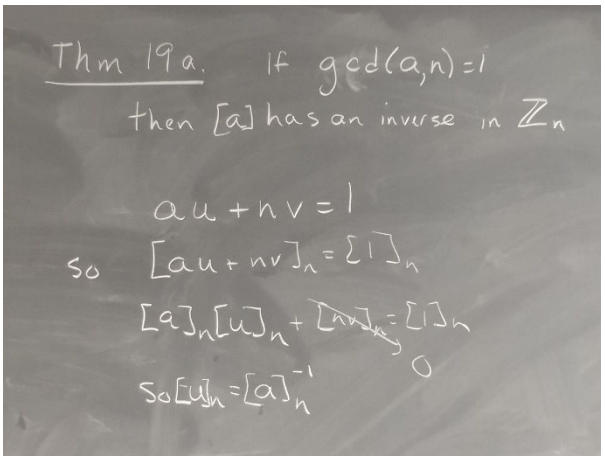
And the easiest one of all is showing that it is a homomorphism:



We passed out the new and improved set of definitions and theorems. **This Friday, you will be turning in the proofs of the following theorems: 19a, 21, 24, 25, 26, 35.**

Theorem 19a: If $\gcd(a,n)=1$ then $[a]_n$ has a multiplicative inverse in $\mathbb{Z}_n$

We re-proved this in class today. Here it is:

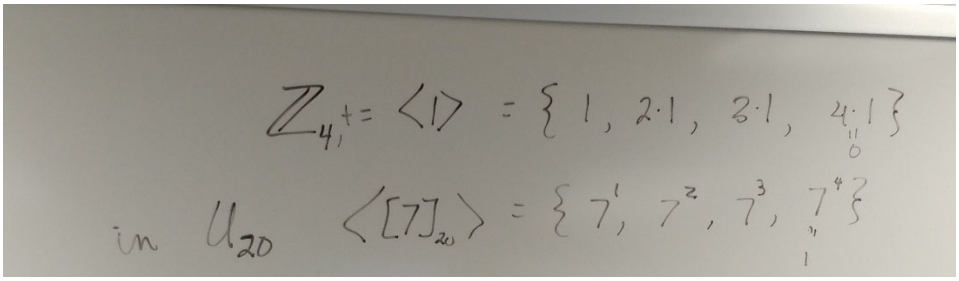


Theorem 21: You may assume that multiplication is associative in $\mathbb{Z}_n$, but you do need to prove that U_n is closed under multiplication, includes a multiplicative identity, and elements have multiplicative inverses. For instance, if two elements are in U_n (so they have inverses), is there product in U_n (does it have an inverse?).

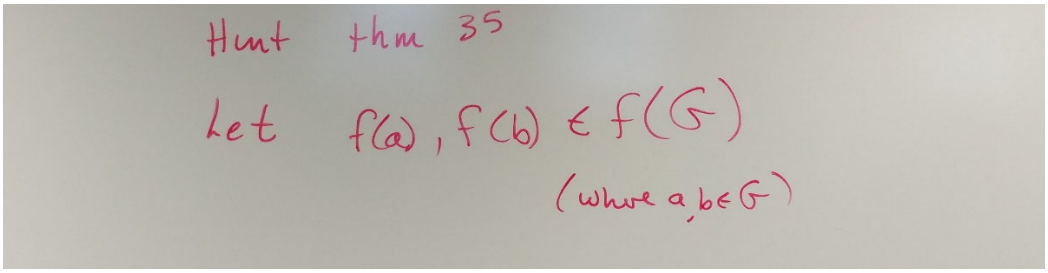
Theorem 24, 25 and 26 all rely on theorem 23 (exponent laws) and on the definition of the order of an element (smallest positive power that gets you to the identity). Please spend at least 10 minutes thinking about theorem 24 and 25 and how you would prove them before class on Wednesday. We will prove 26 together on Wednesday.

Theorems 24-29 are all developing properties of cyclic subgroups. A really cool property (Theorems 33 and 34) is that all cyclic groups that have the same order are isomorphic to each other.

We did an example of this in the previous class with the cyclic group $\mathbb{Z}_4, +$ which is generated by the number 1, and the cyclic group $<[7]_{20}>$ which is generated by 7 in U_{20}, both of which have order 4, and when we line them up so that the generator of $\mathbb{Z}_4, +$ is matched with the generator of $<[7]_{20}>$ (and all of the other elements are matched up in a way that uses those generators), then we got an isomorphism.



Theorem 35: prove the homomorphic image of a group is a group. You are going to prove it is a subgroup by verifying the closure and inverses properties. I gave the hint below (if you name your elements in a useful way, then proving theorem 35 isn't too hard).



I also shared a challenge problem (optional): Given groups G and H and a homomorphism $f: G \to H$, then $\ker(f) = \{x \mid x \in G,\ f(x) = e \in H\}$ is a subgroup of G. This set (group) is called the **kernel** of f.