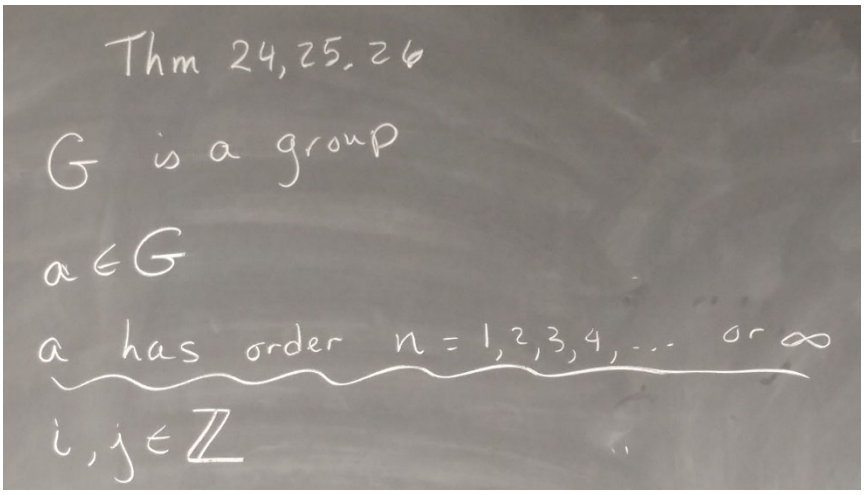
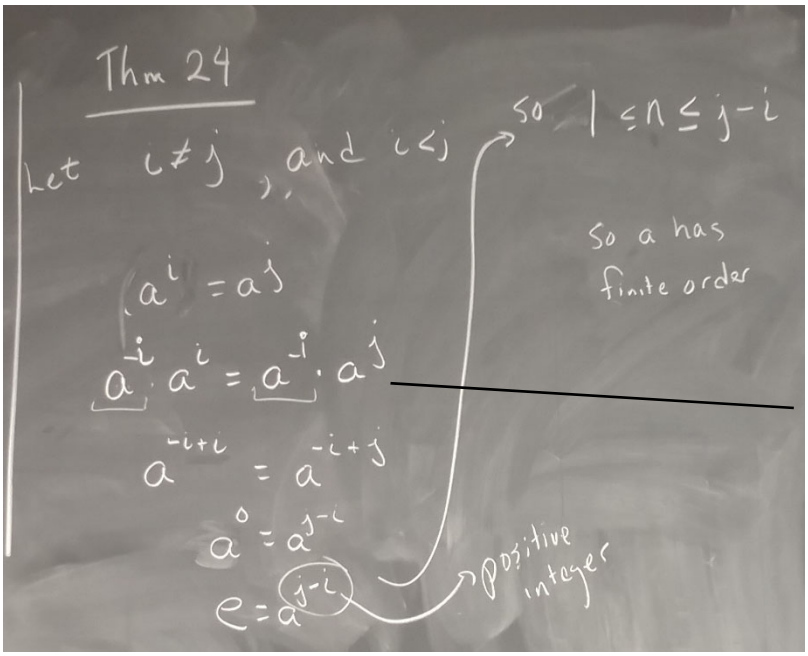
Today's class started by doing part of problem 13, and then proving theorem 26. By hindsight, maybe we should have done theorem 26 first, so I'm going to reorder the slides here.

I started with giving this notation for my discussion of theorems 24-26:



Remember that the order of an element is the smallest positive integer for which $a^n = e$. Note that everything we did today was for multiplicative groups, but if you were working with an additive group, we would be writing $na = e$ instead of $a^n = e$.

We then looked at Theorem 24:

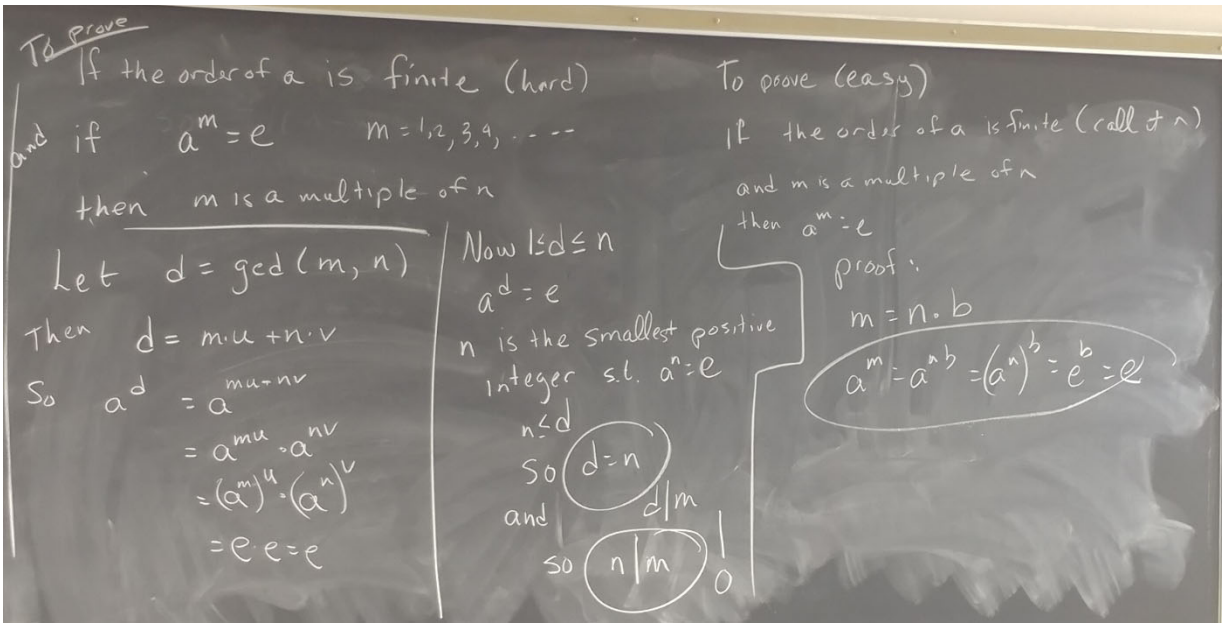


Notice here that I multiplied on both sides by a^{-i} to simplify the equation.

Note that I multiplied on the left side of both sides, so I didn't have to worry about whether G is commutative or not.

The conclusion of this is that if you have *a* raised to any positive integer giving *e*, then the order of *a* has to be less than or equal to that positive integer.

So next we looked at a variation of Theorem 26:



Theorem 26 is an if and only if statement, and this version was also an if and only if statement, so there were two things to prove, and one is hard (the left 2/3) and one is easy (right 1/3)

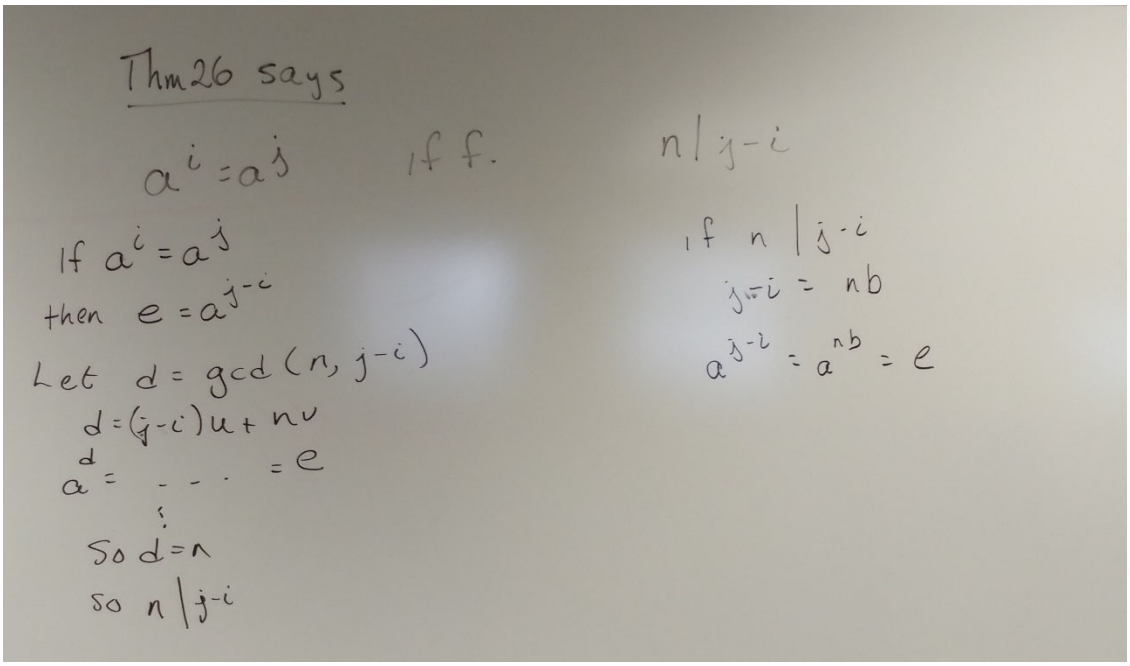
In this, we are still using *n* to represent the order of *a*, and we are assuming that it is finite.

Notice that the key to the hard part was to name the gcd of the two exponents. We used property of gcd's to prove that $a^d = e$. Then we said because *d* is the gcd it has to be both positive and less than or equal to *n*. Next, we used the definition of the order of *a* to say that *d* must be greater than or equal to *n*, so *n=d*.

Finally we used that *d* is a divisor of *m* to say that *n* is also a divisor of *m* (which was what we wanted to prove).

I hope that the easy half is easy enough that you don't need extra explanation here.

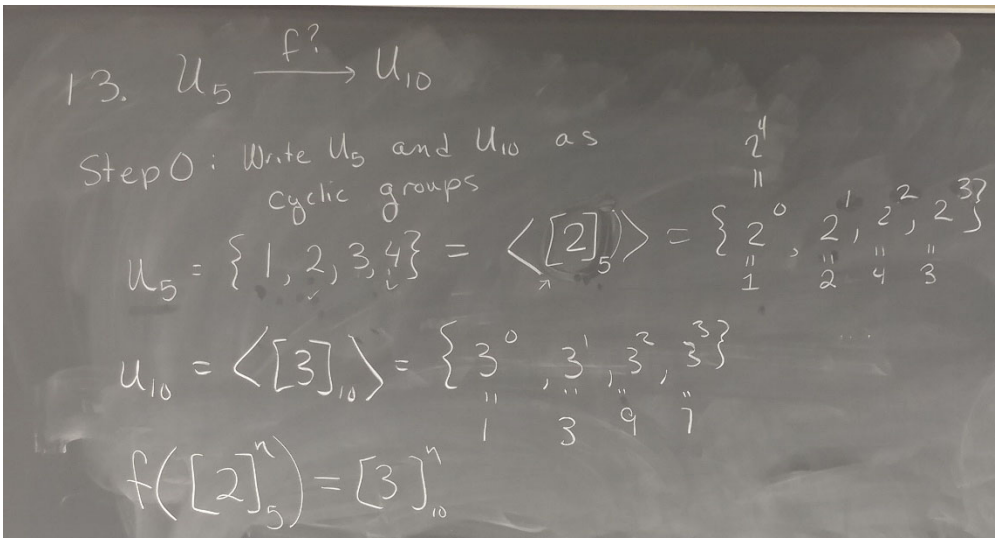
The next thing we did (which was at the very end of class) was to show that this was equivalent to what Theorem 26 exactly says.



So if you look at theorem 26, if you start with integers i, j such that $a^i = a^j$, then by doing the same algebra we used for theorem 24, we can turn that equation into one that says $a^{j-i} = e$ (where $j-i$ is an integer). This is essentially the same as the assumption on the page above that $a^m = e$, where *m* is a positive integer. On the previous page, we assumed that $m = j-i$ was a positive integer, but if you look up the gcd properties, it's only required that one of the two integers be non-zero, so if we know that the order *n* is a positive integer, then $m = j-i$ can be any integer (even negative or zero), and we can still write down the gcd equation, and we can still use exponent laws, and we will still get that *d=n* at the end. We allow every number to be a factor of 0, so there are no problems if $m = j-i$ is 0 (or negative).

And, of course, the easier side is still easier.

I rearranged to put Theorem 26 first in my notes here because it's going to help us with problem 13:



The first key to solving problem 13 is to write the groups as cyclic groups with a single generator. If you look at powers of $[2]_5$, you find that you get all four elements in U_5 as powers of $[2]_5$, so we can think of the group as being the cyclic group generated by $[2]_5$. You also find that the order of $[2]_5$ is 4.

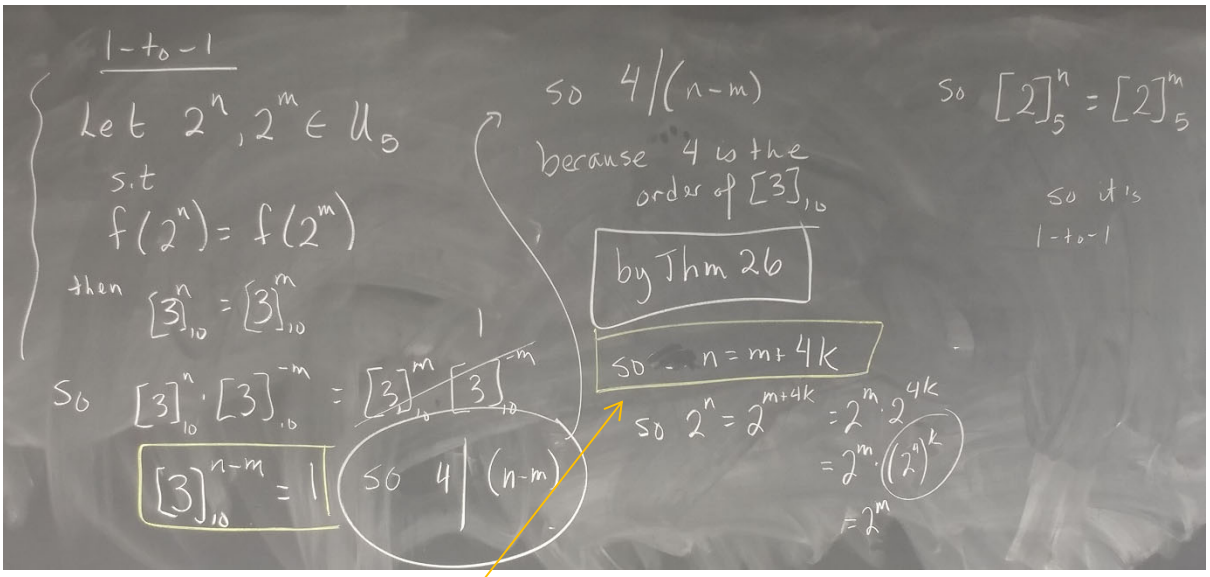
Then (by experimenting with powers of elements of U_{10}), we find that U_{10} is the cyclic group generated by $[3]_{10}$, and $[3]_{10}$ also has order 4.

A theorem we discussed on Monday says that these groups have to be isomorphic. The key to defining the isomorphism is to use the cyclic group notation, and to make sure we map the generator of one group to the generator of the other group, so $f([2]_5^n) = [3]_{10}^n$

……

I asked some students to choose two of the isomorphism properties to work out, and they chose 1-to-1 and onto.

One-to-one looks like this:



The equation in the second yellow box is key to doing this completely (and getting full credit): if those two powers of 3 are equal: $3^n = 3^m$ then you know that $m - n$ is a multiple of the order of 3. Notice that you don't necessarily know that *n=m*, because these are mod-numbers, but you do know that *n=m+4k*. You can then substitute that in for *n* in 2^n to get that $2^n = 2^m$ because 2 also has order 4.

Note, that you should be doing something very similar to this when you are proving that *f* is a function, except that you will start with $2^n = 2^m$ and then use theorem 26 to get *n=m+4k*, and eventually get to $3^n = 3^m$.

Finally, proving that *f* is onto is fast and easy (compared to 1-to-1):