Discussion Section Time

My discussion time is with Jet Situ in Hearst Mining 310 on Wednesday and Friday 6-7pm.

Discussion 3A: Modular Inverses

I'd ask students to take a moment and digest the problem statement. Specifically, the phrase that if $ax \equiv 1 \pmod{m}$ then x is the modular inverse of x modulo m.

- Parts (a) and (b) familiarize students them with modular inverses using examples. Here, $3 \cdot 5 = 15 \not\equiv 1 \pmod{10}$, so 3 is not an inverse of 5 mod 14. However, since $15 \equiv 1 \pmod{14}$, then 3 is an inverse of 5 mod 14.
- Part (c) is a natural extension of this concept, illustrating that we can multiply them together and then simplify the expression to see if we get 1. I'd first ask students to take a look again at how we verified inverses in the previous two parts, and see if we can generalize that process here.
- To start part (d), I'd encourage students to write down an arithmetic equation that represents the modular equation, then arrive at a contradiction. Once this is solved, I want to encourage students to look back on the proof, and notice that we haven't used anything else besides the fact that $\gcd(a, m) \neq 1$ in the proof, meaning that our conclusion can be made much more general: if $\gcd(a, m) \neq 1$, then a does not have an inverse modulo m. This is also the statement at the end of Theorem 6.2 in Note 6.
- For part (e), I'd encourage students to set up the equation involving x and x', and look at what operations we can do to combine these two equations to arrive at the fact that $x \equiv x' \pmod{m}$.

Discussion 3B: Baby Fermat

(a) I'd ask students to consider what the pigeonhole principle is really saying, hopefully getting them to realize since the sequence is infinite and there are only m possible values modulo m, that there must be repetitions.

(b) The first guidance I'd give is to notice that normally we'd write $a^{i-j} = a^i/a^j$, so I'd ask how do we achieve this in modular arithmetic. Here, the emphasis should be on the fact that a^j is multiplied by a^*, that the exponent of a^j is reduced, analogous to how it normally would be under division. Once we realize this then we can realize that if we multiply both sides by $(a^*)^j$ times, then the equation simplifies perfectly into $a^{i-j} \equiv 1 \pmod{m}$.

(c) This part just relies on noticing that we can take one from the exponent and write it out explicitly, giving us that a^{i-j-1} is the inverse of a modulo m. The only guidance I can think of here is to ask students how else could they represent a^{i-j} as the product of two powers of a which look similar in form to the equation $ax \equiv 1 \pmod{m}$, hopefully leading them to realize this idea of bringing down a factor of a.