In-Class Problems Week 6, Fri.

Problem 1. This problem gives you practice with modular arithmetic. If you wish to shout "Woohoo!", go ahead— we understand.

(a) Prove: If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.

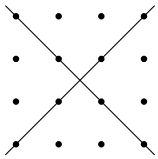
(b) Prove: $(a \text{ rem } n) \equiv a \pmod{n}$

(c) Sketch an induction proof that $10^k \equiv 1 \pmod{9}$ for all $k \geq 0$. Why is a number written in decimal evenly divisible by 9 if and only if the sum of its digits is a multiple of 9?

Problem 2. Two nonparallel lines in the real plane intersect at a point. Algebraically, this means that the equations

$$\begin{aligned} y &= m_1 x + b_1 \\ y &= m_2 x + b_2 \end{aligned}$$

have a unique solution (x, y), provided $m_1 \neq m_2$. This statement would be false if we restricted x and y to the integers, since the two lines could cross at a noninteger point:



However, an analogous statement holds if we work over the integers *modulo a prime* p. Find a solution to the congruences

$$\begin{aligned} y &\equiv m_1 x + b_1 \pmod{p} \\ y &\equiv m_2 x + b_2 \pmod{p} \end{aligned}$$

of the form $x \equiv ? \pmod{p}$ and $y \equiv ? \pmod{p}$ where the ?'s denote expressions involving m_1, m_2, b_1, and b_2. You may find it helpful to solve the original equations over the reals first.

Problem 3. Suppose that p is a prime.

(a) An integer k is *self-inverse* if $k \cdot k \equiv 1 \pmod{p}$. Find all integers that are self-inverse mod p.

(b) *Wilson's Theorem* says that $(p-1)! \equiv -1 \pmod{p}$. The English mathematician Edward Waring said that this statement would probably be extremely difficult to prove because no one had even devised an adequate notation for dealing with primes. (Gauss proved it while standing.) Your turn! Try cancelling terms of $(p-1)!$ in pairs. See if you can do it while standing on one leg.