Solutions to 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 $ac \equiv bc \pmod{n}$.

Solution. The condition $a \equiv b \pmod{n}$ is equivalent to the assertion $n \mid (a-b)$. This implies that $n \mid (a-b)c$ by part (a) of Problem 1, and so $n \mid (ac-bc)$. This is equivalent to $ac \equiv bc \pmod{n}$. ■

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

Solution. The remainder a rem n is equal to $a - qn$ for some integer q. However, for every integer q:

$$\begin{aligned} & n \mid qn \\ \Rightarrow \quad & n \mid (a-qn) - a \\ \Rightarrow \quad & n \mid (a \text{ rem } n) - a \end{aligned}$$

The last statement is equivalent to $(a \text{ rem } n) \equiv a \pmod{n}$. ■

(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?

Solution. The claim holds for $k = 0$, since $10^0 \equiv 1 \pmod{9}$. Suppose the claim holds for some $k \geq 0$; that is, $10^k \equiv 1 \pmod{9}$. Multiplying both sides by 10 gives $10^{k+1} \equiv 10 \equiv 1 \pmod{9}$. So the claim holds for $k+1$ as well.

A number in decimal has the form:

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0$$

From the observation above, we know:

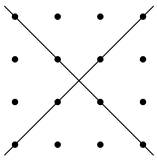
$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \quad \equiv \quad d_k + d_{k-1} + \ldots + d_1 + d_0 \pmod{9}$$

This shows something stronger: the remainder when the original number is divided by 9 is equal to the remainder when the sum of the digits is divided by 9. In particular, if one is zero, then so is the other. ■

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.

Solution. Subtracting the second congruence from the first, we have:

$$\begin{aligned} 0 &\equiv m_1 x + b_1 - (m_2 x + b_2) \pmod{p} \\ (m_1 - m_2)x &\equiv b_2 - b_1 \pmod{p} \\ x &\equiv (m_1 - m_2)^{-1} \cdot (b_2 - b_1) \pmod{p} \end{aligned}$$

Substituting this value of x into the first congruence, we have

$$y \equiv m_1 \cdot (m_1 - m_2)^{-1} \cdot (b_2 - b_1) + b_1 \pmod{p}$$

■

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.

Solution. The congruence holds if and only if $p \mid k^2 - 1$ which is equivalent to $p \mid (k+1)(k-1)$. This holds if and only if either $p \mid k+1$ or $p \mid k-1$. Thus, $k \equiv \pm 1 \pmod{p}$. ■

(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.

Solution. If $p = 2$, then the theorem holds, because $1! \equiv -1 \pmod{2}$. If $p > 2$, then $p-1$ and 1 are distinct terms in the product $1 \cdot 2 \cdot \cdots (p-1)$, and these are the only self-inverses. Consequently, we can pair each of the remaining terms with its multiplicative inverse. Since the product of a number and its inverse is congruent to 1, all of these remaining terms cancel. Therefore, we have:

$$\begin{aligned} (p-1)! &\equiv 1 \cdot (p-1) \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

■