MATH 113: DISCRETE STRUCTURES
FRIDAY WEEK 12 HANDOUT

In §6.8 you learned that there are commutative, associative operations $+, \cdot$ on $\mathbb{Z}/n\mathbb{Z}$ and that $+$ admits an inverse $-$ such that $\overline{a} - \overline{a} = \overline{0}$. When n is prime, everything in $\mathbb{Z}/n\mathbb{Z}^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$ admits a multiplicative inverse as well, *i.e.*, for each $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^\times$, there exists $\overline{a}^{-1} \in \mathbb{Z}/n\mathbb{Z}^\times$ such that $\overline{a} \cdot \overline{a}^{-1} = \overline{1}$. We sometimes write $\overline{1}/\overline{a}$ for $\overline{a}^{-1}$ and $\overline{a}/\overline{b}$ for $\overline{a}\overline{b}^{-1}$.

Problem 1. Our previous version of Fermat's little theorem said that if p was prime and $1 \leq a \leq p-1$, then $p \mid a^p - a$. Of course, $p \mid 0 = 0^p - 0$, so this holds for $0 \leq a \leq p-1$ as well.

(a) Check that this is equivalent to $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.
(b) Suppose $a \not\equiv 0 \pmod{p}$. Prove that $a^{p-1} \equiv 1 \pmod{p}$.
(c) For $p > 2$, what are the possible values of $a^{(p-1)/2}$ mod p? (Note that $p-1$ is even when $p > 2$, so $(p-1)/2$ makes sense.)
(d) For $a \in \mathbb{Z}$ such that $a \not\equiv 0 \pmod{p}$, define $o_p(a)$ (the *order of a modulo p*) to be the smallest positive integer such that $a^{o_p(a)} \equiv 1 \pmod{p}$. Since $a^{p-1} \equiv 1 \pmod{p}$, we know that $1 \leq o_p(a) \leq p-1$. Prove that $o_p(a) \mid p-1$.
(e*) Prove that there exists $a \in \mathbb{Z}$ such that $o_p(a) = p-1$.
(f) Assume (e*) (which is a challenge problem you can try outside of class) and take $a \in \mathbb{Z}$ such that $o_p(a) = p-1$. Show that each a^n, $1 \leq n \leq p-1$, is in a distinct congruence class modulo p and thus the values of a^n cycle through all the nonzero congruence classes mod p with period $p-1$.[1]

Problem 2. Make a multiplication table for $\mathbb{Z}/7\mathbb{Z}^\times$. Select a congruence class and circle all its occurrences in the table. Observe that this is a solution to the non-capturing rooks problem on a 6×6 chessboard. Does it work for other congruence classes? For $\mathbb{Z}/p\mathbb{Z}^\times$ and $(p-1) \times (p-1)$ chessboards in general? Why?

Problem 3. How many squares are there mod p? *i.e.*, how large is $\{\overline{x}^2 \mid \overline{x} \in \mathbb{Z}/p\mathbb{Z}^\times\}$? What is the probability that $x^2 \equiv a \pmod{p}$ will have a solution? Suppose $x^2 \equiv a \pmod{p}$ has a solution; how many solutions does it have? In the diagonal of the multiplication table for $\mathbb{Z}/p\mathbb{Z}^\times$, why does $\overline{1}$ always and only appear in the top left and bottom right corner?

Problem 4. Your vitamin regimen requires you to take *Doctor Snoggleswarf's Health Elixir* ® every five days. You take the first dose in the bottle on a Sunday and the final dose on a Thursday. You're not sure how many doses you took, but you know that there are at least 50 doses in a bottle. What is the minimum number of doses you took?

[1] An algebraist would say that $\mathbb{Z}/p\mathbb{Z}^\times$ is a cyclic group of order $p-1$.