**PROBLEM-SOLVING AND PROOFS: ASSIGNMENT 8**
**DUE FRIDAY, MAY 5, 4PM.**

**Warm-up problems.** These do not need to be written up, but I strongly recommend thinking about them.

(1) The following statement is not always true: "If $ac \equiv bc \mod n$, then $a \equiv b \mod n$." Give an explicit counterexample and describe an extra hypothesis on $c$ and $n$ that would make the statement true.

(2) Define a relation $R$ on the set of all persons by defining $(x, y) \in R$ if $x$ and $y$ are citizens of the same country. Is $R$ an equivalence relation?

(3) Prove that congruence modulo $n$ defines an equivalence relation on $\mathbb{Z}$.

**Problems to be handed in.** Solve four of the following five problems. One of the four must be Problem (5).

7.47, 7.48

(1) *Variations on Wilson's Theorem*
   (a) Prove that if $p$ is prime, $2(p-3)! + 1$ is divisible by $p$.
   (b) Prove that if $p$ divides $(p-1)! + 1$, then $p$ is prime. (This is the converse to Wilson's Theorem.)

7.14

(2) *An important equivalence relation in analysis.* Fix a function $f : \mathbb{R} \to \mathbb{R}$, and let $O(f)$ denote the set of functions $g : \mathbb{R} \to \mathbb{R}$ for which there exist positive constants $c$ and $a$ such that $|g(x)| \leq c|f(x)|$ for all $x > a$. Now let $S$ denote the set of all functions from $\mathbb{R}$ to $\mathbb{R}$, and define a relation $R$ on $S$ by setting $(g, h) \in R$ if and only if $g - h \in O(f)$. Prove that $R$ is an equivalence relation.

(3) *Linear Equations in Modular Arithmetic.* Let $n \in \mathbb{N}$, let $a, b \in \mathbb{Z}$, and set $d = \gcd(a, n)$. Prove that the equation

$$ax \equiv b \mod n$$

7.32

has a solution if and only if $d|b$. Furthermore, prove that when $d|b$, there are exactly $d$ distinct congruence classes of solutions.

(4) *Euler's Theorem.* This is a generalization of Fermat's little theorem to nonprime moduli. Let $\phi(n)$ denote the number of integers less than $n$ which are relatively prime to $n$. For example, $\phi(10) = 4$ since $1, 3, 7, 9$ are relatively prime to 10. Prove that if $a \in \mathbb{Z}$ is relatively prime to $n$, then

$$a^{\phi(n)} \equiv 1 \mod n$$

Hint: Consider the set

$$\{ia : 1 \leq i \leq n-1, \gcd(i, n) = 1\}$$

and mimic our proof of Fermat's Little Theorem.

7.41

(5) *Functional Digraphs from Modular Arithmetic.* Define $f$ and $g$ from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ by

$$f(x) \equiv x + a \mod n$$
$$g(x) \equiv ax \mod n$$

(a) Draw the functional digraphs of $f$ and $g$ in the cases $(n, a) = (19, 4)$ and $(n, a) = (20, 4)$.
(b) Give a complete description of the functional digraph of $f$ in terms of $a$ and $n$.
(c) Describe a property of the digraph of $g$ which is true whenever $n$ is prime and false whenever $n$ is not prime.