Homework #9

Problems to hand in on Thursday, April 4, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) (a) Prove Fermat's Little Theorem: if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.
   (b) If G is a group of prime order p, then G is cyclic.
   (c) A nontrivial group G has no nontrivial proper subgroups if and only if G is finite and of order p where p is prime.

2) The goal of this problem is to prove the following fact:

> Given positive integers n and p, if p is prime then $n!$ divides $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

   (a) Describe a subgroup of $GL_n(\mathbb{Z}_p)$ that is isomorphic to $\mathbb{S}_n$.
   (b) Count the elements in $GL_n(\mathbb{Z}_p)$.
   (c) Prove the fact.

3) Let X be any set and $\sim$ be an equivalence relation on X. Write $\mathscr{E}(x)$ to denote the equivalence class of x.
   (a) Given $x, y \in X$, show that $x \sim y$ if and only if $\mathscr{E}(x) = \mathscr{E}(y)$.
   (b) Given $x, y \in X$, show that either $\mathscr{E}(x) = \mathscr{E}(y)$ or $\mathscr{E}(x) \cap \mathscr{E}(y) = \emptyset$.
   (c) Show that X is the disjoint union of all the equivalence classes for $\sim$.

4) Let $R = \mathbb{R}[x]$. Consider the group action of $G = \mathbb{Z}_2$ on R by the rules

$$[0]_2 \cdot f(x) = f(x) \qquad \text{and} \qquad [1]_2 \cdot f(x) = f(-x).$$

   Show that the set of *invariant polynomials* $\{r \in R \mid g \cdot r = r \text{ for all } g \in G\}$ is a subring of R, and describe this subring explicitly.