Homework #4. Due Wednesday, February 13th, in class

Reading:

1. For this homework assignment: Chapter 4 and Section 5.1.
2. For the next two classes: Chapter 5 and Section 6.1.

Problems:

1. Let R be a commutative ring with 1. Prove that $R^{\times}$, the set of units of R, is a group with respect to multiplication.

2. The goal of this problem is to give a group-theoretic proof of Wilson's theorem: $(p-1)! \equiv -1 \mod p$ for every prime p.

(a) Let G be a finite group, and let $S = \{g \in G : g^{-1} = g\}$ be the set of all elements of G which are equal to their inverse. Prove that $|G| - |S|$ is even.

(b) Let $G = \mathbb{Z}_p^{\times}$. Prove that the only elements of G equal to their inverses are $[1]$ and $-[1]$.

(c) Now use (a) and (b) to prove that $(p-1)! \equiv -1 \mod p$. **Hint:** Reformulate the desired congruence as equality in $\mathbb{Z}_p$.

3. Recall that if G is a group and g is an element of G, the order of g (denoted by $o(g)$) is the smallest positive integer n such that $g^n = e$ (if no such n exists, we set $o(g) = \infty$).
In all parts below G is a finite group (so all its elements have finite order).

(a) Let $g \in G$ and $n \in \mathbb{Z}$. Prove that $g^n = e$ if and only if $o(g) \mid n$.

(b) Let S be the set of possible orders of elements of G. Prove that if $n \in S$, then every positive divisor of n also lies in S.

(c) Now assume that G is abelian, and let $g, h \in G$. Let $k = o(g)$, $l = o(h)$ and $m = lcm(k, l)$. Prove that $(gh)^m = e$. If in addition $gcd(k, l) = 1$, prove that $o(gh) = m = kl$.

(d) Again assume that G is abelian. Prove that there exists an element $h \in G$ s.t. $g^{o(h)} = e$ for all $g \in G$.

Hint for (d): Let P be the set of primes which divide at least one element of S. For each $p \in P$ let e_p be the largest integer such that $p^{e_p} \in S$. For each $p \in P$, choose an element $h_p \in G$ with $o(h_p) = p^{e_p}$. Then prove that the element $h = \prod_{p \in P} h_p$ has desired property.

4. Let p be a prime.

(a) Use Problem 3(d) and Corollary 7.5 from class to prove that the group $\mathbb{Z}_p^\times$ is cyclic. **Hint:** A group of order n is cyclic if and only if it contains an element of order n.

(b) Let $m \in \mathbb{Z}$. Prove that the following are equivalent:

(i) $a^m \equiv 1 \mod p$ for all a with $p \nmid a$;

(ii) $(p-1) \mid m$.

5. Let p be a prime and $e \geq 1$ an integer.

(a) Prove that the congruence

$$x^p - x \equiv p \mod p^e$$

has precisely p solutions mod p^e.

(b) Find all solutions to the congruence in (a) for $p = 3$ and $e = 2$.

6. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree 3. Prove that the congruence $f(x) \equiv 0 \mod 25$ cannot have precisely 8 solutions $\mod 25$.

7. Read about Carmichael numbers in Section 4.2.