Homework #4. Due Thursday, February 13th, by 4pm

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

(b) Now use (a) to prove that $(p-1)! \equiv -1 \mod p$. **Hint:** Reformulate the desired congruence as equality in $\mathbb{Z}_p$ and note that $[(p-1)!]$ is the product of all elements of G.

3. Let G be a finite group. The exponent of G, denoted by $\exp(G)$, is the smallest positive integer m such that $g^m = e$ for all $g \in G$. Note that $g^{|G|} = e$ for all $g \in G$ by (a corollary of) Lagrange theorem, so we always have $\exp(G) \leq |G|$.

(a) Prove that $\exp(G)$ is equal to the least common multiple of orders of elements of G. **Hint:** Use Problem 5 from HW#1.

(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.

In the remaining parts of this problem we assume that the group G is abelian.

(c) Let $g, h \in G$, let $k = o(g)$, $l = o(h)$ (where $o(x)$ is the order of x). Let $m = lcm(k, l)$. Prove that $(gh)^m = e$. If in addition $gcd(k, l) = 1$, prove that $o(gh) = m = kl$.

(d) Prove that for any $g, h \in G$ there exists an element $f \in G$ with $o(f) = lcm(o(g), o(h))$. **Hint:** Let $p_1, \ldots, p_k$ be the set of primes which divide $o(g)$ or $o(h)$, so we can write $o(g) = p_1^{a_1} \ldots p_k^{a_k}$ and $o(g) = p_1^{b_1} \ldots p_k^{b_k}$.

By (b), there exist elements $g_1, \ldots, g_k, h_1, \ldots, h_k$ with $o(g_i) = p_i^{a_i}$ and $o(h_i) = p_i^{b_i}$ for $1 \leq i \leq k$. Now use this fact, part (c) (several times) and Problem 2 from HW#3 to construct the desired element f.

(e) Let $g \in G$ be an element of maximal order (among all elements of G). Prove that $o(h) \mid o(g)$ for all $h \in G$ and deduce that $o(g) = exp(G)$. **Hint:** use (d).

4. Let p be a prime. Prove that the group $\mathbb{Z}_p^\times$ is cyclic. **Hint:** Assume that $\mathbb{Z}_p^\times$ is not cyclic and use Problem 3(e) to construct a nonzero polynomial in $\mathbb{Z}_p[x]$ which has more roots in $\mathbb{Z}_p$ than its degree. This contradicts Lemma 5.4 from class.

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 reduced solutions.

(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 reduced solutions.

7. Read about Carmichael numbers in Section 4.2.