Homework #4. Solutions to selected problems

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 $\exp(G) \le |G|$.

(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 $o(f) = lcm(o(g), o(h))$.

(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).

Solutions to (c)-(e):

(c) Since G is abelian, $(gh)^m = g^m h^m$. Since $o(g)$ and $o(h)$ both divide m, we have $g^m h^m = e \cdot e = e$.

Assume now that $gcd(k, l) = 1$. We already know that $o(gh) \le lcm(k, l) = kl = m$. To prove the equality we need to argue that if $(gh)^M = e$ for some $M \in \mathbb{N}$, then $M \ge m$. Again since G is abelian, $(gh)^M = e$ implies $g^M h^M = e$, so $g^M = h^{-M}$. Hence the element g^M lies in $\langle g \rangle \cap \langle h \rangle$, the intersection of cyclic subgroups generated by g and h.

Note that $\langle g \rangle \cap \langle h \rangle$ is a subgroup of both $\langle g \rangle$ and $\langle h \rangle$, so by Lagrange theorem $|\langle g \rangle \cap \langle h \rangle|$ divides both $|\langle g \rangle| = o(g) = k$ and $|\langle h \rangle| = o(h) = l$. Since $gcd(k, l) = 1$, we conclude that $|\langle g \rangle \cap \langle h \rangle| = 1$. Thus, the intersection $\langle g \rangle \cap \langle h \rangle$ is trivial, so we must have $g^M = h^{-M} = e$ (hence $h^M = e$). By

HW 1.5, this implies that M is a multiple of both $o(g) = k$ and $o(h) = l$, so $M \geq lcm(k, l) = kl$, as desired.

(d) 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 $1 \leq i \leq k$. For each i put $f_i = g_i$ if $a_i \geq b_i$ and $f_i = h_i$ otherwise. In either case $o(f_i) = p_i^{\max\{a_i, b_i\}}$.

Let $f = f_1 \ldots f_k$. We claim that this element has the desired property. By construction, the orders of elements $f_1, \ldots, f_k$ are pairwise coprime, so repeated applications of part (c)(combined with HW 2.1) show that $o(f) = o(f_1) \ldots o(f_k)$. Hence the formula for LCM of several integers from HW 3.2(ii) implies that $o(f) = lcm(o(g), o(h))$.

(e) This is a simple proof by contradiction. Suppose that there exists $h \in G$ such that $o(h)$ does not divide $o(g)$. Then $lcm(o(h), o(g))$ is strictly larger than $o(g)$. On the other hand, by (d) there exists $f \in G$ with $o(f) = lcm(o(h), o(g))$, which contradicts the assumption that g is an element of maximal order.

4. Let p be a prime. Prove that the group $\mathbb{Z}_p^\times$ is cyclic.

Solution: Let $G = \mathbb{Z}_p^\times$ and $m = \exp(G)$. By definition of exponent, $g^m = e$ for all $g \in G$, that is, $[x]_p^m = [1]_p$ for all $x \in \mathbb{Z}$ with $p \nmid x$. Equivalently, whenever $p \nmid x$ we have $x^m \equiv 1 \mod p$, whence $x^{m+1} \equiv x \mod p$. Note that the congruence $x^{m+1} \equiv x \mod p$ is also valid if $p \mid x$, so it holds for all $x \in \mathbb{Z}$ and thus has p reduced solutions. On the other hand, since p is prime, by Corollary 7.5 from class, the number of reduced solutions cannot exceed $\deg(x^{m+1} - x) = x^{m+1}$. Hence $m + 1 \geq p$ and thus $m \geq p - 1 = |G|$. Since we always have $\exp(G) \leq |G|$, we conclude that $m = |G|$.

By Problem 3(e), there exists $g \in G$ with $o(g) = m$, so G has an element g with $o(g) = |G| = p - 1$, and therefore G is cyclic.

Before discussing problems 5 and 6 we introduce some convenient terminology and recall basic results about lifts of solutions to polynomial congruences modulo a prime power. So, let $f(x) \in \mathbb{Z}[x]$ and let p be a prime.

Definition. Let x_0 be a reduced solution to $f(x) \equiv 0 \mod p^e$ for some $e \in \mathbb{N}$. A **lift of** x_0 is a reduced solution y to the congruence $f(x) \equiv 0 \mod p^{e+1}$ satisfying $y \equiv x_0 \mod p^e$.

It is clear that any reduced solution to $f(x) \equiv 0 \mod p^{e+1}$ arises as a lift of unique reduced solution to $f(x) \equiv 0 \mod p^e$.

Definition. A solution x_0 to $f(x) \equiv 0 \mod p^e$ will be called

regular if $p \nmid f'(x_0)$ and

singular if $p \mid f'(x_0)$

The following is the main result describing the possible number and type of lifts.

Lifting Theorem: *Let x_0 be a reduced solution to $f(x) \equiv 0 \mod p^e$*

(a) If x_0 is a regular solution, then x_0 has a unique lift.

(b) If x_0 is a singular solution, then x_0 has either p lifts or no lifts.

(c) Lifts of regular solutions are regular and lifts of singular solutions are singular.

Parts (a) and (c) imply the following:

Corollary: *If for some $e \in \mathbb{N}$ the congruence $f(x) \equiv 0 \mod p^e$ has k reduced solutions and all these solutions are regular, then the congruence $f(x) \equiv 0 \mod p^f$ has k reduced solutions for any $f \geq e$.*

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 $e = 2$.

Solution: (a) Let $f(x) = x^p - x$. By Fermat's little theorem the congruence $f(x) \equiv 0 \mod p$ holds for all $x \in \mathbb{Z}$ (and thus has p reduced solutions, namely $0, 1, \ldots, p-1$). Since $f'(x) = px^{p-1} - 1$ is never divisible by p, all those p solutions are regular. Hence $f(x) \equiv 0 \mod p^e$ has p reduced solutions for any e.

(b) Using the method discussed in class, we find that $x = 5, 6$ and 7 are reduced solutions to $x^3 - x \equiv 3 \mod 9$. The general solution is given by $x \equiv 5, 6$ or $7 \mod 9$.

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.

Solution: We consider two cases.

Case 1: Not all coefficients of $f(x)$ are divisible by 5. In this case, by Corollary 7.5 from class, the congruence $f(x) \equiv 0 \mod 5$ has at most 3 reduced solutions. Suppose that among those three a are regular and b are singular. Let c be the number of singular solutions which have lifts. Then by the lifting theorem the total number of lifts (which is precisely the number of reduced solutions to $f(x) \equiv 0 \mod 25$) is $a + 5c$. In order to have precisely 8 solutions we must have $a+5c = 8$. Since a and c are non-negative integers, the only possibilities are $a = 8$, $c = 0$ or $a = 3$ and $c = 1$. Neither of these can happen since by construction $a + c \leq 3$.

Case 2: All coefficients of $f(x)$ are divisible by 5. Then all coefficients of $f'(x)$ are also divisible by 5, so all the solutions to $f(x) \equiv 0 \mod 5$ are singular. Then by the lifting theorem, the total number of lifts should be divisible by 5, so again it cannot equal 8.