WRITTEN HOMEWORK #1, DUE APRIL 9, 2010

Unless explicitly noted, you are to justify all of your responses with work and/or proofs. In this assignment, you will probably want to use the Euler φ function, where $\varphi(n)$ equals the number of integers between 1 and n, inclusive, which are relatively prime to n. For example, $\varphi(2) = 1, \varphi(4) = 2, \varphi(5) = 4$.

(1) (a) Let $G = \mathbb{Z}/n\mathbb{Z}$. We know that $\overline{1}$ (equivalently, $1 \mod n$) generates the additive group G. What is the order of $k \mod n$, in terms of k and n?
(b) If $g \in G$, we know that $|g|$ divides $|G|$. Therefore, if $m \nmid n$, then there are no elements of order m in $\mathbb{Z}/n\mathbb{Z}$. Suppose instead that $m|n$. How many elements of $\mathbb{Z}/n\mathbb{Z}$ have order m?

(2) (a) Let $(g_1, g_2) \in G_1 \oplus G_2$, where $|g_1| = n_1, |g_2| = n_2$. What is the order of (g_1, g_2)?
(b) Use your answer from part (a) to determine the number of elements of each order in $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

(3) (a) Show that two isomorphic finite groups have the same number of elements of each order.
(b) With this in mind, show that $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$ are not isomorphic.
(c) More generally, give necessary and sufficient conditions on m, n for when $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\mathbb{Z}/mn\mathbb{Z}$.

(4) Let $f(x)$ be a polynomial with complex coefficients, and let α be a root of $f(x)$. Show that α has multiplicity greater than or equal to 2 if and only if α is also a root of $f'(x)$. You may assume that the familiar rules of differentiation still apply for polynomials with complex coefficients.

(5) Let p be a prime. Show that there are at most two solutions $\mod p$ to $x^2 \equiv a \mod p$. Show that this is not true in general for $x^2 \equiv a \mod m$, where m may not be prime, by exhibiting an explicit counterexample.

(6) Exercise A1 from Appendix A of the text.

(7) Exercise A4 from Appendix A of the text.

(8) Exercise A5 from Appendix A of the text.