Mathematics 243, section 3 – Algebraic Structures
Problem Set 5
due: October 19, 2012

'A' Section

1. Apply the division algorithm to find q, r satisfying $a = qb + r$ and $0 \leq r < b$:
   a. $a = 326$, $b = 17$
   b. $a = 1245$, $b = 249$
   c. $a = -3432$, $b = 29$

2. a. Find all the positive common divisors of $a = 240$ and $b = 450$. (Hint: Factoring a, b as much as possible may be helpful here.)
   b. What is the smallest positive element of the set
   $$S = \{240m + 450n \mid m, n \in \mathbb{Z}\}?$$
   c. Apply the Euclidean algorithm to find $\gcd(240, 450)$. What are the integers m, n such that $240m + 450n = \gcd(240, 450)$?

3. Repeat all the parts of question 2 for $a = 2312$ and $b = 584$.

'B' Section

1. Let f, g, h be permutations of a set A. In this problem, the notation $h^0 = I_A$, the identity mapping on A, and for $n \geq 1$, h^n means the n-fold composition of h with itself:
   $$h^n = h \circ h \circ \cdots \circ h \quad (n \text{ copies of } h).$$
   a. Show by mathematical induction that h^n is a permutation of A for all $n \geq 0$. You may use facts we proved before here; look back at Chapter 1 or your notes as necessary.
   b. Show that for all $n \geq 1$
   $$(f \circ g \circ f^{-1})^n = f \circ g^n \circ f^{-1}.$$

2. Let $a, b, c, d \in \mathbb{Z}$.
   a. Show that if $a|c$ and $b|d$, then $(ab)|(cd)$.
   b. Is it true that $a|(bc)$ implies $a|b$ or $a|c$? Prove or give a counterexample.
   c. Give two different proofs that $(a - b)|(a^n - b^n)$ for all $n \geq 1$, one using mathematical induction, one not using mathematical induction.
   d. Show that $(a + b)|(a^{2n} - b^{2n})$ for all $n \geq 1$.

3. Suppose $a, b > 0$ and $a = qb + r$ by the division algorithm in $\mathbb{Z}$. What are the quotient and remainder on division of $-a$ by b? Express in terms of q and r, and prove your result.
4. Show that if $a, b, c \in \mathbb{Z}$, then $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.
5. Suppose $\gcd(a, b) = 1$. Is it true that the integers m, n such that $ma + nb = 1$ guaranteed in Theorem 2.12 also satisfy $\gcd(m, n) = 1$? Prove or give a counterexample.