MATH 343, PROBLEM SET 2

ANDREW J. BLUMBERG

1. Problems

(1) Please write a computer program that performs Elgamal encryption. The input is a file "input.txt" that has p on the first line, g on the second line, m on the third line, and g^a (the value sent by Alice) on the fourth line. Output the result to "output.txt".

(2) Please write a computer program that implements the Babystep-Giantstep algorithm for solving the discrete log problem. The input is a file "input.txt" that has p on the first line, g on the second, and h on the third. Output the result to "output.txt".

(3) In this problem, you will prove Fermat's little theorem by way of Lagrange's theorem.
   (a) A subgroup H of a group G is a subset that is itself a group under the operation on G. (Notice that this means for instance that H must contain the identity and be closed under taking inverses.)
      (i) Please find the subgroups of the groups $\mathbb{Z}/5$ and $\mathbb{Z}/10$.
      (ii) Show that $m\mathbb{Z} = \{km \,|\, k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$, for any m.
   (b) For a subgroup $H \subseteq G$ and $g \in G$, the (left) coset gH is the set $\{gh \,|\, h \in H\}$.
      (i) When $G = \mathbb{Z}$, describe the (additive) cosets of the subgroups $m\mathbb{Z}$.
      (ii) When is a coset gH itself a subgroup of G?
      (iii) Prove that the union of all the cosets of H is G.
      (iv) Prove that all cosets of H have the same size.
      (v) Prove that for two cosets g_1H and g_2H, either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$.
   (c) From the work above, deduce that the order of a subgroup divides the order of a group.
   (d) From the preceding statement, deduce Fermat's little theorem.

(4) From the text: 1.36, 2.10.