# MATH 343, PROBLEM SET 4

ANDREW J. BLUMBERG

## 1. Problems

(1) Please write a program which takes as input $e$, $c$, and $p$, and solves the equation $x^e = c \mod p$.
(2) Please write a program which takes as input a composite number $N = pq$ and outputs $p$ and $q$; use Pollard's $p - 1$ algorithm.
(3) From the text: 3.5, 3.8, 3.10, 3.11, and 3.13.