Homework Assignment 4
CS 6104: Algorithmic Number Theory

Each problem in this assignment is worth 50 points. The assignment is due by 9:30AM on **June 16, 1998.** Prepare your solutions in LaTeX, preferably using this file as a starting point. You may submit your solutions in printed form or by email to `cs6104@ei.cs.vt.edu`. Explain your solution to each problem, including references to the appropriate theorems in the textbook.

Help is available by email as well as during my office hours. It is especially helpful to request clarification or hints by email to `cs6104@ei.cs.vt.edu`, so I can send the response to everyone.

The person assigned to present the solution to a problem is noted at the beginning of the problem.

Problem 1. [Wen] Chapter 6, problem 9.

Problem 2. [Craig] This problem is inspired by problem 13 in Chapter 6. For $m \geq 1$, define

$$\tau(m) \quad = \quad \frac{m}{\phi(m)},$$

where ϕ is the Euler phi function.

A. For what value of m, where $1 \leq m \leq 10,000,000$, is $\tau(m)$ maximized?

B. More generally, for what values of m (as m goes from 1 to ∞), does $\tau(m)$ reach new maxima? (A new maximum is an m such that $\tau(m') < \tau(m)$, whenever $m' < m$.)

C. Use methods from Chapter 2 to show Landau's result that $\tau(m) = O(\log \log m)$.

D. Fix a prime p. Give an asymptotic lower bound on the probability that a randomly selected polynomial in $\mathbb{F}_p[X]$ of degree n is primitive.

Problem 3. [Song] Chapter 7, problem 4. Flesh out the solution in the back of the book.

NOTE. If you are stuck on any of these problems, come see the instructor for hints.