Homework Assignment 1 (Corrected)
CS 6104: Algorithmic Number Theory

Each problem in this assignment is worth 50 points. The assignment is due by 9:30AM on May 26, 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 (if anyone) is noted at the beginning of the problem.

Problem 1. [Qin] Use the techniques in Chapter 2 to derive an asymptotic estimate for

$$h(x,k) \quad = \quad \sum_{p \le x} p^k,$$

where $k \ge 1$ is an integer. For $k \in \{1,2,3,4\}$ and $x \in \{10, 50, 100, 200\}$, use *Mathematica* to compute $h(x,k)$ precisely. Present these results in a table along with the values of your asymptotic estimates.

Problem 2. [Nick] Let R be the ring $\mathbb{Z}/(3)$, and consider the polynomial ring $R[X]$. Let $f \in R[X]$ be the polynomial

$$f(X) \quad = \quad X^2 + 3X + 2.$$

Finally, let

$$I \quad = \quad \{g(X)f(X)h(X) \mid g, h \in R[X]\}.$$

A. Prove that I is an ideal in $R[X]$.

B. Let $T = R[X]/I$. How many elements does T have? What are they?

C. Give addition and multiplication tables for T.

D. Is T a field? Why or why not?

Problem 3. [**Jeremy**] Chapter 3, Problem 8.

A. Give pseudocode for your algorithm to solve $f(x) = n$. Analyze its worst case time complexity.

B. Program your algorithm in *Mathematica* or other symbolic computation system. Include the *Mathematica* code in your solution.

C. Use your algorithm to determine whether a solution exists to

$$f(x) \quad = \quad 331104019746398614665567837536000231540518038888587048939300,$$

where $f(x)$ is this polynomial

$$14x^{17} + 99x^7 + 3x^2 + 94.$$
