Homework Assignment 2
CS 6104: Algorithmic Number Theory

Each problem in this assignment is worth 50 points. The assignment is due by 9:30AM on June 1, 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. **[John]** Chapter 4, Problem 14. You may assume the result in Problem 2.22. Use *Mathematica* to calculate the actual probability for

$$n \in \{100, 200, 300, 400, 500, 600, 700, 800, 900, 1000\}.$$

Put those results in a table that also gives the relative error if the probability is taken to be $6/\pi^2$.

Problem 2. **[Lynn]** Implement the Extended Euclidean algorithm in *Mathematica*. (*Mathematica* has the Euclidean and Extended Euclidean algorithms built in, but do not use those in your implementation.)

Let

$$\begin{aligned} c_1 &= 1717424330343597918506415 \\ c_2 &= 151412298672983368484874188480781 \\ c_3 &= 24448035656469598033595744122413. \end{aligned}$$

Show how your implementation can be used to find a solution $x, y, z \in \mathbb{Z}$ to the equation

$$c_1 x + c_2 y + c_3 z = \gcd(c_1, c_2, c_3).$$

Give the *Mathematica* steps to obtain one such solution.
