Homework 5, 550.371 Cryptology, Spring 2017

You may discuss generalities of mathematics and MATLAB with others in the class, but the solutions and code that you submit should be entirely your own. You may not look up the answers to hw questions on Wikipedia or in other textbooks, nor may you access existing solutions.

Problem 1: Write a MATLAB function that implements the Chinese Remainder Theorem result. The input is two vectors, $\vec{n}$ and $\vec{b}$, of the same length. The vector $\vec{n}$ consists of pairwise relatively prime positive integers and the vector $\vec{b}$ consists of integers. The function outputs x, the unique nonnegative integer less than the product of the entries of $\vec{n}$ such that x is congruent to each respective entry of $\vec{b}$ modulo the respective entry of $\vec{n}$. Be sure to provide several nontrivial examples to illustrate that your code is working properly; in particular, the length of $\vec{n}$ and $\vec{b}$ in your examples should be at least 5.

Problem 2:

a) Write a MATLAB function that estimates the probability ϱ that two independently selected integers are relatively prime. The input consists of positive integers M and N; your code performs the following experiment N times. It randomly selects two integers between 1 and M (each possibility equally likely) and tests if these two integers are relatively prime. If n times out of the N experiments the two random integers were relatively prime, then the desired probability estimate of ϱ is $\frac{n}{N}$.

b) Test your code when $M = 10,000,000$ and $N = 10,000,000$ to estimate ϱ.

c) Argue that the probability is $1 - \frac{1}{2^2}$ that two independently selected integers don't have common divisor 2. Argue that the probability is $1 - \frac{1}{3^2}$ that two independently selected integers don't have common divisor 3.

d) Argue that $\varrho = \prod_{p \in \mathcal{P}}(1 - \frac{1}{p^2})$, where $\mathcal{P}$ denotes the set of all prime numbers. (You may assume the truth of a certain plausible independence.)

e) Compute $\prod(1 - \frac{1}{p^2})$ over all primes p less than 10000 and compare your answer to part b. (Hint: There are 1229 such prime numbers less than 10000, and MATLAB will give you the list with the command `primes(10000)`.

Problem 3:

a) The *Reimann zeta function* is defined as $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Use MATLAB to compute $\sum_{n=1}^{10,000,000} \frac{1}{n^2}$, which will be an approximation of $\zeta(2)$. (Note: The so-called "Basel Problem" solved in the year 1735 by Euler was finding the exact value $\zeta(2) = \frac{\pi^2}{6} = 1.644934....$)

b) Prove that for any real number $s > 1$, it holds that $\zeta(s) = \prod_{p \in \mathcal{P}}(1 - \frac{1}{p^s})^{-1}$, where $\mathcal{P}$ denotes the set of all prime numbers. (Hint: Recall from calculus the *geometric series*; that is, $\sum_{i=0}^{\infty} r^i = (1-r)^{-1}$ for all r such that $|r| < 1$.)

c) Now show that $\varrho = \frac{1}{\zeta(2)}$, where ϱ is from Problem 2, and give an exact value of ϱ by using Euler's solution to the Basel Problem that $\zeta(2) = \frac{\pi^2}{6} = 1.644934....$