Homework 3, 550.371/650.471 Cryptology and Coding, Spring 2017

Important: You may discuss this homework (including MATLAB questions) with students currently in the class, with the TAs, and with me, up until the time that you do your write-up; but the solutions and code that you submit should be entirely your own. At no time may you consult any existing written solutions; this would be in violation of the homework rules and, in addition, would be plagiarism if sources are not cited..

Problem 1: Write a MATLAB function to perform the Extended Euclidean Algorithm. The input will be positive integers a, b and the output should be $\gcd(a, b)$, as well as integers x, y such that $xa + yb = \gcd(a, b)$. Hand in the .m file, as well as a diary in which you verifiably illustrate via nontrivial examples that your code is working.

Problem 2: Write a MATLAB function to compute the inverse of any integer a mod n, if a is indeed invertible. (Hint: $x \in \mathbf{Z}_n$ is the multiplicative inverse of $a \in \mathbf{Z}_n$ if xa divided by n has the remainder 1; in other words, $xa = qn + 1$ for some integer q. If we find any integers x and q that satisfy the above, then x can be easily adjusted so that $0 \leq x < n$. Use the MATLAB code from previous problem as a subroutine.) Hand in the .m file, as well as a diary in which you verifiably illustrate via nontrivial examples that your code is working.

Problem 3: [Trappe and Washington textbook, Section 3.13 on page 104, Problem 4]
a) Use the Euclidean Algorithm to compute $\gcd(30030, 257)$.
b) Using the result of part (a), and the fact that $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, show that 257 is prime.

Problem 4: [Trappe and Washington textbook, Section 3.13 on page 104, Problem 5]
a) Compute $\gcd(4883, 4369)$.
b) Factor 4883 and 4369 into products of primes.

Problem 5: [Trappe and Washington textbook, Section 3.13 on page 104, Problem 6]
a) Let $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ define the Fibonacci numbers $1, 1, 2, 3, 5, 8, \ldots$. Use the Euclidean Algorithm to compute $\gcd(F_n, F_{n-1})$ for all $n \geq 1$.
b) Find $\gcd(11111111, 11111)$.
c) Let $a = 111\cdots11$ be formed with F_n repeated 1's, and let $b = 111\cdots11$ be formed with F_{n-1} repeated 1's. Find $\gcd(a, b)$.

Problem 6:
a) (Due to F. Gobbo) Consider the polynomial $p(x) = 8x^2 - 488x + 7243$. For $x = 0, 1, 2, \ldots, 61$

compute $p(x)$ and see if its absolute value is prime. You may use MATLAB's "isprime" command.

b) (Due to E. Pegg) Consider the polynomial $p(x) = x^4 + 29x^2 + 101$. For $x = 0, 1, 2, \ldots, 19$ compute $p(x)$ and see if it is prime. You may use MATLAB's "isprime" command.

c) Prove that there does not exist a nonconstant polynomial $q(x)$ with integer coefficients such that for all positive integers x it holds that $q(x)$ is prime. Hint: Think about $q(a + b)$ if $q(a) = b$. Another hint: If a polynomial q has an infinite number of points x where $q(x)$ are all the same then q is a constant polynomial.