EE 8372 CRYPTOGRAPHY & DATA SECURITY

Homework 7 **Professor Dunham**
5 March 2020 **Due: 24 March 2020**

Review Paar and Pelzl Text: Chapter 6
Suggested Reading in Menezes, Oorschot and Vanstone: Chapter 2, section 4, 5, and 6.

1. Using the basic form of Euclid's algorithm, compute the greatest common divisor (gcd) of the pairs of numbers below. For this problem use only a hand calculator. Show every iteration step of Euclid's algorithm, *i.e.*, don't write just the answer, which is only a number. Also, for every gcd, provide the chain of gcd computations, $\gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots$.

   (a) $8,885$ and $5,331$.

   (b) $14,931$ and $6,320$.

2. Using the extended Euclidean algorithm discussed in section 6.3.2 of Paar and Pelzl, compute the greatest common divisor and the parameters s and t of the pairs of numbers below. As in the Problem 1, use only a hand calculator and show every iteration step of Euclid's algorithm.

   (a) $1,078$ and 165.

   (b) $11,025$ and 440.

3. With the extended Euclidean algorithm we finally have an efficient algorithm for finding the multiplicative inverse in Z_m that is much better than exhaustive search. Find the inverses in Z_m of the following elements a modulo m. *Note:* Inverses must again be elements in Z_m and that you can easily verify your answers.

   (a) $a = 11$, $m = 26$ (affine cipher).

   (b) $a = 35$, $m = 999$.

4. You are given $Z_2[x]/(x^7 + x + 1)$ which is isomorphic to GF(2^7). Find the multiplicative inverse of $x^5 + 1$. *Hint:* Apply the extended Euclidean algorithm using polynomials.

5. Develop formulas for $\varphi(m)$ for the special cases below:

   (a) When m is a prime.

   (b) When $m = p \cdot q$, where p and q are primes. This case is of great importance for the RSA cryptosystem. Verify your formula for $m = 21$ by finding all the positive integer n less than 21 where the$\gcd(n, 21) = 1$. You do not have to apply Euclid's algorithm.

6. Compute Euler's totient function $\varphi(n)$ for the following numbers:
   (a) 35.
   (b) 136.
   (c) 1,111.
7. Compute the inverse $a^{-1} \text{mod } (n)$ using Euler's Theorem:
   (a) $a = 3$ and $m = 7$.
   (b) $a = 7$ and $m = 12$.
   (c) $a = 3$ and $m = 40$.
8. Consider the group Z_{252} under the group operation of addition.
   (a) Using the Chinese Remainder Theorem, find all possible distinct representations of Z_{252}.
   (b) For the element $143 \in Z_{252}$, find its representation in each of the distinct representations found in part (a) of this problem.
9. Let $n = 991 \times 997 \times 1009 = 996,919,243$. Find x if the following congruent relationships hold: $x \equiv 172 \pmod{991}$, $x \equiv 900 \pmod{997}$ and $x \equiv 28 \pmod{1009}$.