EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Discussion 5M-S

1. Extended GCD and Multiplicative Inverse

Apply the extended GCD for the following, and find the multiplicative inverse of a mod m and m mod a if it exists, where (a, m) are the smaller and larger numbers respectively.

1. 15, 19

2. 69, 88

3. 38, 42

2. Chinese Remainder Theorem Using the Chinese Remainder Theorem, find the smallest positive integer solution to the following system of linear congruences.

$$x = 3 \mod 4$$
$$x = 2 \mod 3$$

1. Before using the Chinese Remainder Theorem, which of the following groups of integers should we check if they are pairwise coprime?

   $(3,2)$
   $(4,3)$

2. First, we establish the basic notation: in this problem, we have $k = 2$, $a_1 = 3$, $a_2 = 2$, $m_1 = 4$, $m_2 = 3$.

$$x = a_i \mod m_i, 1 \leq i \leq k \Leftrightarrow x = y \mod N$$

What is N?

3. Then, what are the values of $z_i = N/m_i$?

4. Now, we solve $z_i y_i \equiv 1 \mod m_i$, what is one possible solution?

5. Finally, $x \equiv a_1 y_1 z_1 + a_2 y_2 z_2 \mod N$. What is the smallest positive integer x?