EE2302 Foundations of Information and Data Engineering

Assignment 6 **Due: 11 pm, Oct 28**

Full mark: 10 points

1. (2 points) Find a value of x that solves the following simultaneous congruences:

$$x \equiv 3 \pmod{37} \text{ and } x \equiv 5 \pmod{87}.$$

2. (3 points) Find a value of x that solves the following simultaneous congruences:

$$x \equiv 5 \pmod{7},\ x \equiv 2 \pmod{12} \text{ and } x \equiv 8 \pmod{13}.$$

3. Consider the use of RSA cipher. The public key of Bob is $N = 55$ and $e = 3$.

   a) (1 point) Alice wants to send the message "HELLO" to Bob. Translate the message into its numeric equivalent (i.e. A $= 1$, B $= 2$, …).

   b) (2 points) Encrypt the message in (a) letter by letter. Show your steps.

   (Remark: In practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words.)

   c) (2 points) Suppose Bob receives a message from Claire. The ciphertext of the message is `08 05 15`. Decrypt it and translate the result into letters of the alphabet to discover the message. Show your steps.