Comp-106, Fall 2019, Questions for HW#3

Only the first 3 problems (Question 1, Question 2 and Question 3) will be graded. Do not submit the solutions for the remaining problems (though you are expected to solve them).

Please provide formal justification for all your answers to the following 4 questions in order to get full credit.

1. Exercise 30 in Chapter 4.4, 8th edition. You can use the result of Exercise 29.
(Exercise 22 in Chapter 4.4, 7th edition. You can use the result of Exercise 21.)
(Exercise 24 in Chapter 3.7, 6th edition. You can use the result of Exercise 23.)

Complete the proof of the Chinese Remainder Theorem by showing that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime integers is unique modulo the product of these moduli. [*Hint:* Assume that x and y are two simultaneous solutions. Show that $m_1 \mid x - y$ for all i. Using the result Exercise 29, conclude that $m = m_1 m_2 \ldots m_n \mid x - y$.]

2. Compute 3^{304} mod 385 by using Fermat's Little theorem and Chinese Remainder theorem.

3. Suppose Alice sends a secret message to Bob, using RSA cryptosystem. We know that her public keys are $n = 35$ and $e = 11$. You have somehow seen the encrypted message which is 12 as a number. Find the original message (as a number).

You are not supposed to submit any solutions for the remaining problems (though you are expected solve them)

4. Exercise 10 in Chapter 3.7, 6th edition (Exercise 6, Chapter 4.4, 7th edition).
Show that an inverse of a modulo m does not exist if $\gcd(a,m) > 1$.
Hint: Use proof by contradiction. Assume an inverse exists and then using the definition of modular congruence, show that it is not possible.

5. Solve the congruence $144x \equiv 5 \pmod{377}$.
Hint: First find the inverse of 144 in mod 377 (if it exists). To find the inverse, you can either reverse the steps of the Euclidean algorithm, or equivalently you can use the **extended** Euclidean algorithm described in Exercise 48 of Chapter 3.7, 6th edition. (Exercise 30, Chapter 4.3, 7th edition; you can as well find the equivalent in the 8th edition.)