Comp 106, HW#3, Fall 2018

Most of the problems below are very similar to or the same as the questions in the Number Theory chapter of your textbook. The last question is from a previous exam.

**Question 1**
Show that an inverse of \( a \) modulo \( m \) does not exist if \( \gcd(a, m) > 1 \).

*Hint:* Use proof by contradiction.

**Question 2**
Solve the congruence \( 3x \equiv 7 \pmod{17} \)

You have to find the solution using a formal procedure as we learned in the class. First find the inverse by reversing the Euclidean algorithm and then use this inverse to find the solution.

**Question 3**
Use Fermat's Little Theorem and Chinese Remainder Theorem to compute \( 3^{302} \pmod{231} \). Note that 231 = 3·7·11.

**Question 4**
Suppose that you are trying to hack the RSA cryptosystem, and the encrypted message you have somehow captured is 2299 1317 2117. Since this is a public key system, you know that \( n = 2537 \) (the modulo) and \( e = 13 \) (encryption key). Find the original message, assuming that during encryption the letters have been translated into integers and then grouped into pairs of integers as in Example 11 of your textbook, 6th edition (Example 8, 7th edition). You can get make use of a calculator (or a computer) for your computations, however you are expected to explain every step you take to find the solution.

**Question 5**
Consider the following system of congruences:

\[
\begin{align*}
x & \equiv a_1 \pmod{p} \\
x & \equiv a_2 \pmod{q}
\end{align*}
\]

where \( p \) and \( q \) are prime.

a) Show that a solution, that satisfies both congruences above, is given by \( x = a_1 \cdot q \cdot y_1 + a_2 \cdot p \cdot y_2 \), where \( y_1 \) is an inverse of \( q \) in modulo \( p \) and \( y_2 \) is an inverse of \( p \) in modulo \( q \).

b) Show that the above system of congruences has **unique** solution in modulo \( n \), where \( n = p \cdot q \).

Note that in this question you are actually asked to prove Chinese Remainder Theorem for a simpler case, so do not use Chinese Remainder Theorem.