CS314: Algorithms
Homework 10: Number theory and cryptography

1. Give formal proofs of the first theorem we used in lecture:

   Theorem: Let a, b, and c be integers. Then:

   - If $a|b$ and $b|c$, then $a|c$.
   - If $a|b$ and $a|c$, then $a|(ib + jc)$ for all integers i and j.
   - If $a|b$ and $b|a$, then $a = b$ or $a = -b$.

2. Let p be a prime. Write an efficient alternative algorithm for computing the multiplicative inverse on an element of Z_p that is not based on the Extended Euclidean Algorithm. And don't forget the proof of correctness and the runtime analysis!

3. Construct a table showing an example of the RSA crypto system with parameters $p = 17$, $q = 19$, and $e = 5$.

   For clarity, your table should have two rows, one for the plaintext M and the other for the cipher text C. Each column should be an ASCII letter/number of your message M which you encode into C. Show how you encode each letter appropriately, and feel free to be creative with your message (although please keep things civil!)