INT202 Complexity of Algorithms

1. Let us consider $Z_{28}$ the set of integers modulo 28.
    1) Give the necessary and sufficient condition required for an element of $Z_{28}$ to have an inverse in $Z_{28}$.
    2) Determine all the elements of $Z_{28}$ that have a multiplicative inverse in $Z_{28}$.
    3) Evaluate $\varphi(28)$ wherein $\varphi$ is the Euler totient function.
    4) Evaluate $4^{-1}$ and $5^{-1}$ if they exist.

2. In the RSA method, suppose that p = 5, q = 17, and e = 13. First find the private key d corresponding to these parameters. Then decrypt the ciphertext messages, C, below to find the original (plaintext) messages.

    a. C = 12

    b. C = 9

3. Alice and Bob are using the RSA algorithm to communicate. Bob's public key is e = 3 and n = 187.

    a. What is Bob's secret key?

    b. Alice wants to send the message M to Bob. Bob receives 9. What was the message M sent by Alice?

4. a. Show that 3-SAT belongs to the class NP;

    b. Reduce the CNF-SAT problem to 3-SAT;

    c. Deduce that 3-SAT is NP-Complete.