1.

1), element x : $x \iff \gcd(x, 28) = 1$

2). Z_{28}^*

3). $\phi(28)$ $\because 28 = 2^2 \times 7$

$\phi(28) = 28\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right)$

$= 28 \times \frac{1}{2} \times \frac{6}{7} = 12$

4). 4^{-1} not exist

use extended Euclidean algorithm

$5^{-1} = 17$

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 (multiplicative) all the elements of Z_{28} that have a multiplicative inverse in Z_{28}.

   3) Evaluate φ(28) wherein φ 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

4,

a), 3-SAT is in NP, if given an assignment of Bool variables, we can check CNF formula C, if C=1, $C = (C_1 \vee C_2) \wedge (\bar{C_3} \vee C_4)$ in polynome

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.

2)

$p=5, q=17, e=13$

$n = p \cdot q = 85$

$\phi(n) = (p-1)(q-1) = 64$

$ed \equiv 1 \pmod{\phi(n)}$

$d = 5$

$M = C^d \bmod n$

a), $M = 12^5 \bmod 85 = 37$

b). $M = 9^5 \bmod 85 = 59$

3)

a), $n = 187$

$p = 17, q = 11$

$\phi(n) = 160$

$ed = 1 \pmod{\phi(n)}$

$d = 107$

b), $M = C^d \bmod n$

$= 9^{107} \bmod 187$

$9^{107} = 9 \cdot 9^{106} = 9 \cdot (9^{53})^2$

$9^{53} = 9 \cdot 9^{52} = 9 \cdot (9^{26})^2$

$9^{26} = (9^{13})^2$ $9^{13} = 9 \cdot (9^6)^2$

$9^6 = (9^3)^2 = (9 \cdot 9^2)^2$

$9^1 \bmod 187 = 9$

$9^3 \bmod 187 = 729 \bmod 187 = 168$

$9^6 \bmod 187 = (168)^2 \bmod 187$

$M = 15$