Tutorial 9

1. Given a theorem: Let a and b be two integers in which at-least one is non-zero then there exists x and y such that GCD(a, b) = ax + by.
   Prove that if d = GCD(a, b) then $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.

2. Prove the following:
   (a) If $a \equiv b (\text{Mod } N)$ then $ac \equiv bc (\text{Mod } N)$
   (b) If $a \equiv b (\text{Mod } N)$ then $a^k \equiv b^k (\text{Mod } N)$ for all $k \geq 1$

3. Find the GCD of the following using Euclidean Algorithm:
   (a) (1475, 1200)
   (b) (766, 1235)

4. Find the remainder when 3^{28} is divided by 5.
   (**Note: Use the properties of congruence relation**)

5. Perform the following operations in Z_n:
   (a) Add 7 to 14 in Z_{15}.
   (b) Subtract 11 from 7 in Z_{13}.
   (c) Multiply 123 by -10 in Z_{19}.
   (**Note: Operations in Z_n can be done in this way –** $(a + b) \bmod n = c$**. Subtraction and Multiplication can also be done in the similar way**).

6. In a Multiplicative cipher, cipher text is calculated from the plaintext by the relation C= (P*k) mod 26.
   What is "hello" encoded to using the key 7.

7. In an affine cipher, the relationship between plaintext and cipher-text is given as
   C=(P*k1+k2) mod 26.
   P=(C-k2)*$k1^{-1}$) mod 26
   Use the affine cipher to encode"hello" with the key pair (7,2).

8. If a|b and a|c, then?
   a) a|bc
   b) c|a
   c) a|(b+c)
   d) b|a

9. Kamal has 6 cans of regular soda and 15 cans of diet soda. He wants to create some identical refreshment tables that will operate during the American football game. He also doesn't want to have any sodas left over. What is the greatest number of refreshment tables that Kamal can stock?

10. The linear combination of gcd (252, 198) = 18 is?
    a) 252*4 – 198*5
    b) 252*5 – 198*4
    c) 252*5 – 198*2
    d) 252*4 – 198*4

11. Find all solutions to the following linear congruences.

(a) $2x \equiv 5 \pmod 7$.
(b) $6x \equiv 5 \pmod 8$.
(c) $19x \equiv 30 \pmod{40}$.

12. How many solutions exist for :
(a) $234x \equiv 60 \pmod{762}$.
(b) $128x \equiv 833 \pmod{1001}$.