**Assignment #3**

Student #:250626065

Name: Zaid Albirawi

UWO email: [zalbiraw@uwo.ca](mailto:zalbiraw@uwo.ca)

1. Prove that if n is an integer that is not a multiple of 3, then n2 = 1 (mod 3)  
     
   Let n be an integer that is equal 1 (mod 3) \*not a multiple of 3  
     
   Therefore, there are only two cases that are not multiples of 3, 3k+1 and 3k+2, where k can be any integer. We can also discard any other cases since all the other cases can be written as a combination of these three cases.  
      
   **Case #1:** n = 3k+1  
     
   n2 = (3k+1)2n2 = (3k+1)(3k+1)  
   n2 = (3k)(3k)+3k+3k+1  
   n2 = (3k)2+3(2k)+1  
   n2 = (3k)2+3(2k)+1  
   n2 = 3(3k2)+3(2k)+1  
   n2 = 3(3k2 + 2k)+1  
     
   Therefore, since 3(3k2) and 3(2k) are both multiples of 3 then we can represent them as 3z, where z is an integer.  
     
   Therefore, n2 = 3z+1 which is not a multiple of 3.  
     
   **Case #2:** n = 3k+2  
     
   n2 = (3k+2)2n2 = (3k+2)(3k+2)  
   n2 = (3k)(3k)+2(3k)+2(3k)+4  
   n2 = (3k)2+3(4k)+4  
   n2 = (3k)2+3(4k)+4  
   n2 = 3(3k2)+3(4k)+4  
   n2 = 3(3k2 + 4k)+2(2)  
     
   Therefore, since 3(3k2) and 3(4k) are both multiples of 3 then we can represent them as 3z, where z is an integer. Also, since 4 is a multiple of 2 we can represent it as 2i, where i is an integer.  
     
   Therefore, n2 = 3z+2i which is not a multiple of 3.

Therefore, proven by cases.

* 1. GCD (580, 50)  
     580 = 50 x 11 + 30  
     50 = 30 x 1 + 20  
     30 = 20 x 1 + 10  
     20 = 10 x 2 + 0  
     Therefore, GCD (580, 50) = GCD (50, 30) = GCD (30, 20) = GCD (20, 10) = 10
  2. GCD(662, 414) = 2,
     1. 662 = 414 x 1 + 248
     2. 414 = 248 x 1 + 166
     3. 248 = 166 x 1 + 82
     4. 166 = 82 x 2 + 2
     5. 82 = 2 x 41 +

Therefore, GCD (662, 414) = GCD (414, 248) = GCD (248, 166) = GCD (166, 82) =   
GCD (82, 2) = 2. This proves that 2 is the GCD for the pair of integers (662, 414) using the Euclidean algorithm.  
Now working backwards (iv, i)

1. 2 = 166 – 2 x 82
2. 82 = 248 – 1 x 166
3. 166 = 414 – 1 x 248
4. 248 = 662 – 1 x 414

Substituting the equations to find the linear combination:

* + 1. Substitute equation 3 into equation 4  
       2 = 166 – 2 x 82 = 166 – 2 x (248 – 1 x 166)  
       2 = 166 – 2 x 248 + 2 x 166  
       2 = 3 x 166 – 2 x 248
    2. Substitute equation 2 into equation the newly obtained equation  
       2 = 3 x (414 – 1 x 248) – 2 x 248  
       2 = 3 x 414 – 3 x 248 – 2 x 248   
       2 = 3 x 414 – 5 x 248
    3. Substitute equation 1 into equation the newly obtained equation  
       2 = 3 x 414 – 5 x (662 – 1 x 414)  
       2 = 3 x 414 – 5 x 662 + 5 x 414  
       2 = 8 x 414 – 5 x 662

Therefore, the linear combination of 2 in terms of the 414 and 662 is 8 x 414 – 5 x 662.



**Binary:**

* 0 = 0000
* 1 = 0001
* 2 = 0010
* 3 = 0011
* 4 = 0100
* 5 = 0101
* 6 = 0110
* 7 = 0111
* 8 = 1000
* 9 = 1001
* A = 1010
* B = 1011
* C = 1100
* D = 1101
* E = 1110
* F = 1111
  + - 1. (11101)2 = (0001 1101)2 = (1D)16(6253)8 = (110 010 101 011)2 = (110010101011)2
      2. Sum = (101011)2 + (1101011)2  
           
          1 1 11  
         0101011  
          +  
         1101011  
         10010110  
         Therefore, (101011)2 + (1101011)2 = (10010110)2Multiplication = (101011)2 x (1101011)2  
           
          0101011  
          x  
          1101011 0000 0010 1011  
          +  
          0000 0101 0110  
          +  
          0000 1010 1100  
          +  
          0010 1011 0000  
          +  
          101 0110 0000  
          1 0001 1111 1001  
           
         Therefore, (101011)2 x (1101011)2 = (1000111111001)2



**Alphabet:**

* A = 0
* B = 1
* C = 2
* D = 3
* E = 4
* F = 5
* G = 6
* H = 7
* I = 8
* J = 9
* K = 10
* L = 11
* M = 12
* N = 13
* O = 14
* P = 15
* Q = 16
* R = 17
* S = 18
* T = 19
* U = 20
* V = 21
* W = 22
* X = 23
* Y = 24
* Z = 25
  + - 1. Message = “AHFXVHFBGZ”  
         A = (0 - 19) **mod** 26 = 7 = H  
         H = (7 - 19) **mod** 26 = 14 = O  
         F = (5 - 19) **mod** 26 = 12 = M  
         X = (23 - 19) **mod** 26 = 4 = E  
         V = (21 - 19) **mod** 26 = 2 = C  
         H = (7 - 19) **mod** 26 = 14 = O  
         F = (5 - 19) **mod** 26 = 12 = M  
         B = (1 - 19) **mod** 26 = 8 = I  
         G = (6 - 19) **mod** 26 = 13 = N  
         Z = (26 - 19) **mod** 26 = 6 = G  
           
         Therefore, the decrypted message is “HOMECOMING.”
      2. Since the encryption function for the affine cipher is   
         f(x) = (3x + 7), then the decryption function is   
         x = f’(x) (c-b) mod 26  
         where x is the decrypted character, f’(x) is the inverse of  
          3 **mod** 26, c is the encrypted character, and b is the   
         shift of the character which equals to 7. Therefore,   
           
         f’(x) = 3 **mod** 26  
         3 f’(x) = 1 **mod** 26  
         3 f’(x) = 27 = 1 in **mod** 26  
         Therefore, f’(x) = 9  
           
         Hence, x = 9 (x-7)**mod** 26 = (9x - 63) **mod** 26 = (9x+15) **mod** 26  
           
         Therefore, the decryption function is x = (9x+15) **mod** 26

1. 1 + 4 + 7 + 10 + … + (3n-2) = n (3n-1)/2, for all n>=1   
     
   **Basis Step:**  
    f(n) = n (3n-1)/2  
    f(1) = (3-1)/2 = 1  
   **Induction Step:** 1 + 4 + 7 + 10 + … + (3n-2+3) = (n+1) (3(n+1)-1)/2  
    1 + 4 + 7 + 10 + … + (3n+1) = (n+1)(3n+3-1)/2  
    1 + 4 + 7 + 10 + … + (3n+1) = (n+1)(3n+2)/2  
    1 + 4 + 7 + 10 + … + (3n+1) = (3n2 + 2n + 3n + 2)/2  
    1 + 4 + 7 + 10 + … + (3n+1) = (3n2 + 5n + 2)/2  
     
   By the induction hypothesis 1 + 4 + 7 + 10 + … + (3n-2) = n (3n-1)/2. Therefore,   
   1+ 4 + 7 + 10 + … + (3n-2) + (3n-2+3) = n (3n-1)/2 + (3n-2+3).  
     
    n (3n-1)/2 + (3n-2+3) = (3n2 + 5n + 2)/2  
    (3n2-n)/2 + (3n-2+3)(2/2) = (3n2 + 5n + 2)/2  
    (3n2-n)/2 + 2(3n+1)/2 = (3n2 + 5n + 2)/2  
    (3n2-n + 6n+2)/2 = (3n2 + 5n + 2)/2  
    (3n2-n + 6n+2)/2 = (3n2 + 5n + 2)/2  
    (3n2 + 5n + 2)/2 = (3n2 + 5n + 2)/2  
     
   Therefore, LS = RS, (3n2-5n+2)/2 = (3n2-5n+2)/2. 1 + 4 + 7 + 10 + … + (3n-2) = n (3n-1)/2, for all n>=1.