

### Assignment #3

Student #: [REDACTED]

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  $n^2 \equiv 1 \pmod{3}$

Let  $n$  be an integer that is equal  $1 \pmod{3}$  \*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:**  $n = 3k+1$

$$\begin{aligned}n^2 &= (3k+1)^2 \\n^2 &= (3k+1)(3k+1) \\n^2 &= (3k)(3k) + 3k + 3k + 1 \\n^2 &= (3k)^2 + 3(2k) + 1 \\n^2 &= (3k)^2 + 3(2k) + 1 \\n^2 &= 3(3k^2) + 3(2k) + 1 \\n^2 &= 3(3k^2 + 2k) + 1\end{aligned}$$

Therefore, since  $3(3k^2)$  and  $3(2k)$  are both multiples of 3 then we can represent them as  $3z$ , where  $z$  is an integer.

Therefore,  $n^2 = 3z+1$  which is not a multiple of 3.

**Case #2:**  $n = 3k+2$

$$\begin{aligned}n^2 &= (3k+2)^2 \\n^2 &= (3k+2)(3k+2) \\n^2 &= (3k)(3k) + 2(3k) + 2(3k) + 4 \\n^2 &= (3k)^2 + 3(4k) + 4 \\n^2 &= (3k)^2 + 3(4k) + 4 \\n^2 &= 3(3k^2) + 3(4k) + 4 \\n^2 &= 3(3k^2 + 4k) + 2(2)\end{aligned}$$

Therefore, since  $3(3k^2)$  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,  $n^2 = 3z+2i$  which is not a multiple of 3.

Therefore, proven by cases.

2.

a. GCD (580, 50)

$$580 = 50 \times 11 + 30$$

$$50 = 30 \times 1 + 20$$

$$30 = 20 \times 1 + 10$$

$$20 = 10 \times 2 + 0$$

$$\text{Therefore, GCD (580, 50) = GCD (50, 30) = GCD (30, 20) = GCD (20, 10) = 10}$$

b. GCD(662, 414) = 2,

$$\text{i. } 662 = 414 \times 1 + 248$$

$$\text{ii. } 414 = 248 \times 1 + 166$$

$$\text{iii. } 248 = 166 \times 1 + 82$$

$$\text{iv. } 166 = 82 \times 2 + 2$$

$$\text{v. } 82 = 2 \times 41 +$$

Therefore,  $\text{GCD (662, 414) = GCD (414, 248) = GCD (248, 166) = GCD (166, 82) = \text{GCD (82, 2) = 2}$ . This proves that 2 is the GCD for the pair of integers (662, 414) using the Euclidean algorithm.

Now working backwards (iv, i)

$$\text{iv. } 2 = 166 - 2 \times 82$$

$$\text{iii. } 82 = 248 - 1 \times 166$$

$$\text{ii. } 166 = 414 - 1 \times 248$$

$$\text{i. } 248 = 662 - 1 \times 414$$

Substituting the equations to find the linear combination:

i. Substitute equation 3 into equation 4

$$2 = 166 - 2 \times 82 = 166 - 2 \times (248 - 1 \times 166)$$

$$2 = 166 - 2 \times 248 + 2 \times 166$$

$$2 = 3 \times 166 - 2 \times 248$$

ii. Substitute equation 2 into equation the newly obtained equation

$$2 = 3 \times (414 - 1 \times 248) - 2 \times 248$$

$$2 = 3 \times 414 - 3 \times 248 - 2 \times 248$$

$$2 = 3 \times 414 - 5 \times 248$$

iii. Substitute equation 1 into equation the newly obtained equation

$$2 = 3 \times 414 - 5 \times (662 - 1 \times 414)$$

$$2 = 3 \times 414 - 5 \times 662 + 5 \times 414$$

$$2 = 8 \times 414 - 5 \times 662$$

Therefore, the linear combination of 2 in terms of the 414 and 662 is  $8 \times 414 - 5 \times 662$ .

3.

- a.  $(11101)_2 = (0001\ 1101)_2 = (1D)_{16}$   
 $(6253)_8 = (110\ 010\ 101\ 011)_2 = (110010101011)_2$   
 b. Sum =  $(101011)_2 + (1101011)_2$

```

    1 1 1 1
0101011
      +
1101011
10010110
Therefore,  $(101011)_2 + (1101011)_2 = (10010110)_2$ 

```

Multiplication =  $(101011)_2 \times (1101011)_2$

```

      0101011
        x
      1101011
0000 0010 1011
      +
0000 0101 0110
      +
0000 1010 1100
      +
0010 1011 0000
      +
101 0110 0000
1 0001 1111 1001

```

Therefore,  $(101011)_2 \times (1101011)_2 = (1000111111001)_2$

**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

4.

**Alphabet:**

a. Message = "AHFXVHFBGZ"

$$\begin{aligned}
 A &= (0 - 19) \bmod 26 = 7 = H \\
 H &= (7 - 19) \bmod 26 = 14 = O \\
 F &= (5 - 19) \bmod 26 = 12 = M \\
 X &= (23 - 19) \bmod 26 = 4 = E \\
 V &= (21 - 19) \bmod 26 = 2 = C \\
 H &= (7 - 19) \bmod 26 = 14 = O \\
 F &= (5 - 19) \bmod 26 = 12 = M \\
 B &= (1 - 19) \bmod 26 = 8 = I \\
 G &= (6 - 19) \bmod 26 = 13 = N \\
 Z &= (26 - 19) \bmod 26 = 6 = G
 \end{aligned}$$

Therefore, the decrypted message is "HOMECOMING."

b. Since the encryption function for the affine cipher is

$f(x) = (3x + 7)$ , then the decryption function is

$$x = f'(x) (c - b) \bmod 26$$

where  $x$  is the decrypted character,  $f'(x)$  is the inverse of

$3 \bmod 26$ ,  $c$  is the encrypted character, and  $b$  is the shift of the character which equals to 7. Therefore,

$$f'(x) = 3 \bmod 26$$

$$3 f'(x) = 1 \bmod 26$$

$$3 f'(x) = 27 = 1 \bmod 26$$

Therefore,  $f'(x) = 9$

$$\text{Hence, } x = 9 (x - 7) \bmod 26 = (9x - 63) \bmod 26 = (9x + 15) \bmod 26$$

Therefore, the decryption function is  $x = (9x + 15) \bmod 26$

-	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

5.  $1 + 4 + 7 + 10 + \dots + (3n-2) = n(3n-1)/2$ , for all  $n \geq 1$

**Basis Step:**

$$f(n) = n(3n-1)/2$$

$$f(1) = (3-1)/2 = 1$$

**Induction Step:**

$$1 + 4 + 7 + 10 + \dots + (3n-2+3) = (n+1)(3(n+1)-1)/2$$

$$1 + 4 + 7 + 10 + \dots + (3n+1) = (n+1)(3n+3-1)/2$$

$$1 + 4 + 7 + 10 + \dots + (3n+1) = (n+1)(3n+2)/2$$

$$1 + 4 + 7 + 10 + \dots + (3n+1) = (3n^2 + 2n + 3n + 2)/2$$

$$1 + 4 + 7 + 10 + \dots + (3n+1) = (3n^2 + 5n + 2)/2$$

By the induction hypothesis  $1 + 4 + 7 + 10 + \dots + (3n-2) = n(3n-1)/2$ . Therefore,  
 $1 + 4 + 7 + 10 + \dots + (3n-2) + (3n-2+3) = n(3n-1)/2 + (3n-2+3)$ .

$$n(3n-1)/2 + (3n-2+3) = (3n^2 + 5n + 2)/2$$

$$(3n^2-n)/2 + (3n-2+3)(2/2) = (3n^2 + 5n + 2)/2$$

$$(3n^2-n)/2 + 2(3n+1)/2 = (3n^2 + 5n + 2)/2$$

$$(3n^2-n + 6n+2)/2 = (3n^2 + 5n + 2)/2$$

$$(3n^2-n + 6n+2)/2 = (3n^2 + 5n + 2)/2$$

$$(3n^2 + 5n + 2)/2 = (3n^2 + 5n + 2)/2$$

Therefore,  $LS = RS$ ,  $(3n^2-5n+2)/2 = (3n^2-5n+2)/2$ .  $1 + 4 + 7 + 10 + \dots + (3n-2) = n(3n-1)/2$ , for all  $n \geq 1$ .