Gloire Rubambiza - MTH 312 - Assignment 1 Reflection

1. What went well

- I am good at encrypting/decrypting messages using the Vigenere Cipher
- Except for one careless mistake in calculations, I am confident in my ability to convert between bases
- I did not fall prey to the mistake of adding spaces and/or adding letters when none are needed in the columnar transposition. There are still areas of improvement (read on).

2. Areas of improvement

- I had a misconception about the greatest common factor (gcf) when it's not 1. Instead, I chose the smallest positive common factor.
- I need to read instructions more carefully and avoid carelessness in calculations (6(f))
- I am still struggling with modular arithmetic involving not only negative numbers, but also additive inverses.
  - I misunderstood and misinterpreted the results of modular arithmetic.
    - For instance, on question 3(b), I thought since I can find the nearest factor of 7 going in the negative direction from 0, whatever number was added/subtracted is the answer. Hence, my *wrong* answer of (13-67) mod 7 = 6.
    - This misconception is perpetuated to the Extended Euclidean Algorithm, too. In question 5(a), I thought finding the multiplicative inverse from the second to last step is the final answer not matter the sign of the answer, not realizing that a negative answer had to be operated on i.e -7 mod 26 to get 19.
    - **Deeper connection:** the misconception was reinforced in the *"send an encrypted message"* assignment where I got a negative number as the multiplicative inverse (-13), and plugged it into my Python program. Since the decrypted message using -13 was legible and sensible, I missed the connection that the multiplicative inverse is actually -13 mod 59 = 46. However, the light bulb went on in class as we went through the assignment and I thought back to the comment from my assignment partner to either get (-13) or (46) as the multiplier.
  - In regards to additive inverses, I keep falling for the trick of asking the wrong question. In other words, asking *"what do we need to subtract to get a factor of the modulus?"* instead of *"what do we need to add and perform a modulo operation to get 0?"*
- I need to be careful when doing columnar transposition by not writing across columns AND reading across columns

Gloire Rubambiza
MTH 312-01
02/11/2018

In-class Assessment 1 - Revisions

1-c) 126 = $1 \cdot 2 \cdot \boxed{3 \cdot 3} \cdot 7$ 135 = $1 \cdot \boxed{3 \cdot 3} \cdot 5$

Greatest common factor of 126 and 135 = 9

2-c) $64 - 2 \cdot 25 = 14$

$25 - 1 \cdot 14 = 11$

$14 - 1 \cdot 11 = 3$

$11 - 3 \cdot 3 = 2$

$3 - 1 \cdot 2 = 1$

$2 - 2 \cdot 1 = 0$

$\Rightarrow \gcf(64, 25) = 1$

3-b) $(13 - 67) \bmod 7$

$= (-54) \bmod 7$

$= (-8 \cdot 7 + 2) \bmod 7$

$\Rightarrow (13 - 67) \bmod 7 = 2$

4-a) The additive inverse of 12 modulo 77 = 65 because $(65 + 12) \bmod 77 = 0$

b) The additive inverse of 45 mod 8 = 3 because $(45 + 3) \bmod 8 = 0$

Gloire Rubambiza
MTH 312-01
02/11/2018

In-Class Assessment 1 – Revisions

5. a) The multiplicative inverse of 11 mod 26 exists if the greatest common factor of 26 and 11 is 1.

$$\begin{bmatrix}26\\1\\0\end{bmatrix} - 2\begin{bmatrix}11\\0\\1\end{bmatrix} = \begin{bmatrix}4\\1\\-2\end{bmatrix}$$

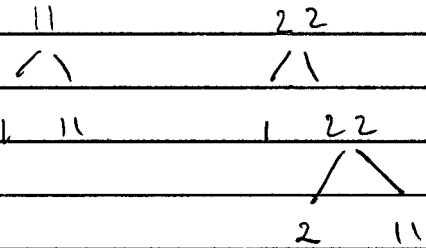
$$\begin{bmatrix}11\\0\\1\end{bmatrix} - 2\cdot\begin{bmatrix}4\\1\\-2\end{bmatrix} = \begin{bmatrix}3\\-2\\5\end{bmatrix}$$

$$\begin{bmatrix}4\\1\\-2\end{bmatrix} - 1\begin{bmatrix}3\\-2\\5\end{bmatrix} = \begin{bmatrix}1\\3\\-7\end{bmatrix} \Rightarrow 1 = 3\cdot 26 + (-7)\cdot 11$$

$$\begin{bmatrix}3\\-2\\5\end{bmatrix} - 3\begin{bmatrix}1\\3\\-7\end{bmatrix} = \begin{bmatrix}0\\-11\\26\end{bmatrix}$$

$\Rightarrow$ The multiplicative inverse of 11 mod 26 = $-7 \bmod 26 = 19$

5. b)



$\Rightarrow$ 11 mod 22 does not have a multiplicative inverse because their greatest common factor is 11 i.e. not 1.

Gloire Rubambiza
MTH 312 -01
02/11/2018.

In-Class Assessment 1 - Revisions

6.a) Convert the decimal number $(985)_{10}$ to octal

$985 = 123 \cdot 8 + 1$

$123 = 15 \cdot 8 + 3$

$15 = 1 \cdot 8 + 7$

$1 = 0 \cdot 8 + 1$

$\Rightarrow (985)_{10} = (1731)_8$

6.b) Convert the decimal number $(985)_{10}$ to binary

ref 6a) $985_{10} = 1731_8$

$\Rightarrow 1731_8 = 001\ 111\ 011\ 001_2$

6.e) Convert the decimal number $(3725)_{10}$ to hexadecimal (base 16)

$3725 = 232 \cdot 16 + 13$

$232 = 14 \cdot 16 + 8$

$14 = 0 \cdot 16 + 14$

$\Rightarrow (3725)_{10} = E8D$

6.f) Convert the hexadecimal number $0xA3C2$ to decimal

$A3C2 = 10 \cdot 16^3 + 3 \cdot 16^2 + 12 \cdot 16^1 + 2 \cdot 16^0$

$= 10 \cdot 4096 + 768 + 192 + 2$

$= 41,922$

Gloire Rubambiza
MTH 312 - 01
02/11/2018

In-class Assessment 1 - Revisions

8. a)

J	U	N	G	L	E
K	E	E	P	C	A
L	M	A	N	D	C
I	P	E	R	O	N

E	G	J	L	N	U
A	P	K	C	E	E
C	N	L	D	A	M
N	R	I	O	E	P

Encoded message: ACNPNRKLICDOEAEEMP

JUNGLE

6

E	G	J	L	N	U
C	R	F	S	U	O
D	A	O	N	E	R
Y	E	S	N	V	E
S	S	E	I	R	A
T	N	A	G	O	L
		I		E	M

J	U	N	G	L	E
F	O	U	R	S	C
O	R	E	A	N	D
S	E	V	E	N	Y
E	A	R	S	I	S
A	L	O	N	G	T
I	M	E			

Decrypted message: four score and seven years is a long time.