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