Math Circles: Affine Shift Ciphers

Recall that the first step of encrypting a message using a shift cipher (or an affine shift cipher...) is to associate each letter to a number mod 27 as shown below.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z	space
14	15	16	17	18	19	20	21	22	23	24	25	26

1. (4 points) Let's start with a shift cipher. Suppose that plaintext is encrypted with the function $x + 13 \equiv y \pmod{27}$ where x is the unencrypted letter and y is the encrypted letter.

   (a) (2 point) What is the decryption function? Please write your answer as $y - b \equiv x \pmod{27}$ where $0 \leq b \leq 26$.

   (b) (2 points) Decrypt the ciphertext RGYRD. Please write all numbers in least nonnegative residue form.

CIPHERTEXT	R	G	Y	R	D
Numbers y					
$y - c \pmod{27}$					
PLAINTEXT					

2. (8 points) Now let's try an affine shift cipher. Suppose that plaintext is encrypted with the function $14x + 3 \equiv y \pmod{27}$.

   (a) (3 points) What is the decryption function? Please write your answer as $a \cdot (y - b) \equiv x \pmod{27}$ for some integers a, b such that $0 \leq a \leq 26$ and $0 \leq b \leq 26$.

(b) (5 points) Decrypt the ciphertext FNEWHS. Please write each number in least nonnegative residue form.

CIPHERTEXT	F	N	E	W	H	S
Numbers y						
$a \cdot (y - b) \pmod{27}$						
PLAINTEXT						

3. (2 points) Suppose that a message is encrypted with the function $10x + 12 \equiv y \pmod{27}$. Find the decryption function $a \cdot (y - b) \equiv x \pmod{27}$ where $0 \leq a \leq 26$ and $0 \leq b \leq 26$ are integers.

4. (4 points) When working with affine shift ciphers, it's important to encrypt with a function $ax + b \equiv y \pmod{m}$ where $\gcd(a, m) = 1$. Let's see why. Suppose that you are told that the encryption function was $6x + 3 \equiv y \pmod{27}$. Find all letters that encrypt to S under this encryption function.