Solutions to HW Set 1

Math 1350

Problem set 1

1. ROMANS becomes ZWUIVA under a shift of 8.

2. Undoing the shift of 5 gives BIOGRAPHY

3. (look to the 2 and 3 letter words! OF becomes WN under a shift of 8, so undo 8 yields)
   WILLIAM SHAKESPEARE WROTE A PLAY ABOUT THE TRAGIC DEATH OF JULIUS CAESAR

4. (b) composing a shift of 9 and a shift of 17 gives a composite shift of $26 \equiv 0 \pmod{26}$.

   From the text book:
   Section 1.2

1. (a) $f(\mathrm{A})=\mathrm{M}$, $f(\mathrm{V})=\mathrm{R}$.
   (b) For the values Y,Z, the function is "the identity" (meaning it gives its input as output, without changing it)
   (c) f is one-to-one since each letter appears exactly once in the rows

giving the $f(x)$ values. Rearranging these so the output is in alphabetical order we see the inverse function:

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$f^{-1}(x)$	G	M	N	O	L	P	Q	I	B	R	S	K	A

x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$f^{-1}(x)$	T	J	F	U	V	W	D	E	X	H	C	Y	Z

(d)

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$f^2(x)$	B	H	V	N	Q	F	M	S	W	D	E	U	I

x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$f^2(x)$	X	T	P	A	O	L	C	G	J	K	R	Y	Z

2. (a) ATHEMATICSMAY ISAY ETHAY ANGUAGELAY OFAY ECRETSAY ITINGWRAY

(b) No. Although the domain of definition is not explicitly stated (is it defined for all combinations of words or only English words?) one finds examples where two distinct words are sent to one. SOUR and OURS is one such example.

(c) OMPOSELAYAY OURSELFYAYAY

Section 2.1

3. (a) 127=126+1=18*7+1, so q=18, r=1.

   (d) 3=0*14 + 3, so q=0, r=3.

   (e) -43=-11*4+1, so q=-11, r=1

   (f) -123=-1*124+1, so q=-1, r=1

4. (a) 2

   (b) 0

   (c) 4

   (d) 14

6. (a) $9+26k$ for any integer k.

   (b) $2+4k$ for any integer k.

10. This is the familiar shift cipher. It yields
    POFNLETZY TD ESP ACZGTDZY QZC ZWO LRP

12. When you come to a fork in the road, take it.

8.(optional) The operation MOD m adds a (possibly negative) multiple of m to the argument it is given (i.e., to the letter before "MOD") so that the resulting sum is non-negative and as small as possible. Since adding multiples of m does not change the value (mod m), this explains why the 3 expressions are all true, given $a \equiv b(mod m)$. In the last one both

expressions are between 0 and m-1, and they are equivalent (mod m), so they are the same.

15.(optional) Glancing at some frequent letters that appear, with their frequency (count, really): G 5, T 5, D 7, H 9, I 11, which may be enough to solve it. If I becomes E, the shift is by 4, and the first block reads
ACZDA
so this can't be right. Next in frequency is T, which gives a shift, T-¿ I, of 15. Decrypting thusly, we find the message
PROSPERITY IS NOT WITHOUT MANY FEARS AND DISTASTES AND ADVERSITY IS NOT WITHOUT COMFORTS AND HOPES