

MATH 1350, FALL 2010  
SOLUTIONS TO SELECTED (UNGRADED) PROBLEMS OF HW 2

1. PAGE 66–69

1. (a) Let's write the encoded text in numbers, with **A** corresponding to 0, **B** corresponding to 1, and so on.

Let's see how to do this for the first word **HOLYLV**

7 14 11 24 11 21

Caesar cipher is a 3-shift. So to decipher the message, we use a 23-shift, or a  $-3$ -shift, which is the shift needed to "cancel" the 3-shift used in Caesar cipher. We obtain.

4 11 21 8 18,

which corresponds to **ELVIS**. Proceeding in the same manner for the rest of the words, we obtain

ELVIS WAS SIGHTED AT MAIN AND UNION

(b) The message is

PRESIDENTAL CONGRESS REACH BUDGET AGREEMENT

8. If  $a \equiv b \pmod{m}$ , then  $a - b = mk$ , or equivalently  $a = mk + b$  for some integer  $k$ . Then

(a) Express  $b = mq + r$  with  $r = b \pmod{m}$ . Then

$$a = mk + b = mk + mq + r.$$

So  $a - r = m(k + q)$  is a multiple of  $m$ . In other words,  $a \equiv (b \pmod{m}) \pmod{m}$

(a) Express  $a = mq' + r'$  with  $r' = a \pmod{m}$ . Then

$$mq' + r' = mk + b.$$

So  $r' - b = m(k - q')$  is a multiple of  $m$ . In other words,  $a \pmod{m} \equiv b \pmod{m}$ .

(c)  $a = mk + b$ , and so  $a \text{ MOD } m = b \text{ MOD } m$  ( $a$  and  $b$  have the same remainder mod  $m$ ).

**12.** Let's write the ciphered text in numbers, with A corresponding to 0, B corresponding to 1, and so on.

Let's see how to do this for the first word OZWF. The corresponding numbers are

$$14 \ 25 \ 22 \ 5$$

Since a 18-shift has been used, one may use an 8-shift to decode, since  $18 + 8 = 26 \equiv 0 \pmod{26}$ . Doing so with the first word we obtain

$$22 \ 7 \ 4 \ 13,$$

which corresponds to WHEN. Proceeding as indicated for the rest of the message, we obtain:

WHEN YOU COME TO A FORK IN THE ROAD TAKE IT.

## 2. PAGE 80–82

**8.** Since the formula  $y = (11x + 8) \pmod{26}$  was used to encode the message, we need to get an expression for  $x$  in terms of  $y$  to decode it.

Notice that  $y - 8 = 11x \pmod{26}$ . Moreover, notice that  $11^{-1} = 19$ , since  $11 \times 19 = 209 \equiv 1 \pmod{26}$ . Thus

$$19 \times (y - 8) = x \quad \text{or} \quad x = 19y - 22.$$

Now we plug-in the numbers corresponding to the letters in the message (0 corresponds to A, 1 corresponds to B and so on). We obtain

IMAGINATION IS MORE IMPORTANT THAN KNOWLEDGE.