

MATH 1350-SPRING 2009  
Worksheet on Decimation Ciphers  
Friday, Jan. 30

1. Complete the following table of inverses modulo 26:

$a$	1	3	5	7	9	11	15	17	19	21	23	25
$a^{-1} \pmod{26}$	1	9	21	15	3	19	7	23	11	5	17	25

**Exercise:** Verify that  $3 \cdot 9 = 1 \pmod{26}$ ,  $5 \cdot 21 = 1 \pmod{26}$ , and so on.

2. (a) Find  $5^{-1} \pmod{17}$ .

**Solution:** Since 5 and 17 are relatively prime, Theorem 2.2.2 (p.74) implies that the inverse of 5 modulo 17 exists. To find it, we apply the brute force method to find an integer  $x$  between 1 and 17 such that

$$5x \equiv 1 \pmod{17}.$$

We have

$x$	$5x$	$5x \pmod{17}$
1	5	5
2	10	10
3	15	15
4	20	3
5	25	8
6	30	13
7	35	1

Since we see that  $5 \cdot 7 = 35 \equiv 1 \pmod{17}$ , we stop and conclude that  $5^{-1} \pmod{17} = 7$ .

- (b) Find  $16^{-1} \pmod{17}$ .

**Solution:** Since 16 and 17 are relatively prime, Theorem 2.2.2 (p.74) implies that the inverse of 16 modulo 17 exists. To find it, we write  $16x = 17x - x$  and note that

$$16x = 17x - x \equiv -x \pmod{17}.$$

Thus, it suffices to find the smallest positive integer  $x$  such that

$$-x \equiv 1 \pmod{17}.$$

Multiplying the above equation by  $-1$  (and applying equation (2.3), p. 69 with  $a = b = -1$ ,  $c = -x$ ,  $d = 1$  and  $m = 17$ ) we obtain

$$x \equiv -1 \pmod{17}.$$

Obviously,  $-1$  is a solution of the above congruence, and so are  $-18, 16, 33, 50, \dots$ . The smallest positive solution is 16 and so  $16^{-1} \pmod{17} = 16$ .

**Exercise.** More generally, show that if  $m > 1$ , then

$$(m-1)^{-1} \pmod{m} = m-1.$$

3. A ciphertext was enciphered using a decimation cipher. We guess that the ciphertext letter T corresponds to the plaintext letter J. If this guess is correct, what is the deciphering multiplier (deciphering key)?

**Solution:** Let  $y$  be the numerical equivalent of the ciphertext, let  $x$  be the numerical equivalent of the plaintext. Let

$$y = kx \text{ MOD } 26$$

be the enciphering formula. Since  $\mathcal{C}_T = \mathcal{P}_J$  from the hypothesis, and since the numerical equivalents of T and J are 19 and 9, respectively, we have to solve the congruence

$$19 = 9k \text{ MOD } 26 \quad \text{or, equivalently,} \quad 9k = 19 \text{ MOD } 26.$$

Since  $9^{-1} \pmod{26} = 3$ , multiplying the above equation by 3 gives us:

$$k = 3 \cdot 19 = 57 \equiv 5 \pmod{26},$$

and so  $k = 5$ . Therefore, the deciphering multiplier is  $5^{-1} \pmod{26} = 21$ .

4. A ciphertext was enciphered using a decimation cipher.

- (i) Is it possible for the ciphertext letter M to correspond to the plaintext letter T? If so, find the enciphering multiplier (enciphering key). If not, explain.

**Solution:** No, it is not. Indeed, let  $y$  be the numerical equivalent of the ciphertext, let  $x$  be the numerical equivalent of the plaintext. Let

$$y = kx \text{ MOD } 26$$

be the enciphering formula. Since  $\mathcal{C}_M = \mathcal{P}_T$  from the hypothesis, and since the numerical equivalents of M and T are 12 and 19, respectively, we have to solve the congruence

$$12 = 19k \text{ MOD } 26 \quad \text{or, equivalently,} \quad 19k = 12 \text{ MOD } 26.$$

Since  $19^{-1} \pmod{26} = 11$ , multiplying the above equation by 11 gives us:

$$k = 11 \cdot 12 = 132 \equiv 2 \pmod{26}.$$

Since 2 is not a possible decimation key, the ciphertext letter M cannot correspond to the plaintext letter T in a decimation cipher.

- (ii) Is it possible for the ciphertext letter M to correspond to the plaintext letter N? If so, find the enciphering multiplier (enciphering key). If not, explain.

**Solution:** No, it is not. Indeed, let  $y$  be the numerical equivalent of the ciphertext, let  $x$  be the numerical equivalent of the plaintext. Let

$$y = kx \text{ MOD } 26$$

be the enciphering formula. Since  $\mathcal{C}_M = \mathcal{P}_N$  from the hypothesis, and since the numerical equivalents of M and N are 12 and 13, respectively, we have to solve the congruence

$$12 = 13k \text{MOD } 26 \quad \text{or, equivalently,} \quad 13k = 12 \text{MOD } 26.$$

We note that 13 is not invertible modulo 26, so we argue as follows: if there is a solution  $k$  to the above equation, then

$$13k - 12$$

must be divisible by 26 and hence by 13 (since 13 divides 26). That is, we must have

$$13k - 12 \equiv 0 \pmod{13}.$$

But

$$13k - 12 \equiv -12 \not\equiv 0 \pmod{13},$$

and so the ciphertext letter M cannot correspond to the plaintext letter N in a decimation cipher.

- (iii) Is it possible for the ciphertext letter M to correspond to the plaintext letter E? If so, find the enciphering multiplier (enciphering key). If not, explain.

**Solution:** Yes, it is. Indeed, let  $y$  be the numerical equivalent of the ciphertext, let  $x$  be the numerical equivalent of the plaintext. Let

$$y = kx \text{MOD } 26$$

be the enciphering formula. Since  $\mathcal{C}_M = \mathcal{P}_E$  from the hypothesis, and since the numerical equivalents of M and E are 12 and 4, respectively, we have to solve the congruence

$$12 = 4k \text{MOD } 26 \quad \text{or, equivalently,} \quad 4k = 12 \text{MOD } 26.$$

We note that 4 is not invertible modulo 26, so we argue as follows: if there is a solution  $k$  to the above equation, then

$$4k - 12$$

must be divisible by 26. Since  $4k - 12 = 2 \cdot (2k - 6)$  and  $26 = 2 \cdot 13$ ,

$$2k - 6$$

must be divisible by 13. That is, we must have

$$2k \equiv 6 \pmod{13}.$$

Applying the brute force method we easily see that  $2^{-1} \text{MOD } 13 = 7$  (because  $2 \cdot 7 = 14 \equiv 1 \pmod{13}$ ). Multiplying both parts of the above equation by 7, we get

$$k \equiv 7 \cdot 6 \equiv 42 \equiv 3 \pmod{13},$$

and so the ciphertext letter M corresponds to the plaintext letter E in the decimation cipher  $y = 3x \text{MOD } 26$ .

5. The ciphertext

CFQGE KAZEMF ZMAGVMC NMO VYSV

was enciphered using a decimation cipher. Decipher it.

**Solution.** This is example 2.2.1, pp. 71-73 from the textbook “Invitation to Cryptology” by Thomas Barr. See also example 4(iii) of Feb. 4’s handout.