# Section 2.1: Shift Ciphers and Modular Arithmetic

Practice HW from Barr Textbook (not to hand in)
p.66 # 1, 2, 3-6, 9-12, 13, 15

The purpose of this section is to learn about modular arithmetic, which is one of the fundamental mathematical concepts we will need to implement the cryptographical techniques that we will study this semester. Afterwards, we will introduce basic concepts in cryptography and illustrate a basic cryptographical involving shift ciphers.

## Modular Arithmetic

In grade school, we first learned how to divide numbers.

**Example 1:** Consider $40 \div 3 = \frac{40}{3}$ **.** Determine the quotient and remainder and write the result as an equation.

**Solution:**

The previous example illustrates a special case of the division algorithm which we state next. Before stating this algorithm, recall that the integers are the numbers in the following set:

Integers: $\{\ldots -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ \ldots\}$

**Division algorithm:** Let $m$ be a positive integer ( $m > 0$ ) and let $b$ be any integer. Then there is exactly one pair of integers $q$ (called the *quotient*) and $r$ (called the *remainder*) such that

$$b = qm + r \quad \text{where } 0 \le r < m .$$

A number of primary interest in this class will be the remainder $r$ that we obtain the division of two numbers. We will find the remainder so often that we use a special term that is used to describe its computation. This is done in the following definition.

**Definition**: We say that $r$ is equal to $b$ MOD $m$, written as $r = b$ MOD $m$, if $r$ is the integer remainder of $b$ divided by $m$. We define the variable $m$ as the modulus.

**Example 2:** Determine 25 MOD 7, 31 MOD 5, 26 MOD 2, and 5 MOD 7.

**Solution:**

**Note**: In the division algorithm, the remainder $r$ is non-negative, that is, $r \ge 0$ This fact means that when doing modular arithmetic that we will never obtain a negative remainder. To compute $b$ MOD $m$ when $b < 0$ correctly, we must always look for the largest number that $m$ evenly divides that is less than $b$. The next example illustrates this fact.

**Example 3:** Compare computing 23 MOD 9 with -23 MOD 9.

**Solution:**

**Doing Modular Arithmetic For Larger Numbers With A Calculator**

To do modular arithmetic with a calculator, we use the fact from the division algorithm that

$$b = qm + r\ ,$$

and solve for the remainder to obtain

$$r = b - qm\ .$$

We put this result in division tableau format as follows:

$$\begin{array}{r} q \quad \leftarrow \text{ Truncated Quotient (chop digits to right of decimal)} \\ m\overline{)\ b} \\ -qm \\ \hline b - qm = r \quad \leftarrow \text{ Remainder} \end{array} \qquad (1)$$

**Example 4**: Compute 1024 MOD 37:

**Solution:**

**Example 5:** Compute 500234 MOD 10301

**Solution:**

**Example 6:** Compute -3071 MOD 107

**Solution:**

**Generalization of Modular Arithmetic**

In number theory, modular arithmetic has a more formal representation which we now give a brief description of. This idea can be expressed with the following example.

**Example 7:** Find solution)s *b* to the equation

$$b \text{ MOD } 7 = 4$$

**Solution:**

The numbers $\{\ldots, -17, -10, -3, 4, 11, 18, 25, 32, \ldots\}$ from the previous example that give a remainder of 4 MOD 7 represents a congruence class. We define this idea more precisely in the following definition.

**Definition:** Let $m$ be a positive integer (the modulus of our arithmetic). Two integers $a$ and $b$ are said to be congruent modulo $m$ if $a - b$ is divisible by $m$. We write

$$a \equiv b \mod m \quad \text{(note the lower case "mod")}$$

**Note:** The previous definition can be thought of more informally as follows. We say that $a \equiv b \mod m$ if $a$ and $b$ give the same integer remainder $r$ when divide by $m$. That is,

$$a \equiv b \mod m \text{ if } r = a \text{ MOD } m = b \text{ MOD } m.$$

The following example illustrates this idea:

**Example 8:** Illustrate why $25 \equiv 11 \mod 7$.

**Solution:**

The last example illustrates that when the uppercase MOD notation is used, we are interested in only the specific integer remainder $r$ when a number is divided by a modulus. The lowercase mod notation with the $\equiv$ notation is used when we are looking for a set of numbers that have the same integer remainder when divided by a modulus. In this class, we will primarily use the MOD notation.

***Note:** When considering $b$ MOD $m$, since $0 \le r < m$, the only possible remainders are $0,\ 1,\ 2,\ \ldots,\ m-1$. This causes the remainders to "wrap" around when performing modular arithmetic. This next example illustrates this idea.

**Example 9:** Make a table of $y$ values for the equation

$$y = (x+5) \text{ MOD } 9$$

**Solution:**

**Fact:** Solving equations (and congruences) if modular arithmetic is similar to solving equations in the real number system. That is, if

$$a \equiv b \mod m$$

then

$$a + k \equiv b + k \mod m$$

and

$$a - k \equiv b - k \mod m$$

for any number $k$. The next example makes use of these facts.

**Example 10:** Make a list of five solutions to

$$x + 7 \equiv 2 \text{ MOD } 8$$

**Solution:**

## Basic Concepts of Cryptography

*Cryptography* is the art of transmitting information in a secret manner. We next describe some of the basic terminology and concepts we will use in this class involving cryptography.

*Plaintext* – the actual undisguised message (usually an English message) that we want to send.

*Ciphertext* – the secret disguised message that is transmitted.

*Encryption* (encipherment) – the process of converting plaintext to ciphertext.

*Decryption* (decipherment) – process of converting ciphertext back to plaintext.

**Notation:** $Z_m$ represents all possible remainders in a MOD $m$ system, that is,

$$Z_m = \{0,\ 1,\ 2,\ \ldots,\ m-2,\ m-1\}$$

For representing our alphabet, we use a MOD 26 system

$$Z_{26} = \{0,\ 1,\ 2,\ \ldots,\ 24,\ 25\}$$

and perform a one to one correspondence between the alphabet letters and the elements of this set.

**Alphabet Assignment**

| | | |
|---|---|---|
| $A \Leftrightarrow 0$ | $K \Leftrightarrow 10$ | $U \Leftrightarrow 20$ |
| $B \Leftrightarrow 1$ | $L \Leftrightarrow 11$ | $V \Leftrightarrow 21$ |
| $C \Leftrightarrow 2$ | $M \Leftrightarrow 12$ | $W \Leftrightarrow 22$ |
| $D \Leftrightarrow 3$ | $N \Leftrightarrow 13$ | $X \Leftrightarrow 23$ |
| $E \Leftrightarrow 4$ | $O \Leftrightarrow 14$ | $Y \Leftrightarrow 24$ |
| $F \Leftrightarrow 5$ | $P \Leftrightarrow 15$ | $Z \Leftrightarrow 25$ |
| $G \Leftrightarrow 6$ | $Q \Leftrightarrow 16$ | |
| $H \Leftrightarrow 7$ | $R \Leftrightarrow 17$ | |
| $I \Leftrightarrow 8$ | $S \Leftrightarrow 18$ | |
| $J \Leftrightarrow 9$ | $T \Leftrightarrow 19$ | |

# Monoalphabetic Ciphers

*Monoalphabetic Ciphers* are substitution ciphers in which the correspondents agree on a rearrangement (permutation) of the alphabet. In this class, we examine 3 basic types of monoalphabetic ciphers

**Types of Monoalphabetic Ciphers**

1. Shift Ciphers (covered in Section 2.1)
2 Affine Ciphers (covered in Section 2.2)
3. Substitution Ciphers (covered in Section 2.3)

Shift Ciphers

If $x$ is a numerical plaintext letter, we encipher $x$ by computing the

Enciphering formula for Shift Ciphers

$$y = (x + k) \text{ MOD } 26, \text{ where } k \text{ is in } Z_{26}.$$

Here $y$ will be the numerical ciphertext letter.

***Note:** $k$ is called the key of the cipher and represents the shift amount.

**Example 11:** The Caesar cipher, developed by Julius Caesar

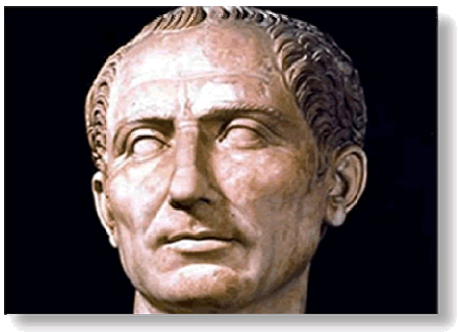

**Figure 1: Julius Caesar**

is a shift cipher given by

$$y = (x + 3) \text{ MOD } 26$$

Note that the key $k = 3$. Use the Caesar cipher to create a cipher alphabet. Then use it to encipher the message "RADFORD".

**Solution:** To create the cipher alphabet, we substitute the MOD 26 alphabet assignment number for each letter into the Caesar shift cipher formula and calculate the corresponding ciphertext letter number as follows:

$$A \Rightarrow x = 0 \Rightarrow y = (0+3) \ MOD \ 26 = 3 \ MOD \ 26 = 3 \Rightarrow D$$

$$B \Rightarrow x = 1 \Rightarrow y = (1+3) \ MOD \ 26 = 4 \ MOD \ 26 = 4 \Rightarrow E$$

$$C \Rightarrow x = 2 \Rightarrow y = (2+3) \ MOD \ 26 = 5 \ MOD \ 26 = 5 \Rightarrow F$$

$$D \Rightarrow x = 3 \Rightarrow y = (3+3) \ MOD \ 26 = 6 \ MOD \ 26 = 6 \Rightarrow G$$

$$\vdots$$

$$W \Rightarrow x = 22 \Rightarrow y = (22+3) \ MOD \ 26 = 25 \ MOD \ 26 = 25 \Rightarrow Z$$

$$X \Rightarrow x = 23 \Rightarrow y = (23+3) \ MOD \ 26 = 26 \ MOD \ 26 = 0 \Rightarrow A$$

$$Y \Rightarrow x = 24 \Rightarrow y = (24+3) \ MOD \ 26 = 27 \ MOD \ 26 = 1 \Rightarrow B$$

$$Z \Rightarrow x = 25 \Rightarrow y = (25+3) \ MOD \ 26 = 28 \ MOD \ 26 = 2 \Rightarrow C$$

This gives the corresponding correspondence between the plain and ciphertext alphabets

| **Plain** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Cipher** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** | **A** | **B** | **C** |

Using the above table, we can encipher the message "RADFORD" as follows

| **Plaintext:** | **R** | **A** | **D** | **F** | **O** | **R** | **D** |
|---|---|---|---|---|---|---|---|
| **Ciphertext:** | **U** | **D** | **G** | **I** | **R** | **U** | **G** |

Hence, the ciphertext is "UDGIRUG" ∎

Of course, in the last example we did not have to create the entire plain and ciphertext alphabets to encipher the message. We could instead just used the shift cipher formula $y = (x + 3) \text{ MOD } 26$ directly. We will illustrate this idea more generally in the next example given below.

The Caesar cipher is just a special case of a shift cipher with a key of $k = 3$. In a general shift cipher, the key $k$ can be any value in a MOD 26 system, that is, any value in the set $\{0,\ 1,\ 2,\ \ldots,\ 24,\ 25\}$. The next example illustrates a more general shift cipher.

**Example 12:** Encipher the message "SEINFELD" using a 12 shift cipher.

**Solution:**

**Deciphering Shift Ciphers**

Given a key $k$, plaintext letter number $x$, and ciphertext letter number $y$, we decipher as follows:

$$y = (x + k) \text{ MOD } 26$$

This gives the

Deciphering formula for shift ciphers

$$x = (y - k) \text{ MOD } 26$$

where $y$ is the numerical ciphertext letter, $x$ is the numerical plaintext letter, and $k$ is the key of the cipher (the shift amount).

***Note:** In the deciphering shift cipher formula, $-k$ MOD 26 can be converted to its equivalent positive form by finding a positive remainder.

The next two examples illustrate how to deciphering process works.

**Example 13:** Suppose we received the ciphertext "YLUJLQLD" that was encrypted using a Caesar cipher (shift $k = 3$). Decipher this message.

**Solution:**

**Example 14:** Decipher the message "EVZCJZXDFE" that was enciphered using a 17 shift cipher.

**Solution:** Using the shift cipher formula

$$y = (x + k) \ \ MOD \ \ 26,$$

we see that the key *k* for this cipher must be $k = 17$. Hence the formula becomes

$$y = (x + 17) \ \ MOD \ \ 26.$$

Recall in this formula that *x* represents the alphabet assignment number for the plaintext and *y* represents the alphabet assignment number for the cipher-text. Since we want to decipher the above cipher-text, we must solve the above equation for *x*. Rearranging first gives:

$$x + 17 = y \ \ MOD \ \ 26.$$

To solve for *x*, we must subtract 17 from both sides. This gives:

$$x = (y - 17) \ \ MOD \ \ 26 \qquad (*)$$

Note that since $-17 \ \ MOD \ \ 26 = 9$ (this can be computed simply by taking –17 + 26 = 9), we can write equation (*) as:

$$x = (y + 9) \ \ MOD \ \ 26 \qquad (**)$$

Either equations (*) or (**) can be used to decipher the message. We will use equation (**). Taking each letter of the cipher-text "EVZCJZXDFE" and using the MOD 26 alphabet assignment, we obtain:

$E \Rightarrow y = 4 \Rightarrow x = (4 + 9) \ \ MOD \ \ 26 = 13 \ \ MOD \ \ 26 = 13 \Rightarrow N$

$V \Rightarrow y = 21 \Rightarrow x = (21 + 9) \ \ MOD \ \ 26 = 30 \ \ MOD \ \ 26 = 4 \Rightarrow E$

$Z \Rightarrow y = 25 \Rightarrow x = (25 + 9) \ \ MOD \ \ 26 = 34 \ \ MOD \ \ 26 = 8 \Rightarrow I$

$C \Rightarrow y = 2 \Rightarrow x = (2 + 9) \ \ MOD \ \ 26 = 11 \ \ MOD \ \ 26 = 11 \Rightarrow L$

$J \Rightarrow y = 9 \Rightarrow x = (9 + 9) \ \ MOD \ \ 26 = 18 \ \ MOD \ \ 26 = 18 \Rightarrow S$

$Z \Rightarrow y = 25 \Rightarrow x = (25 + 9) \ \ MOD \ \ 26 = 34 \ \ MOD \ \ 26 = 8 \Rightarrow I$

$X \Rightarrow y = 23 \Rightarrow x = (23 + 9) \ \ MOD \ \ 26 = 32 \ \ MOD \ \ 26 = 6 \Rightarrow G$

$D \Rightarrow y = 3 \Rightarrow x = (3 + 9) \ \ MOD \ \ 26 = 12 \ \ MOD \ \ 26 = 12 \Rightarrow M$

$F \Rightarrow y = 5 \Rightarrow x = (5 + 9) \ \ MOD \ \ 26 = 14 \ \ MOD \ \ 26 = 14 \Rightarrow O$

$E \Rightarrow y = 4 \Rightarrow x = (4 + 9) \ \ MOD \ \ 26 = 13 \ \ MOD \ \ 26 = 13 \Rightarrow N$

Hence, the plaintext is "NEIL SIGMON". ∎

**Cryptanalysis of Shift Ciphers**

As the last two examples illustrate, one must know the key $k$ used in a shift cipher when deciphering a message. This leads to an important question. How can we decipher a message in a shift cipher if we do not know the key $k$? *Cryptanalysis* is the process of trying to break a cipher by finding its key. Cryptanalysis in general is not an easy problem. The more secure a cipher is, the harder it is to cryptanalyze. We will soon see that a shift cipher is not very secure and is relatively easy to break.

Methods for Breaking a Shift Cipher

1. Knowing $x = (y - k)$ MOD 26, we can test all possibilities for $k$ (there are 26 total in a MOD 26 alphabet $\{0,\ 1,\ 2,\ \ldots,\ 24,\ 25\}$) until we recover a message that makes sense.
2. Frequency analysis: Uses the fact that the most frequently occurring letters in the ciphertext produced by shift cipher has a good chance of corresponding to the most frequently occurring letters in the standard English alphabet. The most frequently occurring letters in English are E, T, A, O, I, N, and T (see the English frequency table on next page).

We will demonstrate these techniques using Maplets.

| Letter | Relative Frequency (%) | | | Letter | Relative Frequency (%) |
|---|---|---|---|---|---|
| A | 8.167 | | | N | 6.749 |
| B | 1.492 | | | O | 7.507 |
| C | 2.782 | | | P | 1.929 |
| D | 4.253 | | | Q | 0.095 |
| E | 12.702 | | | R | 5.987 |
| F | 2.228 | | | S | 6.327 |
| G | 2.015 | | | T | 9.056 |
| H | 6.094 | | | U | 2.758 |
| I | 6.966 | | | V | 0.978 |
| J | 0.153 | | | W | 2.360 |
| K | 0.772 | | | X | 0.150 |
| L | 4.025 | | | Y | 1.974 |
| M | 2.406 | | | Z | 0.074 |

**Table 1: Relative Frequencies of letters of English Language**
**Most Common are E, T, A, O, I, N, and R**

| | |
|---|---|
| **1. TH** | **9. HA** |
| **2. ER** | **10. AT, EN, ES, OF, OR** |
| **3. ON** | **11. NT** |
| **4. AN** | **12. EA, TI, TO** |
| **5. RE** | **13. IT, ST** |
| **6. HE** | **14. IO, LE** |
| **7. IN** | **15. IS, OU** |
| **8. ED, ND** | **16. AR, AS, DE, RT, VE** |

**Table 2: Most Common Digraphs in the English Language**
**(Based on a 2000 letter sample)**

| | | | | |
|---|---|---|---|---|
| **1. THE** | | **6. TIO** | | **11. EDT** |
| **2. AND** | | **7. FOR** | | **12. TIS** |
| **3. THA** | | **8. NDE** | | **13. OFT** |
| **4. ENT** | | **9. HAS** | | **14. STH** |
| **5. ION** | | **10. NCE** | | **15. MEN** |

**Table 3: Most Common Trigraphs in the English Language**