Module 10.2: The Basics of Modular Arithmetic

Gregory V. Bard

January 28, 2020

- This is a practice workbook for the basics of modular arithmetic.
- There is a with-answers version, and a without-answers version.
- In the with-answers version of this workbook, the black ink represents the question, and the blue ink represents the answer.

Problem 10-2-1

Please compute the following:

- What is $(8)(7) \bmod 11$?
- What is $(9)(11) \bmod 25$?
- What is $(14)(13) \bmod 17$?

Problem 10-2-2

Please compute the following:

- What is $7(9) + 3 \bmod 11$?
- What is $8(17) - 5 \bmod 25$?
- What is $5(9) - 11 \bmod 17$?

Problem 10-2-3

Please evaluate the following functions:

- Evaluate $h(x) \equiv 9x + 4 \bmod 17$ at $x = 11$.
- Evaluate $f(x) \equiv 2x + 5 \bmod 11$ at $x = 4$.
- Evaluate $g(x) \equiv 17x + 19 \bmod 25$ at $x = 5$.

The Affine Cipher

The following is a bijection between the letters of the English alphabet and the integers modulo 26.

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

We can define the affine cipher as follows. First, change the letters to numbers (as shown above). Second, put the number into a function, such as $c = f(p) = 17p + 19 \bmod 26$. Third, change the output of that function back into a letter (as shown above).

Of course, there are many possible functions of the form $c = f(p) = mp + b \bmod 26$. As you might have guessed, p represents the plaintext and c represents the ciphertext.

Note: The affine cipher is a toy cipher meant to train us in cryptography. It is less secure than the secret-decoder ring in a cracker-jack box. Never use the affine cipher in practice, in the real world.

Problem 10-2-4

Using the table given above, please attempt the following encryptions. (We are working mod 26 in all cases.)

- Using $f(p) = 17p + 19$, encrypt FROG.
- Using $f(p) = 17p + 19$, encrypt BEER.
- Using $f(p) = 11p + 14 \bmod 26$, how would you encrypt "STATS"?

Problem 10-2-5

Now that we've practiced encrypting with the affine cipher, let's practice decrypting. . (Again, we are working mod 26 in all cases.)

- Using the decryption function $p = g(c) = 21c + 8 \bmod 26$, how would you decrypt "BEQ"?
- Using $p = g(c) = 23c + 5$, how would you decrypt AWXR?
- Using $p = g(c) = 23c + 5$, how would you decrypt KJJW?

Problem 10-2-6

Let's continue with the affine cipher.

You've received two ciphertext messages. The decryption function is $c = g(p) = 19p + 17 \mod 26$.

- Decrypt the ciphertext "XTIWVIV."
- Decrypt the ciphertext "VABVILVL."

Problem 10-2-7

We are still continuing with the affine cipher.

- Using $c = f(p) = 13p + 3$, encrypt "BEERS."
- Using $c = f(p) = 13p + 3$, encrypt "BOATS."
- Based on your answer to the first two subproblems, do you think $f(p) = 13p + 3$ is a good encryption function?
- Based on your answer to the first two subproblems, do you think $f(p) = 13p + 3$ is injective?

Problem 10-2-8

Suppose that Alice makes a physical device to carry out the affine cipher, using $c = f(p) = 15p + 9 \mod 26$. Of course, she has to keep the function secret, otherwise anyone can figure out what her plaintexts are. She decides to give a demo.

- Bob tells her to encrypt "AAABC." What is the ciphertext?
- If Alice tells Bob what that ciphertext is, how will that enable Bob to determine Alice's encryption function?