Module 10.2: The Basics of Modular Arithmetic

Gregory V. Bard

January 27, 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 $(8)(7) \bmod 11$?
  $(8)(7) = 56 = 55 + 1 = 5(11) + 1 \equiv 1 \bmod 11$
- What is $(9)(11) \bmod 25$?
  $(9)(11) = 99 = 75 + 24 = 3(25) + 24 \equiv 24 \bmod 25$
- What is $(14)(13) \bmod 17$?
  $(14)(13) = 182 = 170 + 12 = 10(17) + 12 \equiv 12 \bmod 17$

Problem 10-2-2

Please compute the following:

- What is $7(9) + 3 \bmod 11$?
  $7(9) + 3 = 66 = 66(11) \equiv 0 \bmod 11$
- What is $8(17) - 5 \bmod 25$?
  $8(17) - 5 = 136 - 5 = 131 = 125 + 6 = 5(25) + 6 \equiv 6 \bmod 25$
- What is $5(9) - 11 \bmod 17$?
  $5(9) - 11 = 45 - 11 = 34 = 2(17) \equiv 0 \bmod 17$

Problem 10-2-3

Please evaluate the following functions:

- Evaluate $h(x) \equiv 9x + 4 \bmod 17$ at $x = 11$.

  $h(11) = 9(11) + 4 = 99 + 4 = 103 = 102 + 1 = 6(17) + 1 \equiv 1 \bmod 17.$

- Evaluate $f(x) \equiv 2x + 5 \bmod 11$ at $x = 4$.

  $f(4) = 2(4) + 5 = 8 + 5 = 13 = 11 + 2 \equiv 2 \bmod 11.$

- Evaluate $g(x) \equiv 17x + 19 \bmod 25$ at $x = 5$.

  $g(5) = 17(5) + 19 = 85 + 19 = 104 = 100 + 4 = 4(25) + 4 \equiv 4 \bmod 25.$

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.

  (F, R, O, G) becomes (5, 17, 14, 6) and encrypts to $(f(5), f(17), f(14), f(6)) \equiv (0, 22, 23, 17)$, which is (A, W, X, R) or "AWXR."

- Using $f(p) = 17p + 19$, encrypt BEER.

  (B, E, E, R) becomes (1, 4, 4, 17) and encrypts to $(f(1), f(4), f(4), f(17)) \equiv (10, 9, 9, 22)$, which is (K, J, J, W) or "KJJW."

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

  (S,T,A,T,S) becomes (18, 19, 0, 19, 18) and encrypts to $(f(18), f(19), f(0), f(19), f(18)) = (4, 15, 14, 15, 4)$ which is (E, P, O, P, E) or "EPOPE."

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"?

  (B,E,Q) becomes (1, 4, 16) and decrypts to $(g(1), g(4), g(16)) = (3, 14, 6)$ which is (D, O, G) or "DOG."

- Using $p = g(c) = 23c + 5$, how would you decrypt AWXR?

  (A, W, X, R) becomes (0, 22, 23, 17) and $(g(0), g(22), g(23), g(17)) \equiv (5, 17, 14, 6)$, which is (F, R, O, G) or "FROG."

- Using $p = g(c) = 23c + 5$, how would you decrypt KJJW?

  (K, J, J, W) becomes (10, 9, 9, 22) and $(g(10), g(9), g(9), g(22)) \equiv (1, 4, 4, 17)$, which is (B, E, E, R) or "BEER."

As you can see, if $c = f(p) = 17p + 19$ is our affine encryption function, then $p = g(c) = 23c + 5$ is our affine decryption function. Once we learn a bit about modular inverses, we can easily compute the affine decryption function for any affine encryption function that we are shown, assuming the decryption function exists. We'll do that in Module 10-4, as an exercise.

Problem 10-2-6

Let's continue with the affine cipher.

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

- Decrypt the ciphertext "XTIWVIV."

  The plaintext is "MONTANA."

- Decrypt the ciphertext "VABVILVL."

  The plaintext is "ARKANSAS."

Problem 10-2-7

We are still continuing with the affine cipher.

- Using $c = f(p) = 13p + 3$, encrypt "BEERS."

  (B, E, E, R, S) becomes (1, 4, 4, 17, 18) and $(f(1), f(4), f(4), f(17), f(18)) \equiv (16, 3, 3, 16, 3)$, which is (Q, D, D, Q, D) or "QDDQD."

- Using $c = f(p) = 13p + 3$, encrypt "BOATS."

  (B, O, A, T) becomes (1, 14, 0, 19, 18) and $(f(1), f(14), f(0), f(19), f(18)) \equiv (16, 3, 3, 16, 3)$, which is (Q, D, D, Q, D) or "QDDQD."

- Based on your answer to the first two subproblems, do you think $f(p) = 13p + 3$ is a good encryption function?

  Hell no. If a military unit is in urgent need of boats, and they get beers instead, then that's a major problem.

- Based on your answer to the first two subproblems, do you think $f(p) = 13p + 3$ is injective? Clearly not. We had several cases of differing inputs getting the same output. For example, $f(4) \equiv 3 \equiv f(18)$ and $f(1) \equiv 16 \equiv f(17)$.

Amazingly, in any environment with a finite domain and range of equal size, a function is either all three (injective, surjective, and bijective) or none of the three. It is okay if this surprises you, because this is a fairly obscure fact.

Since we have shown that the cipher is not injective (and therefore not surjective and not bijective), then we know that it cannot be inverted. Since it cannot be inverted, then the message cannot be read by the intended recipient. For this reason, we require all encryption functions to be injective, and we call this "unique decodability." Generally speaking, ciphers must be uniquely decodable to be acceptable in the real world.

Problem 10-2-8

Suppose that Alice makes a physical device to carry out the affine cipher, using $c = f(p) = 15p + 9 \bmod 26$. 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?

  The ciphertext is "JJJYN."

- If Alice tells Bob what that ciphertext is, how will that enable Bob to determine Alice's encryption function?

  Here is my way of describing how Bob can use this plaintext-ciphertext pair to find Alice's encryption function. Most students would provide somewhat less detail.

Bob certainly knows that "A" becomes "J." This means that he knows 0 encrypts to 9, or $f(0) = 9$. If we think of $c = f(p) = mp + b$, then Bob now knows that $b = 9$, since

$$9 = f(0) = m0 + b = 0 + b = b$$

Next, Bob knows that "B" encrypts to "Y." This means that he knows 1 encrypts to 24, or $f(1) = 24$. If we think of $f(1) = m1 + b = m + b$, Bob now knows that $24 = m + b$.

However, because Bob also knows $b = 9$, then Bob knows $m = 24 - b = 24 - 9 = 15$. Now Bob knows the encryption function, $c = f(p) = mp + b = 15p + 9$.

Bob can also use the last letter to check his work. Since "C" is 2, if he is correct, he expects

$$f(2) = 15(2) + 9 = 30 + 9 = 39 = 26 + 13 \equiv 13$$

and indeed, 13 becomes "N." Now Bob is certain that $c = f(p) = 15p + 9$ is Alice's encryption function.