

Up to section 5.3 in the textbook, we can easily see how most of the ideas are built upon previous ideas. Now we have encountered the special nature of section 5.4 : *Clock Arithmetic*. It may seem as though this material is unrelated to what the book has been covering, but upon further review, we can see many uses. We take the time in this worksheet to understand modulo arithmetic (a.k.a.”clock arithmetic”) and to also give an application to the real world.

Recall we first introduced a 12 hour clock and condensed our number system down to 12 numbers (0,1,...11). From this point forward, we refer to the clock as modulo 12. Of course there is nothing spectacular about 12. For this worksheet, we will be considering modulo 27 (\mathbb{Z}_{27} for short) arithmetic. Furthermore, we will associate each number with a symbol. Observe that there are 27 numbers; i.e.

$$\mathbb{Z}_{27} = \{0, 1, 2, \dots, 25, 26\}.$$

As promised, our association is

0	1	2	3	4	5	6	7	8	9	10	11	12	
a	b	c	d	e	f	g	h	i	j	k	l	m	
13	14	15	16	17	18	19	20	21	22	23	24	25	26
n	o	p	q	r	s	t	u	v	w	x	y	z	

Note that 26 represents a space, which will come into play later on when encoding messages. To warm up, we do some \mathbb{Z}_{27} arithmetic. Recall to do the arithmetic, we solve the problem as a regular arithmetic problem and divide by 27. Please show work off to the side.

1. $25 +_{27} 25 =$

2. $13 \times_{27} 17 =$

3. $12 -_{27} 25 =$

Looking further, we note that negative integers are equivalent to one of the numbers in \mathbb{Z}_{27} . For instance, observe that 1, 28, and 55 are all **1** in \mathbb{Z}_{27} , and so adding 27 gets us an equivalent number. For the integer -1 , we see $-1 + 27 = 26$ is the number in \mathbb{Z}_{27} that -1 is equivalent to. Lets try some more problems, this

time using this “code”. We will drop the subscript on the operation, and assume from this point forward that we are always in \mathbb{Z}_{27} .

1. $b + p =$

2. $m \times w =$

3. $g - z =$

Now, we want to introduce some techniques in which one can encode and decode a message using \mathbb{Z}_{27} .

1. Encoding by adding a Scalar

Say we want to encode the message “Math is awesome”. Numerically, this message is (with dashes separating each digit)

$$12 - 0 - 19 - 7 - 26 - 8 - 18 - 26 - 0 - 22 - 4 - 18 - 14 - 12 - 4.$$

One could simply add 5 to each number (adding 5 in \mathbb{Z}_{27}) to encode this message. For instance, the first letter $m = 12$ would encode to 17, which is the letter r. The word “math”, represented as $12 - 0 - 19 - 7$, would encode as $17 - 5 - 24 - 12$, which is “rfym”. Notice, we are taking the original message, and then evaluating it with a function $f(\alpha) = \alpha + 5$; i.e. we add 5 to each piece. Note that I use α so as not to be confused with the letter “x”. Please encode the rest of the message as I have done with “math” to “rfym”, and write it below.

Of course, for this communication to be successful, you also need to know how to decode a message once received. For this, the receiver must know the original function. For instance, we encoded previously by adding five, so to decode the message, we would just subtract five. Suppose the message sent to you is “th_ogpzgnylh_”. Moreover, you know that the person sending this to you used the function $f(\alpha) = \alpha + 7$. Please decode this message.

As we have seen, adding and subtracting a number is a way to send messages, but this is a code that is very easy to break. It is not hard to find the constant which is being added and then solve the message. We proceed into another technique.

2. Encoding by adding/multiplying a Scalar

Now, to complicate the problem, we introduce multiplication. Now use the function $f(\alpha) = 7\alpha + 5$ to encode a message. For instance, the letter “b” = 1 would encode as $7(1) + 5 = 12$, which is the letter “m”. Use this function to encode the word “kentucky” into a coded message. Write the encoded message below:

Unlike before, we cannot just subtract a number (assuming we know the function which is being used). Observe from earlier that “b” = 1 was encoded as $7(b) + 5 = m$. To get “b” back observe that

$$\begin{aligned}7(b) &= m - 5 \\(4 \times 7)(b) &= 4(m - 5) \\1(b) &= b = 4(m - 5).\end{aligned}$$

Observe that $4 \times 7 = 28 = 1$ in \mathbb{Z}_{27} . Thus 4 and 7 are multiplicative inverses in \mathbb{Z}_{27} ; i.e. they multiply together to give 1 in the set of 27 elements. This is no accident! Thus the decoding function to decode a message using the pre-defined function is

$$g(\beta) = 4(\beta - 5).$$

Use g as defined above to decode the message

“ifdagifdhtxzqkbgx ”

which was encoded use f as defined before.

