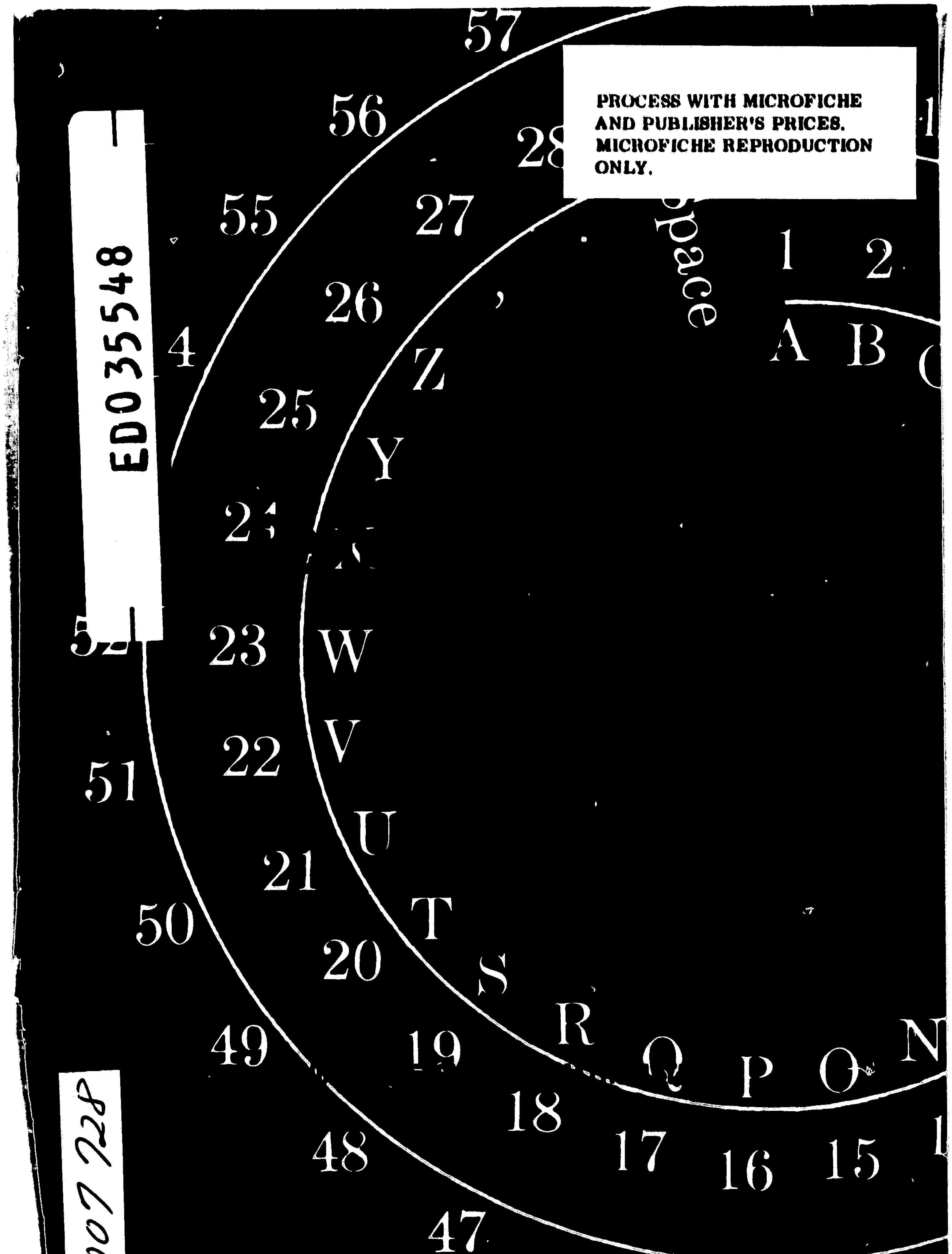
DOCUMENT RESUME

ED 035 548 SE 007 728

AUTHOR	Peck, Lyman C.
TITLE	Secret Codes, Remainder Arithmetic, and Matrices.
INSTITUTION	National Council of Teachers of Mathematics, Inc., Washington, D.C.
PUB DATE	61
NOTE	60p.
AVAILABLE FROM	National Council of Teachers of Mathematics, 1201 Sixteenth Street, N.W., Washington, D.C. 20036
EDRS PRICE	EDRS Price MF-$0.50 HC Not Available from EDRS.
DESCRIPTORS	Arithmetic, *Enrichment Activities, High Achievers, *Instructional Materials, *Mathematical Enrichment, *Modern Mathematics, Number Concepts, *Secondary School Mathematics

ABSTRACT

This pamphlet is designed for use as enrichment material for able junior and senior high school students who are interested in mathematics. No more than a clear understanding of basic arithmetic is expected. Students are introduced to ideas from number theory and modern algebra by learning mathematical ways of coding and decoding secret messages. Modular arithmetic matrix multiplication, and finite number systems are discussed. Applications of some of the ideas presented in this booklet are presented in order to stimulate further study in these areas. (FL)



PROCESS WITH MICROFICHE
AND PUBLISHER'S PRICES.
MICROFICHE REPRODUCTION
ONLY.

ED035548

SE 007 728

ED035548

PROCESS WITH MICROFICHE
AND PUBLISHER'S PRICES.
MICROFICHE REPRODUCTION
ONLY.

Secret Codes, Remainder Arithmetic, and Matrices

LYMAN C. PECK
Ohio Wesleyan University
Delaware, Ohio

U.S. DEPARTMENT OF HEALTH, EDUCATION & WELFARE
OFFICE OF EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL OFFICE OF EDUCATION POSITION OR POLICY.

NATIONAL COUNCIL OF TEACHERS OF MATHEMATICS
1201 Sixteenth Street, N.W. Washington, D.C., 20036

"PERMISSION TO REPRODUCE THIS COPYRIGHTED MATERIAL BY MICROFICHE ONLY HAS BEEN GRANTED BY Nat. Counc. Teach. Math.
TO ERIC AND ORGANIZATIONS OPERATING UNDER AGREEMENTS WITH THE U. S. OFFICE OF EDUCATION. FURTHER REPRODUCTION OUTSIDE THE ERIC SYSTEM REQUIRES PERMISSION OF THE COPYRIGHT OWNER."

All Rights Reserved
Copyright © 1961 by
THE NATIONAL COUNCIL OF TEACHERS OF MATHEMATICS

Second Printing, 1964
Third Printing, 1965
Fourth Printing, 1967

Permission to reproduce this copyrighted work has been granted to the Educational Resources Information Center (ERIC) and tc the organization operating under contract with the Office oi Education to reproduce documents included in the ERIC system by means of microfiche only, but this right is not conferred to any users of the microfiche received from the ERIC Document Reproduction Service. Further reproduction of any part requires permission of the copyright owner.

Library of Congress Catalog Card Number: 61-12376

Printed in the United States of America

PREFACE FOR TEACHERS

This pamphlet is presented for junior and senior high school students with serious interest ir mathematics who can do good work with little or no supervision. We often wonder what to do with such students. When we ask them to "do more problems on p. 73," we know deep inside that such assignments are no challenge. We should offer projects that awaken and keep alive an interest in mathematics. One of the aims of this booklet is to offer such a project.

Selections from modern mathematics are appropriate for this purpose. I have tried to select material that can be presented intuitively and structured to strengthen arithmetical understandings, without duplicating much of the content of current secondary school mathematics.

I suggest that you skim through the text for the main ideas and the flavor of their presentation. Then offer the pamphlet to one of your "ablesters" to work on independently. Of course you will be better equipped to answer his questions if you have worked through the material yourself, but this is not essential. For you and for him, the book is self-contained. Only in the event that you or he should want to know more would it be necessary to refer to outside material. Most references now available are appropriate only for you, the teacher, to read. At the end of this pamphlet is a list of such references to help you obtain more background.

It is a pleasure to acknowledge the inspiration and guidance I received from members of the mathematics staff at Iowa State Teachers College. While there, I used many of the topics of this book in demonstration classes, from 4th grade to 10th grade. It was the recollection of the eagerness of those Iowa youngsters that compelled me to collect these exercises in their present form.

PREFACE FOR STUDENTS

You have this book in your hands for several reasons, probably including the following:

You are interested in and curious about mathematics.

You have shown your teachers that you can do good work by yourself.

All you need in addition to the interest and the ability to work independently is an understanding of basic arithmetic. You will be surprised to see how far you can go with arithmetic. To help you, there are answers to most questions at the back of the book. For a while we considered printing them upside down to remind you to use them properly. Write *your* answer first; then look up the answer in the back.

You should keep all your work and answers neatly in a notebook. Many times you will want to go back and see how you answered an earlier question. Then, too, you will want to show your teacher, your parents, or your friends what you have done.

These are all the directions you need. I won't keep you any longer. This book was written for you to use. Get to work and have fun!

CONTENTS

CHAPTER ONE

MAKING AND BREAKING SECRET CODES

1·1. Introduction

Most boys and girls are interested in the idea of sending messages in code. We can show you some mathematical ways to make codes. If you do it right, you can learn:

- How to make secret codes that hardly any of your classmates will be able to break.
- How there can be an arithmetic different from what you have studied and know.
- How general mathematical ideas can arise from simple, concrete experiences.

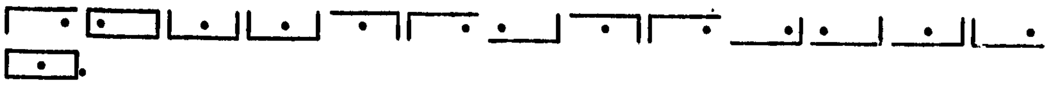
1·2. Some codes you may already know

Let's look first at some codes that are often used by boys and girls in school. Suppose you want to send a message to your friend Zeke: ZEKE, MEET AT CABIN. Then you decide to use the following arrangement to code your message:

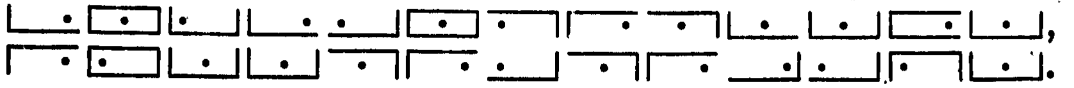
A B C	D E F	G H I
J K L	M N O	P Q R
S T U	V W X	Y Z

Key 1.

Whenever you want to use a letter you replace it by some lines and a dot to show where the letter lies in the key. For example, you code A as ·⌟, D as ⊔·, R as ⊏·, the space between words as ⌜·, and so on. The message you send to Zeke looks like this: ⌜· ⊔· ⊐· ⊔·,



When Zeke gets this message, he decodes it with his copy of Key 1. Then he sends the following answer. Can you decode it? Stop now and try. (Don't look yet, but the answer is at the end of the practice below.)



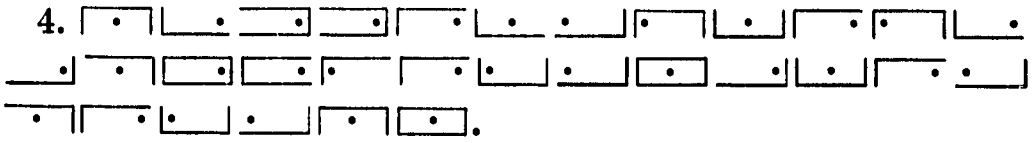
The secret in any code lies, of course, in the key. The main secret in the code above is one of position. The position of each letter in the frame tells which lines to use and where to place the dot. This key has the advantage of being easy to remember. After using it a few times, you will not even need a written copy. You can easily jot one down when you need it, or even refer to a mental picture. When you have finished with a written copy of the key, you can burn or even eat it, if the "enemy" is on your heels! Unfortunately, codes that are easy to remember are easy for experts to decode or break. Before we look at a different sort of key, let's practice coding and decoding some messages using Key 1.

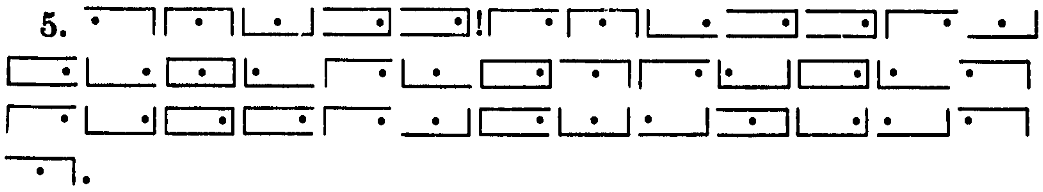
PRACTICE

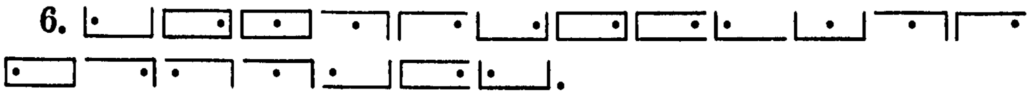
Code the following messages, using Key 1:

1. INDIANS COMING. HELP!
2. SENDING TEN MEN AT ONCE.
3. WE WON BATTLE. CAPTURED CHIEF.

Decode the following. They continue the story of the first three.

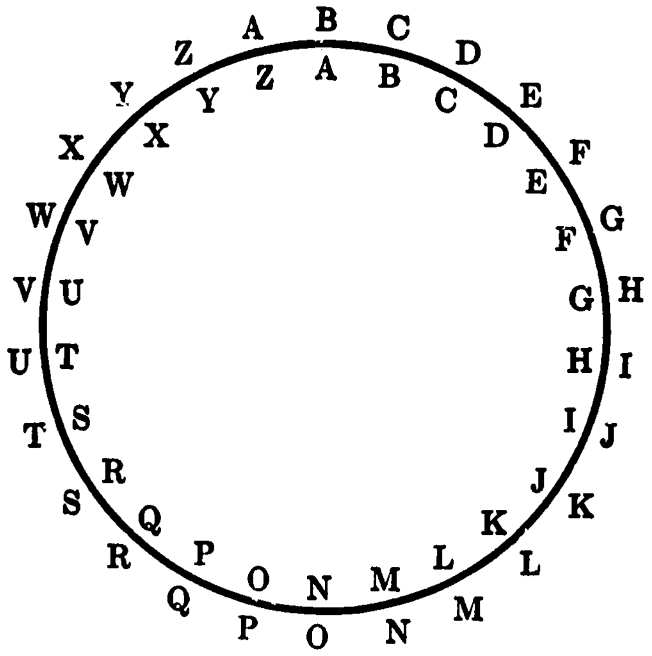
4. 

5. 

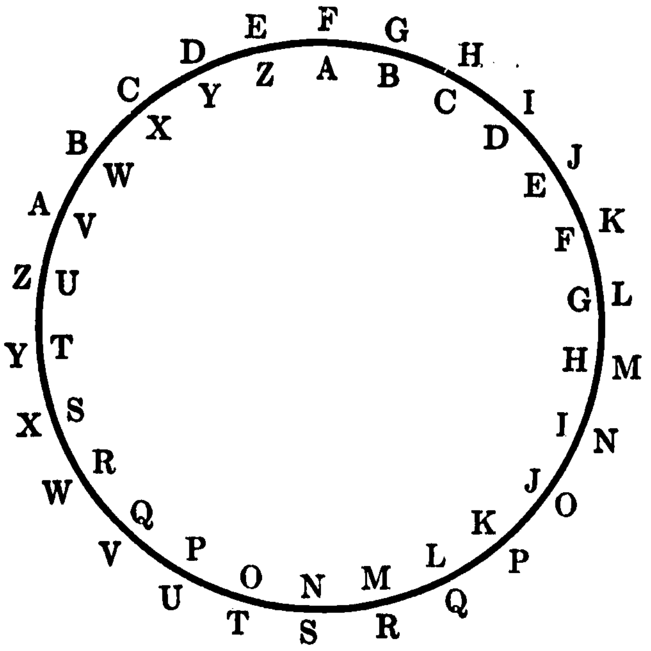
6. 

(Zeke's answer reads: INDIANS THERE, MEET AT CAVE.)

Now we shall show you a different key. It is much simpler than the first, but worth seeing because it can be changed into one that is harder to break. Take the original message to Zeke: ZEKE, MEET AT CABIN. This time replace each letter by the one following it in the alphabet. A is replaced by B, B by C, and so on. Z has no letter following it, but you replace Z by A. The first message to Zeke would then be AFLF, NFFU


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
Z 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

Key 2. Alphabet Circle # 1.


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

Key 3. Alphabet Circle #2.

BU DBCJO. This key hardly needs writing down, but by writing it we can begin to establish a pattern for you to follow later. The letters of the original message are on the inside of the circle. You can see why this key is named *Alphabet Circle* (see Key 2).

If your enemies catch on to Key 2 quickly, you can be a little more clever. You can replace each letter by the *fifth* one following. Here a written key is more helpful, although not essential. (See Key 3.) Now the message to Zeke reads as follows: EJPJ, RJJY FY HFGNS. You will want to practice coding and decoding messages using Key 3. Then you will learn about a code that uses numerals in place of letters.

PRACTICE

7. Code the following messages, using the method just described (Key 3). They tell a different story, continuing from "ZEKE, MEET AT CABIN."

(a) CANNOT COME NOW.
(b) COME AT ONCE. REPEAT, AT ONCE.
(c) FLAT TIRE ON BIKE. HAVE TO WALK.
(d) WALK? DONT! DONT! RUN!

8. Decode the following messages. They continue the story begun in the four messages above.

(a) BMFY NX YMJ MZWWD?
(b) HFZLMY YBT GNL KNXM.
(c) LTTI. QJYX MFAJ KNXM KWD.
(d) YMJD FWJSY YMFY GNL.

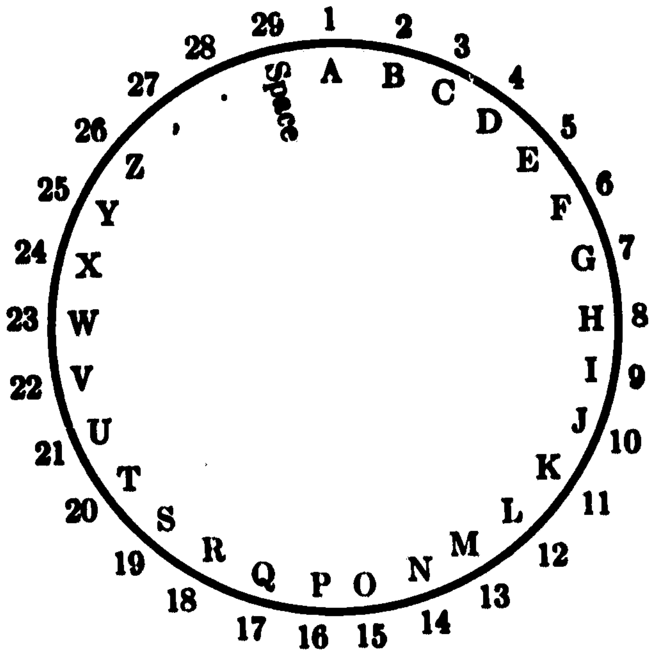
You can very easily make a slide rule for coding and decoding messages. Get some thin, smooth cardboard (a piece of manilla folder, for example) and cut out a circular disc of convenient size, no smaller than 3 inches across. Print around its edge the letters from A to Z, spaced equally as in the inner circle of Key 2 or 3, and no closer than $\frac{1}{4}$ inch apart. Then use this disc to mark an equal circle on a larger piece of cardboard. Print A to Z, on the outside of the circle this time, exactly opposite the positions of the letters on the disc. Finally, use a pin or other device to fix the two pieces center-to-center, allowing the disc to turn.

To code in Key 2 with your slide rule, set the inner A opposite the outer B, just as pictured in Key 2. You make similar adjustments for Key 3 or any other key you choose. You may find it helpful to mark the outer card *Code* and the inner disc *Plain*, to remind you whether you are coding or decoding.

Most slide rules you see are straight, not circular. Try to make a straight slide rule that will code and decode in Key 2 or 3. There are a few troublesome pitfalls to avoid. Perhaps you can figure them out before you are far along with your work. Try it.

1•3. Some number codes and codes that use arithmetic

Perhaps the simplest code that replaces letters by numbers is the one shown in Key 4. Notice that this key allows you to code periods, commas,



Key 4. Alphabet Circle #3.

and spaces between words. This last feature is very important. With it, you can keep secret the number of words in a message. Check the following example. For all an outsider knows, the numbers indicate a 15-letter word.

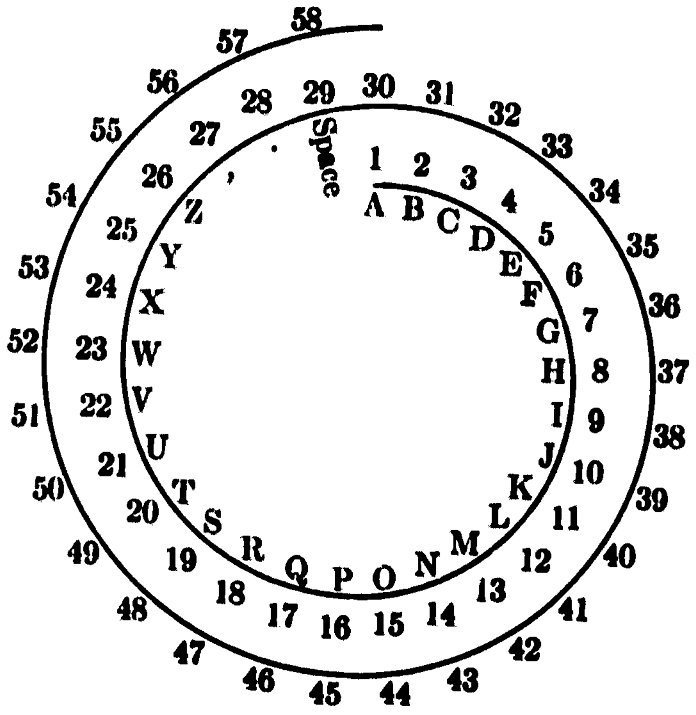
HELP, NEED GAS. $\xrightarrow{\text{Key 4}}$ 8 5 12 16 27 29 14 5 5 4 29 7 1 19 28

Since you may have trouble properly spacing the numbers in a message like the one above, we shall change cur method by taking two more steps. First, we multiply each number in the message by 2; then we use Key 4 to change back to letters, commas, periods, and spaces. Follow the word HELP through the complete process:

HELP $\xrightarrow{\text{Key 4}}$ 8 5 12 16 $\xrightarrow[\text{by 2}]{\text{Multiply}}$ 16 10 24 32 $\xrightarrow{\text{Key 4}}$ PJX?

The question mark shows our doubt about handling 32. Since there are only 29 places in Key 4, there is no replacement for 32. One way to handle this difficulty is to change the circle into a spiral, so that the numbers can continue beyond 29. This process gives us Key 5. Now the number 32 appears in the outer part of the spiral, opposite C, so we use C for 32. Thus HELP codes into PJXC.

To be sure that you understand Key 5 and how it is an extension of Key 4, you should stop now and code the entire HELP message. Then



Key 5. Alphabet Spiral #1.

check your work against the work below:

HELP, NEED GAS. $\xrightarrow{\text{Key 5}}$

8 5 12 16 27 29 14 5 5 4 29 7 1 19 28 $\xrightarrow[\text{by 2}]{\text{Multiply}}$

16 10 24 32 54 58 28 10 10 8 58 14 2 38 56 $\xrightarrow{\text{Key 5}}$

PJXCY .JJH NBI,

Notice how mixed-up this looks when you compare it with the original. The second "word" begins with a period and the message ends with a comma. You'll agree that the more mixed-up a message appears, the more secret it remains. We are getting better at the code business!

You should now begin to wonder about decoding a message sent in Key 5. The job will be a little more complicated than simple reference to the key because of the multiplication by 2 in coding. Obviously you must divide by 2 to undo that operation. In words used by mathematicians, the operation *divide by 2* is the inverse operation of ***multiply by 2***.

The following message was coded in Key 5 as a reply to HELP, NEED GAS. Let's use the idea of inverse operations to decode it.

FAZR.N BK A.FJ,

Recall that the coding steps were: Key 5; Multiply by 2; Key 5. The decoding steps, using the inverse operation, will be: Key 5; Divide by 2;

Key 5. We begin below:

FAZR.N BK A.FJ, $\xrightarrow{\text{Key 5}}$

6 1 26 18 28 14 29 2 11 29 1 28 6 10 27 $\xrightarrow[\text{by 2}]{\text{Divide}}$

3 ?

Almost immediately you get stuck. It is not that you cannot divide 1 by 2. The answer is ½, of course. But knowing that there are no fractions in Key 5, you are lost for a way to proceed. The solution is not hard to find, though. If you look at Alphabet Spiral #1 you will see that either 1 or 30 is a substitute for A. Since 2 divides 30 evenly, you can reason this way: Whoever coded the message must have had O for the second letter. Key 5 changed it to 15; multiplying by 2 changed it to 30; Key 5 changed it to A. Thus, the second number is 15. Let us continue our division by 2.

$\xrightarrow[\text{by 2}]{\text{Divide}}$ 3 15 13 9 14 7 ?

We pause again, for 29 ÷ 2 = 14½, which is not in Key 5. A look at Alphabet Spiral #1 shows that 29 stands for a space, and that you can also use 58. Since 58 is an even number, you replace 29 with 58. Then, 58 ÷ 2 = 29. We proceed.

$\xrightarrow[\text{by 2}]{\text{Divide}}$ 3 $\textcircled{15}$ 13 9 14 7 $\textcircled{29}$ 1 $\textcircled{20}$ $\textcircled{29}$ $\textcircled{15}$ 14 3 5 $\textcircled{28}$

We have circled the numbers for which you must use the Alphabet Spiral to get an even number. Finally, we use Key 5 to arrive at the letters in the message:

$\xrightarrow{\text{Key 5}}$ COMING AT ONCE.

Looking back over the work, you see that the inverse operation, *divide by 2*, gives no trouble with even numbers in the message. When you have odd numbers, you refer to the Alphabet Spiral to get an even number representing the same letter. Now try coding and decoding some messages.

PRACTICE

Code the following messages, using the method just described (Key 5, multiply by 2, Key 5):

9. ROCKET TO MOON LEAVES AT NOON.
10. GOOD LUCK. HAPPY LANDING.
11. ARRIVED AT NOON. NO ONE HERE.

Decode the following messages; they continue the story started in messages 9, 10, and 11 above:

12. FA.NGBKMXBKRA.I, B.U NGJJ. FPJJIJ,
13. .A.J, IBQ AKPJG IRHJ AL ZAA.,
14. QPBK QBI RK XRVJ,
15. TMIK XRVJ AKPJG IRHJ,

Even though the Alphabet Spiral gives you even numbers to replace odd numbers in the message, there is an easier way to handle the odd numbers. The following table will help you:

Odd numbers in message	1	29	11	29	1	27
Even numbers from Spiral	30	58	40	58	30	56
Divide by 2	15	29	20	29	15	28

Do you see that each number in the second row is exactly 29 more than the number above it? This fact suggests that you do not need to refer to the Alphabet Spiral when you meet an odd number. You merely add 29 to it. Then division by 2 gives a whole number.

Now it is time for you to practice with this new method of coding and decoding.

PRACTICE

16. Return to Exercises 12–15 and decode, using the trick of adding 29 when you need an even number.

If you have not already made a slide rule for coding by Keys 2 and 3, you should read the instructions on page 4 before doing what follows.

A slide rule for Key 5 is not much different from the one for Keys 2 and 3. The inner disc is the same, but the numerals on the outer piece must follow a spiral. Again, you must carefully match up opposite positions. You may be interested in trying to make a straight slide rule for Key 5, rather than a circular one. Do you see what is needed on a straight slide rule to do the work of the spiral? Notice that on a slide rule (circular or straight) you can complicate your code further by turning the inner disc first (making A code into 6, for example), then multiplying by 2.

1·4. Remainder arithmetic—multiplication

It is now time for a close look at some of the arithmetic you have been doing. Most people find that they need to use numbers and number operations in their work, and they hunt for a system that will let them do this work easily and rapidly. In working the last set of exercises you may have found that you can eliminate some references to the spiral by using arithmetic. Now we will point out some other simplifications.

In the preceding messages you used numbers as large as 58. You could have managed with only the numbers from 1 to 29. For example, to code S you began with 19; $2 \times 19 = 38$, and for 38 you used I. But since you can also use 9 for I, in this code 9 and 38 mean the same thing. Anyone who has not followed our steps to this point will think it is foolish to say that 9 and 38 mean the same thing. But for our code, ***means the same thing*** means ***stands for the same letter***. Why not write $9 = 38$ to show this fact? The "=" sign has too special a meaning. Mathematicians use a different sign. They write $9 \equiv 38$. They read this "9 is congruent to 38." You may say "means the same as" for ≡ if you wish. You should not use the word ***equals***, for that does not express the idea you have in mind.

To get used to this new sign and what it means, consider Table 1. You should have no trouble with the first column of the table. There you use familiar arithmetic. However, you should check carefully all of the entries in the second column. Do you understand how they were obtained? For example, $2 \times 23 \equiv 17$ is correct because $2 \times 23 = 46$, and 46 and 17 both stand for Q in the Alphabet Spiral. Stop now in your reading to check the rest of Table 1.

Have you seen that you don't need the Alphabet Spiral to help you in the second column of Table 1? The trick, if you want to call it that, is to subtract 29 from each of the answers you get by ordinary multiplica-

TABLE 1. MULTIPLICATION BY 2 IN REMAINDER ARITHMETIC

$2 \times 1 \equiv 2$	$2 \times 15 \equiv 1$
$2 \times 2 \equiv 4$	$2 \times 16 \equiv 3$
$2 \times 3 \equiv 6$	$2 \times 17 \equiv 5$
$2 \times 4 \equiv 8$	$2 \times 18 \equiv 7$
$2 \times 5 \equiv 10$	$2 \times 19 \equiv 9$
$2 \times 6 \equiv 12$	$2 \times 20 \equiv 11$
$2 \times 7 \equiv 14$	$2 \times 21 \equiv 13$
$2 \times 8 \equiv 16$	$2 \times 22 \equiv 15$
$2 \times 9 \equiv 18$	$2 \times 23 \equiv 17$
$2 \times 10 \equiv 20$	$2 \times 24 \equiv 19$
$2 \times 11 \equiv 22$	$2 \times 25 \equiv 21$
$2 \times 12 \equiv 24$	$2 \times 26 \equiv 23$
$2 \times 13 \equiv 26$	$2 \times 27 \equiv 25$
$2 \times 14 \equiv 28$	$2 \times 28 \equiv 27$
	$2 \times 29 \equiv 29$

tion. You would figure $2 \times 18 \equiv 7$ this way:

$$2 \times 18 = 36; \quad 36 - 29 = 7; \quad \text{therefore, } 2 \times 18 \equiv 7.$$

In every case, however, it is the Alphabet Spiral that supplies the final check.

A mathematician would write such a multiplication fact completely in this form:

$$2 \times 18 \equiv 7 \pmod{29}.$$

He would read $36 \equiv 7 \pmod{29}$ as "36 is congruent to 7, modulo 29." (*Modulo* means *for the modulus.*) Two numbers are congruent modulo 29 (or any number) if and only if they have the same remainder when divided by 29 (or any number).

To become more familiar with this new arithmetic, which we call *remainder arithmetic,* you should work some practice examples.

PRACTICE

17. Make a multiplication table for 3's. It will be similar to Table 1 on page 9. Notice that you can figure each multiplication in two different ways. For example, $3 \times 20 \equiv 2$ is figured below:

(a) In the Alphabet Spiral there is no 60. Make another loop on the spiral beyond 58. Then 60 represents B. So does 2. Therefore, $3 \times 20 \equiv 2$.

(b) With arithmetic, $3 \times 20 = 60; 60 - 29 = 31; 31 - 29 = 2$; therefore, $3 \times 20 \equiv 2$.

18. The statement above, *Two numbers are congruent modulo 29 if and only if they have the same remainder when divided by 29*, is a definition. Use this definition to find whether or not the numbers in each of the following pairs are congruent modulo 29.

(a) (91, 62).

SOLUTION: $\begin{array}{r} 3 \\ 29\overline{)91} \\ \underline{87} \\ 4 \end{array}$ Remainder: 4. $\begin{array}{r} 2 \\ 29\overline{)62} \\ \underline{58} \\ 4 \end{array}$ Remainder: 4.

CONCLUSION: $91 \equiv 62$, since both have a remainder of 4 on division by 29. (A check in the spiral confirms this fact, for both 91 and 62 represent D.)

(b) (91, 72).

CONCLUSION: These numbers are not congruent, for their remainders on division by 29 are not equal (you should check the arithmetic).

This fact is confirmed by the spiral since 91 represents D, and 72 represents N.

(c) (40, 69).
(d) (79, 108).
(e) (60, 118).
(f) (65, 136).
(g) (44, 103).
(h) (115, 57).
(i) (72, 14).
(j) (122, 141).
(k) (3, 61).

19. Can a number be congruent to itself? Give some examples to prove your answer.

20. Choose a number between 1 and 29, say 3.

(a) How many numbers are congruent to it?
(b) List them in order of increasing size.

21. For each of the numbers 4, 10, 15, 22, and 29, list the six smallest numbers that are congruent to it.

22. For each of the following state a rule that tells how to find *all* the numbers congruent to it:

(a) 4.
(b) 10.
(c) 15.
(d) a number between 1 and 29.
(e) any number, not necessarily less than 29.

CHAPTER TWO

A NEW KIND OF ARITHMETIC

2·1. Remainder arithmetic—addition

We shall now leave the topic of codes, and shall return to it later in the next chapter. There are many situations in life where remainder mathematics can be used. In fact you use it quite often. Don't you believe it? Then answer the following question: What time will a clock show four hours after ten o'clock? Did you answer "two o'clock"? Why not "fourteen o'clock"? Everyone knows that most clocks "start again" after 12 o'clock. Of course it is true that in the armed forces a 24-hour clock is used, and 14 o'clock and 22 o'clock are everyday terms. We could say that 14 o'clock means the same as 2 o'clock, or that $14 \equiv 2 \pmod{12}$. If you want to explore this idea further, see Exercise 29.

There is another place where you use remainder arithmetic, perhaps without realizing it. Answer this question:

What day of the week comes 16 days after Wednesday?

The answer is Friday, of course. You can get it by referring to a calendar, by reciting the days of the week in order, by counting on your fingers, and by other methods. Let us suggest the following way. Make a calendar that starts with Sunday on the 1st, Monday the 2nd, and so on, like the one below. Since Wednesday is day 4, 16 days after Wednesday will be $4 + 16 = 20$, or Friday. If you want to know only the *day* of the week, not the *date*, then 20 means the same as 13 or 27 or 6. Is this another example of congruences? That is, is $20 \equiv 13 \pmod 7$? Cer-

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

tainly. Check the following divisions:

$$\begin{array}{r} 2 \\ 7\overline{)20} \\ \underline{14} \\ 6 \end{array} \quad \text{Remainder: 6.} \qquad \begin{array}{r} 1 \\ 7\overline{)13} \\ \underline{7} \\ 6 \end{array} \quad \text{Remainder: 6.}$$

Referring to the calendar on page 12, you see that each column contains integers congruent to one another modulo 7. Choose the smallest from each column. You get the set of integers {1, 2, 3, 4, 5, 6, 7}. To represent any of the days of the week, all you need are these seven integers. Though it may not be clear to you now, you need no other integers to do any arithmetic concerning the days of the week. Suppose you want the 5th day from Monday; $2 + 5 = 7$ tells you it is Saturday. Suppose you want the 5th day from Thursday; $5 + 5 = 10$ tells you it is Tuesday, but since $10 \equiv 3 \pmod 7$, you don't need the 10. You need write only $5 + 5 \equiv 3 \pmod 7$. In the same way, you can figure the 6th day from Tuesday by $3 + 6 \equiv 2 \pmod 7$, to get Monday.

TABLE 2. ADDITION MODULO 7

+	1	2	3	4	5	6	7
1	2	3	4	5	6	7	1
2	3	4	5	6	7	1	2
3	4	5	6	7	1	2	3
4	5	6	7	1	2	3	4
5	6	7	1	2	3	4	5
6	7	1	2	3	4	5	6
7	1	2	3	4	5	6	7

By now you may wonder how you can possibly remember facts like $5 + 5 \equiv 3$ and $3 + 6 \equiv 2$. If you had to use them regularly, they would soon be as easy to recall as ordinary addition facts. You don't need to memorize them now, but you will find it helpful to have an addition table for reference. Stop your reading and check Table 2 to see if it makes sense. Be sure that you know how to read it. Any integer in the table is in both a row and a column, and is the sum (mod 7) of the integers at the head of its row and of its column. For example, "3" in the 4th row and 6th column shows that $4 + 6 \equiv 3 \pmod 7$. You should check other places in the table.

There are several interesting things to observe in this table. For example:

- There is a diagonal of seven 1's running from lower left to upper right.

- There are incomplete diagonals for the other integers, but each integer appears seven times.
- In each row the integers appear in increasing order (left to right) until 7 is reached; then they drop back to 1 and start to increase again.
- Each integer appears once and only once in each row or column.

We want to be sure that you see another important aspect of Table 2. The last column on the right shows the facts listed below:

$$\begin{array}{ll} 1 + 7 \equiv 1 & 5 + 7 \equiv 5 \\ 2 + 7 \equiv 2 & 6 + 7 \equiv 6 \\ 3 + 7 \equiv 3 & 7 + 7 \equiv 7 \\ 4 + 7 \equiv 4 & \end{array}$$

Think about ordinary arithmetic. What integer, when added to another integer, gives the other integer as the sum? That is, what integer could you use for N below?

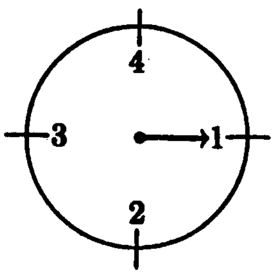
$$\begin{array}{c} 1 + N = 1 \\ 2 + N = 2 \\ 3 + N = 3 \\ 4 + N = 4 \\ \cdots\cdots\cdots\cdot \end{array}$$

Zero is the number, of course. Thus you have observed something rather remarkable. In modulo 7 addition, 7 behaves like 0. Adding 7 to another integer does not change the identity of the other integer. Thus, 7 is called the *identity element* in addition modulo 7.

There are other places in everyday life where you can use arithmetic like addition modulo 7. Look for them in the practice exercises below.

PRACTICE

A professional boxing match is divided into three-minute rounds with one minute for rest between rounds. Once the match starts, the clock usually goes round and round through a four-minute circle until the end of the match. To the right is a picture of the clock. Write the addition facts that will answer the following questions:



23. What time will the clock above show
    (a) Two minutes from now? (Ans.: $1 + 2 = 3$.)
    (b) Five minutes from now? (Ans.: $1 + 5 \equiv 2$.)
    (c) Four minutes from now?

(d) Eight minutes from now?
(e) Six minutes from now?
(f) Ten minutes from now?
(g) Twelve minutes from now?

24. Suppose the clock points at 3. What time will it show in

(a) One minute?
(b) Two minutes?
(c) Three minutes?
(d) Four minutes?
(e) Five minutes?
(f) Six minutes?
(g) Seven minutes?
(h) Eight minutes?

(You should have written most of the facts above with the congruence sign, ≡, not the equals sign, =.)

25. (a) In Exercises 23 and 24, the addition is modulo what integer?
(b) For addition modulo 4, list the smallest set of integers that we need.

26. Make an addition table modulo 4, using the set of integers {1, 2, 3, 4}.

27. In your addition table for Exercise 26, what integer behaves like zero? (Recall what an *identity element* is from page 14.)

28. A football game is divided into 15-minute quarters. (Usually the half-time period takes exactly 15 minutes.) Arithmetic dealing with time in a football game can be arranged modulo 15.

(a) Make an addition table modulo 15.
(b) What integer behaves like zero in addition modulo 15?

29. Make an addition table (mod ?) to show the arithmetic done on an ordinary twelve-hour clock. (See page 12.)

30. Look for other situations where you can use addition modulo some integer. Try other sporting events such as hockey, basketball, and soccer.

31. You do not need a real-life situation such as using the clock or calendar, or timing a game to do remainder arithmetic (addition modulo some integer).

(a) Make an addition table modulo 5.
(b) Make an addition table modulo 6.
(c) Make an addition table modulo 2. Notice how few integers are needed!
(d) Make an addition table modulo 1. You need hardly any integers for this one!

32. On page 13 you saw that the set of integers {1, 2, 3, 4, 5, 6, 7} contains all the integers you need for addition modulo 7. Each integer in this set is congruent to an unlimited number of integers. For example,

1 is congruent to 8, 15, 22, 29, $\cdots$. We shall write this fact as follows:

$$1_7 = \{1, 8, 15, 22, \cdots\}.$$

This set of integers is called a *residue class*, modulo 7. The remainder, or residue, on dividing each member of the class by 7 is 1.

(a) Write all the other residue classes, modulo 7.
(b) How many residue classes are there, modulo 4? Write them.
(c) Write all of the residue classes, modulo 5.

We shall show you, in the following sections, more about remainder arithmetic. We shall not always try to connect the arithmetic with such applications as figuring time of day or day of the week. Instead we shall follow certain ideas about arithmetic by playing with numbers. This is very much like the work that a mathematician does in pure mathematics. Following partly his hunches and partly logic, he does not feel forced to think of practical applications of his work. For the moment he is creating and developing a mathematical idea. There may be many applications of his ideas. They may be seen immediately or, as has often happened, they may not be seen until years after his death.

2•2. Zero, the identity element

You have seen (page 14 and Exercises 27 and 28 above) that an identity element appears in every set of integers, modulo some integer. Since an identity element behaves like zero in addition, we are going to ask you to write "0" for the identity element wherever it occurs.

If it seems strange to use zero, go back to the calendar on page 12 and put in a Saturday, using 0, *before* Sunday the 1st. Then 0 stands for Saturday just as 7 does (or 14, 21, or 28). This use of zero will make it necessary to go back over all of your addition tables and either make new ones or cross out the identity element in each and write in 0. To help you, Table 3 shows addition for integers modulo 7, using zero. Notice that we have placed 0 before 1 instead of after 6. It could go in either place. We prefer to have it before 1 because this agrees with the position of 0 in ordinary arithmetic.

PRACTICE

33. Make an addition table modulo 4, using the set of integers {0, 1, 2, 3}. (See Exercise 26.)

34. Make an addition table modulo 15, using 0 for the identity element. (See Exercise 28.)

35. Change your addition table for Exercise 29 so that it has 0 as the identity element.

TABLE 3. ADDITION MODULO 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

36. Change the addition tables for each part of Exercise 31, using 0 for the identity element in each.

37. Notice the following facts in Table 3:

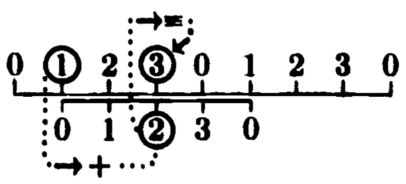
$$0 + 0 \equiv 0$$
$$1 + 6 \equiv 0$$
$$2 + 5 \equiv 0$$

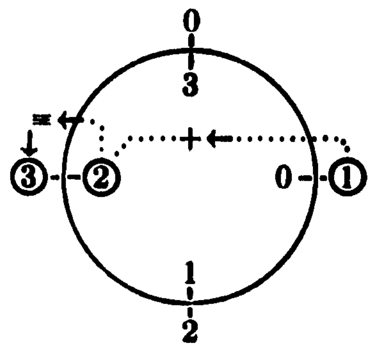
At first glance, two of these facts look strange. Then you realize that they are not equals (=), but congruences (≡). List the remaining facts in Table 3 that show sums of zero.

38. (a) For addition modulo 4, list all sums that give zero.
(b) For addition modulo 15, list all addition facts that have 0 for the sum.

39. In ordinary arithmetic, 0 is the identity element with respect to addition.
(a) What is the identity element with respect to multiplication?
(b) Give some examples to illustrate.

40. Make a slide rule for addition modulo 4. Earlier you made slide rules for coding in Keys 2, 3, and 5. The process is much the same for an addition slide rule. Read the directions on pages 4 and 8. Then see the diagrams below for both a straight and a circular slide rule showing $1 + 2 \equiv 3$. Notice also that this setting of the slide rule is good for adding 1 and *any* number modulo 4.





(a) Make a slide rule for addition modulo 15. See Exercise 34.

(b) Make a slide rule for each of the systems used in Exercise 31. See also Exercise 36.

2·3. Subtraction, the inverse of addition

You are familiar with the fact, in ordinary arithmetic, that some subtractions are impossible. (We are assuming that our readers are not familiar with negative integers. They, of course, make all substractions possible.) For example, you might try to answer the question $4 - 6 = ?$ If you think of $4 - 6$ as taking 6 things from 4 things, there is no answer. It is impossible to do. You may think of this as asking *What must be added to 6 to give 4*? It is still impossible. Adding something to 6 will give a sum greater than 6. Thus the sum certainly cannot equal 4.

But now ask the question $4-6 \equiv ?$ for the integers modulo 7. If you think of this as "take-away" it is still impossible. But think of it as *What integer added to 6 gives 4*? There is an answer. Look in Table 3 for it. The next to the last number in the last row shows that $6 + 5 \equiv 4$. Therefore $4 - 6 \equiv 5$. Perhaps this is a surprising conclusion for you. By now you should begin to realize that remainder arithmetic holds certain surprises for anyone willing to follow its rules. Let us look at some other examples of subtraction.

EXAMPLE 1. What is $1 - 3 \pmod 7$?

Solution: This is the same as the question,

$$3 + ? \equiv 1 \pmod 7.$$

Table 3 shows that $3 + 5 \equiv 1$. Therefore,

$1 - 3 \equiv 5 \pmod 7$.

EXAMPLE 2. $1 - 4 \equiv ? \pmod 7$.

Solution: This means $4 + ? \equiv 1$. From Table 3 you find $4 + 4 \equiv 1$. Therefore, $1 - 4 \equiv 4 \pmod 7$.

Before giving you some practice with subtraction, let us summarize two important ways to look at the operation of subtraction.

1. Subtraction is "taking away" ($8 - 6 = 2$ because taking 6 things from 8 things leaves 2 things).
2. Subtraction "undoes" addition ($8 - 6 = 2$ because $6 + 2 = 8$).

In some elementary schools subtraction is first taught to children by the second method above. Most of us, however, learned subtraction as "take away." But then our teachers went on to show us how to check a subtraction exercise, as follows:

Subtract 256 from 819.

$$\text{Your work:}\quad \begin{array}{r} 819 \\ -256 \\ \hline 563 \end{array} \qquad\qquad \text{Your check:}\quad \begin{array}{r} 563 \\ +256 \\ \hline 819 \end{array}$$

Here you see that any careful subtraction uses the idea that subtraction "undoes" an addition. The more mathematical way to say this is *subtraction is the inverse operation of addition.* This statement has helped many people learn their subtraction facts in ordinary arithmetic. Indeed, many feel that $5 - 2 = 3$ is no different from the addition fact, $2 + 3 = 5$.

As an exploration into a new (for you) part of mathematics, we are going to ask you to do some subtraction in remainder arithmetic. You may find, as you work along, that you are learning some addition and subtraction facts in remainder arithmetic. However, we do not expect you to try to memorize any facts. You should have addition tables at hand to look them up.

PRACTICE

41. Do the following subtractions modulo 7. We suggest that you use the idea of inverse operations first. Then use an addition table modulo 7.

(a) $5 - 3 =$
(b) $5 - 6 =$
(c) $3 - 5 =$
(d) $6 - 5 =$
(e) $6 - 2 =$
(f) $2 - 6 =$
(g) $3 - 0 =$
(h) $0 - 3 =$
(i) $0 - 6 =$
(j) $0 - 5 =$
(k) $4 - 0 =$
(l) $0 - 4 =$
(m) $0 - 0 =$
(n) $5 - 5 =$

42. Make an addition table for the integers modulo 8, and then work the subtractions in Exercise 41.

43. Make an addition table for the integers modulo 6, and work the subtractions in Exercise 41 that make sense for the integers modulo 6.

44. Make an addition table for the integers modulo 15. (Refer to Exercise 34.) Then do the following subtraction exercises:

(a) $13 - 8$
(b) $8 - 13$
(c) $7 - 14$
(d) $0 - 11$
(e) $13 - 9$
(f) $9 - 13$
(g) $12 - 13$
(h) $11 - 12$
(i) $10 - 11$
(j) $9 - 10$
(k) $10 - 12$
(l) $12 - 14$
(m) $0 - 1$
(n) $0 - 2$

45. Examine the results in parts (g), (h), (i), (j), and (m) of Exercise 44. Describe what these have in common with one another.

46. Describe what (k), (l), and (n) in Exercise 44 have in common.

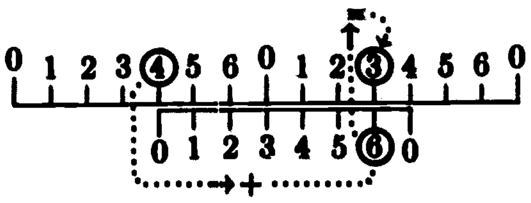
47. Do the subtraction, $0 - 3$, in the set of integers modulo 7, then modulo 8, then 9, 10, 11, 12, and 13. Describe the relation you see between the answers and the moduli. (Moduli is the plural of modulus. In the set of integers modulo 7, 7 is the modulus.)

Hint: When you are looking for a relation between two sets of numbers, a table is often helpful. Make a table like the following:

Modulus:	7	8	9	10	11	12	13
$0 - 3 \equiv$	?	?	?	?	?	?	?

48. Do the subtraction, $3 - 5$, in the set of integers modulo 9, then 10, 11, 12, 13, 14, and 15. What relation exists between these answers and the moduli?

49. To do subtraction in remainder arithmetic use the slide rule(s) that you made in Exercise 40. Here is another chance to use the idea of inverse operations to make the work easier to see. Below is a sketch of a straight slide rule, modulo 7, showing how to find $3 - 4 \equiv ?$ (mod 7). Remember, this is the same as asking $4 + ? \equiv 3$ (mod 7).



2·4. The inverse of an element with respect to addition

Let us look more closely at one of the surprising facts about remainder arithmetic. In the integers modulo 7 we have found such addition facts as $2 + 5 \equiv 0$. How strange this would be in ordinary arithmetic! Yet how sensible it is when you know the meaning of congruence ($\equiv$), or when you recall that on a calendar 7 and 0 "mean the same thing." Mathematicians have given a special name to numbers that behave in this way ($2 + 5 \equiv 0$). Since their sum is zero, you could say that each cancels out the other. In more careful mathematical language you say that each integer is the *inverse* of the other with respect to addition. Thus, 2 is the inverse of 5 (mod 7) and 5 is the inverse of 2 (mod 7).

A more precise definition of inverse follows:

> *In a number system two numbers whose sum is 0 (the identity element for addition) are called inverses of each other with respect to addition.*

You may need to go back to Section 2·2 to review the discussion of *identity element.* Although the idea of an identity element does not depend on the idea of an inverse, the opposite is not true. You cannot speak of an inverse without also speaking of the identity element.

As we have seen before, the best way to become familiar with a new idea is to practice with it. You have already done some practice that paved the way for the idea of inverse. Go back and look over your work for Exercises 37 and 38 on page 17. Now we shall give you some more practice exercises.

PRACTICE

50. For each number system listed below, list all pairs of numbers that are inverses of each other with respect to addition.

(a) The integers modulo 7.
(b) The integers modulo 4.
(c) The integers modulo 12.
(d) The integers modulo 15.
(e) The integers modulo 2.
(f) The integers modulo 1. (See Exercise 31 (d). It is hardly fair to speak of *integers* modulo 1, for there's only one!)

51. In Exercise 39, page 17, you found that 1 is the identity element with respect to multiplication for ordinary arithmetic. What is the inverse of each of the following numbers, if multiplication is the operation? Use ordinary arithmetic.

(a) 2 (Ans: $\frac{1}{2}$).
(b) 5
(c) 10
(d) 7
(e) 100
(f) 1,000,000
(g) $\frac{1}{4}$
(h) $\frac{1}{2}$
(i) $\frac{2}{3}$
(j) $\frac{3}{4}$
(k) $\frac{1}{1,000,000}$
(l) 1
(m) 0

52. (a) Complete the table below. It will show the result of subtracting 3 from each integer in the set of integers modulo 7.

$N =$	0	1	2	3	4	5	6
$N - 3 =$							

(b) The second row in the table above is exactly the same as a row in Table 3 (page 17). Which row?
(c) Your answers to (a) and (b) above lead logically to a conclusion: In the set of integers modulo 7, subtracting 3 from an integer is the same as adding______to the integer.
(d) Answer questions similar to (a), (b), and (c) above for each of the other integers modulo 7.
(e) Complete the following statement, which summarizes the results of parts (a), (b), (c), and (d) of this exercise: In the set of integers modulo 7, subtracting an integer can be done by adding the______of the integer.

53. Inverses can be helpful in addition. Observe how we calculate

$3 + 5 \pmod 7$ below:

$3 + 5 \equiv 3 + (4 + 1)$ because $5 = 4 + 1$.

$3 + (4 + 1) \equiv (3 + 4) + 1$ because regrouping the integers in a sum does not change the sum.

$(3 + 4) + 1 \equiv 0 + 1$ because 4 and 3 are inverses of each other.

$0 + 1 \equiv 1$ because 0 is the identity element

Therefore, $3 + 5 \equiv 1 \pmod 7$

Show how to use inverses to do the following additions:

(a) $3 + 6 \pmod 7$

(b) $4 + 5 \pmod 7$

(c) $4 + 6 \pmod 7$

(d) $8 + 9 \pmod{12}$

(e) $10 + 10 \pmod{15}$

(f) $10 + 10 \pmod{12}$

(g) $7 + 8 \pmod 9$

(h) $3 + 3 \pmod 4$

2·5. Remainder arithmetic—multiplication

Here again we shall ask you to go along with us without looking for "useful" applications of the ideas we develop. We should like to pursue the question, *How does multiplication behave in remainder arithmetic?* First you need to know how to multiply. We will show you multiplication in the system of integers modulo 7. Recall that this is the set of integers, $\{0, 1, 2, 3, 4, 5, 6\}$. Here are the rules:

1. The product of zero and any integer is zero.

For example:

$$0 \times 0 \equiv 0; \quad 0 \times 1 \equiv 0; \quad 5 \times 0 \equiv 0.$$

2. The product of two non-zero integers is their ordinary product if it is less than 7. If their ordinary product is 7 or greater, it is replaced by the integer congruent to it modulo 7. For example:

$3 \times 1 \equiv 3;$ $1 \times 6 \equiv 6.$

$2 \times 6 \equiv 5;$ proof: $2 \times 6 = 12,$ and $12 \equiv 5 \pmod 7$.

$6 \times 4 \equiv 3;$ proof: $6 \times 4 = 24,$ and $24 \equiv 3 \pmod 7$.

The rules for multiplication in remainder arithmetic are similar for a modulus different from 7. The exercises that follow will give you the experience needed to feel at home with multiplication.

PRACTICE

54. The multiplication table for the integers modulo 7 is Table 4. Check each entry in the table. Be sure that you can prove each multiplication fact.

55. In ordinary arithmetic, multiplication can be done by repeated addition. For example, $3 \times 4 = 12$ can be shown as $4 + 4 + 4 = 12$. In fact, we often read such a fact as *three 4's are 12*.

TABLE 4. MULTIPLICATION MODULO 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(a) Show how to get, by repeated addition, the multiplication facts in the row headed "4."

Partial solution: $4 \times 3 \equiv 5$ can be shown as follows:

$$4 \times 3 = 3 + 3 + 3 + 3$$
$$3 + 3 + 3 + 3 = 12$$
$$12 \equiv 5 \pmod 7$$
$$\text{Therefore, } 4 \times 3 \equiv 5 \pmod 7$$

(b) Show how to get, by repeated addition, the multiplication facts in the row headed "5."

(c) Show how to get, by repeated addition, the multiplication facts in the row headed "6."

56. Make a multiplication table for integers with each of the following moduli:

(a) 11 (c) 17 (e) 2
(b) 13 (d) 5 (f) 1

2·6. The identity element for multiplication

Just as 0 is the identity element for the operation of addition, you can see that 1 is an identity element for multiplication. The examples below (mod 7) illustrate this idea:

$$1 \times 3 \equiv 3 \qquad 4 \times 1 \equiv 4$$
$$1 \times 5 \equiv 5 \qquad 0 \times 1 \equiv 0$$

In every case, multiplying an integer by 1 gives the other integer as the product. The multiplication does not change the *identity* of the other integer.

You will see later (Section 2·9) that integers different from 1 can act as identity elements of their number systems. However, if the modulus is an integer not evenly divisible by another integer (except 1), there is but one identity element, 1. (An integer that is evenly divisible only by itself or 1 is called a *prime integer*.)

2·7. Division, the inverse of multiplication

There are several ways to describe division, but we will use only one. You are familiar with the way to check a division. We find that $6 \div 3 = 2$ is true because it checks: $3 \times 2 = 6$. This checking process shows that division is the inverse of multiplication. Division in the set of integers modulo 7 works the same way. See the examples below:

EXAMPLE 1. $1 \div 2 \equiv ?$ (mod 7).

Solution: The quotient is not $\frac{1}{2}$, as in ordinary arithmetic, for there is no such number as $\frac{1}{2}$ in the set of integers modulo 7. However, the question, $1 \div 2 \equiv ?$ can be asked another way: $2 \times ? \equiv 1$. You can answer this by looking at the multiplication table on page 23. Since $2 \times 4 \equiv 1$, you conclude that $1 \div 2 \equiv 4$ (mod 7).

EXAMPLE 2. $6 \div 5 \equiv ?$ (mod 7).

Solution: This is the same as $5 \times ? \equiv 6$ (mod 7). From the multiplication table modulo 7, you find that $5 \times 4 \equiv 6$. Therefore $6 \div 5 \equiv 4$ (mod 7).

The definition of division as the inverse of multiplication works in any set of integers based on any modulus. The example below is an illustration:

EXAMPLE 3. $6 \div 5 \equiv ?$ (mod 11).

Solution: This is the same as $5 \times ? \equiv 6$ (mod 11). From a multiplication table modulo 11, you find that $5 \times 10 \equiv 6$ (see Exercise 56(a), above). Therefore, $6 \div 5 \equiv 10$ (mod 11).

Notice that the speed and ease with which you can do division depends on how familiar you are with multiplication. In the practice below we do not intend that you depend on your memory of multiplication facts. Have a multiplication table at hand for easy reference.

PRACTICE

57. Use a multiplication table modulo 7 to do the following divisions:

(a) $5 \div 3$
(b) $3 \div 4$
(c) $1 \div 6$
(d) $5 \div 6$
(e) $2 \div 4$
(f) $4 \div 2$
(g) $1 \div 3$
(h) $1 \div 4$
(i) $0 \div 3$
(j) $0 \div 2$
(k) $6 \div 4$
(l) $5 \div 2$

58. Use a multiplication table modulo 11 to do the divisions in Exercise 57.

59. Use a multiplication table modulo 5 to do the divisions in Exercise 57. (*Hint*: Some can be simplified first. Since $5 \equiv 0$ (mod 5), $5 \div 3$ becomes $0 \div 3$. Likewise, $1 \div 6$ becomes $1 \div 1$. A similar simplification could have been made in parts of Exercise 43.)

60. When you search in Table 4 for an answer to $3 \div 0 \equiv ?$ (mod 7), what do you find? Is it different for $5 \div 0 \equiv ?$, $1 \div 0 \equiv ?$, or $6 \div 0 \equiv ?$

61. When you search in Table 4 for an answer to $0 \div 0 \equiv ?$ (mod 7), what do you find?

62. Review your answers to Exercises 60 and 61, and then state in your own words a rule about division by zero in the set of integers modulo 7.

63. Is the rule about division by zero for the integers modulo 7 different from the rule about division by zero in ordinary arithmetic? If so, explain the difference.

64. (a) Complete the table below. It should show the result of dividing each integer in the set of integers modulo 7 by 2.

$N =$	0	1	2	3	4	5	6
$N \div 2 \equiv$							

(b) The second row in the table above is exactly the same as a row in Table 4. Which row?

(c) Your answers to (a) and (b) above lead logically to a conclusion: In the integers modulo 7, dividing an integer by 2 is the same as multiplying the integer by ________.

(d) Answer questions similar to (a), (b), and (c) above for division by each of the other integers modulo 7.

65. Another way to divide is suggested by (or is a logical result of) the following three statements:

1. Division is the inverse of multiplication.
2. Multiplication can be performed by repeated additions. (See Exercise 55.)
3. Subtraction is the inverse of addition.

Describe the method of division suggested above.

66. The division method of Exercise 65 is illustrated below:

Ordinary arithmetic:

$6 \div 2 = 3$

$$\begin{array}{r} 6\\ -2\\ \hline 4\\ -2\\ \hline 2\\ -2\\ \hline 0 \end{array}$$

Three 2's are subtracted and 0 is the difference.

Arithmetic modulo 7:

$6 \div 5 \equiv 4$

$$\begin{array}{r} 6\\ -5\\ \hline 1\\ -5\\ \hline 3\\ -5\\ \hline 5\\ -5\\ \hline 0 \end{array}$$

Four 5's are subtracted and 0 is the difference.

Use the method of repeated subtraction to do each part of Exercise 57.

2·8. The inverse of an element with respect to multiplication

By now you should be familiar enough with congruence ($\equiv$) so that you will not confuse it with equality ($=$). Yet multiplication facts such as $4 \times 2 \equiv 1 \pmod 7$ may still look strange to you. Recall that 1 is the identity element for multiplication. Recall the definition (page 20) of the inverse of any number for addition. You may then conclude that $4 \times 2 \equiv 1$ shows that 4 and 2 are inverses of each other with respect to the operation of multiplication.

PRACTICE

67. From Table 4 list the multiplication facts that show inverses for multiplication in the system of integers modulo 7 (for example, $4 \times 2 \equiv 1$).

68. For each number system listed below, give all pairs of numbers that are inverses of each other with respect to multiplication:

(a) The integers modulo 11.
(b) The integers modulo 13.
(c) The integers modulo 17.
(d) The integers modulo 5.
(e) The integers modulo 2.
(f) The integers modulo 1.

69. Write a careful definition of what it means for a number to be the inverse of another with respect to multiplication. (*Hint*: Follow the style of the definition on page 20.)

70. If you have not already worked Exercise 64, do so now. Summarize the results of Exercise 64 with a statement similar to that used in Exercise 52(e).

2·9. Remainder arithmetic—modulus not-a-prime

This topic is a little off the main track. You will not need it when you return to the study of codes in the next section, but you may find it interesting.

Strange results occur in arithmetic in a system of integers modulus not-a-prime. (See page 23, where *prime* is defined.) Consider the examples that follow. Since 4 may be expressed as 2×2, 4 is not a prime. Similarly, 6 is not a prime, for it may be factored as 3×2. Let us show you a multiplication table for the integers modulo 4. Inspect it carefully. How is it different from other multiplication tables you have seen? The differences are in the third row, headed by "2," and in the third column, also headed by "2." Below is a list of some unusual aspects of Table 5:

1. No product of 2 and an integer is 1 or 3. (In other tables each

integer appears once in each row or column, except when zero is the multiplier.)

2. Not only is $2 \times 1 \equiv 2$, as you would expect, but also $2 \times 3 \equiv 2$! (Evidently 2 has an identity element in addition to 1.)

3. Perhaps the most unusual is the fact that $2 \times 2 \equiv 0$!

TABLE 5. MULTIPLICATION MODULO 4

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

It is natural to wonder what other mathematical oddities you can discover in the integers modulo 4. You may anticipate some strange division facts because of the close relation between division and multiplication.

We would like to have you discover some of these new features. Therefore we have tried to make the questions in the following list helpful and suggestive.

PRACTICE

71. One of the integers modulo 4 has no inverse for multiplication. Which one?

72. Using Table 5 and the definition of division (see Section 2·7), compare the results of the following:

(a) $2 \div 1$ (b) $2 \div 3$

73. Divide 2 by itself. (*Hint*: There are two different quotients.)

74. Divide 0 by 2.

Below is a multiplication table for the integers modulo 6. Check to see that you understand it. Then continue with the questions following.

TABLE 6. MULTIPLICATION MODULO 6

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

75. List the multiplication facts from Table 6 that have this form:

$$(\text{not-zero}) \times (\text{not-zero}) \equiv 0.$$

76. List the integers that on occasion act as identity elements. Show also the multiplication fact that proves this. (One such fact is $2 \times 4 \equiv 2$, showing that 4 acts as an identity element for 2 in multiplication.)

77. Usually, $0 \div N \equiv 0$ if N is not zero. When is this *not* true in the integers modulo 6?

78. What integers in this system have no inverse?

79. (a) Make a multiplication table for the integers modulo 10.
(b) Show that 10 is not a prime integer.
(c) Investigate the peculiarities of multiplication and division modulo 10 by answering questions similar to 75, 76, 77, and 78.

80. Repeat Exercise 79 for a modulus of 12.

81. Repeat Exercise 79 for a modulus of 8.

82. Write a paragraph, or make an outline, that tells what you have found about multiplication and division in remainder arithmetic with a modulus that is not a prime.

CHAPTER THREE

CODES THAT USE MATRICES

3·1. Using a matrix in coding

Let us now return to the problem of making codes. The last code you used was based on the following steps: Key 5, multiply by 2 (mod 29), Key 5. You may find it helpful to refer to Section 1·3 where this was done. Recall that all of the arithmetic there was modulo 29. We shall need the Alphabet Spiral again and have duplicated it below.

Also remember our suggestion that you make a slide rule to help you in coding. See page 8 if you want to make a slide rule for Key 5. It would be a great help in the work that follows.

To review, check the coding of the word WAR below:

$$\text{WAR} \xrightarrow{\text{Key 5}} 23\ 1\ 18 \xrightarrow[\text{modulo 29}]{\text{Multiply by 2}} 17\ 2\ 7 \xrightarrow{\text{Key 5}} \text{QBG}$$

The secret of this code lies in arithmetic modulo 29 and the multi plier 2. Obviously the code is no longer a secret when these are discovered. To disguise the multiplier further, we shall make it more complex. We shall use a "super number," which mathematicians call a *matrix*. We put the word WAR into matrix form as follows:

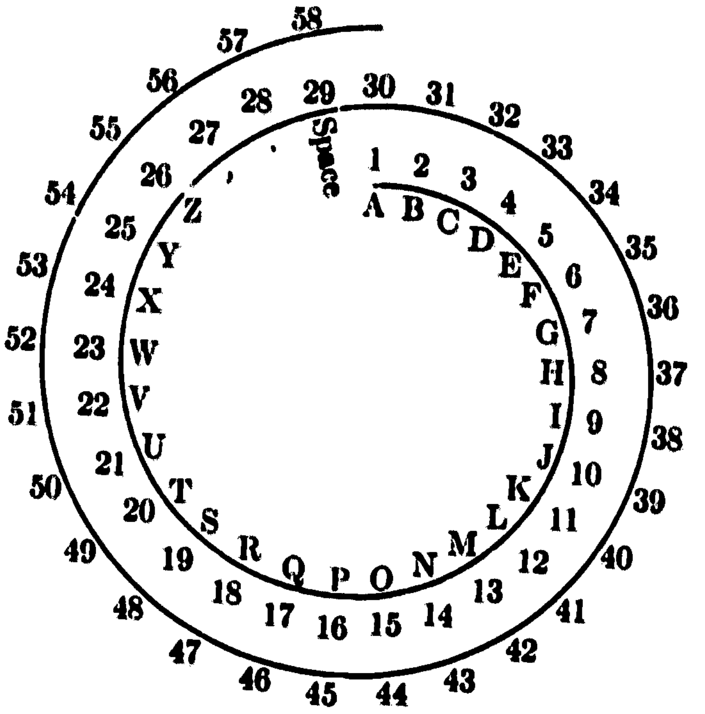
$$\begin{pmatrix} \text{W} \\ \text{A} \\ \text{R} \end{pmatrix}$$

Then we use Key 5 to change letters into numbers:

$$\begin{pmatrix} 23 \\ 1 \\ 18 \end{pmatrix}$$

(We call this matrix M, for *message*.)

Next we choose another matrix to be used as a multiplier. The numbers in this matrix do not represent letters. They do the same sort of thing as the multiplier 2 did in previous coding.



Key 5. Alphabet Spiral #1.

$$\begin{pmatrix} 2 & 0 & 1 \\ 3 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}$$ (This is matrix C, for coding.)

Matrix C is called a *square* matrix, or a three-by-three matrix. It has three rows and three columns. Matrices need not be square, obviously, for M is not. M is a three-by-one matrix, having three rows and one column. (We stretch a point in saying that M has three rows.)

It is doubtful that you could ever guess the rule for multiplying matrices. See below how we multiply C × M:

$$\begin{pmatrix} 2 & 0 & 1 \\ 3 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 23 \\ 1 \\ 18 \end{pmatrix} = \begin{pmatrix} [2 \times 23] + [0 \times 1] + [1 \times 18] \\ [3 \times 23] + [1 \times 1] + [2 \times 18] \\ [1 \times 23] + [0 \times 1] + [1 \times 18] \end{pmatrix}$$

At this stage the product looks like a big matrix, but it is only a three-by-one matrix. This becomes clear after the next two simplifying steps.

$$\begin{pmatrix} 46 + 0 + 18 \\ 69 + 1 + 36 \\ 23 + 0 + 18 \end{pmatrix} = \begin{pmatrix} 64 \\ 106 \\ 41 \end{pmatrix}$$

Written in summary form, the product we found is:

$$C \times M = \begin{pmatrix} 2 & 0 & 1 \\ 3 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 23 \\ 1 \\ 18 \end{pmatrix} = \begin{pmatrix} 64 \\ 106 \\ 41 \end{pmatrix}$$

Notice that each number in the product matrix is the result of adding the products of corresponding numbers in a *row* of the first matrix and a *column* of the second. This is why matrix multiplication is often called *row-by-column* multiplication.

The final step in coding WAR is to reduce the integers in the product matrix modulo 29 and use Key 5 to change back to letters. This is done below:

$$\begin{pmatrix} 64 \\ 106 \\ 41 \end{pmatrix} \underset{(\text{mod } 29)}{\equiv} \begin{pmatrix} 6 \\ 19 \\ 12 \end{pmatrix} \xrightarrow{\text{Key 5}} \begin{pmatrix} \text{F} \\ \text{S} \\ \text{L} \end{pmatrix}$$

Thus we would send WAR in coded form as FSL.

Let us now consider how to code a longer message. In the process you will learn more about matrix multiplication. Follow closely below as we matrix-code WAR SCARE OVER:

$$\text{(line 1)}\quad \text{WAR SCARE OVER.} \xrightarrow[\text{matrix}]{\text{3-by-5}} \begin{pmatrix} \text{W} & - & \text{A} & - & \text{E} \\ \text{A} & \text{S} & \text{R} & \text{O} & \text{R} \\ \text{R} & \text{C} & \text{E} & \text{V} & \cdot \end{pmatrix} \xrightarrow{\text{Key 5}}$$

$$\text{(line 2)}\quad \begin{pmatrix} 23 & 0 & 1 & 0 & 5 \\ 1 & 19 & 18 & 15 & 18 \\ 18 & 3 & 5 & 22 & 28 \end{pmatrix} \xrightarrow[\text{by C}]{\text{Multiply}}$$

$$\text{(line 3)}\quad \begin{pmatrix} \boxed{2 \;\; 0 \;\; 1} \\ 3 \;\; 1 \;\; 2 \\ 1 \;\; 0 \;\; 1 \end{pmatrix} \begin{pmatrix} 23 & \boxed{0} & 1 & 0 & 5 \\ 1 & \boxed{19} & 18 & 15 & 18 \\ 18 & \boxed{3} & 5 & 22 & 28 \end{pmatrix} = \begin{pmatrix} 64 & \boxed{3} & 7 & 22 & 38 \\ 106 & 25 & 31 & 59 & 89 \\ 41 & 3 & 6 & \boxed{22} & 33 \end{pmatrix} \underset{(\text{mod } 29)}{\equiv}$$

$$\text{(line 4)}\quad \begin{pmatrix} 6 & 3 & 7 & 22 & 9 \\ 19 & 25 & 2 & 1 & 2 \\ 12 & 3 & 6 & 22 & 4 \end{pmatrix} \xrightarrow{\text{Key 5}} \begin{pmatrix} \text{F} & \text{C} & \text{G} & \text{V} & \text{I} \\ \text{S} & \text{Y} & \text{B} & \text{A} & \text{B} \\ \text{L} & \text{C} & \text{F} & \text{V} & \text{D} \end{pmatrix}$$

Therefore, the coded message is FSLCYCGBFVAVIBD (with no period, all one word).

The following points may help you understand this process.

1. In line 1 spaces in the matrix of letters correspond to the spaces between words.

2. In line 2, 0 stands for a space. You could use 29, but since $29 \equiv 0 (\text{mod } 29)$, this replacement gives an easier number for computing.

3. In line 3 you can see how 22 in row 3, column 4 of the product comes from row 3 of the first matrix and column 4 of the second. You can see the same for 3 in row 1, column 2 of the product. Perhaps this helps you see (with your eyes) the row-by-column multiplication.

To feel sure of yourself in matrix multiplication, you need practice. Exercise 83 will give you practice in mutiplying several different types of matrices. The remaining exercises will involve coding.

PRACTICE

83. Do the following matrix multiplications:

(a) $\begin{pmatrix}5 & 2\\2 & 1\end{pmatrix}\begin{pmatrix}4 & 1\\7 & 2\end{pmatrix}$ (b) $\begin{pmatrix}4 & 1\\7 & 2\end{pmatrix}\begin{pmatrix}5 & 2\\2 & 1\end{pmatrix}$

(c) $\begin{pmatrix}5 & 2\\2 & 1\end{pmatrix}\begin{pmatrix}5 & 2\\2 & 1\end{pmatrix}$ (d) $\begin{pmatrix}3 & 5\\1 & 2\end{pmatrix}\begin{pmatrix}5 & 2 & 0 & 4 & 1 & 2\\1 & 3 & 1 & 0 & 3 & 5\end{pmatrix}$

(e) $\begin{pmatrix}1 & 2 & 3\\0 & 1 & 4\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1 & 0 & 2 & 3\\2 & 2 & 1 & 1 & 0\\5 & 0 & 2 & 4 & 1\end{pmatrix}$

(f) $\begin{pmatrix}4 & 2 & 3\\4 & 1 & 4\\1 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1 & 0\\2 & 2 & 1\\5 & 0 & 2\end{pmatrix}$

(g) $\begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1 & 0\\2 & 2 & 1\\5 & 0 & 2\end{pmatrix}$

(h) $\begin{pmatrix}1 & 1 & 0\\2 & 2 & 1\\5 & 0 & 2\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}$

(i) $\begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1 & 0 & 2 & 3\\2 & 2 & 1 & 1 & 0\\5 & 0 & 2 & 4 & 1\end{pmatrix}$

(j) $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}2 & 3 & 0 & 8 & 1 & 5\\1 & 5 & 2 & 6 & 4 & 0\end{pmatrix}$

(k) $\begin{pmatrix}5 & 2\\2 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$ (l) $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}5 & 2\\2 & 1\end{pmatrix}$

(m) In the 12 multiplications you have just done, are there any matrices that act as an identity for multiplication?

(n) From your experience in exercises (g) through (m), write a description of an identity matrix for multiplication.

The following multiplications are to be done modulo 29:

(o) $\begin{pmatrix}3 & 1\\5 & 2\end{pmatrix}\begin{pmatrix}2 & 28\\24 & 3\end{pmatrix}$ (p) $\begin{pmatrix}2 & 28\\24 & 3\end{pmatrix}\begin{pmatrix}3 & 1\\5 & 2\end{pmatrix}$

(q) $\begin{pmatrix}5 & 2\\2 & 1\end{pmatrix}\begin{pmatrix}1 & 27\\27 & 5\end{pmatrix}$ (r) $\begin{pmatrix}1 & 2 & 3\\0 & 1 & 4\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 27 & 5\\0 & 1 & 25\\0 & 0 & 1\end{pmatrix}$

(s) $\begin{pmatrix}1 & 27 & 5\\0 & 1 & 25\\0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\0 & 1 & 4\\0 & 0 & 1\end{pmatrix}$

(t) In each of the five multiplications you have just done you should have obtained an identity matrix. What does this mean about each pair of matrices in those exercises?

84. Use matrix C as a multiplier to code the following messages:

(a) COME HOME (no period in this message)

(b) NOT NOW.

(c) REPEAT, COME HOME (no period)

(d) IN A MINUTE.

After learning to code by matrix multiplication, your next step, naturally, is to investigate decoding. Your experience with identity elements (Section 2·6), inverse operations (Section 2·7), inverses of numbers (Section 2·8), and matrices (Exercises 83(m) and (n)) leads you to consider two possibilities, namely:

1. Decode by dividing by a matrix (division is the inverse of multiplication).

2. Multiply by the inverse (with respect to multiplication) of the coding matrix.

A rule for dividing by a matrix would be extremely complicated. Therefore we use the inverse of a matrix when we want to divide by it. (Not all matrices have inverses. This is similar to the fact that not all integers modulo 4 have inverses.) We shall not go into the details of how to find the inverse (for multiplication) of a matrix, but shall supply an inverse whenever you need it.

When we coded WAR SCARE OVER, we got FSLCYCGBFVAVIBD as the coded message. The matrix multiplier was

$$C = \begin{pmatrix} 2 & 0 & 1 \\ 3 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}$$

The inverse of C is given below:

$$C^{\text{inverse}} = \begin{pmatrix} 1 & 0 & 28 \\ 28 & 1 & 28 \\ 28 & 0 & 2 \end{pmatrix}$$

To be sure that the matrix above is in fact the inverse of matrix C, let us go through the multiplication of the two:

$$C \times C^{\text{inverse}} = \begin{pmatrix} 2 & 0 & 1 \\ 3 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 28 \\ 28 & 1 & 28 \\ 28 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 30 & 0 & 58 \\ 87 & 1 & 116 \\ 29 & 0 & 30 \end{pmatrix}$$

$$\underset{(\text{mod } 29)}{\equiv} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which is the identity for 3-by-3 matrices.

Just as multiplying 15 by $\frac{1}{3}$ will result in 5, the number that was multiplied by 3 to get 15, so multiplying the matrix for FSLCYCGBFVAVIBD by the inverse of C should give WAR SCARE OVER. Below you can follow the process:

$$\text{(line 1) FSLCYCGBFVAVIBD} \xrightarrow[\text{matrix}]{\text{3-by-5}} \begin{pmatrix} F & C & G & V & I \\ S & Y & B & A & B \\ L & C & F & V & D \end{pmatrix} \xrightarrow{\text{Key 5}}$$

$$\text{(line 2)} \quad \begin{pmatrix} 6 & 3 & 7 & 22 & 9 \\ 19 & 25 & 2 & 1 & 2 \\ 12 & 3 & 6 & 22 & 4 \end{pmatrix} \xrightarrow[C^{\text{inverse}}]{\text{Multiply by}}$$

$$\text{(line 3)} \quad \begin{pmatrix} 1 & 0 & 28 \\ 28 & 1 & 28 \\ 28 & 0 & 2 \end{pmatrix} \begin{pmatrix} 6 & 3 & 7 & 22 & 9 \\ 19 & 25 & 2 & 1 & 2 \\ 12 & 3 & 6 & 22 & 4 \end{pmatrix} =$$

$$\text{(line 4)} \quad \begin{pmatrix} 342 & 87 & 175 & 638 & 121 \\ 523 & 193 & 366 & 1233 & 366 \\ 192 & 90 & 208 & 660 & 260 \end{pmatrix} \equiv \text{(mod 29)}$$

$$\text{(line 5)} \quad \begin{pmatrix} 23 & 0 & 1 & 0 & 5 \\ 1 & 19 & 18 & 15 & 18 \\ 18 & 3 & 5 & 22 & 28 \end{pmatrix} \xrightarrow{\text{Key 5}} \begin{pmatrix} W & - & A & - & E \\ A & S & R & O & R \\ R & C & E & V & . \end{pmatrix}$$

Following are some comments on this decoding.

1. In line 4 the arithmetic becomes involved, unfortunately, because of the size of the numbers. If negative numbers are used, the arithmetic is simpler, since the numbers are smaller. Using negative integers modulo 29, we obtain the inverse of C as follows:

$$\begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & -1 \\ -1 & 0 & 2 \end{pmatrix}$$

The reader may try this form of the inverse of C to decode FSLCYCGBFVAVIBD.

2. To go from line 4 to line 5, we reduce all the integers in line 4 to congruent integers, modulo 29. To accomplish this easily without the aid of a calculator, a list of multiples of 29 is needed (see Table 7). For example, we find that 342 $\equiv$ 23 (mod 29) by locating 342 in Table 7 between 319 and 348. Since 342 = 319 + 23, and 319 is exactly divisible by 29, then 23 is the remainder for 342 ÷ 29. Therefore 342 $\equiv$ 23 (mod 29).

TABLE 7. MULTIPLES OF 29

29	319	609	899	1189
58	348	638	928	1218
87	377	667	957	1247
116	406	696	986	1276
145	435	725	1015	1305
174	464	754	1044	1334
203	493	783	1073	1363
232	522	812	1102	1392
261	551	841	1131	1421
290	580	870	1160	1450

PRACTICE

85. Decode the messages coded in Exercise 84, using the inverse of matrix C given on page 33.

86. Below are some messages that were coded by using matrix C. Find the original messages. They are all related to one topic.

(a) TIQ I IKAMUHBUA
(b) KBOFUFOIOZOM.WWXCL
(c) RQIFKTAGAC N
(d) UNTVLGWBCHFJAGO
(e) DPZPXH

3•2. Additional facts about matrix multiplication

Perhaps you noticed that the answers to Exercises 83(a) and (b) (page 32) are not the same, although the same two matrices were multiplied in each case. This interesting fact bears repeating below:

$$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix} = \begin{pmatrix} 34 & 9 \\ 15 & 4 \end{pmatrix} \text{but} \begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix}\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 22 & 9 \\ 39 & 16 \end{pmatrix}$$

If we let A and B stand for these two matrices, the fact above can be stated quite simply as follows:

$$A \times B \neq B \times A.$$

In other words, the product of these two matrices depends on the order in which they are multiplied. This is certainly different from the way numbers usually behave in multiplication. Of course we have not called matrices numbers. True, we called them "super numbers," but were careful to use quotation marks to show that we were not dead serious. The law that these matrices seem to be breaking is called the *Commuta-*

tive Law for Multiplication. If x and y represent any two numbers such as integers, fractions, irrational numbers, or imaginary numbers, then the commutative law for multiplication appears as follows:

$$xy = yx.$$

Some matrix multiplications are commutative; some are not. Below are exercises that will offer you more experience with this new idea:

PRACTICE

87. In Exercises 83(f) and (g) multiply in reverse order and comment on your results.

88. In Exercise 83(d) what is the result when you try to multiply in reverse order?

89. In view of your answers in Exercise 83 and all of your matrix multiplication to date, state a rule that tells what sizes two matrices must be before they can be multiplied.

Another fact about matrix multiplication may be discovered by examining again Exercises 83(g) and (h), repeated below:

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&0\\2&2&1\\5&0&2\end{pmatrix}=\begin{pmatrix}1&1&0\\2&2&1\\5&0&2\end{pmatrix}$$

$$\begin{pmatrix}1&1&0\\2&2&1\\5&0&2\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1&0\\2&2&1\\5&0&2\end{pmatrix}$$

Evidently, the matrix shown below is an identity matrix, for it does not change the other matrix in the multiplication. (You may want to refer back to Section 2·6.)

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \qquad \text{(An identity matrix)}$$

PRACTICE

90. Will the matrix above be an identity matrix for the one below?

$$\begin{pmatrix}1&1&0&2&3\\2&2&1&1&0\\5&0&2&4&1\end{pmatrix} \qquad \text{(Use this matrix on the right.)}$$

91. Using the identity matrix above as a guide, find the identity ma-

trix for multiplication (used on the left) for each matrix below. Do the multiplication to show that you are correct.

(a) $\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$ (b) $\begin{pmatrix} 5 & 2 & 0 & 4 & 1 & 2 \\ 1 & 3 & 1 & 0 & 3 & 5 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 3 & 1 & 0 & 2 \end{pmatrix}$

(e) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 2 & 1 & 3 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

92. What seems to be true about the form of all of the identity matrices you have found so far?

93. In Exercise 91 you found for each matrix another matrix that, *used on the left*, is an identity matrix for multiplication. Mathematicians call this a *left identity*. Now, for each matrix in Exercise 91, try its left identity on the right to see if it is also a right identity.

There are other aspects of inverses of matrices that will interest you. (It may help you to refer to Section 2·8.) You have already seen how the inverse of a coding matrix can be used to decode a message (page 34). Although we shall not show you how to find the inverse of a matrix, there are some interesting facts about inverses which you can observe by working with them. Try the exercises that follow:

PRACTICE

94. Below are some matrices and their inverses. Multiply them together, first in the order given, then in reverse order. (Notice that some negative integers appear in most of the inverses. If you are not familiar enough with negative integers in arithmetic, you may change each negative integer to a positive one modulo 29, and use remainder arithmetic

modulo 29. To do this, make the following replacements: 28 for -1; 27 for -2; 26 for -3; 25 for -4; 24 for -5; 23 for -6; and 22 for -7.)

(a) $M = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$; $\quad M^{\text{inverse}} = \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix}$

(b) $M = \begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix}$; $\quad M^{\text{inverse}} = \begin{pmatrix} 2 & -1 \\ -7 & 4 \end{pmatrix}$

(c) $M = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}$; $\quad M^{\text{inverse}} = \begin{pmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{pmatrix}$

(d) $M = \begin{pmatrix} 4 & 2 & 3 \\ 4 & 1 & 4 \\ 1 & 0 & 1 \end{pmatrix}$; $\quad M^{\text{inverse}} = \begin{pmatrix} 1 & -2 & -5 \\ 0 & 1 & -4 \\ -1 & 2 & -4 \end{pmatrix}$

(e) $M = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$; $\quad M^{\text{inverse}} = \begin{pmatrix} 1/3 & 0 & 0 \\ 0 & 1/3 & 0 \\ 0 & 0 & 1/3 \end{pmatrix}$

(f) $M = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1/3 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & .2 \end{pmatrix}$; $\quad M^{\text{inverse}} = \begin{pmatrix} .5 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & .25 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$

CHAPTER FOUR

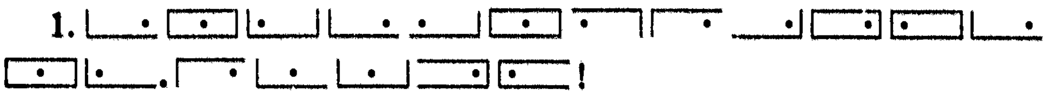
CONCLUSION

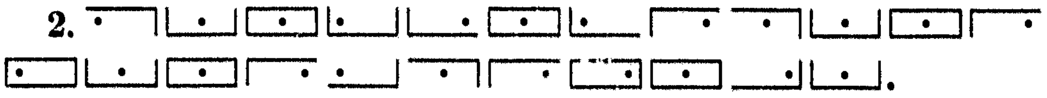
We have tried, in this booklet, to introduce you to some ideas that are found in modern mathematics. Our "gimmick" was coding and decoding secret messages. There are much better ways to code than our matrix modulo-29 method. We intended this merely to be an enjoyable way to become acquainted with some ideas from number theory (arithmetic modulo an integer), from foundations of mathematics (identity, inverse, miniature number systems), and from modern algebra (arithmetic with matrices).

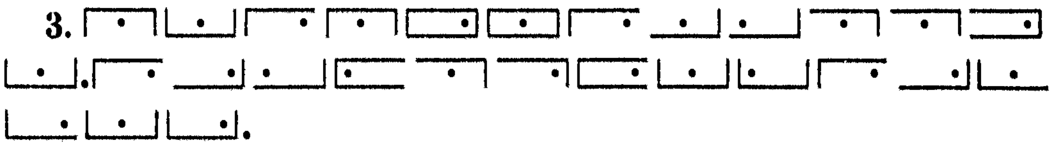
As we have said before, these topics were introduced to you for the fun of it. From the work you have done with them, you may have the idea that a matrix is a sort of "super number." Matrices are used in many ways that are practical, in the sense of helping solve problems in physical and social sciences, and theoretical, in the sense of developing general mathematical theories. In algebra, matrices are helpful in solving sets of equations, such as a set of six equations in six unknowns. They are also used in deriving theories (or rules) for solving many sorts of sets of equations. In geometry, matrices can be used to describe and work with transformations of points. The field of physics makes use of matrix theory in many of its areas, an important one being quantum mechanics. Probability, as developed mathematically, uses matrices to good advantage. When you consider that the topic of probability can in turn apply to many other areas, you see that the idea of a matrix and its arithmetic has broad usage.

Although we can only suggest some areas of application for the ideas in this booklet, we hope we have shown you that these ideas are much more than playthings. There are many interesting and challenging uses to be made of mathematics today and in the future. Mathematics is not a completed, finished, or dead subject; it is alive and growing, and new mathematics is being created continually. Truly, you can never get enough mathematics. We hope that your experience with this booklet will leave you hungry for more.

ANSWERS

1. 

2. 

3. 

4. WILL HAVE VICTORY DANCE AT DAWN.

5. SWELL! WILL BRING HOT DOGS FOR BREAKFAST.

6. DONT FORGET MUSTARD.

7. (a) HFSSTY HTRJ STB.
   (b) HTRJ FY TSHJ. WJUJFY, FY TSHJ.
   (c) KQFY YNWJ TS GNPJ. MFAJ YT BFQP.
   (d) BFQP? ITSY! ITSY! WZS!

8. (a) WHAT IS THE HURRY?
   (b) CAUGHT TWO BIG FISH.
   (c) GOOD. LETS HAVE FISH FRY.
   (d) THEY ARENT THAT BIG.

9. GAFVJK KA ZAA. XJBOJI BK .AA.,

10. NAAH XMFV, PBCCU XB.HR.N,

11. BGGROJH BK .AA., .A A.J PJGJ,

12. CONGRATULATIONS. ANY GREEN CHEESE.

13. NONE. SAW OTHER SIDE OF MOON.

14. WHAT WAS IT LIKE.

15. JUST LIKE OTHER SIDE.

17.	3 × 1 ≡ 3	3 × 10 ≡ 1	3 × 20 ≡ 2
	3 × 2 ≡ 6	3 × 11 ≡ 4	3 × 21 ≡ 5
	3 × 3 ≡ 9	3 × 12 ≡ 7	3 × 22 ≡ 8
	3 × 4 ≡ 12	3 × 13 ≡ 10	3 × 23 ≡ 11
	3 × 5 ≡ 15	3 × 14 ≡ 13	3 × 24 ≡ 14
	3 × 6 ≡ 18	3 × 15 ≡ 16	3 × 25 ≡ 17
	3 × 7 ≡ 21	3 × 16 ≡ 19	3 × 26 ≡ 20
	3 × 8 ≡ 24	3 × 17 ≡ 22	3 × 27 ≡ 23
	3 × 9 ≡ 27	3 × 18 ≡ 25	3 × 28 ≡ 26
		3 × 19 ≡ 28	3 × 29 ≡ 29

18. (c) 40 ≡ 69, for each has a remainder of 11. Both stand for K.

(d) $79 \equiv 108$, for each has a remainder of 21.

(e) $60 \equiv 118$, for each has a remainder of 2.

(f) $65 \not\equiv 136$ (read: "65 is not congruent to 136"), for 65 has a remainder of 7 while 136 has a remainder of 20. Also, 65 stands for G, but 136 stands for T.

(g) $44 \not\equiv 103$.

(h) $115 \equiv 57$.

(i) $72 \equiv 14$. (Notice that $14 \div 29 = 0$ with a remainder of 14. Thus, $14 \equiv 14$!)

(j) $122 \not\equiv 141$.

(k) $3 \equiv 61$. (Notice that $3 \equiv 3$, for 3 has a remainder of 3 when divided by 29.)

19. Yes. Every number is congruent to itself. $125 \equiv 125 \pmod{29}$, because 125 has a remainder of 9 when divided by 29. So does 125! See also remarks in 18 (i) and (k) above.

20. (a) There is an unlimited number.
(b) The numbers congruent to 3 are 3, 32, 61, 80, 109, 138, and so on, without end.

21. $4 \equiv 4, 33, 62, 91, 120, 149$.
$10 \equiv 10, 39, 68, 97, 126, 155$.
$15 \equiv 15, 44, 73, 102, 131, 160$.
$22 \equiv 22, 51, 80, 109, 138, 167$.
$29 \equiv 29, 58, 87, 116, 145, 174$.

22. (a) The numbers congruent to 4 (mod 29) are 4, 33, 62, and so on, where the next number in the sequence is 29 more than the one before it.
(b)–(e) Each rule is similar to that in (a).

23. (c) $1 + 4 \equiv 1$
(d) $1 + 8 \equiv 1$
(e) $1 + 6 \equiv 3$
(f) $1 + 10 \equiv 3$
(g) $1 + 12 \equiv 1$

24. (a) $3 + 1 = 4$
(b) $3 + 2 \equiv 1$
(c) $3 + 3 \equiv 2$
(d) $3 + 4 \equiv 3$
(e) $3 + 5 \equiv 4$
(f) $3 + 6 \equiv 1$
(g) $3 + 7 \equiv 2$
(h) $3 + 8 \equiv 3$

25. (a) 4 (b) (1, 2, 3, 4)

26.

+	1	2	3	4
1	2	3	4	1
2	3	4	1	2
3	4	1	2	3
4	1	2	3	4

27. 4 behaves like zero.

28. (a) The first five rows are as follows:

+	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1
2	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2
3	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3
4	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4
5	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5
·	·	·	·												
·	·	·	·												
·	·	·	·												

(b) 15.

29. The first three rows are as follows:

+	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
·	·	·	·									
·	·	·	·									
·	·	·	·									

31. (a)

+	1	2	3	4	5
1	2	3	4	5	1
2	3	4	5	1	2
3	4	5	1	2	3
4	5	1	2	3	4
5	1	2	3	4	5

(b)

+	1	2	3	4	5	6
1	2	3	4	5	6	1
2	3	4	5	6	1	2
3	4	5	6	1	2	3
4	5	6	1	2	3	4
5	6	1	2	3	4	5
6	1	2	3	4	5	6

(c)

+	1	2
1	2	1
2	1	2

(d)

+	1
1	1

32. (a) $2_7 = \{2, 9, 16, \cdots\}$ $5_7 = \{5, 12, 19, \cdots\}$
$3_7 = \{3, 10, 17, \cdots\}$ $6_7 = \{6, 13, 20, \cdots\}$
$4_7 = \{4, 11, 18, \cdots\}$ $7_7 = \{7, 14, 21, \cdots\}$.

(b) 4.
$1_4 = \{1, 5, 9, \cdots\}$ $3_4 = \{3, 7, 11, \cdots\}$
$2_4 = \{2, 6, 10, \cdots\}$ $4_4 = \{4, 8, 12, \cdots\}$.

(c) $1_5 = \{1, 6, 11, \cdots\}$ $4_5 = \{4, 9, 14, \cdots\}$
$2_5 = \{2, 7, 12, \cdots\}$ $5_5 = \{5, 10, 15, \cdots\}$.
$3_5 = \{3, 8, 13, \cdots\}$

33.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

34. Replace every 15 by 0. Rearrange the rows and columns so that 0 comes before 1.

35. Replace every 12 by 0. Rearrange rows and columns as in Exercise 34.

37. $3 + 4 \equiv 0; 4 + 3 \equiv 0; 5 + 2 \equiv 0; 6 + 1 \equiv 0$. Notice that the last three addition facts are "repeats." You get the same sum no matter what order you use for adding. For example, $3 + 4$ is the same as $4 + 3$.

38. (a) $0 + 0 \equiv 0; 1 + 3 \equiv 0; 2 + 2 \equiv 0; 3 + 1 \equiv 0$.
(b) $0 + 0 \equiv 0; 1 + 14 \equiv 0; 2 + 13 \equiv 0; 3 + 12 \equiv 0; 4 + 11 \equiv 0; 5 + 10 \equiv 0; 6 + 9 \equiv 0; 7 + 8 \equiv 0$; plus seven more facts that repeat the preceding seven.

39. (a) 1.
(b) $1 \times 3 = 3; 5 \times 1 = 5; 4.25 \times 1 = 4.25$.

41.

(a)	2	(f)	3	(k)	4
(b)	6	(g)	3	(l)	3
(c)	5	(h)	4	(m)	0
(d)	1	(i)	1	(n)	0.
(e)	4	(j)	2		

42.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a)	2	(h)	5
(b)	7	(i)	2
(c)	6	(j)	3
(d)	1	(k)	4
(e)	4	(l)	4
(f)	4	(m)	0
(g)	3	(n)	0

43.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(a) 2
(b) No answer, because 6 is not in the set of integers modulo 6.
(c) 4
(d) No answer
(e) No answer
(f) No answer
(g) 3
(h) 3
(i) No answer
(j) 1
(k) 4
(l) 2
(m) 0
(n) 0

44. (a) 5
(b) 10
(c) 8
(d) 4
(e) 4
(f) 11
(g) 14
(h) 14
(i) 14
(j) 14
(k) 13
(l) 13
(m) 14
(n) 13

45. In each case the difference is the same, 14. In each case the number subtracted (subtrahend) is an integer 2 larger than the one subtracted from (minuend).

46. In each case the difference is 12. In each case the subtrahend is 1 larger than the minuend.

47.

Modulus	7	8	9	10	11	12	13
$0 - 3 \equiv$	4	5	6	7	8	9	10

As the modulus increases, the value of $0 - 3$ increases by the same amount.

48.

Modulus	9	10	11	12	13	14	15
$3 - 5 \equiv$	7	8	9	10	11	12	13

The relation is the same as that seen in Exercise 47.

50. (a) 1 and 6, 2 and 5, 3 and 4, 0 and 0.
(b) 1 and 3, 2 and 2, 0 and 0.
(c) 1 and 11, 2 and 10, 3 and 9, 4 and 8, 5 and 7, 6 and 6, 0 and 0.
(d) 1 and 14, 2 and 13, 3 and 12, 4 and 11, 5 and 10, 6 and 9, 7 and 8, 0 and 0.
(e) 1 and 1, 0 and 0.
(f) 0 is the only integer, and is its own inverse!

51. (b) $\frac{1}{5}$
(c) $\frac{1}{10}$, or 0.1
(d) $\frac{1}{7}$
(e) 0.01
(f) 0.000001
(g) 4
(h) 2
(i) $\frac{3}{2}$, or 1.5
(j) $\frac{4}{3}$, or $1\frac{1}{3}$
(k) 1,000,000
(l) 1
(m) There is none.

52. (a) 4, 5, 6, 0, 1, 2, 3.
(b) The row headed "4."
(c) 4.
(d) Partial answer, using the integer 5:

1.

$N =$	0	1	2	3	4	5	6
$N - 5 \equiv$	2	3	4	5	6	0	1

2. The row headed "2."
3. In the set of integers modulo 7, subtracting 5 from an integer is the same as adding 2 to the integer.

(e) Inverse.

53. (a)

$$\begin{aligned} 3 + 6 &\equiv 3 + (4 + 2) \\ 3 + (4 + 2) &\equiv (3 + 4) + 2 \\ (3 + 4) + 2 &\equiv 0 + 2 \\ 0 + 2 &\equiv 2 \\ \text{Therefore,}\quad 3 + 6 &\equiv 2 \pmod{7}. \end{aligned}$$

(b)

$$\begin{aligned} 4 + 5 &\equiv 4 + (3 + 2) \\ &\equiv (4 + 3) + 2 \\ &\equiv 0 + 2 \\ &\equiv 2 \pmod{7}. \end{aligned}$$

(c) Hint: $6 = (3 + 3)$.
(d) Hint: $9 = 4 + 5$, and $8 + 4 \equiv 0$.
(e) Hint: $10 = 5 + 5$.
(f) Hint: $10 \equiv 2 + 8$.
(g) Hint: $8 = 2 + 6$.
(h) Hint: $3 \equiv 1 + 2$.

56. (a)

×	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

(b)

×	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	1	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	1	4	7	10
4	0	4	8	12	3	7	11	2	6	10	1	5	9
5	0	5	10	2	7	12	4	9	1	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	1	7
7	0	7	1	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	1	9	4	12	7	2	10	5
9	0	9	5	1	10	6	2	11	7	3	12	8	4
10	0	10	7	4	1	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	1	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	1

(c)

×	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	0	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	0	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	0	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	0	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	0	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	0	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	0	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	0	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	0	11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	0	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	0	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	0	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	0	15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	0	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

(d)

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(e)

×	0	1
0	0	0
1	0	1

(f)

×	0
0	0

!

57.	(a) 4	(c) 6	(e) 4	(g) 5	(i) 0	(k) 5
	(b) 6	(d) 2	(f) 2	(h) 2	(j) 0	(l) 6
58.	(a) 9	(c) 2	(e) 6	(g) 4	(i) 0	(k) 7
	(b) 9	(d) 10	(f) 2	(h) 3	(j) 0	(l) 8
59.	(a) 0	(c) 1	(e) 3	(g) 2	(i) 0	(k) 4
	(b) 2	(d) 5	(f) 2	(h) 4	(j) 0	(l) 0

60. There is no integer modulo 7 that gives 3 when multiplied by 0. Therefore, $3 \div 0$ has no answer. This is true of the others.

61. Each one of the integers modulo 7 could serve as the quotient in $0 \div 0 \equiv ?$ (mod 7). For example, $0 \div 0 \equiv 3$ checks, for $0 \times 3 \equiv 0$. But $0 \div 0 \equiv 5$ checks also, for $0 \times 5 \equiv 0$.

62. The rule has two parts:
   (a) There is no answer when a non-zero number is divided by zero. In other words, it is impossible to divide a non-zero number by zero.
   (b) Any integer in the set of integers modulo 7 can be the answer to $0 \div 0 \equiv ?$. (Since there is no way to find out which one of the integers is *the* answer, mathematicians usually say that $0 \div 0$ is also impossible.)

63. There is no difference.

64. (a) 0, 4, 1, 5, 2, 6, 3.
   (b) The row headed by "4."
   (c) 4.
   (d) Partial solution, using the integer 5:
      (1)

$N =$	0	1	2	3	4	5	6
$N \div 5 \equiv$	0	3	6	2	5	1	4

      (2) The row headed by "3."
      (3) In the set of integers modulo 7, dividing an integer by 5 is the same as multiplying the integer by 3.

65. Division can be performed by repeated subtraction. The divisor is subtracted again and again from the dividend until the difference becomes zero. The quotient is the number of subtractions done.

67. $1 \times 1 \equiv 1$, $2 \times 4 \equiv 1$, $3 \times 5 \equiv 1$, $4 \times 2 \equiv 1$, $5 \times 3 \equiv 1$, $6 \times 6 \equiv 1$. Notice that two facts are repeated, showing that the order

in which two integers are multiplied does not change the product. To summarize, the following integers are inverses of each other, modulo 7:

2 and 4   3 and 5   1 and 1   6 and 6

68. (a) See Exercise 56(a).

1 and 1   3 and 4   7 and 8
2 and 6   5 and 9   10 and 10

(b) See Exercise 56(b).

1 and 1   4 and 10   6 and 11
2 and 7   5 and 8   12 and 12
3 and 9

(e) See Exercise 56(c).

1 and 1   4 and 13   10 and 12
2 and 9   5 and 7   11 and 14
3 and 6   8 and 15   16 and 16

(d) See Exercise 56(d).

1 and 1   2 and 3   4 and 4

(e) See Exercise 56(e).

1 and 1

(f) See Exercise 56(f).

0 is its own inverse. There is only one integer in this set. Since $0 \times 0 \equiv 0$, then 0 must be the identity element. Also, $0 \div 0$ must be 0. (Notice that if you decide to rename 0, calling it 1 because it is the identity element, then 1 is the one integer in this set. The one multiplication fact would then be $1 \times 1 \equiv 1$.)

69. In any number system two numbers whose product is the identity element for multiplication are called inverses of each other with respect to multiplication.

70. In the set of integers modulo 7, division by an integer can be done by multiplying by the inverse of the integer.

71. 2 has no inverse. (Perhaps this makes up for its having an extra identity!)

72. $2 \div 1 \equiv 2$; $2 \div 3 \equiv 2$. (This is surprising. Ordinarily when you divide an integer by two different integers, the quotients are different.)

73. $2 \div 2 \equiv 1$; $2 \div 2 \equiv 3$. (Proof of the latter: $2 \times 3 \equiv 2$ modulo 4.)

74. $0 \div 2 \equiv 0$; $0 \div 2 \equiv 2$.

75. $2 \times 3 \equiv 0$ (also $3 \times 2 \equiv 0$).
$3 \times 4 \equiv 0$ (also $4 \times 3 \equiv 0$).

76. (a) 1, of course, is always an identity element, since $1 \times N \equiv N$ for any N whatsoever.

(b) 5 acts as an identity element for 3: $5 \times 3 \equiv 3$.

(c) 3 acts as an identity element for itself: $3 \times 3 \equiv 3$.

(d) 4 acts as an identity element for itself: $4 \times 4 \equiv 4$.

77. (a) For $N = 2$: $0 \div 2 \equiv 3$ (as well as $0 \div 2 \equiv 0$).

(b) For $N = 3$: $0 \div 3 \equiv 2$ (as well as $0 \div 3 \equiv 0$).

(c) For $N = 4$: $0 \div 4 \equiv 3$ (as well as $0 \div 4 \equiv 0$).

78. 2, 3, and 4.

83. (a) $\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix} = \begin{pmatrix} 20 + 14 & 5 + 4 \\ 8 + 7 & 2 + 2 \end{pmatrix} = \begin{pmatrix} 34 & 9 \\ 15 & 4 \end{pmatrix}$

(b) $\begin{pmatrix} 22 & 9 \\ 39 & 16 \end{pmatrix}$ (c) $\begin{pmatrix} 29 & 12 \\ 12 & 5 \end{pmatrix}$

(d) $\begin{pmatrix} 20 & 21 & 5 & 12 & 18 & 31 \\ 7 & 8 & 2 & 4 & 7 & 12 \end{pmatrix}$

(e) $\begin{pmatrix} 20 & 5 & 8 & 16 & 6 \\ 22 & 2 & 9 & 17 & 4 \\ 5 & 0 & 2 & 4 & 1 \end{pmatrix}$ (f) $\begin{pmatrix} 23 & 8 & 8 \\ 26 & 6 & 9 \\ 6 & 1 & 2 \end{pmatrix}$

(g) $\begin{pmatrix} 1 & 1 & 0 \\ 2 & 2 & 1 \\ 5 & 0 & 2 \end{pmatrix}$ (Notice that one of the two matrices in g "acts like" 1 in multiplication.)

(h) $\begin{pmatrix} 1 & 1 & 0 \\ 2 & 2 & 1 \\ 5 & 0 & 2 \end{pmatrix}$ (i) $\begin{pmatrix} 1 & 1 & 0 & 2 & 3 \\ 2 & 2 & 1 & 1 & 0 \\ 5 & 0 & 2 & 4 & 1 \end{pmatrix}$

(j) $\begin{pmatrix} 2 & 3 & 0 & 8 & 1 & 5 \\ 1 & 5 & 2 & 6 & 4 & 0 \end{pmatrix}$ (k) $\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$ (l) $\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$

(m) Yes. The matrix on the left in (i), (j), and (l); the matrix on the right in (h) and (k).

(n) An identity matrix is a square matrix with 1's on the main diagonal (upper left to lower right) and 0's everywhere else.

(o) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (p) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (q) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

(r) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (s) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

(t) In each case, one of the two matrices being multiplied is the inverse of the other. For example:

$$\begin{pmatrix}3 & 1\\5 & 2\end{pmatrix} \text{ is the inverse of } \begin{pmatrix}2 & 28\\24 & 3\end{pmatrix};$$

$$\begin{pmatrix}1 & 27 & 5\\0 & 1 & 25\\0 & 0 & 1\end{pmatrix} \text{ is the inverse of } \begin{pmatrix}1 & 2 & 3\\0 & 1 & 4\\0 & 0 & 1\end{pmatrix}.$$

84. (a) COME HOME $\xrightarrow[\text{matrix}]{\text{3-by-3}} \begin{pmatrix}C & E & O\\O & - & M\\M & H & E\end{pmatrix} \xrightarrow{\text{Key 5}}$

$$\begin{pmatrix}3 & 5 & 15\\15 & 0 & 13\\13 & 8 & 5\end{pmatrix} \xrightarrow[\text{by C}]{\text{multiply}}$$

$$\begin{pmatrix}2 & 0 & 1\\3 & 1 & 2\\1 & 0 & 1\end{pmatrix}\begin{pmatrix}3 & 5 & 15\\15 & 0 & 13\\13 & 8 & 5\end{pmatrix} = \begin{pmatrix}19 & 18 & 35\\50 & 31 & 68\\16 & 13 & 20\end{pmatrix} \underset{(\text{mod } 29)}{\equiv}$$

$$\begin{pmatrix}19 & 18 & 6\\21 & 2 & 10\\16 & 13 & 20\end{pmatrix} \xrightarrow{\text{Key 5}} \begin{pmatrix}S & R & F\\U & B & J\\P & M & T\end{pmatrix}$$

Therefore, the coded message is SUPRBMFJT.

(b) The product matrix is $\begin{pmatrix}48 & 15 & 46\\97 & 44 & 69\\34 & 15 & 23\end{pmatrix}$,

which results in the coded message, SJEOOOQKW.

(c) WDEA,Y. AFJTOIOZOM

(d) RLIO NJYAKGT

86. (a) CAN I HAVE CAR

(b) YES IF HOME EARLY

(c) IS ONE EARLY

(d) ABSOLUTELY NOT

(e) GOSH (Notice that the original message was a four-letter word, but when coded it became a six-letter word.)

87. For 83(f), the result shows that multiplication is not commutative for these two matrices.

$$\begin{pmatrix}8 & 3 & 7\\17 & 6 & 15\\22 & 10 & 17\end{pmatrix}$$

For 83(g), the result shows that multiplication *is* commutative for these two matrices. To see whether this is caused by one or both, you will have to experiment further.

$$\begin{pmatrix}1 & 1 & 0\\2 & 2 & 1\\5 & 0 & 2\end{pmatrix}$$

88. The multiplication cannot be performed. The two-by-five matrix, when put on the left, has too many columns (or the other matrix has too few rows) for row-by-column multiplication.

89. Two matrices can be multiplied when the left-hand matrix has as many rows as the right-hand matrix has columns.

90. Yes.

91. (a) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

(e) A seven-by-seven matrix with 1's on the main diagonal (upper left to lower right) and 0's everywhere else.

92. They are square; they have 1's on the main diagonal (upper left to lower right); they have 0's everywhere else.

93. For (a) and (c), the left identities are also right identities. For (b), (d), and (e), they are not; in each of these cases the left identity does not have enough rows or columns.

94. Each result should be an identity matrix of the proper size.

ERIC

REFERENCE LIST

ALBERT, A. ADRIAN. *Introduction to Algebraic Theories*. Chicago: University of Chicago Press, 1941.

ANDREE, RICHARD V. *Modern Abstract Algebra*. New York: Henry Holt & Co., 1958.

BIRKHOFF, GARRETT, AND MACLANE, SAUNDERS. *A Survey of Modern Algebra*. New York: The Macmillan Co., 1958.

COURANT, RICHARD, AND ROBBINS, HERBERT. *What Is Mathematics?* New York: Oxford University Press, 1941.

KEMENY, JOHN G.; SNELL, J. LAURIE; AND THOMPSON, GERALD L. *Introduction to Finite Mathematics*. Englewood Cliffs, N. J.: Prentice-Hall, 1957.

MURDOCH, DAVID CARRUTHERS. *Linear Algebra for Undergraduates*. New York: John Wiley & Sons, 1957.

STEWART, BONNIE M. *Theory of Numbers*. New York: The Macmillan Co., 1952.

TRIMBLE, HAROLD C., AND LOTT, FRED W., JR. *Elementary Analysis*. Englewood Cliffs, N. J.: Prentice-Hall, 1960.

INDEX