

Session 9

Algebraic Structure

Key Terms for This Session

Previously Introduced

- algorithm [Session 3]
- set [Session 6]
- solution set [Session 6]
- modular arithmetic [Session 8]

New in This Session

- algebraic structure
- binary operation
- commutativity
- associativity
- distributivity
- closure
- identity element
- inverse
- group
- field

Introduction and Review

In Session 8, we concluded our study of functions by looking at cyclic and inverse functions. You learned that cyclic functions have repeating outputs and that in an inverse proportion, the outputs get smaller as the inputs get larger, and vice versa. Finally, you found that many different kinds of functions can be drawn through the same two points. [SEE NOTE 1]

Throughout the past several sessions, we've seen that functions are relationships between inputs and outputs. We have explored properties of different kinds of functions, situations in which they arise, and how they can be expressed in tables, equations, and graphs. This session explores algebraic structure by taking a closer look at the properties of functions.

Learning Objectives

The main goal for Session 9 is to find out what is meant by "algebraic structure," a relatively modern branch of mathematics. To that end, in this session you will:

- Explore important concepts in the study of algebraic structure
- Explore a new algebraic structure
- Solve equations in the new structure

NOTE 1. In this session, we'll explore a primary focus of modern algebra: *algebraic structure*. Algebraic structures are systems with objects and operations, and the rules or properties governing those operations, that can be used to calculate and solve equations. The objects are often rational numbers and the operations are usually addition, subtraction, division, and multiplication. In other areas of mathematics, however, different objects or operations may be used to solve different kinds of equations. Important concepts in the study of algebraic structure include comparing processes, doing and undoing, equivalence, and properties of systems.

NOTE 1 cont'd. next page

Part A: Comparing Operations (10 MINUTES)

Students begin to move from arithmetic to algebra (in the structural sense) when they start thinking about properties of *operations* rather than properties of *numbers*. This happens quite early. For example, “missing addend” problems (such as $4 + ? = 9$) can be solved one at a time, each as a special case, by any number of techniques (counting up, counting back, even subtracting). But when your students start saying things like “subtraction is the opposite of addition” or “subtraction undoes addition,” they are starting to realize a structural relationship between two operations rather than a collection of relationships between pairs of numbers. [SEE NOTE 2]

We took an initial look at algebra from a structural approach when we examined the concept of doing and undoing in Session 3. At that point, we were looking at relationships between operations with a focus on undoing, or inverting, operations. Another hallmark of a move to algebraic structure is a focus on comparing algorithms. For example, consider the following two algorithms:

Algorithm A

- Take a number
- Add 1
- Double your answer

NOTE 1, CONT’D.

In Part A, we’ll focus on properties of operations as they start to develop “operation sense.” The activities in this part revisit the idea of doing and undoing as a way of thinking about the structural relationships between operations.

In Part B, we’ll examine the idea of equivalence through the “Guess My Rule” activity. (For example, in what sense is the algorithm “Take a number, add 2, and then multiply the result by 2” the same as “Take a number, double it, and then add 4”?) This section will also reinforce the idea that the same function can be described by different rules.

We’ll also look at the units digit of whole numbers in Parts C and D, thinking about an arithmetic structure whose objects are the digits 0 through 9 (essentially, mod 10), and whose operations are addition and multiplication. We’ll explore inverses, reciprocals, and the commutative property in this system to expand our conceptual understanding of these properties in a different environment. We’ll also have a chance to compare this finite system to our familiar, real number system. Finally, we’ll look at cryptography as an application of modular systems.

Review

Groups: Discuss any questions from the homework. You may want to spend some time on the “mod 3” function, Problems H1-H5, because this session covers several “mod” functions. Review the function of “taking the remainder.” Note that this is in fact a cyclic function.

Note that “mod 3” was arbitrary. You can work mod on any positive whole number. Take a moment to think about what numbers make sense as inputs (integers), outputs (integers less than the mod number), and remainders (again, integers) before moving on to this session.

NOTE 2. When we begin to think about properties of *operations* rather than of *numbers*, we’re moving from arithmetic to algebra, in a structural sense. You may recall that in Session 3 we looked at algorithms through the lens of “doing and undoing.” A focus on “what undoes what” often marks the beginning of reasoning about operations. In this session, we’ll continue to examine algorithms, as well as other systems that represent a structural approach to algebra. Spend some time thinking through the following exercise. **Groups:** You may want to put this on an overhead.

One hallmark of a move to algebra as structure is a focus on undoing, or inverting, processes; another is comparing them. A simple case of this is the following:

Is adding 3 to 2 the same as adding 2 to 3? Is subtracting 3 from 2 the same as subtracting 2 from 3?

Thinking about properties rather than individual numbers indicates a move to a structural point of view. Keep this in mind as you work on Problems A1 and A2.

Part A, cont'd.

Algorithm B

- Take a number
- Double it
- Add 2 to your answer

Problem A1. Explain why algorithms A and B will always give the same output if you give them the same input.

Problem A2. In what sense are algorithms A and B “the same”? In what sense are they different? Do you think algebra students would classify them as the same or different? Would you classify them as equivalent?

Part B: Guess My Rule (20 MINUTES)

One way to compare algorithms is to play the “Guess My Rule” game. Here’s how it goes:

- Someone makes up a mystery algorithm (like “take a number, double it, and add 2 to the answer”). He or she writes it down or draws a picture of it (with machines, for example) and keeps it secret.
- The algorithm writer then takes “requests.” Other people suggest inputs and request outputs. Everyone records the results.
- Other people try to guess the algorithm with as few requests as possible. If someone says, “I’ve got it,” that person writes down his or her guess of the algorithm, either in words or pictures.
- If the guess is the same as the mystery algorithm, the round is over. If (as often happens) the guessed algorithm looks different from the mystery algorithm, the guessers have to either prove that they will always produce the same result, or they must find an input where the algorithms produce different outputs. For example, a match for “take a number, double it, and add 2” might be “take a number, add 1, and double the answer.” [SEE NOTE 3]

Try It Online!

This problem can be explored online as an Interactive Activity. Go to the ***Patterns, Functions, and Algebra*** Web site at www.learner.org/learningmath and find Session 9, Part B, Guess My Rule.

Problem B1. Describe some strategies for playing “Guess My Rule.”

Problem B2. When you play “Guess My Rule,” you often come up with an algorithm that acts the same as the mystery algorithm but contains different steps. In what sense are these algorithms the same? In what sense are they different? Do you think they represent the same function?

NOTE 3. The “Guess My Rule” game motivates the comparison of algorithms. Think about why there’s often more than one possibility for the mystery algorithm. Look at two algorithms in particular, $2x + 2$ and $2(x + 1)$. In what sense are the algorithms the same, and in what sense are they different? Would your students classify them as the same or different?

In fact, these algorithms are the same *function*, even though their rules are different. That is, they produce the same input/output tables, and therefore define the same function.

Part C: Algebraic Structures (50 MINUTES)

Units Digit

Mathematicians have always been interested in solving equations. Over the past 150 years they have studied techniques for solving equations, properties of operations that allow one to develop strategies for solving equations, and, eventually, entire *systems* in which one can calculate, and hence solve, equations. [SEE NOTE 4]

These algebraic structures have become the primary focus of modern algebra. An algebraic structure is a collection of objects and operations that can be used to calculate and solve equations. The objects can be numbers, polynomials, geometric figures, points in space, card shuffles, or just about any mathematical object you can think of. The operations are usually *binary operations*, operations that combine two objects and form another of the same type.

Examples of systems include the system of integers and the system of rational (whole and fractional) numbers. Here, the operations are the usual operations of arithmetic—addition, multiplication, etc. The structural approach to algebra has enormously widened the kinds of systems in which algebraists work, and hence has changed the face of what’s considered “algebra.”

Algebraic structures come up naturally in mathematical investigations. In Part C, we will investigate units digit arithmetic. Our goal here is to look at the underlying structure of this arithmetic, not just the calculations involved in it. Suppose, for example, that you are looking at the last digit, or units digit, of whole numbers. (Note: In Parts C and D of this session, an “*” is used to represent multiplication.)

Find the units digit of:

$$(22 * 43 + 59 * 27) * (47 + 1,432 * 268 * 21,343)$$

One way to do this is to carry out the entire calculation and then to look at the units digit. But there’s no need for that much work; you can predict what the units digit will be without making the explicit calculations. For example, the units digit of $22 * 43$ will be $2 * 3 = 6$. And the units digit of $59 * 27$ will be the units digit of $9 * 7$ (that is, 3), so $(22 * 43 + 59 * 27)$ will have the same units digit as $6 * 3$. In other words, you can replace the numbers in the calculation by their units digits, turning the very large problem into a more manageable one:

$$(2 * 3 + 9 * 7) * (7 + 2 * 8 * 3)$$

Then, you can simplify as you go, so that, for example, $(2 * 3 + 9 * 7)$ becomes $6 + 3$, which becomes 9. These calculations depend upon order of operations. Look at the tip in Problem C1 if you are unfamiliar with this concept.

Problem C1. Using this line of reasoning, find the units digit of $2,314 * 426 + 573 * 234$. [SEE NOTE 5] [SEE TIP C1, PAGE 242]

NOTE 4. We are all familiar with our real number system. It’s one thing to be handed a system and to learn how to work in it; it’s another to see how a system evolves and then work in it. In this session, we’ll develop an algebraic system and work in it. Suppose you’re interested in looking at units digits of whole numbers. Think about this problem:

Find the units digit of $364 * 123 + 48 * 135$.

Groups: Take five minutes or so to come up with a solution. (You may have to review order of operations.) Share solutions, along with how you thought about the problem. In particular, discuss whether there is some way to do this problem without doing all the actual calculations. Have the whole group suggest possibilities. Be sure to discuss why you can just look at units digits.

NOTE 5. What you have developed in Problems C1-C5 is a “units digit arithmetic,” an arithmetic whose objects are the digits 0 through 9, and whose operations are “add and take the units digit” and “multiply and take the units digit.” The whole system can be captured in the two tables provided. These tables define an algebraic structure on the set of numbers $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Part C, cont'd.

Problem C2. True or false: The units digit of $2,314 * 426 + 573 * 234$ is the same as that of $2,312 * 422 + 576 * 232$.
[SEE TIP C2, PAGE 242]

Problem C3. Find the units digit of:

$$(312 * 423 + 57 * 57) * (28 + 1,045 * 68 * 68 * 68)$$



VIDEO SEGMENT (approximate times: 5:21-10:05): You can find this segment on the session video approximately 5 minutes and 21 seconds after the Annenberg/CPB logo. Zero the counter on your VCR clock when you see the Annenberg/CPB logo.

In this video segment, Prof. Cossey asks participants to find the units digit of the product in Problem C3 above. Try Problem C3 yourself, then compare your work to that of the onscreen participants.

What shortcuts did you use while working on Problem C3? Can these shortcuts always be used in this algebraic structure?

Write and Reflect

Problem C4. Some people say that “the units digit of the sum is the units digit of the sum of the units digits” and “the units digit of the product is the units digit of the product of the units digits.” Explain what they mean. Is what they say correct? Why or why not?

The kind of reasoning you are doing in Problem C4 is one that begins to address the structure of units digit arithmetic.

Take It Further

Problem C5. Explain why “taking the units digit” is the same as “divide by 10 and take the remainder.” The fact that these are the same explains why “taking the units digit” is a modular arithmetic.

Part C, cont'd.

A New Algebraic Structure

What we have been exploring is a “units digit arithmetic,” an arithmetic whose objects are the digits 0 through 9, and whose operations are “add and take the units digit” and “multiply and take the units digit.” The whole system can be captured in two tables (with some of the results left blank for you to complete later):

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6						
4	4	5								
5	5									
6				0						
7										
8			1							
9				3						

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5				
4	0	4	8	2						
5		5			5				0	
6	0		2			6				
7				1	8		2		6	
8		8			2	0		6		2
9	0		8					3		

These tables define an algebraic structure on the set of numbers:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

You can forget that these tables came from “taking the units digit” and concentrate on the system they describe. There are sophisticated words for this process of “ignoring where it came from and concentrating on the behavior” like “abstraction” and “decontextualization.” These are useful mathematical habits of mind. In some situations, you want to forget the meanings of these operations and just work with them. In other situations, it’s just as important to be able to go back to the source of these things (to “contextualize” them) and to remember that these tables came from looking at units digits or remainders. **[SEE NOTE 6]**

In some of the following problems, you can work with the tables without worrying where the operations come from. In others, especially when you need to think about why a property you see in the table holds, you’ll need to go back to the context (taking units digits or taking remainders on division by 10). This fluctuation in and out of context is typical of the way mathematics is performed.

NOTE 6. Groups: Read the text before Problems C6-C19, and then work on these problems in small groups. Share what patterns you see in the table.

Part C, cont'd.

Problem C6. Fill in the missing entries in each table. As you complete the tables, look for patterns in the numbers you enter.

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6						
4	4	5								
5	5									
6					0					
7										
8				1						
9					3					

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5				
4	0	4	8	2						
5		5				5			0	
6	0		2				6			
7				1	8		2		6	
8		8			2	0		6		2
9	0		8					3		

Properties

Problem C7. Does order count in addition? How can you tell just by looking at the “shape” of the + table? For completed table, see Solutions, Problem C6. [SEE TIP C7, PAGE 242]

Problem C8. Go back to the context (units digits or remainders by 10) and explain your answer to Problem C7.

Problems C7 and C8 show that this algebraic structure is *commutative* under addition; that is, the order of objects being added does not matter.

Part C, cont'd.

Problem C9. Does order count in multiplication? How can you tell just by looking at the “shape” of the $*$ table? For completed table, see Solutions, Problem C6.

Problem C10. Go back to the context (units digits or remainders by 10) and explain your answer to Problem C9.

Problems C9 and C10 show that this structure is *commutative* under multiplication; that is, the order of objects being multiplied does not matter.

Problem C11. Is it true of this new addition that adding 0 doesn't change a number? Explain.

Since 0 does not change a number under addition, it is the *identity element* of this structure; that is, adding 0 to a number does not change the value of that number.

The *opposite* or *negative* of a number is the number you have to add to it to get 0. In ordinary arithmetic, the opposite of 4 is -4 (think of a thermometer). In ordinary arithmetic, every number has a negative (what's the negative of 0?). In our little algebraic structure above, units arithmetic, the opposite of 4 is 6, because $4 + 6 = 0$.

Problem C12. Does every number have an opposite in this system? Explain. [SEE TIP C12, PAGE 242]

Under addition, 4 and 6 are *additive inverses*, because $4 + 6 = 0$. Numbers which are inverses under addition are more typically referred to as *opposites*.

Problem C13. Give a rule for determining the opposite of a number, if it has one.

Part C, cont'd.

VIDEO SEGMENT (approximate times: 13:43-13:58): You can find this segment on the session video approximately 13 minutes and 43 seconds after the Annenberg/CPB logo. Zero the counter on your VCR clock when you see the Annenberg/CPB logo.

This short video segment describes how to find opposites using the table of addition in mod 10.

More Properties

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Problem C14. Is it true of this new multiplication that multiplying by 1 doesn't change a number? Explain.

Under multiplication, 3 and 7 are inverses, because $3 * 7 = 1$. Numbers which are inverses under multiplication are more typically referred to as reciprocals. The *reciprocal* of a number is the number you have to multiply it by to get 1. In ordinary arithmetic, the reciprocal of 3 is $1/3$, because $3 * 1/3 = 1$. In ordinary arithmetic, every number except 0 has a reciprocal. In our algebraic structure above, the reciprocal of 3 is 7, because $3 * 7 = 1$.

Problem C15. Which numbers have a reciprocal in this system? [SEE TIP C15, PAGE 242]

Take It Further

Problem C16. What's common among all the numbers that have reciprocals? What's common among all the numbers that don't have reciprocals? [SEE TIP C16, PAGE 242]

Part C, cont'd.



Video Segment (approximate times: 14:43-17:58): You can find this segment on the session video approximately 14 minutes and 43 seconds after the Annenberg/CPB logo. Zero the counter on your VCR clock when you see the Annenberg/CPB logo.

This video segment describes how to find reciprocals using the table of multiplication in mod 10, followed by a short discussion of why some numbers do not have reciprocals. Watch this video segment after you have completed Problem C16.

Problem C17. Which of the properties found in units digit arithmetic are also true in ordinary integer arithmetic?

Problem C18. In ordinary arithmetic, if the product of two numbers is 0, one of them must be 0. Is that true here? What makes it work in ordinary arithmetic that doesn't carry over to our new system? [SEE TIP C18, PAGE 242]

Problem C19. Find, describe, and explain at least two patterns in each table that you haven't yet used. [SEE TIP C19, PAGE 242]

Part C, cont'd.

Groups and Fields (Optional)

Take It Further

The development of mathematical structures in the 19th century included the expansion of number systems into larger sets. Mathematicians studied the properties of these sets, and their operations, so that equations in any system would have roots in the new expanded system. These explorations led Galois to develop the concept of what is now known as a group. The definition of a group is as follows: [SEE NOTE BELOW]

With a set S and an operation $*$, S is a *group* under $*$ if all four of the following conditions are satisfied: (Note that on this page, the “ $*$ ” represents any binary operation, and not only multiplication as elsewhere in this part.)

1. S is closed under $*$
2. S is associative under $*$
3. S has an identity element under $*$
4. Every element of S has an inverse

S can be any set of objects, and $*$ can be any binary operation. Here is more information about each of these:

S is *closed* under $*$ if the operation *always* produces outputs within S . The set of whole numbers is closed under addition and multiplication—add two whole numbers, and the answer is always a whole number. The set of whole numbers is not closed under subtraction or division, however, since the output is *not always* a whole number.

Problem C20. Which of the following sets are closed under addition? Which are closed under multiplication? Which are closed under division?

- a. Positive whole numbers: $\{1, 2, 3, 4, \dots\}$
- b. Full set of integers: $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- c. All real numbers on the number line
- d. Positive real numbers
- e. Positive odd integers: $\{1, 3, 5, 7, \dots\}$

S is *associative* if, for elements a , b , and c in S , $(a * b) * c = a * (b * c)$. This property is especially useful in solving equations.

S has an *identity element* “ e ” if, for every element a in S , $a * e = a$ **and** $e * a = a$. Then, e is the identity. 0 is the identity for addition, and 1 is the identity for multiplication.

S has *inverses* if, for every element a in S , there is an element b in S for which $a * b = e$, the identity. The inverse of 3 under addition is -3 , and the inverse of 3 under multiplication is $1/3$. If a set S has no identity under $*$, it cannot have inverses.

NOTE. This part introduces some key mathematical terms involved in current work in algebraic structures. All groups share these properties, and all groups share certain methods for solving equations (specifically, solutions involving inverting operations). It is as important to show examples of algebraic structures which are *not* groups in order to understand the relationship between structures which *are* groups. **Groups:** Work on Problems C20-C22 in small groups.

Part C, cont'd.

Problem C21. Which of these sets and operations have an identity element? Which have inverses?

- Positive whole numbers, under addition
- Positive whole numbers, under multiplication
- Full set of integers, under addition
- Full set of integers, under multiplication
- Full set of integers, under division

All mathematical groups share these four fundamental properties. Many groups are also *commutative* if $a * b = b * a$ for any element in S .

Another related concept is a mathematical field. If set S has two operations (usually $+$ and $*$) defined on it, it may be a *field* if *all* of these properties hold:

- $(S, +)$ is a commutative group
- $(S, *)$ is a commutative group when the identity of the first operation is removed
- The first operation, $+$, is *distributive* over the second operation, $*$. This means that for any elements a, b , and c in S , it must be true that $a * (b + c) = (a * b) + (a * c)$.

This is a total of 11 properties. While it is rare for a set and two operations to be a field, many mathematical properties of one field translate directly to any other field.

The real numbers are a field under addition and multiplication.

Problem C22. Which of these are fields under the operations of addition and multiplication?

- Positive real numbers
- Rational numbers (integers and fractions)
- Even numbers: $\{\dots, -4, -2, 0, 2, 4, \dots\}$
- Mod 4
- Mod 5

Part D: Working With Algebraic Structures (45 MINUTES)

Units Digit Equations

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

How might you solve equations in this new system? [SEE NOTE 7]

Let's start with the equation $3x = 8$. Looking at the multiplication table, we can see that $3 * 6 = 8$, so $x = 6$ is a solution. In fact, it's the only solution, because there is only one "8" in the third row of the multiplication table.

Or you could reason like this: "To solve $3x = 8$, I want to divide both sides by 3. That's the same as multiplying by the reciprocal of 3. In this system, $3 \times 7 = 1$, so 7 is the reciprocal of 3."

So you can calculate as follows:

$$3x = 8$$

$$7(3x) = 7 * 8$$

$$(7 * 3)x = 6 \quad (7 * 8 = 6 \text{ from the table})$$

$$x = 6$$

NOTE 7. One of the interesting extensions of these algebraic systems is the connection to equation solving. Many of the techniques for solving equations become automatic with experience, and solving equations in modular systems (mod 10 is the modular system for units digit arithmetic) draws attention to the properties of numbers that are sometimes assumed or taken for granted. For example, in solving $3x = 8$, we need to determine whether or not 3 has an inverse in the system we're dealing with. **Groups:** Write $3x = 8$ on an overhead, and discuss how you might solve this equation in units digit arithmetic. Some may say you should divide by 3; others may say you should multiply by $1/3$. Remember that the only operations we have in our system are addition and multiplication, and $1/3$ is not in the domain of units digit arithmetic. In fact, you need to consider what number is the reciprocal of 3 in our new system. If you have trouble, you can look at the table to see what number multiplied by 3 yields 1. Then go through the steps to solve the equation. Next, write $x + 4 = 2$ on an overhead, and discuss how to solve this equation by adding the opposite of 4 to both sides.

Part D, cont'd.

Multiplying by 7 is the equivalent of dividing by 3 in this system. If you need to subtract, you can add the opposite of a number. If you need to solve the equation $x + 4 = 2$, you could reason like this: "To solve $x + 4 = 2$, I want to subtract 4 from both sides. In this system, 6 is the opposite of 4, so I can add 6 to both sides in order to remove the 4."

You would calculate as follows:

$$x + 4 = 2$$

$$x + (4 + 6) = 2 + 6$$

$$x + 0 = 8$$

$$x = 8$$

Try to solve these equations. If you have trouble, you can always use the operations table.

Problem D1. Solve the equation $7x + 5 = 9$ in this system. Explain how you did it. [SEE NOTE 8] [SEE TIP D1, PAGE 242]

Problem D2. Solve the equation $3x + 7 = 4$ in this system. Explain how you did it. [SEE TIP D2, PAGE 242]

Problem D3. Solve the equation $4x + 1 = 9$ in this system. Explain how you did it. [SEE TIP D3, PAGE 242]

Problem D4. Solve the equation $4x + 1 = 8$ in this system. Explain how you did it.

Take It Further

Problem D5. Describe conditions that make the equation $Ax = B$ in this system have no solution, exactly one solution, or more than one solution. How is this different from solving equations in the real number system?

NOTE 8. Groups: Work on Problems D1-D4 in small groups. You may notice that in mod 10, there are certain numbers that don't have reciprocals: all of the numbers that share a factor with 10. (Another way to say this is: The only numbers that do have reciprocals are relatively prime to 10.) You may also want to take time to discuss how solving equations in units arithmetic differs from solving equations in the real number system.

Part D, cont'd.

Cryptography

This system of “units digit arithmetic” may seem like abstract nonsense—when would you need to compute just with units digits? In fact, different algebraic systems arise in all kinds of applications. [SEE NOTE 9]

In the past few activities, you have been looking at a modular system. The “mod 10” system means you divide by 10 and take the remainder—in other words, take the units digit. We'll now focus on an application involving another modular system: enciphering and deciphering messages.

First, notice that you can assign each letter of our alphabet a number from 0 to 25:

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

One of the oldest known substitution ciphers (a code where one letter stands for another) is the one reportedly used by Julius Caesar himself: To get the ciphered letter (C), add 3 to the original letter, or “plaintext” (P). In symbols, this is: $C = P + 3$. [SEE NOTE 10]

Problem D6. Encipher your name using Caesar’s cipher.

Problem D7. Shelly didn’t know how to encipher the “y” in her name? What should she do?

Problem D7 suggests that the algebraic description $C = P + 3$ is not quite right. We need some way to describe “wrapping around” so that the answers are always between 0 and 25. The solution? A modular system! Here’s a new rule:

To get the ciphered letter, add 3 to the original letter or “plaintext,” then take the remainder when you divide by 26. In symbols, this is: $C = P + 3 \pmod{26}$.

NOTE 9. Working in different algebraic systems has applications not just inside mathematics, but in other fields as well. In this part, we’ll explore an applied use of modular systems. We’ll see how modular systems are helpful when you want to keep the answers to calculations within a certain range (in this case, the alphabet).

NOTE 10. Use the “letter tables” to work on Problems D6 and D7. **Groups:** After thinking about how to encipher a “Y” with Caesar’s rule, have a discussion about how modular systems keep the results of calculations within a certain range. In the case of mod 10, all the answers were 0 to 9 (that is, units digits). If you want the answers to be between 0 and 25, you should work modulo 26, or just mod 26. Put Caesar’s modified cipher on an overhead:

$$C = P + 3 \pmod{26}$$

Part D, cont'd.

Problem D8. Decipher this message, which was created using Caesar's code. Explain how you did it. [SEE NOTE 11]

VRPH SHRSOH WKLOQ WKDW PDWKHPDWLWV
LV D VHULRXV EXVLQHVV WKDW PXVW
DOZDBV EH FROG DQG GUB; EXW ZH WKLOQ
PDWKHPDWLWV LV IXQ DQG ZH DUHQ'W
DVKDPHG WR DGPLW WKH IDFW.

Problem D9. Here's a new rule:

$$C = 3P + 2 \pmod{26}$$

Use this rule to encipher a secret word (at least 5 letters long) for a partner. [SEE NOTE 12]

NOTE 11. Groups: Work on Problem D8 alone or with a partner. You may find that even though you know the rule, you will work on this as a "cryptogram," making guesses and trying to see words. Explain your strategy to the group (usually looking at the letter table and subtracting 3 from each letter in the coded message).

Once you have a modular system, there's no reason to restrict yourself to the rule "add 3." You can perform any algebraic rule before using mod 26, and you'll still get a cipher. (Some ciphers are better than others, though. Working mod 26, if you multiply by an even number or by 13, you will have several plaintext letters map to the same ciphertext letters. This is no good, because the cipher can't be "undone," even by its intended recipient! The reasons for this are beyond the scope of this course. We have stayed with multiples that create good ciphers.)

NOTE 12. Groups: Work on Problems D9-D11 with a partner. Problem D11 is quite challenging, and you may approach it any number of ways, either by using "data" from their secret words, or by trying to solve the equation for P .

Remember that there is no "divide by 3" rule in a mod 26 system. If you come up with the equation $P = (C - 2) / 3 \pmod{26}$, how would you decipher M ? $M = 12$, so $P = (12 - 2) / 3 = 10 / 3$. How can you find $10 / 3$ in this system?

Groups: Before wrapping up this part of the session, share your equations and solutions. If no one actually solved the equation for P , you can look at this solution on an overhead or on the board:

$$C = 3P + 2 \pmod{26} \qquad C - 2 \pmod{26} = 3P \pmod{26}$$

Notice that we need mod 26 on both sides at this point, because although C is between 0 and 25, $C - 2$ may not be (it may be -2, for example).

Now you need to multiply both sides of the equation by the reciprocal of 3. There is no $1/3$ in a mod 26 system, but there is a number R , so that $3R = 1 \pmod{26}$. Discuss what that number must be [the answer is 9, because $3 * 9 = 27 = 1 \pmod{26}$].

$$9 * (C - 2) \pmod{26} = 9 * (3P) \pmod{26} \qquad P = 9 * (C - 2) \pmod{26}$$

If you worked on this another way, you may have come up with different but equivalent equations:

$$P = 9C - 18 \pmod{26} \qquad P = 9C + 12 \pmod{26} \qquad \text{and so on.}$$

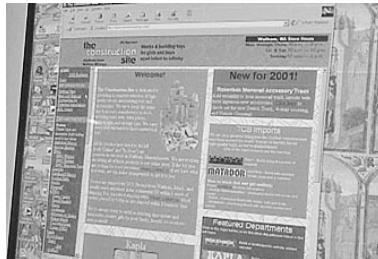
Part D, cont'd.

Problem D10. Trade words with your partner and decipher their secret rule. Explain how you did it.

Problem D11. Can you find a rule that would undo this cipher? That is, can you find a and b so that $P = aC + b \pmod{26}$ is an equation that “undoes” $C = 3P + 2 \pmod{26}$?

Modular systems for enciphering messages are not just for fun and games. It’s essential that a secret message be hard to decipher if you’re not the intended recipient, but easy to decipher if you are the intended recipient. Algorithmic ciphers are much better than “code books” because people can remember the algorithm, so it can’t be lost or stolen.

Modern cryptography, based on these modular systems—using blocks of letters instead of single letters, exponential functions, and very large prime numbers—is what’s used these days to keep your credit card number safe when you purchase something on the Internet!



VIDEO SEGMENT (approximate times: 21:32-23:17): You can find this segment on the session video approximately 21 minutes and 32 seconds after the Annenberg/CPB logo. Zero the counter on your VCR clock when you see the Annenberg/CPB logo.

In this video segment, Ari Juels of RSA Security describes the methods and applications of modular arithmetic to modern cryptography.

Part E: Summing Up (10 MINUTES)

Write and Reflect

Problem E1. In the first session, you were asked to reflect on what you thought algebraic thinking was. Go back and read what you wrote. Have your ideas changed? If so, in what way? [SEE NOTE 13]

Homework

Problem H1. In this game, starting with a string of Ys and Zs, the object is to simplify the string by following strict rules. The rules are:

- YYY can be erased.
- ZZ can be erased.
- The commutative law holds: $YZ = ZY$.
- E is the empty string (a string with no Ys or Zs).

Example 1:

Step 1: $YZZYYZYZZ$ (first erase ZZ)

Step 2: $Y YZYZZ$ (erase YY)

Step 3: $ZYZYZ$ (commute YZ)

Step 4: $ZZYYZ$ (erase ZZ and YY)

Step 5: Z (can't be simplified)

Example 2:

Step 1: $ZYYZ$ (erase YYY)

Step 2: ZZ (erase ZZ)

Step 3: E (empty string is left)

Simplify the following strings:

- $YZYZZYZ$
- $YYYYZZYZ$
- $YZYZYZYZYZYZZZYZYZYZ$

NOTE 13. Groups: Be sure to leave at least 10 minutes at the end of the session in order to reflect on your conception of algebraic thinking at the beginning of the course and how your thinking has evolved. How can you ensure that your students have access to algebraic thinking? You may want to share reactions and responses with the whole group.

Homework, cont'd.

Problem H2. Including the empty string E , there are six essentially different strings that cannot be simplified. They are called the elements of the YZ group. Find all the elements of the YZ group.

Problem H3. The symbol $*$ represents the operation “put together and simplify.” For example:

$$YZ * YZ = YY$$

$$Y * E = Y$$

Compute:

- $E * YZ$
- $YZ * YY$
- $Z * YZ$

Problem H4. Find the missing term.

- $YZ * \underline{\quad} = E$
- $Z * \underline{\quad} = YZ$
- $YY * \underline{\quad} = Z$

Problem H5. For the YZ group, $*$ works a little bit like multiplication. Another way to write the first two rules is $Y^3 = E$ and $Z^2 = E$. Explain.

Problem H6. The only powers of Y are Y , Y^2 , and E . Explain.

Problem H7. Find all the powers of each element of the YZ group.

Homework, cont'd.

Problem H8. Simplify:

- a. $Y^{1,000}$
- b. $(YZ)^{1,001}$

Problem H9. Make a * table.

Problem H10. What element of the group works like the number 1 for multiplication?

Problem H11. What is the reciprocal of each element?

Homework problems are taken from Algebra: Themes, Tools and Concepts, by Anita Wah and Henry Picciotto (New York: Creative Publications, Wright Group/McGraw-Hill, 1993), p.159. The above materials may not be reproduced without the written permission of Creative Publications.

Tips

Part C: Algebraic Structures

TIP C1. The order of operations—which operations you do first, second, and so on—are: inner parentheses, exponents, multiplication or division, addition or subtraction.

TIP C2. Try to answer this question by doing as little calculation as possible.

TIP C7. How is the location of $5 + 8$ related to the location of $8 + 5$ in the table?

TIP C12. You can use the addition table above to find opposites.

TIP C15. You can use the multiplication table above to find reciprocals. Not all numbers have reciprocals in this system!

TIP C16. Think about the types of numbers which do not have reciprocals, then see if you can decide why.

TIP C18. Is there more than one whole number that is equivalent to 0 in this structure? How is this different from ordinary arithmetic?

TIP C19. Is there any relationship between rows of numbers that are inverses?

Part D: Working With Algebraic Structures

TIP D1. Remove the 5 first by adding its opposite, which is 5. Then “divide” by 7 by multiplying by the reciprocal of 7, which is $\frac{1}{7}$.

TIP D2. Add the opposite of 7, then multiply by the reciprocal of 3.

TIP D3. This problem is much harder! Why? Because 4 does not have a reciprocal. There may be no solution, or there may even be more than one solution!

Solutions

Part A: Comparing Operations

Problem A1. Follow both algorithms using N as the input number:

Algorithm A: $N \gg N + 1 \gg 2(N + 1) = 2N + 2$

Algorithm B: $N \gg 2N \gg 2N + 2$

Each algorithm produces the same output, as long as you're willing to trust that the distributive property is always true! If you don't trust or remember the distributive property, remember that $2(N + 1)$ is the same as $(N + 1) + (N + 1)$.

Problem A2. Most algebra students would classify them as identical, since they determine identical expressions. But the steps are different—it's like giving two sets of directions to the same place. Certain problems have many different algorithms of solution, some much more difficult than others.

Part B: Guess My Rule

Problem B1. One strategy is to pick consecutive inputs, trying to find the pattern to the output. This will help decide if the rule is linear, quadratic, exponential, inverse, or cyclic. Guessing numbers that are in proportion may help as well; if you've tried 10, see what happens with 20.

Problem B2. These algorithms produce the same final result, but may have completely different intermediate steps. One important concern is that the final result is *always* identical, not just for a few values of the input. Graphically, the functions should be identical, even though they may be created from different steps.

Part C: Algebraic Structures

Problem C1. Don't forget about the order of operations. The units digit will be identical to that of $(4 * 6) + (3 * 4)$, or $4 + 2 = 6$.

Problem C2. The units digit of the second number is the same as that of $(2 * 2) + (6 * 2)$, or $4 + 2 = 6$. Therefore, it's true.

Problem C3. The units digit is the same as that of $(2 * 3 + 7 * 7) * (8 + 5 * 8 * 8 * 8)$, or:

$$(6 + 9) * (8 + 0), \text{ or } 5 * 8 = 0.$$

Problem C4. Yes, this is true. At each step, we reduce our calculation to the units digit—for example, $7 * 7 = 49$, so we use 9. The end result is the units digit of the sum, or product, of all the units digits used throughout. We can do this only because things that occur in the tens digit, or any other higher digit, cannot affect the result in the units digit.

Problem C5. When dividing by 10, the quotient will always be the number, beginning with the tens digit. For example, 7,536 divides into 10 a total of 753 times. The remainder is, therefore, the units digit only.

Solutions, cont'd.

Problem C6.

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Problem C7. No, order doesn't count. This can be seen from the symmetry in the table—each side of the main diagonal is identical.

Problem C8. Because addition on numbers is commutative already ($a + b = b + a$), we would expect the remainder of two identical numbers to still be identical. So our table, made of remainders, must be commutative.

Problem C9. No. Again, both sides of the main diagonal are identical.

Problem C10. Multiplication on numbers is commutative ($ab = ba$), so our table of remainders, based on a full multiplication table, must also be commutative.

Problem C11. Sure. Adding 0 to an original number doesn't change it, so it cannot change the remainder.

Problem C12. Yes. It can be read from the table: We want to find the second number that makes the sum 0. In each row and column of our table, 0 occurs exactly once, so there is a single opposite number for each given number.

Problem C13. If our number is n , the opposite is $(10 - n)$. If our number is 0, the opposite is 0, since 10 is not in the system.

Problem C14. Sure. Multiplying by 1 won't change an original number, so it can't change the remainder.

Problem C15. Only 1, 3, 7, and 9 have reciprocals, since they each have exactly one 1 in their rows and columns of the table. No other number has any 1 in its row or column.

Problem C16. The numbers 1, 3, 7, and 9 are all the numbers that do not share a common factor with 10. This allows the 1 to appear as a units digit. For example, multiples of 2 will all be even, so there cannot be a multiple of 2 that ends with a 1. The same is true of any number that shares a common factor with 10, so these do not have reciprocals. It is more difficult to guarantee (prove!) that the others must have a single 1 in their rows and columns, but a useful observation is that each number of 0 through 9 occurs exactly once in these numbers' rows and columns.

Solutions, cont'd.

Problem C17. For addition and multiplication, both systems have commutativity, associativity, and identity. In both systems, every number has an opposite.

Problem C18. No, it isn't true—for example, $5 * 4 = 0$. One explanation is that there is now more than one number that equals 0: 10, 20, 30, 40.... If we can find two numbers that multiply to make any multiple of 10, this will be a 0 in our table. Also, there are numbers in our table that share factors with 10, so it is possible to find a pair that creates a multiple of 10. This is not possible in ordinary arithmetic, because no number has 0 as a factor.

There is a lot more here; you might try making the same table with other bases. Low numbers are good starting points, because their tables are easy to produce. Some tables do have the property that if two numbers multiply to 0, one must be 0—maybe you can find which ones.

Problem C19. There are tons of patterns. One is that two numbers which are opposites (3 and 7, for example) will have rows and columns which reverse each other. Another is that 0 appears in a multiplication row twice for multiples of 2, five times for multiples of 5, and ten times for multiples of 10. Another is that 1, 3, 7, and 9 occur only in their own rows and columns in the multiplication table.

Problem C20. All are closed under addition, except for the odd integers. All five sets are closed under multiplication. The only set which is closed under division is the positive real numbers.

Problem C21.

- The first set does not have identity or inverses. The identity should be 0, but 0 is not in the set.
- The second set has identity, but does not have inverses. The identity, 1, is in the set, but most numbers do not have inverses.
- The third set has identity and inverses. The identity, 0, is in the set, and every number has an inverse (its opposite).
- The fourth set has identity, but does not have inverses. The identity, 1, is in the set, but most numbers do not have inverses.
- The fifth set has neither identity nor inverses. There is no identity element for division; many people think 1 is the identity, since $7 / 1 = 7$ works for any number. However, $1 / 7 = 7$ would also have to be true, and it is not.

Problem C22.

- The first is not a field, since there is no identity for addition (0 is not in the set).
- The second is a field.
- The third is not a field, since there is no identity for multiplication (1 is not in the set).
- The fourth is not a field, since one element (2) does not have an inverse under multiplication.
- The fifth is a field.

Solutions, cont'd.

Part D: Working With Algebraic Structures

Problem D1. First, add the opposite of 5 to both sides. This is 5, because $5 + 5 = 0$. Then:

$$7x + 5 = 9$$

$$7x + 5 + 5 = 9 + 5$$

$$7x + 0 = 4$$

$$7x = 4$$

Now, we need to multiply by the reciprocal of 7. This is $\frac{1}{7}$, because $7 * \frac{1}{7} = 1$. Then:

$$7x = 4$$

$$\frac{1}{7}(7x) = \frac{1}{7} * 4$$

$$x = \frac{4}{7}$$

$$x = \frac{4}{7}$$

This method will be effective so long as the opposite of our added number exists, and so long as the inverse of our multiplied number exists.

Problem D2. Follow the same procedure as in Problem D1. The opposite of 7 is 3, and the reciprocal of 3 is $\frac{1}{3}$. The answer is $x = 9$.

Problem D3. Since the opposite of 1 exists (it's 9), we get $4x = 8$. But 4 doesn't have a reciprocal! The next step is to look through the multiplication table, trying to find any numbers that, when multiplied by 4, produce 8. There are two: $x = 2$ and $x = 7$. These are the two solutions. This means that a linear equation in the system of units digit arithmetic can have more than one solution.

Problem D4. Since 4 does not have a reciprocal, we need to use the table to find all solutions to $4x = 7$. No such solution exists!

Problem D5. If A has an inverse, then there will be exactly one solution. If A does not have an inverse, then the number of solutions depends on the common factors of A and B . If A has no inverse, and A and B do not have a common factor, then there will be no solutions. If A has no inverse, and A and B **do** have a common factor, then there will be more than one solution. Specifically, the number of solutions will be two if A and B have 2 as a common factor, and five if A and B have 5 as a common factor.

Problem D6. MDQH GRH is one possible solution.

Problem D7. Wrap around: $Y + 3 = B$. This works partially because B has been vacated by moving the rest of the alphabet forward.

Problem D8. "Undo" the steps by moving everything backward 3 letters. The result is "Some people think that mathematics is a serious business that must always be cold and dry; but we think mathematics is fun and we aren't ashamed to admit the fact."

The origin of the quote you have deciphered is a wonderful book called *Concrete Mathematics* by Graham, Knuth, and Patashnik.

Problem D9. An example: CODES becomes KUNQG.

Solutions, cont'd.

Problem D10. One way to do this is to build a table of plaintext and ciphertext, then decode using the table (like a decoder ring). For example, this table tells you that C becomes K, so if you are given ciphertext letter K, you know the original letter was C.

Problem D11. The rule requires you to “undo” the operations, solving for the variable P (since P is the original letter).

$$C = 3P + 2, \text{ so we'll "undo" the 2 by adding its opposite, which is 24 (2 + 24 = 0 in mod 26)}$$

$$C + 24 = 3P + 2 + 24$$

$$C + 24 = 3P \pmod{26}$$

Now, we'll “undo” the 3 by finding its reciprocal, a number which makes $3R = 1$ in mod 26. This number is not too hard to find, since “1” is the same number as $1 + 26 = 27$. This means $R = 9$ is the reciprocal.

$$C + 24 = 3P$$

$$9(C + 24) = 9(3P)$$

$$9C + (9 * 24) = (9 * 3)P$$

$9C + 8 = P$ is the rule. Try it to see if it changes KUNQG into CODES.

Homework

Problem H1.

- a. Step 1: YZYZZYYZ
Step 2: ZYZZYZ (erase ZZ)
Step 3: YZZ (erase YYY)
Step 4: Y (erase ZZ)
- b. Step 1: YYYZZYZY
Step 2: YZZYZY (erase YYY)
Step 3: YYZY (erase ZZ)
Step 4: YYYZ (commute last ZY)
Step 5: Z (erase YYY)
- c. Step 1: YZYZYZYZYZYZZZZZYZYZY (better think more systematically)
Step 2: YYYYYYYYYYYYYZZZZZZZZZZZZ (commute all Ys first, Zs last)
Step 3: YZ (erase 12 Ys by threes, 12 Zs by twos)

Problem H2. The elements of the YZ group are $E, Y, YY, Z, YZ,$ and YYZ .

Solutions, cont'd.

Problem H3.

- a. $E * YZ = YZ$
- b. $YZ * YY = Z$
- c. $Z * YZ = Y$

Note that in all of these, any three occurrences of Y can be removed, as can any two occurrences of Z . Since the commutative law exists for this group, order is not important.

Problem H4.

- a. $YZ * YYZ = E$
- b. $Z * Y = YZ$
- c. $YY * YZ = Z$

Problem H5. Y^3 means the same as $Y * Y * Y$, which is YYY , which is the same as E . The same is true of Z^2 , which is identical to $Z * Z$.

Problem H6. Since Y^3 is identical to E , Y^4 will be identical to Y , $Y^5 = YY$, $Y^6 = E$, etc.

Problem H7. Powers of each element:

E : E only

Y : $Y^1 = Y, Y^2 = YY, Y^3 = E$

YY : $YY^1 = YY, YY^2 = Y, Y^3 = E$

Z : $Z^1 = Z, Z^2 = E$

YZ : $YZ^1 = YZ, YZ^2 = YY, YZ^3 = Z, YZ^4 = Y, YZ^5 = YYZ, YZ^6 = E$

YYZ : $YYZ^1 = YYZ, YYZ^2 = Y, YYZ^3 = Z, YYZ^4 = YY, YYZ^5 = YZ, YYZ^6 = E$

Problem H8.

- a. $Y^{1,000} = Y^1$, since $1,000 = 1 \pmod{3}$, and the powers of Y repeat every three powers.
- b. $(YZ)^{1,001} = (YZ)^5$, since $1,001 = 5 \pmod{6}$, and the powers of YZ repeat every six powers. According to the list of powers of YZ , $(YZ)^5 = YYZ$. Another way to do this is to imagine a line of 1,001 Y s and 1,001 Z s, and decide what would be left after all the cancellation.

Solutions, cont'd.

Problem H9. The completed table is below. Note that every element appears exactly once in each row, and once in each column.

*	E	Y	YY	Z	YZ	YYZ
E	E	Y	YY	Z	YZ	YYZ
Y	Y	YY	E	YZ	YYZ	Z
YY	YY	E	Y	YZ	Z	YZ
Z	Z	YZ	YYZ	E	Y	YY
YZ	YZ	YYZ	Z	Y	YY	E
YYZ	YYZ	Z	YZ	YY	E	Y

Problem H10. The element E works this way, since $E * A = A$ for any element A in the table, just like $1 * N = N$ for any number N .

Problem H11. The reciprocals can be found by finding E within the row and column of each element. Here are the reciprocals, in pairs:

E and E Y and YY Z and Z YZ and YYZ

Notes
