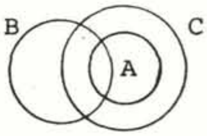
BLOCK 1:
VECTOR ARITHMETIC

Pretest

1.



In the given diagram both assumptions are obeyed but not the conclusion. This means that the conclusion does not follow inescapably from the assumptions. By definition, then, the argument is invalid.

2. $7x - 4y = 3$.

3. $(7/3, 14/3, 3)$.

4. $x + y + z = 9$.

5. Any scalar multiple of $-14\vec{i} + 10\vec{j} + 9\vec{k}$.

6. 12.

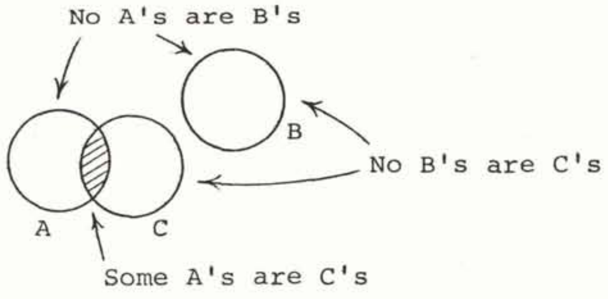
Unit 1: An Introduction to Mathematical Structure

1.1.1(L)

a. To show that an argument is invalid, all we need do is give one set of conditions in which the assumptions are obeyed but the conclusion is false. This is the "beauty" of proving that something is false rather than trying to prove that something is true. To show that something is true we must show that it happens every time, and this can be quite difficult. To show that a statement is false, however, requires only that we show one instance in which it is not true. Albert Einstein said this rather cryptically in his quotation: "All the experiments in the world can never prove me right, but a single one may prove me wrong."

Returning to our exercise, the stated conclusion is "No A's are C's." The negation (contradiction) of this statement is "It is false that no A's are C's." This, in turn, may be paraphrased as "At least one A is also a C," and this is often rewritten as "Some A's are C's." (In logic, the phrase "at least one" is usually written as "some.") Thus, as soon as we can depict a situation in which it is true that no A's are B's, no B's are C's, and some A's are C's, we will have shown that both hypotheses in our argument are true while the conclusion is false; hence, that the argument is invalid.

One such situation is depicted below.



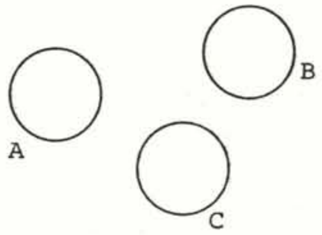
The main point is this. If we look at the last diagram, exactly as drawn, then we see that "No A's are B's" is a true statement (since the circles denoted by A and B do not intersect) and we see that "No B's are C's" is also true. Yet the conclusion that

1.1.1(L) continued

"No A's are C's" is clearly false in our diagram since the circles denoted by A and C do intersect.

Thus, our diagram gives us a situation in which the assumptions are true but the conclusion is false. This is enough to guarantee that the argument is invalid since in a valid argument the truth of the assumptions guarantees the truth of the conclusion.

The key lies in the idea of inescapable. As soon as the conclusion can be false in even one case while the assumptions are true is enough to guarantee that the conclusion is not an inescapable consequence of the assumptions. In this vein, notice that we could have drawn our three circles as



in which case the assumptions and the conclusion would have been true, but this is not enough to make the argument valid, since validity means that the conclusion can never be false if the assumptions are true.

To see this in more concrete detail, consider the argument

No lions are tigers
No tigers are elephants
Therefore, no lions are elephants

Certainly, our conclusion is as true as each of our assumptions, but the truth of the conclusion is independent of the truth of the assumptions, at least in the sense that we can give an argument of the same format in which the conclusion is false even though the assumptions are true. For example,

1.1.1(L) continued

No men are women
No women are males
Therefore, no men are males

and we now see that, while both arguments have the same form of "No A's are B's and no B's are C's, therefore, no A's are C's," in one case the assumptions are true and the conclusion is false while in the other case the assumptions are true and the conclusion is true. This is enough to prove that the truth of the conclusion rests on more than the truth of the assumptions - so the argument is invalid.

In terms of our course, we only want to accept those things as theorems which follow inescapably from our assumptions. We do not want our personal bias to allow us to accept invalid conclusions simply because we want to believe the conclusion. Rather, we want only inescapable consequences of our rules to bear the stamp of "facts."

In other words, it often happens, if we are not on our guard, that if we like the conclusion of an argument we will accept the argument on which the conclusion was based, even if the argument is invalid. This, among other reasons, is why, when we make proofs in mathematics, we often use letters such as a, b, and c to denote numbers rather than use particular examples. The abstract letters do not suggest special properties that particularly chosen numbers (but not others) might possess. The same is true in geometry. When we want to prove things about triangles in general, we try not to draw an isosceles triangle, since the picture might then lead us to conjectures which are true for these special triangles but not for others. This is also why we have written such things as "All A's are B's" rather than, say, "All mathematicians are brilliant." Namely, the latter statement lends itself to a more emotional analysis than the former. In fact, it is for this reason that the type of logic we are talking about in this exercise is known as formal logic to indicate that validity depends on the form of the argument rather than the truth of the statements which comprise the argument.

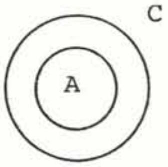
1.1.1(L) continued

b. Here all we wish to do is review our language of sets. Notice that (b) is precisely the same as (a), only rewritten in the language of sets. For example, to say that no A's are B's is the same as saying that no element of the set A is an element of the set B. This, in turn, says the same thing as the intersection of A and B is the empty set or, more symbolically, $A \cap B = \emptyset$. In a similar way, $A \cap B \neq \emptyset$ says that the intersection of A and B is not empty which, in turn, means that there is at least one element that belongs to both A and B, or at least one element is both an A and a B. That is, some A's are B's.

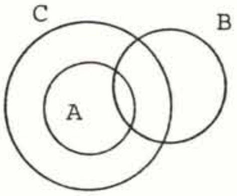
1.1.2

a. "Some A's are not C's" is negated by "It is false that some A's are not C's." That is, "It is false that even one A is not a C." This, in turn, may be paraphrased as "All A's are C's."

Thus, to show that the argument is invalid we need only construct a circle diagram of the form



in which the assumptions are obeyed. Since "Some A's are not B's" is fulfilled as soon as at least parts of the A and B circles do not overlap etc., we have, for example,



This diagram is sufficient to establish the invalidity of the argument, since in terms of this diagram the assumptions of the given argument are obeyed but the conclusion isn't.

1.1.2 continued

b. "Some A's are not B's" means the same as "Some A's are non-B's." In the language of sets, we denote the set non-B's by B', the complement of B. That is, "Some A's are non-B's" means that at least one element belongs to both A and B'. In other words, in the language of sets "Some A's are not B's" is written as $A \cap B' \neq \emptyset$*.

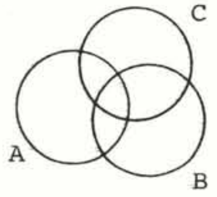
Thus, the argument "$A \cap B' \neq \emptyset$ and $B \cap C' \neq \emptyset$ implies that $A \cap C' \neq \emptyset$ is invalid as it is merely a paraphrase of part (a).

c. The assumptions and the conclusion are true but the argument is not valid. The reason that the argument is not valid is that it has the form

Some A's are not B's
Some B's are not C's
Therefore, some A's are not C's

(where in this case A = set of all numbers which are divisible by 2, B the set of all numbers divisible by 7, and C the set of all numbers divisible by 3).

The circle diagram, in this particular real case, is given by



in which case the assumptions and the conclusion are obeyed, but based on the form of the argument alone, the circles did not have to be drawn this way.

*The more astute student may notice that B' is ambiguous in the sense that it depends on the universe of discourse I. That is, $B' = \{x : x \in I \text{ but } x \notin B\}$. This problem, however, is irrelevant here since $A \cap B'$ denotes those members of A which are non-B's. In other words, the fact that all elements under consideration must belong to A removes the need for our having to know the entire universe of discourse (universal set), I.

1.1.2 continued

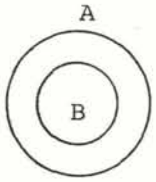
In still other words, while it is true that some numbers which are divisible by 2 are not divisible by 3, this truth requires more than the facts that

(1) some numbers which are divisible by 2 are not divisible by 7

(2) some numbers which are divisible by 7 are not divisible by 3.

1.1.3

a. In the diagram



it is true that some A's are not B's, but it is false that some B's are not A's. Hence, "Some A's are not B's" and "Some B's are not A's" do not have the same meaning.

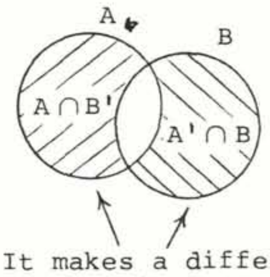
b. In the language of sets

$A \cap B' \neq \emptyset$

and

$A' \cap B \neq \emptyset$

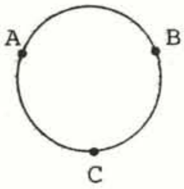
do not mean the same thing, Pictorially,



It makes a difference as to whether it is $A \cap B'$ or $A' \cap B$ which is non-empty.

1.1.4

a. If aRb means that a lives next door to b, then since a person doesn't necessarily live next door to himself, it follows that aRa need not be true. Hence, R is not reflexive. On the other hand, if a does live next door to b then b also lives next door to a. Hence, in this case if aRb is true so also is bRa. Thus, R is symmetric. Finally, if a lives next door to b and b lives next door to c, in general c will not be next door to a but rather two doors removed from a. An exception is that if the three houses form a "circle"; that is



In other words, the truth of both aRb and bRc is not enough to guarantee the truth of aRc. Thus, R is not transitive.

b. If aRb means that 2a + b = 15 (in the language of analytic geometry, this problem says that aRb means that (a,b) is on the line 2x + y = 15) then 7R1 is true (since 2(7) + 1 = 15 is a true statement) and 1R13 is true (since 2(1) + 13 = 15 is a true statement). On the other hand, 7R13 is false because $2(7) + 13 \neq 15$. Since it is true that 7R1 and 1R13 but that $7\not R13$ (just as $\neq$ denotes the negation of =, $\not R$ denotes the negation of R; that is, $a\not R b$ means that aRb is false), this shows that R is not transitive since if it were it would have to follow that 7R13 was true since both 7R1 and 1R13 are true (in the language of our definition here a = 7, b = 1, and c = 13).

c. 1R7 says that 2(1) + 7 = 15, and this is false. Hence, 1R7 is false. But from (b) we saw that 7R1 was true. If R were symmetric the truth of 7R1 would insure the truth of 1R7. Since this is not the case, R is not symmetric.

d. If aRb, then we know that a + b = 15. On the other hand, we also know that a + b = b + a. Hence, if a + b = 15, then b + a = 15. In terms of our definition of R in this example, it follows that

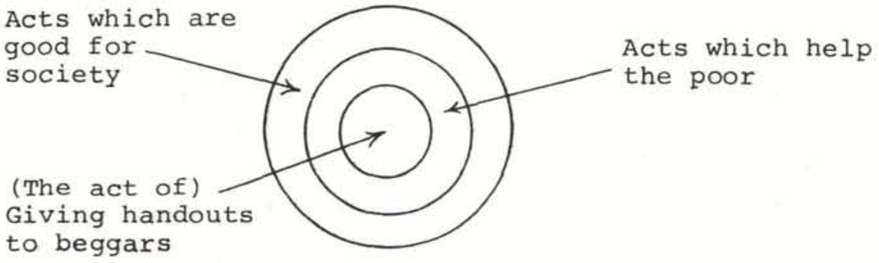
1.1.4 continued

aRb implies also that bRa. Hence, R is symmetric. In the language of analytic geometry, we are saying that the line x + y = 15 has the property that (a,b) is on this line if and only if (b,a) is. NOTE: We are not saying here that aRb is true. All we are saying is that if aRb is true then so also is bRa. For example, since (3,4) is not on the line x + y = 15, 3R4 is false in this example.

1.1.5(L)

If we assume that parts (a) and (b) of the same problem should be related (otherwise they should have been two different problems), it might seem strange that we have chosen (a) and (b) as we have here. The point is that both problems say the same thing, but in one case the situation transcends mathematics while in the other we give a specific illustration in mathematics.

a. Hopefully, at this stage it is not a learning exercise to discover the argument is valid. In terms of a circle diagram we have


Acts which are good for society
Acts which help the poor
(The act of) Giving handouts to beggars

While the argument is valid, we do not have to accept the truth of the conclusion. In particular, false assumptions plus valid reasoning may well lead to false conclusions. In this exercise, if we reject the truth of either

(1) Giving handouts to beggars helps the poor

or

(2) Helping the poor is good for society

then the valid conclusion needs no longer be accepted as true by us (though it should be noted that even if we reject the truth of the assumptions, we can still believe the conclusions, since there

1.1.5(L) continued

might be another valid argument which leads to the same conclusion but one in which we feel we can accept the assumptions as being true). In summary, we have to accept the conclusion of a valid argument as being true only if we agree that the assumptions upon which the conclusion is based are true.

b. The discussion in (a) applies very nicely to (b). Notice that the usual rule for n! whereby we consider the product of all integers from 1 to n inclusive presupposes that n is a natural number (i.e., a positive whole number). Since 0 is not a positive whole number, it has not been defined by the above definition of factorial. In other words, at this moment 0! is undefined.

Now as we mention in the exercise, the structural property of the factorial that we want to use is that

$$(n + 1)! = (n + 1)n! \qquad (1)$$

If we now want (1) also to be true when n = 0, we see that with n = 0, (1) becomes

$$(0 + 1)! = (0 + 1)0! \qquad (2)$$

Since we know that 1! = 1 and that 0 + 1 = 1, we may transform (2) into

$$1 = 1(0!) \qquad (3)$$

Since 1(0!) = 1, (3) then becomes

$$0! = 1 \qquad (4)$$

Equation (4) establishes the desired result, but the major learning experience here is to note that it is foolish, at least in one manner of speaking, to ask whether (4) is true. We could have defined 0! any way we wished. What is true is that (4) is an inescapable conclusion only if we agree that we want to accept (1) as still being true.

1.1.5(L) continued

In other words, to the student who didn't particularly care whether (1) was preserved or not, he would have no logical reason to define 0! as 1 (unless we believe that the fact that he was told is reason enough). What happens in most mathematical situations is that the alternative of not having the structure obeyed is far worse than accepting the structurally-imposed definition. In still other words, armed with the choice that he can let 0! = 0 (which seems to be what most students intuitively want to believe) but that he must then agree to forego the use of equation (1) when there is the possibility that n = 0, the intelligent student would sooner give up the option of believing that 0! = 0. In more general form, many difficult mathematical choices as to how to define things are decided by how well these choices allow us to maintain the previously-defined structure.

1.1.6(L)

a. The aim of this part of the exercise is to establish a structural similarity between the properties of additions and those of multiplication. Clearly, the product of two numbers is again a number, the product does not depend on the order of the factors, nor does the product depend on "voice inflection." Stated more formally, it is clear that for multiplication, we have

M-1: If a and b are numbers so also is their product, ab.
M-2: ab = ba
M-3: If a, b, and c are numbers then a(bc) = (ab)c

Next, we observe that the number 1 does for multiplication what 0 does for addition. That is,

M-4: There exists a number, denoted by 1, such that a1 = a for all numbers, a.

Notice that M-1 through M-4 are obtained from A-1 through A-4 simply by interchanging 0 with 1 and the addition notation with the multiplication notation.

1.1.6(L) continued

In a similar way, one might suspect that $1/a$, or, equivalently, a^{-1} would play the role in multiplication that $-a$ plays in addition. This is almost correct. Only we must be careful to notice that any number times 0 is still 0 (this will be discussed again in part (b)); hence, there is no number by which we can multiply 0 to obtain 1. Once this is taken into account, however, we see that

M-5: Given any number $a \neq 0$ there exists a number denoted by a^{-1} (or $1/a$) such that $aa^{-1} = 1$.

These five rules are the multiplicative counterparts for our rules for addition. Notice that M-5 indicates the usual wariness about dividing (since division is the inverse of multiplication) by 0.

As yet, however, we do not have a single rule which combines addition and multiplication within the same "recipe." This is discussed in part (b).

b. The distributive rule which tells us that for any three numbers a, b, and c

$$a(b + c) = ab + ac$$

is a link between addition and multiplication. In particular, if we take the special case in which $b = c = 0$, the rule tells us that

$$a(0 + 0) = a0 + a0 \qquad (1)$$

We also know that $m + 0 = m$ for any number m. With $m = 0$ this says that $0 + 0 = 0$. Replacing $0 + 0$ by 0 in (1) we obtain

$$a0 = a0 + a0 \qquad (2)$$

Stripped of embellishment, we may now subtract a0 from both sides of (2) to obtain the desired result. To do this more formally within the framework of our game and at the same time emphasize the use of previously proven theorems, notice that we are sure,

1.1.6(L) continued

from M-1, that, whatever else is true, a0 is at least a number. Let's call it b. Then (2) becomes

$$b = b + b \tag{3}$$

We now want to show that b = 0. To this end we observe that since the cancellation law for addition has already been established as valid in the "game" of arithmetic, it would follow that b = 0 if we knew, for example, that b + 0 = b + b, for we could then simply "cancel" b from both sides of the equation (that is $\cancel{b} + 0 = \cancel{b} + b$). Now what we do know from A-4 is that b = b + 0. Thus if we replace b on the left side of (3) by b + 0, we obtain

$$b + 0 = b + b \tag{4}$$

and our result follows from (4).

Notice that we are not saying that our proof is unique. Often times there is more than one valid way to establish a conclusion. For example, in (3) once we observe that -b exists (from A-5), we have that

$$b + (-b) = (b + b) + (-b) \tag{4'}$$

and from (4') we can derive our result just as we did in the original proof of the cancellation law for addition.

The important point that transcends the result of this part of the exercise is not so much that a0 = 0 is true for numbers, but rather that the truth follows inescapably from sixteen rather obvious properties of arithmetic (namely, rules E-1 through E-5, A-1 through A-5, M-1 through M-5, and the distributive rule). In other words, once a system had a structure that obeyed these sixteen properties the result of part (b) follows inescapably. We shall explore this idea in more detail in Exercises 1.1.8 and 1.1.9.

c. We have already proven in our supplementary notes that the cancellation law is true for addition (i.e., if a + b = a + c then b = c). The point is that the same rules which were true for addition that were used in this proof are also true for multiplication, once we make sure that a ≠ 0. In fact, once a ≠ 0, we

1.1.6(L) continued

need only take the proof in the addition case, and everywhere replace 0 by 1, + by x, and -a by a^{-1}. Without bothering to recopy the proof of the cancellation law for addition, this process would yield

$ab = ac$

and $a \neq 0$ implies that

$a^{-1}(ab) = a^{-1}(ac)$,

and this implies that

$(a^{-1}a)b = (a^{-1}a)c$,

which in turn implies

$1 \times b = 1 \times c$,

or

$b \times 1 = c \times 1$,

and by M-4 we have

$b = c$

A quick check should show that the above proof was obtained "mechanically" from the corresponding proof for addition. On the other hand, if we forget about this and simply look at the above proof as it appears, without reference to any other proof, the proof is self-contained in terms of the appropriate rules of the game. It is in this sense that we mean that two different models "behave alike" provided that they share the same "rules of the game."

1.1.7

Paraphrased, this exercise asks us to prove that if the product of two numbers is zero then at least one of the two numbers is zero.

Step 1

We know that $a0 = 0$ [from (b)]. Hence,

$ab = 0$ implies $ab = a0$.

Step 2

Since $a \neq 0$ we may cancel [by (c)] a from both sides in the equation $ab = a0$.

Therefore, $b = 0$.

Note that we could have started from scratch as if (b) and (c) hadn't existed to obtain the same result. Namely, $a \neq 0 \rightarrow a^{-1}$ exists. Therefore, $ab = 0 \rightarrow a^{-1}(ab) = a^{-1}0 \rightarrow a^{-1}(ab) = 0$. But, $a^{-1}(ab) = (a^{-1}a)b = 1b = b$; therefore, $b = 0$.

However, we chose again to emphasize the structure of our game and to show how previously proven theorems are later used as "facts."

1.1.8(L)

The main aim of this exercise is to reinforce the concept of the game of mathematics from several points of view. In part (a) we want to emphasize the use of "=" as an equivalence relation even though it does not have the properties of what we usually think of as being equal.

a. Here, for any integers a and b we are defining $a = b$ to mean that a and b leave the same remainder when divided by 7. (If the equal sign seems to cause a mental block, replace $a = b$ by aRb.) While this may seem to be a strange form of "equality," there are often cases in which the remainder is more important than the quotient. For example, the ancient Greek often came to grips with so-called Diophantine equations in which one equation had two or more unknowns subject to the condition that the values of the unknowns

1.1.8(L) continued

had to be integers. As an illustration suppose we want to find positive integers x and y such that

$$5y = 100 - 19x \tag{1}$$

In such an example, we are more concerned with values of x for which 100 and 19x leave the same remainder when divided by 5. Namely, since the left side of (1) is divisible by 5, the right side must also be divisible by 5 if the equality is to hold. But for 100 - 19x to be divisible by 5 it is necessary (and sufficient) that 100 and 19x leave the same remainder when divided by 5.

As far as this exercise is concerned, the calendar gives us an excellent physical example in which remainders when we divide by 7 are important. Suppose we would like to know what day of the week it will be 100 days from now. Since there are seven days in a week, every seventh day will be the same day of the week as the present day. Notice that 100 leaves a remainder of 2 when divided by 7. That is,

$$100 = 14(7) + 2 \tag{2}$$

In other words, 100 days from now is precisely 14 weeks plus 2 days, and as a result 100 days from now will occur on the same day of the week as will 2 days from now. Notice that if all we want is the day, it is not so important that there are 14 weeks in 100 days as it is that when the greatest number of weeks is deducted from 100 there are 2 days left over.

Historically, the study of numbers having the same remainder when divided by a given number was known as the theory of congruences and more modernly as modular arithmetic.

In terms of the language of congruences, one wrote

$$a \equiv b \text{ modulo } 7$$

or more compactly

$$a \equiv b \pmod 7 \tag{3}$$

1.1.8(L) continued

(read as "a is congruent to b modulo seven") to indicate that a and b left the same remainder when divided by 7.

By way of a few illustrations, we would write that

$$21 \equiv 0 \pmod{7},\ 21 \equiv 7 \pmod{7},\ 38 \equiv 3 \pmod{7}.$$

On the other hand, $38 \not\equiv 4 \pmod{7}$ since 38 does not leave a remainder of 4 when divided by 7.

Of course, there is no need to emphasize 7. Quite in general, we write

$$a \equiv b \pmod{m}$$

to indicate that a and b leave the same remainder when divided by m. Correspondingly, we write

$$a \not\equiv b \pmod{m}$$

if a and b leave different remainders when divided by m.

Obviously, congruence depends on what number we are dividing by as well as on the numbers themselves. For example, $40 \equiv 5 \pmod{7}$ since both 40 and 5 leave a remainder of 5 when divided by 7, $40 \not\equiv 5 \pmod{4}$ since 40 leaves a remainder of 0 when divided by 4 while 5 leaves a remainder of 1 when divided by 4.

An interesting pictorial way of visualizing "congruence modulo m" is to think of the integers arranged sequentially in m columns. For example, to study congruence modulo 7, we think of the integers arranged in seven columns:

0	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	31	32	33	34
35	36	37	38	39	40	41

1.1.8(L) *continued*

Then two numbers are congruent modulo 7 if and only if they appear in the same column in our chart. For example, 5 and 40 appear in the same column. On the other hand, if we wrote the numbers sequentially in four columns, 5 and 40 would appear in different columns.

To illustrate our chart we began with 0, but it should be pointed out that our chart is not restricted to non-negative numbers. Indeed, we could also write

-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6

In this way, it is still true that numbers in the same column leave the same remainder when divided by 7. For example, -12 appears in the same column as does 2. Notice that

$$-2 = 7(-2) + 2$$

and thus -12 leaves a remainder of 2 when divided by 7. (We must keep in mind here that the <u>definition</u> of remainder <u>requires</u> that a remainder be <u>non-negative</u>.)

In any event, any number is in the same column as itself (that is when a is divided by m it leaves the same remainder as a when it is divided by m); thus for congruence mod m we have that for any number a, a = a; that is, $a \equiv a \pmod{m}$.

Secondly, if the first number is in the same column as the second then the second is in the same column as the first. In terms of the arithmetic language, if a and b leave the same remainder when divided by m so also do b and a. That is, if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

Finally, if the first and the second numbers are in the same column and the second and the third numbers are in the same column then the first and the third numbers are also in the same column. That is, if a and b leave the same remainder when divided by m and b and c leave the same remainder when divided by m, then a and c leave the same remainder when divided by m.

1.1.8(L) continued

These three results show that congruence modulo m is an equivalence relation.

b. The fact that we have an equivalence relation means in terms of our chart that once we know one number in a column we know them all. For example, with respect to modulo 7, the column which contains 0 contains all numbers which leave a remainder of 0 when divided by 7 (that is, the multiples of 7). Similarly, the column which contains 1 contains precisely those numbers which leave a remainder of 1 when divided by 7. In this way, we can use 0, 1, 2, 3, 4, 5, and 6 to name the seven columns. Notice that we then have a "natural" way to add and to multiply columns. For example, suppose we take any number in the column which contains 3 and add to it any number in the column which contains 5. It follows that the sum must be in the column that contains 1. Namely, to be in the column which contains 3 means that the number must have the form 7k + 3 where k is an integer (that is, all numbers of this form leave a remainder of 3 when divided by 7, and the value of k merely picks out the particular number under consideration). For example, if k takes on all integral values from -3 to 3 inclusively, 7k + 3 takes on the values -18, -11, -4, 3, 10, 17, and 24. All of these numbers leave a remainder of 3 when divided by 7.

In a similar way, all numbers in the column which contains 5 have the form 7m + 5 where m is an integer. Thus, the sum of any number in the column containing 3 and the column containing 5 has the form

$$\begin{aligned}&(7k + 3) + (7m + 5) =\\&(7k + 7m) + 3 + 5 =\\&7(k + m) + 8 =\\&7(k + m) + 7 + 1 =\\&7(k + m + 1) + 1 =\\&7n + 1\end{aligned}$$

where

$$n = k + m + 1.$$

1.1.8(L) continued

Since the sum of integers is again an integer, n is an integer; hence, 7n + 1 leaves a remainder of 1 when divided by 7. Therefore, the sum is in the column which contains 1 as asserted.

As a second example, if we multiply a number in the column which contains 4 by a number in the column which contains 3 the product must be in the column which contains 5. Namely, we have

$$\begin{aligned}(7k + 3)\ (7m + 4) &= 49km + 21m + 28k + 12\\ &= 49km + 21m + 28k + 7 + 5\\ &= 7(7km + 3m + 4k + 1) + 5\\ &= 7p + 5,\end{aligned}$$

where

$$p = 7km + 3m + 4k + 1$$

In this way, it is left to the reader to show that

+	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

x	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

Notice that the above tables give us an arithmetic which consists of seven elements (not to be confused with the fact that, for example, in ordinary arithmetic we have only ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9 but these may be combined to form infinitely many different numbers; in our tables, notice that we combine the numbers 0, 1, 2, 3, 4, 5, and 6 so as always to obtain one of these same numbers). This is why this type of arithmetic is often referred to as finite arithmetic. For example, in ordinary arithmetic, we can never test all triplets of numbers to see whether it is always true that a + (b + c) = (a + b) + c, since there are

1.1.8(L) continued

infinitely many tests to be made. However, if a, b, and c are restricted to elements listed in our tables, there are 343 tests that allow us to check whether addition is associative. In other words, a, b, and c can each be chosen in 7 ways; hence, there are 7 x 7 x 7 or 343 ways to choose a triplet of numbers (a,b,c). We shall talk more about this in part (c) of this exercise.

As a final note, let us observe that when we do the arithmetic implied by our two tables, we refer to this arithmetic as modular arithmetic. In other words, when we deal with the columns denoted by 0, 1, 2, 3, 4, 5, and 6, we talk about modular-7 arithmetic. When we talk about the numbers in general and wish to discuss when two numbers belong to the same column, then we refer to congruence modulo 7. For our purposes, we need not pursue this fine point.

c. We use the addition and multiplication tables constructed in (b).

(1) If we were trying to prove that for all a, b, and c in modular-7 arithmetic that $a + (b + c) = (a + b) + c$, among the 343 tests to be made would be the comparison of $4 + (5 + 6)$ and $(4 + 5) + 6$. From our table, we have

$$4 + (5 + 6) = 4 + 4 = 1$$

and

$$(4 + 5) + 6 = 2 + 6 = 1$$

Thus, at least when $a = 4$, $b = 5$, and $c = 6$, the rule $a + (b + c) = (a + b) + c$ is obeyed. Before we can say that the rule holds, we must make similar tests for the remaining 342 cases. While this may seem tedious, it involves a relatively small number of steps - at least compared with the concept of infinity.

(2) From our table $3 + 4 = 0$ and $1 \times 5 = 5$. Hence,

$$(3 + 4) \times 5 = 0$$

On the other hand, $4 \times 5 = 6$ and $3 + 6 = 2$. Hence,

$$3 + (4 \times 5) = 3 + 6 = 2$$

1.1.8(L) continued

Since $2 \neq 0$, it follows that $(3 + 4) \times 5$ need not equal $3 + (4 \times 5)$. In other words, it would not be a realistic rule of the game to require that $(a + b) \times c = a + (b \times c)$ for all a, b, and c, since we have seen at least one case in which it isn't true. To be sure, there may be special cases when the two results may be the same, such as: $(a + b) \times 1 = a + (b \times 1) = a + b$, but this is not what's important.

(3) $3^1 = 3$

$3^2 = 3 \times 3 = 2$

$3^3 = 3^2 \times 3 = 2 \times 3 = 6$

$3^4 = 3^3 \times 3 = 6 \times 3 = 4$

$3^5 = 3^4 \times 3 = 4 \times 3 = 5$

$3^6 = 3^5 \times 3 = 5 \times 3 = 1$

The fact that $3^6 = 1$ now gives us a very quick way of determining 3^n for any integral value of n. For example, if n = 105, we may write that $105 = 6(17) + 3$. Hence,

$$\begin{aligned} 3^{105} &= 3^{6(17) + 3} \\ &= (3^6)^{17}3^3 \\ &= (1)^{17}3^3 \\ &= 3^3 \\ &= 6 \end{aligned}$$

(By the way, if we remember the connection between modular arithmetic and congruences, the fact that $3^{105} = 6$ in modular-7 arithmetic means that $3^{105} \equiv 6 \pmod 7$. This, in turn, means that 3^{105} and 6 leave the same remainder when divided by 7. In particular, since 6 leaves a remainder of 6 when divided by 7, it follows then that 3^{105} also leaves a remainder of 6 when divided by 7. We have therefore found a very convenient way of solving the problem: "Find the remainder when 3^{105} is divided by 7." To be sure we could have actually computed the number 3^{105} and then divided by 7 to compute the remainder. Notice, however, that since the log (base ten) of 3^{105} is $105 (\log 3) = 105 (0.477) \approx 50$, then 3^{105} is

1.1.8(L) continued

approximately 10^{50}, so that in place value notation 3^{105} has about 51 digits, and this is far from a pleasant computation. We make this point only to illustrate that if there were any situation in which we wanted to know the remainder when 3^{105} is divided by 7, then modular-7 arithmetic would certainly be a practical invention. In fact, for this particular problem, modular-7 arithmetic is more practical than "ordinary" arithmetic.

d. By 3^{-1} we mean that number with the property that $3 \times 3^{-1} = 1$. If we look at our multiplication table we see that $3 \times 5 = 1$. Hence, 3^{-1} is another name for 5. In other words, whether it seems unnatural or not, in modular-7 arithmetic, $3^{-1} = 5$.

e. In a similar way, looking at the table reveals that

$1 \times 1 = 1$; $2 \times 4 = 1$; $3 \times 5 = 1$; and $6 \times 6 = 1$.

From this we may conclude that

$1^{-1} = 1$; $2^{-1} = 4$; $3^{-1} = 5$; $4^{-1} = 2$; $5^{-1} = 3$; and $6^{-1} = 6$.

f. This is the final point we wish to make in this exercise about structure. The proof that $ab = 0$ implies that $a = 0$ or $b = 0$ required only those properties of ordinary arithmetic that are also true in modular-7 arithmetic. (Although we did not verify all 343 cases of the associative rule etc., we did check that M-5 was true for modular-7 arithmetic since this was exactly the role of part (e) of this exercise.) In other words, structurally, we may mimic our proof in the case of ordinary arithmetic, noticing that step-by-step, each statement is also valid in modular-7 arithmetic.

It is not our main purpose to teach modular arithmetic in this exercise, but rather to emphasize further the structure of mathematics. The interested reader should feel free, of course, to pursue the study of modular arithmetic on his own. This topic is included in most number theory texts as well as in textbooks on modern (abstract) algebra.

1.1.9

a.

+	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

x	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

b. (1)

$$\left.\begin{array}{l}(3 \times 5) \times 2 = 3 \times 2 = 0 \\ \\ 3 \times (5 \times 2) = 3 \times 4 = 0\end{array}\right\} \text{Therefore, } (3 \times 5) \times 2 = 3 \times (5 \times 2)$$

(2)

$$\left.\begin{array}{l}(3 \times 5) + 4 = 3 + 4 = 1 \\ \\ 3 \times (5 + 4) = 3 \times 3 = 3\end{array}\right\} \text{Therefore, } (3 \times 5) + 4 \neq 3 \times (5 + 4)$$

(3) $5^1 = 5$, $5^2 = 5 \times 5 = 1$, $5^3 = 5^2 \times 5 = 1 \times 5 = 5$, etc. In other words,

$$5^n = \begin{cases} 5, \text{ if n is odd} \\ \\ 1, \text{ if n is even} \end{cases}$$

Therefore, $5^{1000} = 1$ which, in terms of divisibility, says that $5^{1000} \equiv 1 \pmod 6$, or 5^{1000} leaves a remainder of 1 when divided by 6.

c. (1) $5^{-1} = 5$, since $5 \times 5^{-1} = 1$ and $5 \times 5 = 1$.

(2) 3^{-1} doesn't exist since $3x = 1$ has no solutions in modular-6 arithmetic (just look at the multiplication table).

d. Notice that $3 \times 2 = 0$ even though neither 2 nor 3 is equal to 0. This is not a contradiction to our previous result that if $ab = 0$ and $a \neq 0$ then $b = 0$. Namely, in the proof of this result we used

1.1.9 continued

the "fact" that if $a \neq 0$ there exists a number a^{-1} such that $a \times a^{-1} = 1$. As we saw in part (c), (2), this need not happen in modular-6 arithmetic (in particular, when $a = 3$). Since the rule does not apply here, neither need any inescapable consequence of the rule apply.

Resource: Calculus Revisited: Multivariable Calculus
Prof. Herbert Gross