

In the previous investigation, you worked with a binary operation  $\boxplus_6$  on the set  $\{0,1,2,3,4,5\}$  defined by the rule

$$a \boxplus_6 b$$

is the remainder obtained when  $a + b$  is divided by 6. In this investigation, we will extend the definition of this operation and introduce an important result about integers.

***Divisibility in the Integers***

Let  $a$  and  $b$  be integers. We say that  $b$  is *divisible* by  $a$  provided there exists an integer  $k$  such that  $b = ak$ . When this is true, we say that  $a$  *divides*  $b$  or that  $a$  is a *factor* of  $b$ .

The following result plays a key role in many of the concepts we will be exploring throughout the course.

***THEOREM 2.1 (The Division Algorithm)***

Let  $a$  and  $b$  be integers and suppose that  $a > 0$ . There exist unique integers  $Q$  and  $R$  such that  $0 \leq R < a$  and

$$b = Qa + R$$

The letters  $Q$  and  $R$  stand for “Quotient” and “Remainder;” and the Division Algorithm simply states a fact that you have known since elementary school --- whenever you divide one integer by another, you get a “quotient” and a “remainder” that is no larger than the divisor. Notice that  $a$  divides  $b$  precisely when  $R = 0$ .

The name “Division Algorithm” is misleading, since the theorem does not provide a systematic way of determining the values of  $Q$  and  $R$  --- the theorem merely states that these values always exist.

**Problem 1.** Determine the values of  $Q$  and  $R$  that will make the equation  $-28 = 3Q + R$  a true statement.

***Proving the Division Algorithm***

To begin, let  $S = \{b - na : n \in \mathbb{Z}\}$ . First, observe that  $b \in S$  (since  $b = b - 0 \cdot a$ ). Also, it will be true that  $b - ba = b(1 - a) \in S$ . Since  $b \in S$ , if  $b \geq 0$  we know that  $S$  contains nonnegative elements. Suppose that  $b < 0$ . We have assumed that  $a > 0$ ; hence, we know that  $1 - a \leq 0$ . Consequently, it follows that  $b(1 - a) \geq 0$ . Consequently, regardless of whether  $b < 0$  or  $b \geq 0$ , we know that the set  $S$  contains nonnegative elements.

Any nonempty collection of nonnegative integers must have a smallest member. Therefore, we are justified in considering the smallest nonnegative member of the set  $S$ . We will prove that this integer satisfies the conditions of the Division Algorithm.

Let  $R = b - Qa$  be the smallest nonnegative member of the set  $S$ . Since  $R$  is nonnegative by assumption, we know that  $0 \leq R$ . We need to show that  $R < a$ . Suppose by way of contradiction that  $a \leq R$  and consider the integer  $y = R - a$ . Observe that

$$y = R - a \Rightarrow y = (b - Qa) - a \Rightarrow y = b - (Q + 1)a$$

Consequently, we know that  $y \in S$ . However, we also know that  $0 \leq y < R$ . This is impossible since we have chosen  $R$  to be the *smallest nonnegative* member of the set  $S$ . We are therefore forced to conclude that  $R < a$ .

To complete the proof, we must show that the integers  $Q$  and  $R$  are unique --- that is, we must show that there is only one pair of integers  $Q$  and  $R$  such that  $R = b - Qa$  and  $0 \leq R < a$ .

To this end, suppose there also exist integers  $M$  and  $N$  such that  $N = b - Ma$  and  $0 \leq N < a$ . We will prove that  $Q = M$  and  $R = N$ . Either  $Q \leq M$  or  $M \leq Q$ . Let's assume  $M \leq Q$ .

Since  $b = Qa + R$  and  $b = Ma + N$ , we know

$$Qa + R = Ma + N \Rightarrow (Q - M)a = N - R$$

This tells us that  $N - R$  is an integer multiple of  $a$ . Now, we have assumed that  $0 \leq N < a$  and  $0 \leq R < a$ . Consequently, we know

$$N < a \Rightarrow N < a + R \Rightarrow N - R < a$$

We have assumed that  $M \leq Q$ . Therefore, we know that  $Q - M \geq 0$ . Since we have assumed that  $a > 0$ , we must conclude that  $N - R \geq 0$ . Therefore, we know

$$0 \leq N - R < a$$

However, we also know that  $N - R$  is an integer multiple of  $a$ . We have no choice but to conclude that  $N - R = 0$ ; in other words, we must conclude that  $N = R$ .

Consequently, we also know that  $(Q - M)a = 0$ ; and since we have assumed that  $a > 0$ , we are forced to conclude that  $Q - M = 0$ . Hence, we know that  $Q = M$  as well.

QED

#### ***Addition and Multiplication Modulo $n$***

Let  $n$  be a fixed positive integer, and let  $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n - 1\}$ . For all  $a, b \in \mathbb{Z}_n$ , let

$$a \boxplus_n b = R \qquad a \boxtimes_n b = S$$

where  $R$  is the remainder obtained when  $a + b$  is divided by  $n$  and  $S$  is the remainder obtained when  $ab$  is divided by  $n$ . The Division Algorithm tells us that  $\boxplus_n$  and  $\boxtimes_n$  are binary operations on the set  $\mathbb{Z}_n$ . We call these operations *addition modulo  $n$*  and *multiplication modulo  $n$* , respectively.

**Problem 2.** Fill in the tables below.

$\boxplus_4$	0	1	2	3
0				
1				
2				
3				

$\boxtimes_4$	0	1	2	3
0				
1				
2				
3				

**Problem 3.** Consider the tables you filled in for Problem 2. Based on the tables, do either of the following equations have multiple solutions in the set  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ ?

$$2 \boxtimes_4 x = 2 \qquad 2 \boxplus_4 x = 2$$

**Problem 4.** Consider the table for multiplication modulo 4. Based on this table, are there any equations of the form  $a \boxtimes_4 x = b$  that have no solution in the set  $\mathbb{Z}_4$ ? How did you decide?

**Problem 5.** Consider the table for addition modulo 4. Based on this table, are there any equations of the form  $a \boxplus_4 x = b$  that have no solution in the set  $\mathbb{Z}_4$ ? How did you decide?

**THEOREM 2.2 (Associativity of Addition and Multiplication Modulo  $n$ )**

The binary operations of addition and multiplication modulo  $n$  on the set  $\mathbb{Z}_n$  are both associative.

**Problem 6.** The proof of Theorem 2.2 is an application of the Division Algorithm. Fill in the gaps in the following proof that addition modulo  $n$  is associative.

**Proof.** Let  $a, b, c \in \mathbb{Z}_n$  and consider the elements  $(a \boxplus_n b) \boxplus_n c$  and  $a \boxplus_n (b \boxplus_n c)$ . We want to show that these elements are the same. Let  $a \boxplus_n b = r$  and let  $(a \boxplus_n b) \boxplus_n c = s$ . There exist unique integers  $x$  and  $y$  such that  $a + b = nx + r$  and  $r + c = ny + s$ .

**[Why?]**

Therefore, we know that  $(a + b) + c = n(x + y) + s$ .

**[Why?]**

Now, since integer addition is associative, we know that  $a + (b + c) = n(x + y) + s$ . Consequently, we must conclude that  $s$  is the remainder obtained when  $a + (b + c)$  is divided by  $n$ .

**[Why can we conclude this?]**

In other words,  $(a \boxplus_n b) \boxplus_n c$  must be the remainder obtained when  $a + (b + c)$  is divided by  $n$ .

Now, let  $b \boxplus_n c = t$  and let  $a \boxplus_n (b \boxplus_n c) = u$ . There exist unique integers  $v$  and  $w$  such that  $b + c = nv + t$  and  $a + t = nw + u$ . Consequently, we know  $a + (b + c) = n(v + w) + u$ . We are forced to conclude that  $u = s$ , as desired.

**[Why must we conclude this?]**

**Homework.**

**Problem 1.** Let  $\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\}$  and let  $\boxplus_8$  and  $\boxtimes_8$  represent the binary operations of addition and multiplication modulo 8, respectively, on the set  $\mathbb{Z}_8$ . Construct the operation tables for the set  $\mathbb{Z}_8$  under each operation.

**Problem 2.** Let  $\mathbb{U}_8 = \{1,3,5,7\}$ .

**Part (a).** Is addition modulo 8 a binary operation on this set? Justify your answer.

**Part (b).** Is multiplication modulo 8 a binary operation on this set? Justify your answer.

**Problem 3.** Complete the following proof.

*Let  $a, b, c$  be integers. If  $a$  divides  $b$  and  $a$  divides  $c$ , then  $a$  divides  $xb + yc$  for any integers  $x$  and  $y$ .*

**Proof.** Since  $a$  divides  $b$ , we know there exists an integer  $k$  such that  $b = ak$ . Likewise, we know there exists an integer  $j$  such that  $c = aj$ . Suppose that  $x$  and  $y$  are any integers. Since we want to show that  $a$  divides  $xb + yc$ , we must find an integer  $m$  such that  $xb + yc = am$ .

[...]

Therefore, we may conclude that  $a$  divides  $xb + yc$ .

**Problem 4.** Let  $a, b, c$  be integers. If  $a$  divides  $b$  and  $b$  divides  $c$ , construct a proof that  $a$  divides  $c$ . (You may assume that integer multiplication is associative.)

**Problem 5.** Consider the set  $\mathbb{Z}_{12}$ .

**Part (a).** Is it true that  $(3 \boxplus_6 4) \boxplus_{12} (3 \boxplus_6 4) = (3 \boxplus_{12} 4) \boxplus_{12} (3 \boxplus_{12} 4)$ ? Justify your answer.

**Part (b).** Is it true that  $(3 \boxplus_5 4) \boxplus_{12} (3 \boxplus_5 4) = (3 \boxplus_{12} 4) \boxplus_{12} (3 \boxplus_{12} 4)$ ? Justify your answer.

**Problem 6.** Let  $n$  be a positive integer, and let  $m = 2n$ . In this exercise, you will prove that, if  $x, y \in \mathbb{Z}_n$ , then

$$(x \boxplus_n y) \boxplus_m (x \boxplus_n y) = (x \boxplus_m y) \boxplus_m (x \boxplus_m y)$$

**Proof.** The Division algorithm tells us that there exist unique integers  $q$  and  $r$  such that  $0 \leq r < n$  and  $x + y = qn + r$ . Now, this tells us that  $x \boxplus_n y = r$ ; and it follows that

$$(x \boxplus_n y) \boxplus_m (x \boxplus_n y) = r \boxplus_m r$$

We know that  $r + r = 0 \cdot m + 2r$ . Consequently, the Division Algorithm tells us that

$$(x \boxplus_n y) \boxplus_m (x \boxplus_n y) = 2r$$

**[Why?]**

Let's consider  $(x \boxplus_m y) \boxplus_m (x \boxplus_m y)$ . The Division Algorithm tells us there unique exist integers  $u$  and  $v$  such that  $x + y = um + v$  and  $0 \leq v < m$ . Furthermore, there exist unique integers  $w$  and  $t$  such that  $0 \leq t < m$  and

$$(x + y) + (x + y) = (2u + w)m + t$$

**[Why?]**

Therefore, we know  $(x \boxplus_m y) \boxplus_m (x \boxplus_m y) = t$ . **[Why?]**

On the other hand, we also know that  $(x + y) + (x + y) = qm + 2r$ . **[Why?]**

We may therefore conclude that  $t = 2r$ . **[Why?]**

We have shown that

$$(x \boxplus_m y) \boxplus_m (x \boxplus_m y) = t = 2r = (x \boxplus_n y) \boxplus_m (x \boxplus_n y)$$