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

Problem 2. To begin, let $S = \{b - na : n \in \mathbb{Z}\}$.
Part (a). Explain why $b \in S$ and $b(1 - a) \in S$.

Part (b). Explain why we know that $1 - a \leq 0$ and use this observation to explain why S must contain 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.

Problem 3. 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 $R < a$.

Part (a). Consider the integer $y = R - a$. Explain why $y = b - (Q + 1)a$.

Part (b). Using Part (a), explain why assuming that $R \geq a$ contradicts our choice of R.

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 $0 \leq R < a$.

Problem 4. 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 $M \leq Q$.

Part (a). Explain why we know that $(Q - M)a = N - R$.

Part (b). Explain why we know that $0 \leq Q - M$ and $N - R < a$.

Part (c). We also know that $N - R$ is an integer multiple of a. Explain why Part (b) forces us to conclude that $N - R = 0$.

We now know that $N = R$, and we know that $(Q - M)a = 0$. 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

The following result is a very useful consequence of the Division Algorithm.

Corollary 2.2

Let n be a fixed positive integer, and let $n\mathbb{Z} = \{n \cdot x : x \in \mathbb{Z}\}$. For all $a, b \in \mathbb{Z}$, the following statements are logically equivalent.

1. The integers a and b have the same remainder when divided by n.
2. We have $b - a \in n\mathbb{Z}$.

Problem 5. Use the Division Algorithm to show that Statement 1 implies Statement 2.

Problem 6. Now, suppose we know $b - a \in n\mathbb{Z}$. We want to show that a and b have the same remainder when divided by n. We know there exists some integer x such that $b - a = nx$.

Part (a). Let r be the remainder obtained when a is divided by n. Use the Division Algorithm to explain why we know $b = (x + q)n + r$ for some integer q.

Part (b). Explain why the Division Algorithm forces us to conclude that r is also the remainder obtained when b is divided by n.

Addition and Multiplication Modulo n

Let n be a fixed positive integer, and let $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n - 1\}$. 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 7. 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 8. 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 9. 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 10. 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?

Let n be a fixed positive integer, and suppose that $u, v, w \in \mathbb{Z}$. The Division Algorithm tells us

- There exist integers p and r such that $u + v = pn + r$ and $0 \leq r < n$.
- There exist integers q and s such that $r + w = qn + s$ and $0 \leq s < n$.

Problem 11. Use algebra to show that $(u + v) + w = kn + s$ for some integer k.

Problem 12. Use the Division Algorithm to explain why we must conclude $(u \boxplus_n v) \boxplus_n w = s$.

Now, the Division Algorithm also tells us

- There exist integers a and b such that $v + w = an + b$ and $0 \leq b < n$.
- There exist integers c and d such that $u + b = cn + d$ and $0 \leq d < n$.

Problem 13. Use algebra to show that $u + (v + w) = jn + d$ for some integer j.

Problem 14. Use the Division Algorithm to explain why we must conclude $u \boxplus_n (v \boxplus_n w) = d$.

Problem 15. Use the fact that integer addition is associative to explain why we must now conclude that the following statement is true.

Addition modulo n is an associative binary operation on the set $\mathbb{Z}_n$.

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. Adjust the arguments from Investigation Problems 10 – 15 above to prove the following statement.

Multiplication modulo n is an associative binary operation on the set $\mathbb{Z}_n$.