In this investigation, we will use of an *assumption* we make about the set of positive integers. This assumption will play a role in many of our future investigations as well.

Axiom of Well-Ordering

Every nonempty subset of positive integers has a smallest member.

It is customary to let $n\mathbb{Z}$ represent the set of all integer multiples of a fixed positive integer n. In symbols, we have

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

Problem 1. Let n be a fixed positive integer larger than 1, and let a be any nonnegative integer (sometimes called a *whole number*).

Part (a). Explain why there must be a positive integer multiple of n that is greater than a.

Part (b). Let $S_a = \{x \in n\mathbb{Z} : a < x\}$. Why can we assume S_a has a smallest member?

Part (c). Let nb be the smallest member of S_a. Explain why we must have $n(b-1) \leq a$.

Part (d). Explain why there exists exactly one integer $0 \leq r < n$ such that $a = n(b-1) + r$.

THEOREM 2.1 (The Division Algorithm)

Let a and n be integers and suppose that $n > 0$. There exists exactly one pair of integers k and r such that $0 \leq r < n$ and

$$a = nk + r$$

In Problem 1, you constructed a proof of the Division Algorithm when $a \geq 0$. You will consider the case when $a < 0$ in the exercises.

The special integers k and r guaranteed by the Division Algorithm are called the *quotient* and *remainder*, respectively, for the integer a *relative to* the integer n. The fixed integer n is called the *measure* (or *modulus*[1]) that determines the quotient and remainder.

Congruence Modulo n

Let a and b be integers, and let $n > 1$ be a fixed positive integer. We say that a is *congruent to b modulo n* provided $a - b \in n\mathbb{Z}$. We write $a \equiv b \pmod{n}$ if this is the case.

Problem 2. Let a and b be integers, and let $n > 1$ be a fixed positive integer.

Part (a). If $a \equiv b(\text{mod } n)$, is it true that $b \equiv a(\text{mod } n)$, ? Justify your answer.

Part (b). If $a \equiv b(\text{mod } n)$, is it true that $a = b$? Justify your answer.

Part (c). If $a \equiv b(\text{mod } n)$, is it true that $a \equiv -b(\text{mod } n)$? Justify your answer.

Problem 3. Let a, b and c be integers, and let $n > 1$ be a fixed positive integer.

Part (a). If $a \equiv b(\text{mod } n)$, and $b \equiv c(\text{mod } n)$, then prove $a \equiv c(\text{mod } n)$.

Part (b). If $b \equiv c(\text{mod } n)$, then prove $a + b \equiv [a + c](\text{mod } n)$.

Part (c). If r is the remainder for a relative to n, prove $a \equiv r(\text{mod } n)$.

[1] The word "*modulus*" is Latin for "measure."

Addition and Multiplication Modulo n

Let $n > 1$ 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

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

where R is the remainder for $a + b$ relative to n and S is the remainder for ab relative to n. We call these operations *addition modulo n* and *multiplication modulo n*, respectively.

Problem 4. Suppose $r, s \in \mathbb{Z}_n$.

Part (a). Explain why we must have $-n < r - s < n$.

Part (b). If $r \equiv s (\mathrm{mod}\, n)$, use Part (a) to prove that we must have $r = s$.

Problem 5. Suppose , $y \in \mathbb{Z}_n$.

Part (a). Use Problem 3 to help prove $x \boxplus_n y \equiv [x + y] (\mathrm{mod}\, n)$.

Part (b). Use Part (a) and Problem 2 Part (a) and Problem 4 to prove $x \boxplus_n y = y \boxplus_n x$.

Problem 6. Suppose , $v, w \in \mathbb{Z}_n$. In this problem, we will use Problems 3, 4, and 5 to prove that

$$u \boxplus_n (v \boxplus_n w) = (u \boxplus_n v) \boxplus_n w$$

In each of the following parts, consider which part (or parts) of Problems 3, 4, or 5 is used to reach the conclusion.

Part (a). Why do we know that $u + (v + w) \equiv ([u + v] + w) (\mathrm{mod}\, n)$?

Part (b). Explain why we know $v \boxplus_n w \equiv [v + w] (\mathrm{mod}\, n)$, then explain why knowing this allows us to conclude $u + (v \boxplus_n w) \equiv (u + [v + w]) (\mathrm{mod}\, n)$.

Part (c). Explain why we can also conclude that $(u \boxplus_n v) + w \equiv ([u + v] + w) (\mathrm{mod}\, n)$.

Part (d). Now, explain why we can conclude $u \boxplus_n (v \boxplus_n w) \equiv (u + [v + w]) (\mathrm{mod}\, n)$ and $(u \boxplus_n v) \boxplus_n w \equiv ([u + v] + w) (\mathrm{mod}\, n)$.

Part (e). Use Parts (a), (b), (c), and (d) to help explain why we know

$$u \boxplus_n (v \boxplus_n w) \equiv [(u \boxplus_n v) \boxplus_n w] (\mathrm{mod}\, n)$$

Part (f). Why does Part (c) allows us to conclude $u \boxplus_n (v \boxplus_n w) = (u \boxplus_n v) \boxplus_n w$?

Problem 7. Fill in the operation tables below for the algebras $\mathbb{Z}_4 = (\mathbb{Z}_4, \boxplus_4)$ and $\mathbb{Z}_4{}^m = (\mathbb{Z}_4, \boxtimes_4)$.

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

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

Homework.

Problem 1. Fill in the operation table for the algebras $\mathbb{Z}_6 = (\mathbb{Z}_6, \boxplus_6)$ and $\mathbb{Z}_6{}^m = (\mathbb{Z}_6, \boxtimes_6)$.

$\boxplus_6$	**0**	**1**	**2**	**3**	**4**	**5**
0						
1						
2						
3						
4						
5						

$\boxtimes_6$	**0**	**1**	**2**	**3**	**4**	**5**
0						
1						
2						
3						
4						
5						

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. Let a, b and c be integers, and let $n > 1$ be a fixed positive integer.

Part (a). Prove that $a \boxtimes_n b \equiv ab (\mathrm{mod}\ n)$.

Part (b). If $b \equiv c (\mathrm{mod}\ n)$, then prove $ab \equiv [ac] (\mathrm{mod}\ n)$.

Problem 4. Let a, b and c be integers, and let $n > 1$ be a fixed positive integer. Use Problem 3 along with Investigation Problem 5 to prove

Part (b). We have $a \boxtimes_n b = b \boxtimes_n a$.

Part (c). We have $(a \boxtimes_n b) \boxtimes_n c = a \boxtimes_n (b \boxtimes_n c)$.

Let a and b be integers. We say that a *divides* b provided $b = ak$ for some integer k.

Problem 5. 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 6. Construct a proof of the following result.

- 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.

Problem 7. Prove the Division Algorithm for negative integers a. In other words, for a fixed positive integer $n > 1$ and any negative integer a, prove that there exists exactly one pair of integers k, r such that $0 \leq r < n$ and $a = nk + r$. (Hint: Start by applying the Division Algorithm to $|a|$, then use the fact that $|a| = -a$.)