Arkansas Tech University
MATH 4033: Elementary Modern Algebra
Dr. Marcel B. Finan

10 The Division Algorithm. Congruence Modulo n

In this section, we want to introduce an important equivalence relation on the set of integers $\mathbb{Z}$. This relation depends on the concept of divisibility of integers which we discuss next.

10.1 Divisibility. The Division Algorithm

In this section we study the divisibility of integers. Our main goal is to obtain the *Division Algorithm*. This is achieved by applying the well-ordering principle which we prove next.

Theorem 10.1 *(The Well-Ordering Principle)*
If S is a nonempty subset of $\mathbb{N}$ then there is an $m \in S$ such that $m \leq x$ for all $x \in S$. That is, S has a smallest element.

Proof.
We will use contradiction to prove the theorem. That is, by assuming that S has no smallest element we will prove that $S = \emptyset$.
We will prove that $n \notin S$ for all $n \in \mathbb{N}$. We do this by induction on n. Since S has no smallest element then $1 \notin S$. Asuume that we have proved that $1, 2, \cdots, n \notin S$. We will show that $n+1 \notin S$. If $n+1 \in S$ then since $1, 2, 3, \cdots \notin S$ then $n+1$ would be the smallest element of S and this contradicts the assumption that S has no smallest element. Thus, we must have $n+1 \notin S$. Hence, by the principle of mathematical induction, $n \notin S$ for all $n \in \mathbb{N}$. But this leads to $S = \emptyset$. This conclusion contradicts the hypothesis of the theorem where S is given to be nonempty. This establishes a proof of the theorem.$\blacksquare$

Remark 10.1
The above theorem is false if $\mathbb{N}$ is replaced by $\mathbb{Z}, \mathbb{Q}$, or $\mathbb{R}$. For example, $\{x \in \mathbb{Z} : x \leq -1\}$ is a nonempty subset of $\mathbb{Z}$ with no smallest element.

Before establishing the Division Algorithm, we introduce the concept of divisibility and derive some of its properties.

Definition 10.1
An integer m is **divisible** by a nonzero integer n if and only if $m = nq$ for some integer q. We also say that n **divides** m, n is a **divisor** of m, m is a **multiple** of n, or n is a **factor** of m. We write $n|m$. If n does not divide m we write $n \not| m$. A positive integer n with only divisors 1 and n is called **prime.**

Example 10.1
Since $8 = 2 \cdot 4$ then $2|\ 8$ and $4|\ 8$. However, $4 \not| 6$.$\blacksquare$

The following theorem discusses some of the properties of divisibility.

Theorem 10.2
(a) If $n|m$ then $n|(tm)$ for any integer t.
(b) If $n|a$ and $n|b$ then $n|(a \pm b)$
(c) If $n|m$ and $m|p$ then $n|p$. That is, division is associative.
(d) If $n|m$ and $m|n$ then either $n = m$ or $n = -m$. In particular, if both m and n are positive integer then $m = n$.

Proof.
(a) Suppose that $n|m$. Then $m = nq$ for some $q \in \mathbb{Z}$. Multiplying the last equation by $t \in \mathbb{Z}$ to obtain $tm = tnq = n(tq) = nq'$ where $q' = tq \in \mathbb{Z}$. This shows that $n|tm$.
(b) Suppose that $n|a$ and $n|b$. Then $a = nq$ and $b = nq'$ for some $q, q' \in \mathbb{Z}$. Thus, $a \pm b = n(q \pm q')$. Hence, $n|(a \pm b)$.
(c) Suppose that $n|m$ and $m|p$. Then $m = nq$ and $p = mq'$ for some $q, q' \in \mathbb{Z}$. Thus, $p = n(qq')$. Since $qq' \in \mathbb{Z}$ then $n|p$.
(d) If $n|m$ and $m|n$ then $m = nq$ and $n = mq'$ for some $q, q' \in \mathbb{Z}$. Thus, $m = mqq'$ or $(1 - qq')m = 0$. Since $m \neq 0$ then $qq' = 1$. This is only true if either $q = q' = 1$ or $q = q' = -1$. That is, $n = m$ or $n = -m$.$\blacksquare$

With the Well-Ordering Principle we can establish the following theorem.

Theorem 10.3 *(Division Algorithm)*
If a and b are integers with $b \neq 0$ then there exist unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

Proof.
We first assume that $b > 0$ so that $|b| = b$.

<u>**Existence**</u>
Consider the sets

$$S = \{a - bt : t \in \mathbb{Z}\}, \quad S' = \{x \in S : x \geq 0\}.$$

The set S' is nonempty. To see this, if $a \geq 0$ then $a - 0t \in S$ and $a - 0t \geq 0$. That is, $a \in S'$. If $a < 0$ then since $a - ba \in S$ and $a - ba = a(1 - b) \geq 0$ so that $a - ba \in S'$.
Now, if $0 \in S'$ then $a - qb = 0$ for some $q \in \mathbb{Z}$ and so $r = 0$ and in this case the theorem holds. So, assume that $0 \notin S'$. By Theorem10.1, there exist a smallest element $r \in S'$. That is,

$$a - qb = r, \quad for\ some\ q \in \mathbb{Z}.$$

Since $r \in S'$ then $r \geq 0$. It remains to show that $r < b$. If we assume the contrary, i.e. $r \geq b$, then

$$a - b(q + 1) = a - bq - b = r - b \geq 0$$

and this implies that $a - b(q + 1) \in S'$. But $b > 0$ so that

$$a - b(q + 1) = a - bq - b < a - bq = r$$

and this contradicts the definition of r as being the smallest element of S'. Thus, we have

$$a = bq + r, \quad 0 \leq r < b.$$

<u>**Uniqueness**</u>
Suppose that

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

and

$$a = bq_2 + r_2, \quad 0 \leq r_2 < b.$$

We must show that $r_1 = r_2$ and $q_1 = q_2$. Indeed, since $bq_1 + r_1 = bq_2 + r_2$ then $b(q_1 - q_2) = r_2 - r_1$. This says that $b|(r_2 - r_1)$. But $0 \leq r_1 < b$ and $0 \leq r_2 < b$ so that $-b < -r_1 < r_2 - r_1 < r_2 < b$. That is, $-b < r_2 - r_1 < b$. The only multiple of b strictly between $-b$ and b is zero. Hence, $r_1 = r_2$. But then $b(q_1 - q_2) = 0$ and since $b \neq 0$ then $q_1 = q_2$. ■

Example 10.2
If $a = 11$ and $b = 4$ then $q = 2$ and $r = 3$.

Remark 10.2
Note that if $b < 0$ then $|b| = -b$. Applying the theorem to a and $-b > 0$ we can find unique integers q and r such that $a = -bq + r$ with $0 \leq r < -b$. Let $q' = -q \in \mathbb{Z}$ then $a = bq' + r$ with $0 \leq r < -b$.

10.2 Congruence Modulo n.

Divisibility leads to the concept of congruence.

Definition 10.2
Let n be a positive integer. Integers a and b are said to be **congruent modulo** n if $a - b$ is divisible by n. This is denoted by writing $a \equiv b(mod\ n)$. We call n the **modulus.** If a is not congruent b modulo n we write $a \not\equiv b\ (mod\ n)$.

Example 10.3
17 and 65 are congruent modulo 6, because $65 - 17 = 48$ is divisible by 6. ■

Theorem 10.4
The following statements are all equivalent:

(i) $a \equiv b(mod\ n)$
(ii) $n|(a - b)$
(iii) $a - b = nt$ for some $t \in \mathbb{Z}$
(iv) $a = b + nt$ for some $t \in \mathbb{Z}$.

Proof.
(i) $\Longrightarrow$ (ii): Suppose that $a \equiv b(mod\ n)$. Then from Definition (10.2), $n|(a - b)$.
(ii) $\Longrightarrow$ (iii): Suppose that $n|(a - b)$. Then by Definition 10.1, there exists a $t \in \mathbb{Z}$ such that $a - b = nt$.
(iii) $\Longrightarrow$ (iv): Suppose that $a - b = nt$ for some $t \in \mathbb{Z}$. Then by adding b to both sides we get $a = b + nt$ which is the statement of (iv).
(iv) $\Longrightarrow$ (i): Suppose that $a = b + nt$ for some $t \in \mathbb{Z}$. Then $a - b = nt$. By Definition 10.1, $a - b$ is divisible by n and so $a \equiv b(mod\ n)$. ■

Congruence modulo n is an equivalence relation on $\mathbb{Z}$ as shown in the next theorem.

Theorem 10.5
For each positive integer n, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proof.
We shall show that $\equiv$ is reflexive, symmetric, and transitive.
Reflexive: Since $a - a = 0t$ for any $t \in \mathbb{Z}$ then $a \equiv a(mod\ n)$.
Symmetric: Let $a, b \in \mathbb{Z}$ be such that $a \equiv b(mod\ n)$. Then $a - b = nt$ for some $t \in \mathbb{Z}$. Multiplying both sides by -1 to obtain $b - a = n(-t)$. Since $(\mathbb{Z}, +)$ is a group then $-t \in \mathbb{Z}$ and so $b \equiv a(mod\ n)$.
Transitive: Suppose that $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$. Then $a - b = nt$ and $b - c = nt'$ for some $t, t' \in \mathbb{Z}$. Adding these equations together to obtain $a - c = n(t + t')$. But $\mathbb{Z}$ is closed under addition so that $t + t' \in \mathbb{Z}$. Hence, $a \equiv c(mod\ n)$. ■

Definition 10.3
The equivalence classes for the equivalence relation $\equiv$ are called *congruence classes*. They form a partition of $\mathbb{Z}$. The set of all congruence classes is denoted by $\mathbb{Z}_n$.

The following theorem shows that for each positive integer n, there are n congruence classes and each integer is congruent to either $0, 1, 2, \cdots, n - 1$. Thus, the set $\{0, 1, 2, \cdots, n - 1\}$ is a complete set of equivalence class representatives of the relation $\equiv$.

Theorem 10.6
Let n be a positive integer. Then each integer is congruent modulo n to precisely one of the integers $0, 1, 2, \cdots, n - 1$. That is, there are n distinct congruence classes, $[0], [1], \cdots, [n - 1]$.

Proof.
Let a be any integer. Then by the Division Algorithm there exist unique integers q and r such that

$$a = nq + r, \quad 0 \leq r < n.$$

This impplies that $a-r=nq$ and so by Theorem 10.4, $a \equiv r(mod\ n)$. Since $0 \leq r < n$ then a is congruent to at least one of the integers,$0, 1, 2, \cdots, n-1$.We will show that a is congruent to exactly one of the integers listed. To see this, assume that $a \equiv s(mod\ n)$ where $0 \leq s < n$. Then by Theorem 10.4, $a = nt + s$ for some $t \in \mathbb{Z}$. By uniqueness, we have $r = s$. This completes a proof of the theorem.■

Remark 10.3
It follows from the previous theorem that

$$\mathbb{Z}_n = \{[0], [1], [2], \cdots, [n-1]\}.$$

Example 10.4
For $n = 4$ the congruence classes are

$$\begin{array}{rcl} [0] & = & \{\cdots, -8, -4, 0, 4, 8, \cdots\} \\ [1] & = & \{\cdots, -7, -3, 1, 5, 9, \cdots\} \\ [2] & = & \{\cdots, -6, -2, 2, 6, 10, \cdots\} \\ [3] & = & \{\cdots, -5, -1, 3, 7, 11, \cdots\} \end{array}$$

Thus, $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$■