Mathematical Proofs
A Transition to Advanced Mathematics

Chapter 9
Equivalence Relations

Gary Chartrand Albert D. Polimeni Ping Zhang

Equivalence Relations

Two real numbers x and y can be related in a variety of ways. For example, (1) x may be less than y, (2) y may be 1 more than the square of x, or (3) x and y may be equal; in symbols,

$$(1)\ x < y, \quad (2)\ y = x^2 + 1 \quad \text{or } (3)\ x = y.$$

In the case of integers a and b, we could have

$$(1)\ a \mid b, \quad (2)\ a \text{ and } b \text{ are of opposite parity} \quad \text{or}$$
$$(3)\ a \equiv b \pmod 3.$$

Equivalence Relations

In the subject of geometry, a line ℓ in 3-space can be related to a plane Π in 3-space if

(1) ℓ lies on Π, (2) ℓ is parallel to Π or
(3) ℓ intersects Π in exactly one point.

A triangle T can be related to a triangle T' if

(1) T is congruent to T', (2) T is similar to T' or
(3) T has the same area as T'.

In all of these examples, there are two sets A and B (where possibly $A = B$) and an element of A is related to an element of B in some manner. The topic of relations turns out to be important in mathematics.

Relations

Relation

A **relation** R **from a set** A **to a set** B is subset of the Cartesian product $A \times B$ of A and B. That is, the relation R is a set of ordered pairs, where the first coordinate of the pair belongs to A and the second coordinate belongs to B.

If $(a, b) \in R$, then a is **related** to b by R and we write $a\ R\ b$.
If $(a, b) \notin R$, then a is *not* related to b by R and we write $a\ \not{R}\ b$.

For example, suppose that $A = \{x, y, z\}$ and $B = \{1, 2\}$ are two sets and we are considering the subset

$$R = \{(x, 2), (y, 1), (y, 2)\}$$

of $A \times B$. Hence, R is a relation from A to B. In this case, $x\ R\ 2$ (x is related to 2) and $x \not R\ 1$ (x is not related to 1). For any two sets A and B, the sets $\emptyset$ and $A \times B$ are always subsets of $A \times B$ and so $\emptyset$ and $A \times B$ are relations from A to B.

Definitions

Let R be a relation from set A to a set B.

By the **domain** of R, which we denote by $\mathrm{dom}(R)$, is meant the subset of A defined by

$$\mathrm{dom}(R) = \{a \in A : \ (a, b) \in R \text{ for some } b \in B\};$$

while the **range** of R, denoted by $\mathrm{range}(R)$, is the subset of B defined by

$$\mathrm{range}(R) = \{b \in B : \ (a, b) \in R \text{ for some } a \in A\}.$$

That is, $\mathrm{dom}(R)$ is that set of elements of A that occur as first coordinates among the ordered pairs in R and $\mathrm{range}(R)$ is the set of elements of B that occur as second coordinates among the ordered pairs in R.

The domain and range of the relation $R = \{(x, 2), (y, 1), (y, 2)\}$ are

$$\mathrm{dom}(R) = \{x, y\} \text{ and } \mathrm{range}(R) = \{1, 2\}.$$

The reason that $z \notin \mathrm{dom}(R)$ is because there is no ordered pair in R whose first coordinate is z.

Inverse Relation

If R is a relation from a set A to a set B, then the **inverse relation** of R is the relation R^{-1} from B to A defined by

$$R^{-1} = \{(b, a) : \ (a, b) \in R\}.$$

That is, to obtain R^{-1} from R, the first and second coordinates of each ordered pair in R are interchanged.

For example, the inverse relation of the relation

$$R = \{(x, 2), (y, 1), (y, 2)\}$$

from $A = \{x, y, z\}$ to $B = \{1, 2\}$ is the relation

$$R^{-1} = \{(1, y), (2, x), (2, y)\}$$

from B to A.

Relation on a Set

By a **relation on a set** A, we mean a relation from A to A. That is, a relation on a single set A is a collection of ordered pairs whose first *and* second coordinates belong to A.

For example,

$$\{(1,2),(1,3),(2,2),(2,3)\}$$

is a relation on the set $A = \{1,2,3,4\}$.

If $A = \{1, 2\}$, then

$$A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}.$$

Since $|A \times A| = 4$, the number of subsets of $A \times A$ is $2^4 = 16$. Since a relation on A is, by definition, a subset of $A \times A$, it follows that there are 16 relations on A. Six of these 16 possible relations are

$$\emptyset,\ \{(1, 2)\},\ \{(1, 1), (1, 2)\},\ \{(1, 2), (2, 1)\},$$
$$\{(1, 1), (1, 2), (2, 2)\},\ A \times A.$$

Properties of Relations

Definition

A relation R defined on a set A is called **reflexive** if $x \; R \; x$ for every $x \in A$. That is, R is reflexive if $(x, x) \in R$ for every $x \in A$.

Definition

A relation R defined on a set A is called **symmetric** if whenever $x \; R \; y$, then $y \; R \; x$ for all $x, y \in A$.

Hence, for a relation R on A to be "not symmetric," there must be some ordered pair (w, z) in R for which $(z, w) \notin R$. Certainly, if such an ordered pair (w, z) exists, then $w \neq z$.

Properties of Relations

Definition

A relation R defined on a set A is called **transitive** if whenever $x \; R \; y$ and $y \; R \; z$, then $x \; R \; z$, for all $x, y, z \in A$.

Notice that in this definition, it is *not* required that x, y and z be distinct.

Hence, for a relation R on A to be "not transitive," there must exist two ordered pairs (u, v) and (v, w) in R such that $(u, w) \notin R$. If this should occur, then necessarily $u \neq v$ and $v \neq w$ (although perhaps $u = w$).

Example 1

Let $S = \{a, b, c\}$ and consider the properties of the following relations defined on S:

$$
\begin{aligned}
R_1 &= \{(a,b),(b,a),(c,a)\} \\
R_2 &= \{(a,b),(b,b),(b,c),(c,b),(c,c)\} \\
R_3 &= \{(a,a),(a,c),(b,b),(c,a),(c,c)\} \\
R_4 &= \{(a,a),(a,b),(b,b),(b,c),(a,c)\}
\end{aligned}
$$

	R_1	R_2	R_3	R_4
reflexive			$\star$	
symmetric			$\star$	
transitive			$\star$	$\star$

Example 1 (continued)

$$
\begin{aligned}
R_5 &= \{(a,a),(a,b)\} \\
R_6 &= \{(a,b),(a,c)\} \\
R_7 &= \{(a,a),(a,b),(b,a),(b,b),(b,c),(c,c)\} \\
R_8 &= \{(a,a),(a,c),(c,a)\}.
\end{aligned}
$$

	R_5	R_6	R_7	R_8
reflexive			$\star$	
symmetric				$\star$
transitive	$\star$	$\star$		

Definition

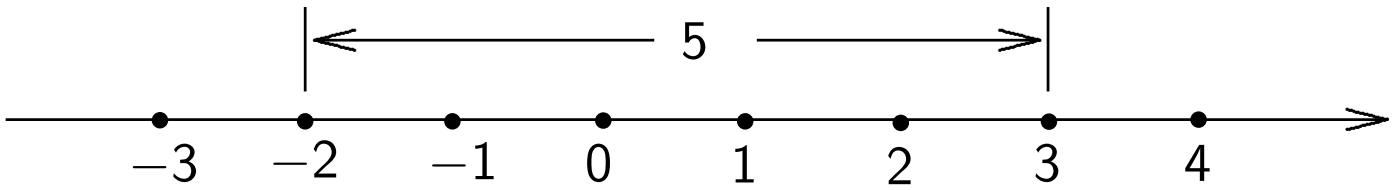
The **distance** between two real numbers a and b is $|a - b|$.

So the distance between 2 and 4.5 is $|2 - 4.5| = |-2.5| = 2.5$.

Thus, if the real numbers (points) a and b are plotted on the real number line (x-axis), then the length of this segment is the distance between them.

This is illustrated in the figure below for the real numbers $a = 3$ and $b = -2$, where the distance between them is

$$|a - b| = |3 - (-2)| = 5 = |(-2) - 3| = |b - a|.$$



Properties of Relations

Define a relation R on the set $\mathbf{R}$ of real numbers by $a\ R\ b$ if $|a - b| \leq 1$, that is, a is related to b if the distance between a and b is at most 1.

- ⋆ Certainly, the distance from a real number to itself is 0, that is, $|a - a| = 0 \leq 1$ for every $x \in \mathbf{R}$. So, $a\ R\ a$ and R is reflexive.
- ⋆ If the distance between two real numbers a and b is at most 1, then the distance between b and a is at most 1. In symbols, if $|a - b| \leq 1$, then $|b - a| = |a - b| \leq 1$; that is, if $a\ R\ b$, then $b\ R\ a$. Therefore, R is symmetric.

Properties of Relations

- Now to the the transitive property. If $a \; R \; b$ and $b \; R \; c$, is $a \; R \; c$? That is, if the distance between a and b is at most 1 and the distance between b and c is at most 1, does it follow that the distance between a and c is at most 1? The answer is no. For example, $3 \; R \; 2$ and $2 \; R \; 1$ since $|3-2| \leq 1$ and $|2-1| \leq 1$. However, $|3-1| = 2$. So, $3 \not R \; 1$ and R is not transitive.

Equivalence Relations

Definition

A relation R defined on a set A is called an **equivalence relation** if R is reflexive, symmetric and transitive.

The equals relation R defined on $\mathbf{Z}$ by $a\ R\ b$ if $a = b$ is an equivalence relation on $\mathbf{Z}$.

For $A = \{1, 2, 3, 4, 5, 6\}$, let R be the relation defined on A that consists of the following ordered pairs:

$$\begin{aligned} R \quad = \quad & \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(1,3),(1,6), \\ & (6,1),(6,3),(3,1),(3,6),(2,4),(4,2)\}. \end{aligned}$$

Since this relation has all three of the properties reflexive, symmetric and transitive, it is an equivalence relation.

Equivalence Relations

Suppose that R is an equivalence relation on some set A. If $a \in A$, then a is related to a since R is reflexive. Quite possibly, other elements of A are related to a as well.

The set consisting of all those elements that are related to a given element of A will turn out to be important and, for this reason, these sets are given special names.

Equivalence Class

For an equivalence relation R defined on a set A and for an element $a \in A$, the set

$$[a] = \{x \in A : \ x \ R \ a\},$$

consisting of all elements in A that are related to a, is called an **equivalence class**.

In fact, $[a]$ is the equivalence class containing a since $a \in [a]$ (because R is reflexive). Loosely speaking then, $[a]$ consists of the "relatives" of a. For the equivalence relation R defined above, the resulting equivalence classes are

$$\begin{aligned} [1] &= \{1,3,6\}, \quad [2] = \{2,4\}, \quad [3] = \{1,3,6\}, \\ [4] &= \{2,4\}, \quad [5] = \{5\}, \quad [6] = \{1,3,6\}. \end{aligned}$$

Since $[1] = [3] = [6]$ and $[2] = [4]$, there are only three distinct equivalence classes in this case, namely $[1], [2]$ and $[5]$.

Example 2

Result The relation R defined on $\mathbf{Z}$ by $x \ R \ y$ if $x + 3y$ is even is an equivalence relation.

Proof. First, we show that R is reflexive. Let $a \in \mathbf{Z}$. Then

$$a + 3a = 4a = 2(2a)$$

is even since $2a \in \mathbf{Z}$. Therefore, $a \ R \ a$ and R is reflexive.

Example 2 (continued)

Next, we show that R is symmetric. Assume that $a\ R\ b$. Thus, $a + 3b$ is even. Hence,

$$a + 3b = 2k \text{ for some integer } k.$$

So, $a = 2k - 3b$. Therefore,

$$\begin{aligned} b + 3a &= b + 3(2k - 3b) = b + 6k - 9b \\ &= 6k - 8b = 2(3k - 4b). \end{aligned}$$

Since $3k - 4b$ is an integer, $b + 3a$ is even. Therefore, $b\ R\ a$ and R is symmetric.

Example 2 (continued)

Finally, we show that R is transitive. Assume that $a\ R\ b$ and $b\ R\ c$. Hence, $a+3b$ and $b+3c$ are even; so

$$a+3b=2k \text{ and } b+3c=2\ell \text{ for some integers } k \text{ and } \ell.$$

Adding these two equations, we obtain

$$(a+3b)+(b+3c)=2k+2\ell.$$

So $a+4b+3c=2k+2\ell$ and

$$a+3c=2k+2\ell-4b=2(k+\ell-2b).$$

Since $k+\ell-2b$ is an integer, $a+3c$ is even. Hence, $a\ R\ c$ and so R is transitive. Therefore, R is an equivalence relation. □

Equivalence Relations

Since the relation $x\ R\ y$ if $x + 3y$ is even is an equivalence relation, there are equivalence classes, namely an equivalence class $[a]$ for each $a \in \mathbf{Z}$. Let's start with 0, say. The equivalence class $[0]$ is the set of all integers related to 0. In symbols, this equivalence class is

$$\begin{aligned}
[0] &= \{x \in \mathbf{Z} :\ x\ R\ 0\} \\
&= \{x \in \mathbf{Z} :\ x + 3 \cdot 0 \text{ is even}\} \\
&= \{x \in \mathbf{Z} :\ x \text{ is even}\} \\
&= \{0, \pm 2, \pm 4, \ldots\}.
\end{aligned}$$

It shouldn't be difficult to see that if a is an even integer, say $a = 2k$, where $k \in \mathbf{Z}$, then

$$\begin{aligned}
[a] &= \{x \in \mathbf{Z} : \ x \ R \ a\} \\
&= \{x \in \mathbf{Z} : \ x + 3a \text{ is even}\} \\
&= \{x \in \mathbf{Z} : \ x + 3(2k) \text{ is even}\} \\
&= \{x \in \mathbf{Z} : \ x + 6k \text{ is even}\}
\end{aligned}$$

is also the set of even integers.

Equivalence Relations

On the other hand, the equivalence class consisting of those integers related to 1 is

$$\begin{aligned}
[1] &= \{x \in \mathbf{Z} : \ x \ R \ 1\} \\
&= \{x \in \mathbf{Z} : \ x + 3 \cdot 1 \text{ is even}\} \\
&= \{x \in \mathbf{Z} : \ x + 3 \text{ is even}\} \\
&= \{\pm 1, \pm 3, \pm 5, \ldots\},
\end{aligned}$$

which is the set of odd integers.

Equivalence Relations

In fact, if a is an odd integer, then $a = 2\ell + 1$ for some integer ℓ and

$$\begin{aligned}[a] &= \{x \in \mathbf{Z} : \ x + 3a \text{ is even}\} \\ &= \{x \in \mathbf{Z} : \ x + 3(2\ell + 1) \text{ is even}\} \\ &= \{x \in \mathbf{Z} : \ x + 6\ell + 3 \text{ is even}\}\end{aligned}$$

is the set of odd integers. Therefore, if a and b are even, then $[a] = [b]$ is the set of even integers; while if a and b are odd, then $[a] = [b]$ is the set of odd integers. Hence, there are only two distinct equivalence classes, namely [0] and [1], the sets of even and odd integers, respectively. We will soon see that there is a good reason for this observation.

Example 3

Result Let $S = \{k\sqrt{2} : \ k \in \mathbf{Z}\}$. The relation R defined on S by $x \ R \ y$ if $xy \in \mathbf{Z}$ is an equivalence relation.

Proof. First, observe that if x and y are any two elements of S, then $x = k\sqrt{2}$ and $y = \ell\sqrt{2}$ for integers k and ℓ. Furthermore,

$$xy = (k\sqrt{2})(\ell\sqrt{2}) = 2k\ell.$$

Since $2k\ell \in \mathbf{Z}$, it follows that $x \ R \ y$. Hence, R is reflexive, symmetric and transitive and so R is an equivalence relation. □

Properties of Equivalence Classes

Theorem

Let R be an equivalence relation on a nonempty set A and let a and b be elements of A. Then $[a] = [b]$ if and only if $a \; R \; b$.

Proof. Assume that $a \; R \; b$. We show that the sets $[a]$ and $[b]$ are equal by verifying that $[a] \subseteq [b]$ and $[b] \subseteq [a]$. First, we show that $[a] \subseteq [b]$. Let $x \in [a]$. Then $x \; R \; a$. Since $a \; R \; b$ and R is transitive, $x \; R \; b$. Therefore, $x \in [b]$ and so $[a] \subseteq [b]$. Next, let $y \in [b]$. Thus, $y \; R \; b$. Since $a \; R \; b$ and R is symmetric, $b \; R \; a$. Again, by the transitivity of R, we have $y \; R \; a$. Therefore, $y \in [a]$ and so $[b] \subseteq [a]$. Hence, $[a] = [b]$.

For the converse, assume that $[a] = [b]$. Because R is reflexive, $a \in [a]$. But, since $[a] = [b]$, it follows that $a \in [b]$. Consequently, $a \; R \; b$. □

Properties of Equivalence Classes

Corollary

Let R be an equivalence relation on a nonempty set A and let a and b be elements of A. If $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$.

Corollary

Let R be an equivalence relation on a nonempty set A and let a and b be elements of A. Then $a \not R\ b$ if and only if $[a] \cap [b] = \emptyset$.

Properties of Equivalence Classes

Theorem

Let R be an equivalence relation defined on a nonempty set A. Then the set of distinct equivalence classes resulting from R is a partition of A.

Proof. Certainly, each equivalence class $[a]$ is nonempty since $a \in [a]$ and so each element of A belongs to at least one equivalence class. We show that every element of A belongs to exactly one equivalence class. If some element x of A belongs to two equivalence classes, say $[a]$ and $[b]$, then $[a] = [b]$. Hence, every element of A belongs to a unique equivalence class. □

Properties of Equivalence Classes

Example 4

Result A relation R is defined on $\mathbf{Z}$ by $x\ R\ y$ if $11x - 5y$ is even. Then R is an equivalence relation.

Proof. First, we show that R is reflexive. Let $a \in \mathbf{Z}$. Then

$$11a - 5a = 6a = 2(3a).$$

Since $3a$ is an integer, $11a - 5a$ is even. Thus, $a\ R\ a$ and R is reflexive.

Example 4 (continued)

Next we show that R is symmetric. Assume that $a\ R\ b$, where $a, b \in \mathbf{Z}$. Thus, $11a - 5b$ is even. Therefore,

$$11a - 5b = 2k, \text{ where } k \in \mathbf{Z}.$$

Observe that

$$\begin{aligned} 11b - 5a &= (11a - 5b) + (-16a + 16b) \\ &= 2k - 16a + 16b = 2(k - 8a + 8b). \end{aligned}$$

Since $k - 8a + 8b$ is an integer, $11b - 5a$ is even. Hence, $b\ R\ a$ and R is symmetric.

Example 4 (continued)

Finally, we show that R is transitive. Assume that $a\ R\ b$ and $b\ R\ c$. Hence, $11a - 5b$ and $11b - 5c$ are even. Therefore,

$$11a - 5b = 2k \text{ and } 11b - 5c = 2\ell, \text{ where } k, \ell \in \mathbf{Z}.$$

Adding these equations, we obtain

$$(11a - 5b) + (11b - 5c) = 2k + 2\ell.$$

Solving for $11a - 5c$, we have

$$11a - 5c = 2k + 2\ell - 6b = 2(k + \ell - 3b).$$

Since $k + \ell - 3b$ is an integer, $11a - 5c$ is even. Hence, $a\ R\ c$ and R is transitive. Therefore, R is an equivalence relation. □

Properties of Equivalence Classes

We now determine the equivalence classes for the equivalence relation just discussed. Let's begin with the equivalence class containing 0, say. Then

$$\begin{aligned}
[0] &= \{x \in \mathbf{Z} : \ x \ R \ 0\} \\
&= \{x \in \mathbf{Z} : \ 11x \text{ is even}\} \\
&= \{x \in \mathbf{Z} : \ x \text{ is even}\} \\
&= \{0, \pm 2, \pm 4, \ldots\}.
\end{aligned}$$

Properties of Equivalence Classes

Recall that the distinct equivalence classes always produce a partition of the set involved (in this case $\mathbf{Z}$). Since the class [0] does not consist of all integers, there is at least one other equivalence class. To determine another equivalence class, we look for an element that does not belong to [0]. Since $1 \notin [0]$, the equivalence class [1] is distinct (and disjoint) from [0]. Thus,

$$\begin{aligned}
[1] &= \{x \in \mathbf{Z} : \ x \ R \ 1\} \\
&= \{x \in \mathbf{Z} : \ 11x - 5 \text{ is even}\} \\
&= \{x \in \mathbf{Z} : \ x \text{ is odd}\} \\
&= \{\pm 1, \pm 3, \pm 5, \ldots\}.
\end{aligned}$$

Since [0] and [1] produce a partition of $\mathbf{Z}$ (that is, every integer belongs to exactly one of [0] and [1]), these are the only equivalence classes in this case.

Congruence Modulo n

Definition

Recall for integers a and b, where $a \neq 0$, the integer a is said to **divide** b, written as $a \mid b$, if there exists an integer c such that $b = ac$. Also, for integers a, b and $n \geq 2$, a is said to be **congruent to** b **modulo** n**,** written $a \equiv b \pmod{n}$, if $n \mid (a - b)$.

$24 \equiv 6 \pmod{9}$ since $9 \mid (24 - 6)$
$1 \equiv 5 \pmod{2}$ since $2 \mid (1 - 5)$
$4 \equiv 4 \pmod{5}$ since $5 \mid (4 - 4)$
$8 \not\equiv 2 \pmod{4}$ since $4 \nmid (8 - 2)$.

Congruence Modulo n

Theorem

Let $n \in \mathbf{Z}$, where $n \geq 2$. Then congruence modulo n (that is, the relation R defined on $\mathbf{Z}$ by $a \; R \; b$ if $a \equiv b \pmod{n}$) is an equivalence relation on $\mathbf{Z}$.

Proof. Let $a \in \mathbf{Z}$. Since $n \mid 0$, it follows that $n \mid (a - a)$ and so $a \equiv a \pmod{n}$. Thus, $a \; R \; a$, implying that R is reflexive.
Next, we show that R is symmetric. Assume that $a \; R \; b$, where $a, b \in \mathbf{Z}$. Since $a \; R \; b$, it follows that $a \equiv b \pmod{n}$ and so $n \mid (a - b)$. Hence, there exists $k \in \mathbf{Z}$ such that $a - b = nk$. Thus,

$$b - a = -(a - b) = -(nk) = n(-k).$$

Since $-k \in \mathbf{Z}$, it follows that $n \mid (b - a)$ and so $b \equiv a \pmod{n}$. Therefore, $b \; R \; a$ and R is symmetric.

Theorem (continued)

Finally, we show that R is transitive. Assume that $a\ R\ b$ and $b\ R\ c$, where $a, b, c \in \mathbf{Z}$. We show that $a\ R\ c$. Since $a\ R\ b$ and $b\ R\ c$, it follows that that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Thus, $n \mid (a - b)$ and $n \mid (b - c)$. Consequently,

$$a - b = nk \quad \text{and} \quad b - c = n\ell \tag{1}$$

for some integers k and ℓ. Adding the equations in (1), we obtain

$$(a - b) + (b - c) = nk + n\ell = n(k + \ell);$$

so $a - c = n(k + \ell)$. Since $k + \ell \in \mathbf{Z}$, we have $n \mid (a - c)$ and so $a \equiv c \pmod{n}$. Therefore, $a\ R\ c$ and R is transitive. □

Congruence Modulo n

In general, for $n \geq 2$, the equivalence relation of congruence modulo n results in n distinct equivalence classes. In other words, if we define $a \; R \; b$ by $a \equiv b \pmod{n}$, then there are n distinct equivalence classes: $[0], [1], \ldots, [n-1]$.

Congruence Modulo n Equivalence Classes

For an integer r with $0 \leq r < n$, an integer m belongs to the set $[r]$ if and only if there is an integer q (the quotient) such that $m = nq + r$ by the Division Algorithm. The equivalence class $[r]$ consists of all integers having a remainder of r when divided by n.

Example 5

Result Let R be the relation defined on $\mathbf{Z}$ by

$$a \; R \; b \text{ if } 2a + b \equiv 0 \pmod 3.$$

Then R is an equivalence relation.

Proof. Let $x \in \mathbf{Z}$. Since $3 \mid 3x$, it follows that $3x \equiv 0 \pmod 3$. So,

$$2x + x \equiv 0 \pmod 3.$$

Thus, $x \; R \; x$ and R is reflexive.

Example 5 (continued)

Next we verify that R is symmetric. Assume that $x \; R \; y$, where $x, y \in \mathbf{Z}$. Thus, $2x + y \equiv 0 \pmod 3$ and so $3 \mid (2x + y)$. Therefore,

$$2x + y = 3r \text{ for some integer } r.$$

Hence, $y = 3r - 2x$. So

$$2y + x = 2(3r - 2x) + x = 6r - 3x = 3(2r - x).$$

Since $2r - x$ is an integer, $3 \mid (2y + x)$. So,

$$2y + x \equiv 0 \pmod 3.$$

Therefore, $y \; R \; x$ and R is symmetric.

Example 5 (continued)

Finally, we show that R is transitive. Assume that $x \ R \ y$ and $y \ R \ z$, where $x, y, z \in \mathbf{Z}$. Then

$$2x + y \equiv 0 \pmod 3 \text{ and } 2y + z \equiv 0 \pmod 3.$$

Thus, $3 \mid (2x + y)$ and $3 \mid (2y + z)$. From this, it follows that

$$2x + y = 3r \text{ and } 2y + z = 3s \text{ for some integers } r \text{ and } s.$$

Example 5 (continued)

Adding these two equations, we obtain

$$2x + 3y + z = 3r + 3s;$$

so

$$2x + z = 3r + 3s - 3y = 3(r + s - y).$$

Since $r + s - y$ is an integer, $3|(2x + z)$; so

$$2x + z \equiv 0 \pmod 3.$$

Hence, $x\ R\ z$ and R is transitive. □

The Integers Modulo n

We have already seen that for each integer $n \geq 2$, the relation R defined on $\mathbf{Z}$ by $a \; R \; b$ if $a \equiv b \pmod{n}$ is an equivalence relation.

Furthermore, this equivalence relation results in the n distinct equivalence classes

$$[0], [1], \ldots, [n-1].$$

Definition

We denote the set of these equivalence classes by $\mathbf{Z}_n$ and refer to this set as the **integers modulo** n.

Definition

Thus, $\mathbf{Z}_3 = \{[0], [1], [2]\}$ and, in general,

$$\mathbf{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

Hence, each element $[r]$ of $\mathbf{Z}_n$, where $0 \leq r < n$, is a set that contains infinitely many integers; indeed, as we have noted, $[r]$ consists of all those integers having the remainder r when divided by n.

For this reason, the elements of $\mathbf{Z}_n$ are sometimes called **residue classes.**

The Integers Modulo n

Just as addition and multiplication are defined in $\mathbf{Z}$, these two operations are defined in $\mathbf{Z}_n$ as well. Regardless of how one might define addition and multiplication in $\mathbf{Z}_n$, we would certainly expect that the sum and product of two elements of $\mathbf{Z}_n$ is also an element of $\mathbf{Z}_n$. There appears to be a natural definition of addition and multiplication in $\mathbf{Z}_n$; namely, for two equivalence classes $[a]$ and $[b]$ in $\mathbf{Z}_n$, we define

$$[a] + [b] = [a + b] \quad \text{and} \quad [a] \cdot [b] = [ab].$$

Let's suppose that we are considering $\mathbf{Z}_6$, for example, where then

$$\mathbf{Z}_6 = \{[0], [1], \ldots, [5]\}.$$

From the definitions of addition and multiplication that we just gave,

$$[1] + [3] = [1 + 3] = [4] \text{ and } [1] \cdot [3] = [1 \cdot 3] = [3].$$

This certainly seems harmless enough but let's consider adding and multiplying two other equivalence classes, say [2] and [3].

Again, according to the definitions $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$,

$$[2] + [3] = [2 + 3] = [5] \text{ and } [2] \cdot [3] = [2 \cdot 3] = [6].$$

However, we have been expressing the elements of $\mathbf{Z}_6$ by $[0], [1], [2], [3], [4]$ and $[5]$ and we don't explicitly see $[2 \cdot 3] = [6]$ among these elements. Since $6 \equiv 0 \pmod 6$, it follows that $6 \in [0]$, that is, $[6] = [0]$.

Also, the remainder is 0 when 6 is divided by 6 and so $[6] = [0]$. Therefore, $[2] \cdot [3] = [0]$. By similar reasoning,

$$[3] + [5] = [2] \text{ and } [3] \cdot [5] = [3].$$

The Integers Modulo n

This is a complete addition table for $\mathbf{Z}_6$.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

The Integers Modulo n

This is a complete multiplication table for $\mathbf{Z}_6$.

$\cdot$	[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]