for each integer n. We can evaluate the equivalence classes $[0]$, $[1]$, and $[2]$ as follows:

$$[0] = \{3k : k \in \mathbb{Z}\} = \{\dots,-9,-6,-3,0,3,6,9,\dots\}$$

$$[1] = \{3k+1 : k \in \mathbb{Z}\} = \{\dots,-8,-5,-2,1,4,7,10,\dots\}$$

$$[2] = \{3k+2 : k \in \mathbb{Z}\} = \{\dots,-7,-4,-1,2,5,8,11,\dots\}.$$

The partition $\mathbb{Z}/\!\sim$ is $\{[n] : n \in \mathbb{Z}\} = \{[0],[1],[2]\}$ (see Exercise 4 of this section) and is illustrated in our next figure:

$$\mathbb{Z} = \begin{array}{|c|c|c|} \hline \vdots & \vdots & \vdots \\ 6 & 7 & 8 \\ 3 & 4 & 5 \\ 0 & 1 & 2 \\ -3 & -2 & -1 \\ -6 & -5 & -4 \\ \vdots & \vdots & \vdots \\ \hline \multicolumn{1}{c}{\uparrow} & \multicolumn{1}{c}{\uparrow} & \multicolumn{1}{c}{\uparrow} \\ \multicolumn{1}{c}{[0]} & \multicolumn{1}{c}{[1]} & \multicolumn{1}{c}{[2]} \end{array}$$

Exercises 7.2

1. Let $\mathbb{R}^* = \{x \in \mathbb{R} : x \neq 0\}$ and define $x \sim y$ if and only if $x \cdot y > 0$, for $x, y \in \mathbb{R}^*$. Prove that $\sim$ is an equivalence relation on $\mathbb{R}^*$ and then identify the equivalence classes of $\sim$.

2. Let $\mathbb{R}^* = \{x \in \mathbb{R} : x \neq 0\}$ and let $\sim$ be the relation on $\mathbb{R}^*$ defined by $x \sim y$ if and only if $x \cdot y^{-1} \in \mathbb{Q}$. Prove that $\sim$ is an equivalence relation on $\mathbb{R}^*$.

3. Let $\mathbb{R}^* = \{x \in \mathbb{R} : x \neq 0\}$ and let $\sim$ be the equivalence relation on $\mathbb{R}^*$ defined by $x \sim y$ if and only if $x \cdot y^{-1} \in \{1,-1\}$. Identify the equivalence classes of $\sim$.

4. Let $\sim$ be the equivalence relation on $\mathbb{Z}$ defined by $m \sim n$ if and only if $3 \mid (m-n)$. Using the division algorithm (see Theorem 4.6.9), show that for every integer i we have that either $i \sim 0$, $i \sim 1$, or $i \sim 2$. Conclude that $[i] = [0]$, $[i] = [1]$, or $[i] = [2]$ for every integer i.

5. Let $\sim$ be the equivalence relation on $\mathbb{Z}$ defined by $m \sim n$ if and only if $3 \mid (m-n)$. From Exercise 4 we know that one of the equations $[i] = [0]$, $[i] = [1]$, $[i] = [2]$ is true for every integer i. Determine which of these equations is true for each of the integers $i = 4, 5, 6, -7$.

6. Let $f : A \to B$ be a function. Define a relation $\sim$ on A by $x \sim y$ if and only if $f(x) = f(y)$ for all $x, y \in A$. Prove that $\sim$ is an equivalence relation on A. Let $a \in A$ be given. Describe the equivalence class $[a]$.

7. Define the equivalence relation $\sim$ $\mathbb{R}$ by $x \sim y$ if and only if $\sin(x) = \sin(y)$. Describe the equivalence classes $[0]$ and $[\frac{\pi}{2}]$.

8. Let $\sim$ be an equivalence relation on a set A and let $a, b, c \in A$. Prove each of the following statements directly from the definition of an equivalence relation and the definition of an equivalence class (that is, do not use the theorems presented in this section).

(a) $a \in [a]$.
(b) if $b \in [a]$, then $a \sim b$.
(c) if $b \sim c$ and $a \in [b]$, then $c \sim a$.
(d) if $b \sim a$ and $[b] = [c]$, then $[a] = [c]$.

9. Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by $(a,b) \sim (c,d)$ iff $a + d = b + c$. Prove that $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$. List five elements in $[(3,1)]$.

10. Let $\sim$ be the relation on $\mathbb{R}$ defined by $x \sim y$ if and only if $x - y \in \mathbb{Q}$. Prove that $\sim$ is an equivalence relation on $\mathbb{R}$. Identify the equivalence classes $[0]$ and $[\sqrt{2}]$.

11. Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by $(a,b) \sim (c,d)$ iff $ad = bc$.

(a) Prove that $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.
(b) Describe the equivalence classes $[(1,1)]$ and $[(1,2)]$.

12. Let $\mathbb{Q}^* = \{x \in \mathbb{Q} : x \neq 0\}$. Define the relation $\sim$ on $\mathbb{Q}^*$ by $x \sim y$ if and only if $x \cdot y^{-1} \in \mathbb{Z}$. Show that $\sim$ is not an equivalence relation on $\mathbb{Q}^*$.

7.3 Congruence Modulo *m*

Karl Friedrich Gauss (1777–1855) has been called the "Prince of Mathematicians" for his many contributions to pure and applied mathematics. One of Gauss's most important contributions to number theory was the introduction of an equivalence relation on the integers called congruence modulo m, where $m \geq 1$ is an integer. We will explore Gauss's congruence relation and show that the operations of addition, subtraction, and multiplication preserve Gauss's relation (see Theorem 7.3.5).

Definition 7.3.1 (Congruence modulo *m*). Let $m \geq 1$ be an integer. For integers a and b, we define $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$.

When $a \equiv b \pmod{m}$ we say that a is **congruent** to b **modulo** m. We also write $a \not\equiv b \pmod{m}$, when we wish to say that a is **not** congruent to b modulo m. Here are some more examples of this notation:

- $10 \equiv 2 \pmod{4}$ because $4 \mid (10 - 2)$,
- $-5 \equiv 3 \pmod{4}$ since $4 \mid (-5 - 3)$,
- $24 \equiv 0 \pmod{4}$ as $4 \mid (24 - 0)$,
- $3 \not\equiv 1 \pmod{4}$ because $4 \nmid (3 - 1)$.