

1 Integers

Copyright © 2026, Gregory G. Smith
Last Updated: 2026-09-18

The set of integers is the prototype for all rings. As a prelude to ring theory, we develop the basic properties of integers.

1.0 Equivalence Relations

What does it mean for two objects to be the same? In mathematics, the concept of an equivalence relation on a set provides the answer.

Let $\mathcal{X}$ be a set. The *Cartesian product* $\mathcal{X} \times \mathcal{X}$ consists of all ordered pairs (x, y) where $x \in \mathcal{X}$ and $y \in \mathcal{X}$. A *binary relation* on $\mathcal{X}$ is a subset $\mathcal{R} \subseteq \mathcal{X} \times \mathcal{X}$. One kind of relation is especially interesting.

1.0.0 Definition. An *equivalence relation* is a binary relation $\mathcal{R}$ on a set $\mathcal{X}$ that has the following three properties.

(*Reflexive*) For all $x \in \mathcal{X}$, the pair (x, x) is in $\mathcal{R}$.

(*Symmetric*) For all $(x, y) \in \mathcal{R}$, the pair (y, x) is in $\mathcal{R}$.

(*Transitive*) For all $(x, y), (y, z) \in \mathcal{R}$, the pair (x, z) is in $\mathcal{R}$.

Given equivalence relation $\mathcal{R}$, we often write $(x, y) \in \mathcal{R}$ as $x \sim y$.

1.0.1 Problem. Let $\mathcal{X}$ be a set. Confirm that the subset $\mathcal{R} := \mathcal{X} \times \mathcal{X}$ is an equivalence relation.

Solution. As the relation $\mathcal{R} := \mathcal{X} \times \mathcal{X}$ contains all pairs, reflexivity, symmetry, and transitivity follow immediately. $\square$

1.0.2 Problem. Let $\mathcal{X}$ be a set. Verify that the diagonal subset

$$\mathcal{R} := \{(x, y) \in \mathcal{X} \times \mathcal{X} \mid x = y\}$$

is an equivalence relation.

Solution. Since $x = x$ for all $x \in \mathcal{X}$, reflexivity follows. Symmetry and transitivity follow from the same properties for equality. $\square$

1.0.3 Problem. Fix $m, n \in \mathbb{N}$. The $(m \times n)$ -matrices $\mathbf{A}$ and $\mathbf{B}$ are *row equivalent* if there is an invertible $(m \times m)$ -matrix $\mathbf{U}$ such that $\mathbf{A} = \mathbf{U}\mathbf{B}$. Show that being row equivalent is an equivalence relation.

Solution. For any matrix $\mathbf{A}$, we have $\mathbf{A} = \mathbf{I}\mathbf{A}$. As the identity matrix $\mathbf{I}$ is invertible, being row equivalent is a reflexive relation.

Suppose that the matrices $\mathbf{A}$ and $\mathbf{B}$ are row equivalent. There exists an invertible matrix $\mathbf{U}$ such that $\mathbf{A} = \mathbf{U}\mathbf{B}$. Since $\mathbf{B} = \mathbf{U}^{-1}\mathbf{A}$ and $\mathbf{U}^{-1}$ is invertible, being row equivalent is a symmetric relation.

Suppose that the matrices $\mathbf{A}$ and $\mathbf{B}$ are row equivalent, and the matrices $\mathbf{B}$ and $\mathbf{C}$ are row equivalent. There are invertible matrices $\mathbf{U}$ and $\mathbf{V}$ such that $\mathbf{A} = \mathbf{U}\mathbf{B}$ and $\mathbf{B} = \mathbf{V}\mathbf{C}$. Since $\mathbf{A} = (\mathbf{U}\mathbf{V})\mathbf{C}$ and $\mathbf{U}\mathbf{V}$ is invertible, being row equivalent is a transitive relation. $\square$

A binary relation may satisfy any two of the defining properties for an equivalence relation but fail to satisfy the third.

1.0.4 Remark. The ‘less-than-or-equal’ relation $\leq$ on the set $\mathbb{N}$ is not an equivalence relation. It is reflexive and transitive, but not symmetric. For instance, we have $2 \leq 3$ and $3 \not\leq 2$.

The English word ‘integer’ comes from the Latin *integer* meaning untouched. This word was first used as a noun in 1571; see T. Digges, *A geometrical practise, named Pantometria*, (1571).

The history of equivalence in mathematics is long and complicated; see A. Asghari, *Equivalence: an attempt at a history of the idea*, *Synthese* 196 (2019) 4657–4677.

Equality of elements is the prototype. In fact, equality is the only relation that is reflexive, symmetric, and antisymmetric.

The largest equivalence relation with the smallest quotient.

The smallest equivalence relation with the largest quotient.

In linear algebra, one proves that $\mathbf{A}$ and $\mathbf{B}$ are row equivalent if and only if they have the same row space.

The binary relation $\{(\mathbf{u}, \mathbf{v}) \in \mathbb{R} \times \mathbb{R} = \mathbb{R}^2 \mid \|\mathbf{u} - \mathbf{v}\| \leq 1\}$ is reflexive and symmetric, but not transitive; we have $\|(0, 0) - (1, 0)\| = 1 \leq 1$, $\|(1, 0) - (1, 1)\| = 1 \leq 1$, and $\|(0, 0) - (1, 1)\| = \sqrt{2} > 1$.

The empty binary relation $\emptyset$ on a set $\mathcal{X}$ is vacuously symmetric and transitive. It is not reflexive unless $\mathcal{X} = \emptyset$.

1.0.5 Definition. Let $\sim$ be an equivalence relation on a set $\mathcal{X}$. For all $x \in \mathcal{X}$, the set $[x] := \{w \in \mathcal{X} \mid x \sim w\}$ is its *equivalence class*.

1.0.6 Remark. For the largest binary relation $\mathcal{R} := \mathcal{X} \times \mathcal{X}$, there is a unique equivalence class: $[x] = \mathcal{X}$ for all $x \in \mathcal{X}$.

1.0.7 Remark. For the diagonal $\mathcal{R} := \{(x, y) \in \mathcal{X} \times \mathcal{X} \mid x = y\}$, each equivalence class is a singleton: $[x] = \{x\}$ for all $x \in \mathcal{X}$.

1.0.8 Remark. Given a matrix $\mathbf{A}$, the equivalence class $[\mathbf{A}]$ under ‘being row equivalent’ consists of all matrices that have the same reduced row echelon form as $\mathbf{A}$.

1.0.9 Proposition. Fix an equivalence relation on the set $\mathcal{X}$. The set $\mathcal{P}$ of equivalence classes enjoys the following three properties.

(nonempty) The family $\mathcal{P}$ does not contain the empty set: $\emptyset \notin \mathcal{P}$.

(cover) The union of all equivalence classes is $\mathcal{X}$: $\bigcup_{\mathcal{A} \in \mathcal{P}} \mathcal{A} = \mathcal{X}$.

(disjoint) The intersection of distinct equivalence classes is empty: for all members $\mathcal{A}$ and $\mathcal{B}$ of the family $\mathcal{P}$, the relation $\mathcal{A} \neq \mathcal{B}$ implies that $\mathcal{A} \cap \mathcal{B} = \emptyset$.

In other words, the equivalence classes form a partition of the set $\mathcal{X}$.

Proof. For all $x \in \mathcal{X}$, reflexivity means $x \sim x$, so $x \in [x]$. It follows that the empty set is not an equivalence class and the union of the equivalence classes equals $\mathcal{X}$. For all $x, y \in \mathcal{X}$, symmetry ensures that $y \in [x]$ implies that $x \in [y]$. For all $x, y, z \in \mathcal{X}$, transitivity asserts that $y \in [x]$ and $z \in [y]$ implies that $z \in [x]$. We deduce that any two equivalence classes are either equal or disjoint. $\square$

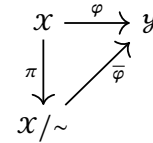
1.0.10 Definition. Given an equivalence relation $\sim$ on a set $\mathcal{X}$, the *quotient* $\mathcal{X}/\sim$ is the set of equivalence classes. The *canonical map* $\pi: \mathcal{X} \rightarrow \mathcal{X}/\sim$ is defined by $\pi(x) := [x]$ for all $x \in \mathcal{X}$. By construction, the canonical map $\pi: \mathcal{X} \rightarrow \mathcal{X}/\sim$ is surjective.

A map $\varphi: \mathcal{X} \rightarrow \mathcal{Y}$ determines a *well-defined* map $\bar{\varphi}: \mathcal{X}/\sim \rightarrow \mathcal{Y}$ if, for all $x, y \in \mathcal{X}$, $[x] = [y]$ implies that $\varphi(x) = \varphi(y)$. In other words, the output of the map φ does not depend on the choice of representatives.

1.0.11 Remark. When $\mathcal{X}$ is the set of all $(m \times n)$ -matrices and the equivalence relation $\sim$ is ‘being row equivalent’, the quotient $\mathcal{X}/\sim$ is the set of all $(m \times n)$ -matrices that are in reduced row echelon form. The rank of a matrix determines a well-defined map $\mathcal{X}/\sim \rightarrow \mathbb{N}$.

A *partition* of a set is a grouping of its elements into nonempty subsets, in such a way that every element is included in exactly one subset.

When $\varphi: \mathcal{X} \rightarrow \mathcal{Y}$ is well-defined, we have $\varphi = \bar{\varphi} \circ \pi$. We visualize this property via the commutative diagram:



1.1 Negative Integers

How do we construct the set $\mathbb{Z}$ of integers from the set $\mathbb{N}$? Except for zero, nonnegative integers do not have additive inverses. The integers address this deficiency by enlarging the set of numbers.

To construct the set $\mathbb{Z}$, each element or integer is represented by a pair of nonnegative integers. However, some pairs represent the same integer. To formalize this idea, we introduce a binary relation on pairs of nonnegative integers.

1.1.0 Definition. For all pairs $(m_1, m_2), (n_1, n_2) \in \mathbb{N}^2 := \mathbb{N} \times \mathbb{N}$, the binary relation $(m_1, m_2) \simeq (n_1, n_2)$ is defined by $m_1 + n_2 = m_2 + n_1$.

1.1.1 Lemma. The binary relation $\simeq$ on $\mathbb{N}^2$ is an equivalence relation.

Proof. For all (m_1, m_2) in $\mathbb{N}^2$, observe that $m_1 + m_2 = m_2 + m_1$, so $(m_1, m_2) \simeq (m_1, m_2)$ and the binary relation $\simeq$ is reflexive.

Suppose that $(m_1, m_2) \simeq (n_1, n_2)$. As $m_1 + n_2 = m_2 + n_1$, we see that $m_2 + n_1 = m_1 + n_2$, so $(n_1, n_2) \simeq (m_1, m_2)$ and $\simeq$ is symmetric.

Suppose that $(k_1, k_2) \simeq (m_1, m_2)$ and $(m_1, m_2) \simeq (n_1, n_2)$. Since $k_1 + m_2 = k_2 + m_1$ and $m_1 + n_2 = m_2 + n_1$, it follows that

$$\begin{aligned} (k_1 + n_2) + (m_1 + m_2) &= (k_1 + m_2) + (m_1 + n_2) \\ &= (k_2 + m_1) + (m_2 + n_1) \\ &= (k_2 + n_1) + (m_1 + m_2) \end{aligned}$$

and $k_1 + n_2 = k_2 + n_1$, so $(k_1, k_2) \simeq (n_1, n_2)$ and $\simeq$ is transitive. $\square$

1.1.2 Definition. The set $\mathbb{Z}$ of integers is the set of all equivalence classes in $\mathbb{N}^2$ under the equivalence relation $\simeq$.

The equivalence class in $\mathbb{Z} := (\mathbb{N}^2) / \simeq$ can be visualized as the nonnegative integral points on lines with slope 1 in the real plane; see Figure 1.1. By choosing the smallest nonnegative integral point on each line, we obtain

$$(m_1, m_2) \simeq \begin{cases} (k, 0) & \text{if } m_1 \geq m_2 \text{ and } m_1 = m_2 + k, \\ (0, k) & \text{if } m_1 < m_2 \text{ and } m_2 = m_1 + k. \end{cases}$$

Hence, $\{(k, 0) \mid k \in \mathbb{N}\} \cup \{(0, k+1) \mid k \in \mathbb{N}\}$ is a complete set of representatives for the equivalence classes—it contains exactly one representative for each class. The traditional notation is $k := (k, 0)$ and $-(k+1) := (0, k+1)$ for all $k \in \mathbb{N}$.

The operations on the set $\mathbb{Z}$ may be defined via representatives. For all $(m_1, m_2), (n_1, n_2) \in \mathbb{N}^2$, we declare that

$$\begin{aligned} (m_1, m_2) + (n_1, n_2) &:= (m_1 + n_1, m_2 + n_2) \\ (m_1, m_2)(n_1, n_2) &:= (m_1 n_1 + m_2 n_2, m_1 n_2 + m_2 n_1). \end{aligned}$$

To ensure that these operations are well-defined, we need to check that they do not depend on the choice of representatives. Consider $(j_1, j_2), (k_1, k_2), (m_1, m_2), (n_1, n_2) \in \mathbb{N}^2$ where $(j_1, j_2) \simeq (m_1, m_2)$ and $(k_1, k_2) \simeq (n_1, n_2)$. Commutativity and associativity for addition in the set $\mathbb{N}$ of nonnegative integers give

$$\begin{aligned} (j_1 + k_1) + (m_2 + n_2) &= (j_1 + m_2) + (k_1 + n_2) \\ &= (j_2 + m_1) + (k_2 + n_1) = (m_1 + n_1) + (j_2 + k_2) \end{aligned}$$

Negative numbers appear in Chapter 8 of *The Nine Chapters on the Mathematical Art* (~200 BCE). In contrast, ancient Greek mathematicians including **Diophantus** (~200–284) regarded negative integers as “absurd”. Nevertheless, negative integers are developed in the Indian text *Brāhma-sphuṭa-siddhānta* (628).

Informally, the pair $(m_1, m_2) \in \mathbb{N}^2$ represents the difference $m_1 - m_2$, and $(m_1, m_2) \simeq (n_1, n_2)$ if and only if $m_1 - m_2 = n_1 - n_2$.

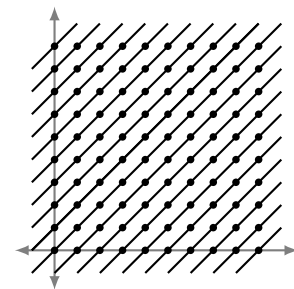


Figure 1.1: The equivalence classes in $\mathbb{N}^2$ visualized as lines

so $(j_1, j_2) + (k_1, k_2) \simeq (m_1, m_2) + (n_1, n_2)$. Since commutativity and associativity for addition in the set $\mathbb{N}$ also give

$$\begin{aligned} & ((j_1 k_1 + j_2 k_2) + (m_1 n_2 + m_2 n_1)) + (m_2 k_1 + m_1 k_2 + m_1 k_1 + m_2 k_2) \\ &= (j_1 + m_2) k_1 + (j_2 + m_1) k_2 + m_1 (k_1 + n_2) + m_2 (k_2 + n_1) \\ &= (j_2 + m_1) k_1 + (j_1 + m_2) k_2 + m_1 (k_2 + n_1) + m_2 (k_1 + n_2) \\ &= ((m_1 n_1 + m_2 n_2) + (j_2 k_1 + j_1 k_2)) + (m_1 k_1 + m_2 k_2 + m_1 k_2 + m_2 k_1), \end{aligned}$$

cancelling the trailing mixed terms yields

$$(j_1 k_1 + j_2 k_2) + (m_1 n_2 + m_2 n_1) = (m_1 n_1 + m_2 n_2) + (j_2 k_1 + j_1 k_2),$$

so $(j_1, j_2)(k_1, k_2) \simeq (m_1, m_2)(n_1, n_2)$. Therefore, both addition and multiplication are well-defined operations on the set $\mathbb{Z}$.

Having introduced the two key operations on integers, we verify that they have the expected properties.

1.1.3 Theorem. For all $k, m, n \in \mathbb{Z}$, we have

(associativity of addition)	$(k + m) + n = k + (m + n)$
(commutativity of addition)	$m + n = n + m$
(distributivity)	$k(m + n) = k m + k n$
(associativity of multiplication)	$k(m n) = (k m) n$
(commutativity of multiplication)	$m n = n m$

Sketch of proof. One verifies these properties by direct computation with representatives using the relevant properties for addition and multiplication on the set $\mathbb{N}$. For example, choose representatives in $\mathbb{N}^2$ so that $k = [(k_1, k_2)]$, $m = [(m_1, m_2)]$ and $n = [(n_1, n_2)]$. The definition of addition in $\mathbb{Z}$ and the associativity of addition in $\mathbb{N}$ give

$$\begin{aligned} (k + m) + n &= ([[(k_1, k_2)] + [(m_1, m_2)]] + [(n_1, n_2)]) \\ &= [(k_1 + m_1, k_2 + m_2)] + [(n_1, n_2)] \\ &= [((k_1 + m_1) + n_1, (k_2 + m_2) + n_2)] \\ &= [(k_1 + (m_1 + n_1), k_2 + (m_2 + n_2))] \\ &= [(k_1, k_2)] + [(m_1 + n_1, m_2 + n_2)] \\ &= [(k_1, k_2)] + ([[(m_1, m_2)] + [(n_1, n_2)])] = k + (m + n). \quad \square \end{aligned}$$

1.1.4 Corollary. Every integer k has the additive inverse $(-1)k$.

Proof. Consider the integer k represented by the pair $(k_1, k_2) \in \mathbb{N}^2$. By definition, the product $(-1)k$ is represented by

$$(0, 1)(k_1, k_2) = ((0)k_1 + (1)k_2, (0)k_2 + (1)k_1) = (k_2, k_1)$$

and the sum $k + (-1)k$ is represented by

$$(k_1, k_2) + (k_2, k_1) = (k_1 + k_2, k_1 + k_2) \simeq (0, 0).$$

We conclude that $k + (-1)k = 0$. □

1.1.5 Remark. Composing the injective map $\eta: \mathbb{N} \rightarrow \mathbb{N}^2$ defined by $\eta(n) := (n, 0)$ for all $n \in \mathbb{N}$ with the canonical map $\pi: \mathbb{N}^2 \rightarrow \mathbb{Z}$ produces an injective map $\pi \circ \eta: \mathbb{N} \rightarrow \mathbb{Z}$. For all $m, n \in \mathbb{N}$, we have

$$\begin{aligned} [\eta(m + n)] &= [(m + n, 0)] = [(m, 0)] + [(n, 0)] = [\eta(m)] + [\eta(n)], \\ [\eta(m n)] &= [(m n, 0)] = [(m, 0)] [(n, 0)] = [\eta(m)] [\eta(n)]. \end{aligned}$$

Thus, the map $\pi \circ \eta$ is compatible with addition and multiplication. Using this composite map, we identify $\mathbb{N}$ with a subset of $\mathbb{Z}$.

The use of the letter “Z” to denote the set of integers comes from the German word ‘Zahlen’ (“number”) and has been attributed to [David Hilbert](#). Nevertheless, the earliest known use of this notation in a textbook occurs in *Algèbre* written by [Nicolas Bourbaki](#) and dating to 1947.

1.2 Division with Remainder

What is the division operation on integers? In its most basic form, division undoes multiplication.

1.2.0 Definition. For all $m, n \in \mathbb{Z}$, we say ‘ n divides m ’, ‘ n is a divisor of m ’, or ‘ m is a multiple of n ’ if there exists $k \in \mathbb{Z}$ such that $m = kn$.

1.2.1 Lemma. Let $m, n \in \mathbb{Z}$. When $m \neq 0$ and n divides m , we have $|n| \leq |m|$.

Proof. Since n divides m , there exists $k \in \mathbb{Z}$ such that $m = kn$. Both k and n are nonzero because m is nonzero. It follows that $|k| \geq 1$ and $|m| = |k| |n| \geq |n|$. $\square$

Even when an integer is not a multiple of another integer, there is a valuable division operation. Euclidean division or division with remainder is the process of dividing one integer, called the *dividend*, by another, called the *divisor*, that produces an integer *quotient* and a nonnegative integer *remainder* that is less than the absolute value of the divisor.

1.2.2 Theorem. Let $0 \neq n \in \mathbb{Z}$. For all $m \in \mathbb{Z}$, there exists unique $q, r \in \mathbb{Z}$ such that $m = qn + r$ and $0 \leq r < |n|$.

Proof. As $(-q)(-n) + r = qn + r$ and $|n| = |-n|$, we may assume that $n > 0$. Consider the subset

$$\mathcal{X} := \{m - kn \mid m - kn \geq 0 \text{ for some } k \in \mathbb{Z}\} \subseteq \mathbb{N}.$$

When $m \geq 0$, we have $m = m - 0(n) \in \mathcal{X}$. When $m < 0$, we have $m(1 - n) = m - mn \in \mathcal{X}$ because $1 - n \leq 0$. As $\mathcal{X}$ is nonempty, the well-ordering of the set $\mathbb{N}$ establishes that the set $\mathcal{X}$ contains a least element r . Hence, there exists $q \in \mathbb{Z}$ such that $r = m - qn$ is the smallest nonnegative integer of the form $m - kn$. By construction, we have $m = qn + r$ and $r \geq 0$. It remains to show that $r < n$ and to prove that q and r are the unique integers with these properties.

Suppose that $r \geq n$. We would have

$$0 \leq r - n = (m - qn) - n = m - (q + 1)n.$$

However, this would imply that $r - n \in \mathcal{X}$, which contradicts the choice of r as the least element in $\mathcal{X}$. Thus, we deduce that $r < n$.

Consider integer pairs (q, r) and (q', r') such that $m = qn + r$, $0 \leq r < n$, $m = q'n + r'$, and $0 \leq r' < n$. The inequalities ensure that $|r' - r| < n$ and the equalities show that $(q - q')n = r' - r$. Assuming $r' - r \neq 0$, the integer n would divide $r' - r$ and Lemma 1.2.1 would show that $|r' - r| \geq |n|$. However, this would produce the contradiction $|n| \leq |r' - r| < n$. Hence, we deduce that $r' - r = 0$. Since $n \neq 0$, it also follows that $q - q' = 0$. $\square$

1.2.3 Notation. In many programming languages, the remainder operator is denoted by $r = m \% n$. In a few programming languages, the quotient operator is denoted by $q = m // n$ or $q = \lfloor m/n \rfloor$. In particular, we have $m = (m // n)n + (m \% n)$.

Every integer divides 0 whereas 0 is a divisor of only 0.

The absolute value function $|\cdot| : \mathbb{Z} \rightarrow \mathbb{N}$ is defined, for all $m \in \mathbb{Z}$, by

$$|m| := \begin{cases} m & \text{if } m \geq 0, \\ -m & \text{if } m < 0. \end{cases}$$

Only division by repeated subtraction appears in Euclid’s *Elements* [Book VII, Proposition 1]. In contemporary pseudo-code, this algorithm is

Input: $m, n \in \mathbb{N}$ with $n \neq 0$.
Output: $q, r \in \mathbb{N}$ such that $m = qn + r$ and $0 \leq r < n$.
Set $(q, r) := (0, m)$;
While $r \geq n$ do
 Set $(q, r) := (q + 1, r - n)$;
Return (q, r) .

1.2.4 Remark. Long division finds both the quotient and remainder;

$$\begin{array}{r} 19 \\ 4 \overline{)79} \\ \underline{4} \\ 39 \\ \underline{36} \\ 3 \end{array} \qquad \begin{array}{r} 15 \\ 5803 \overline{)88278} \\ \underline{5803} \\ 30248 \\ \underline{29015} \\ 1233 \end{array}$$

so $79 = (19)(4) + 3$ and $88278 = (15)(5803) + 1233$.

1.2.5 Definition. For all $m, n \in \mathbb{Z}$, a *greatest common divisor* of m and n is a nonnegative integer $d := \gcd(m, n)$ such that d divides both m and n , and any integer that divides both m and n also divides d .

1.2.6 Lemma. For all $0 \neq m \in \mathbb{Z}$, we have $\gcd(m, 0) = |m|$.

Proof. As $|m|$ divides m and $|m|$ divides 0, we see that $|m|$ is a common divisor of m and 0. Moreover, any common divisor of m and 0 clearly divides $|m|$, so $\gcd(m, 0) = |m|$. $\square$

Greatest common divisors have another interpretation.

1.2.7 Theorem (Bézout identity). For all $m, n \in \mathbb{Z}$, there exist $j, k \in \mathbb{Z}$ such that $\gcd(m, n) = jm + kn$. When m and n are not both 0, the greatest common divisor $\gcd(m, n)$ is the smallest positive integer linear combination of m and n .

Proof. When $m = n = 0$, we have $\gcd(m, n) = \gcd(0, 0) = 0$ and $0 = (0)m + (0)n$, so we may assume that m and n are not both zero. Consider $\mathcal{X} := \{jm + kn \in \mathbb{N} \mid j \in \mathbb{Z}, k \in \mathbb{Z}, \text{ and } jm + kn > 0\}$. As $(m)m + (n)n = m^2 + n^2 > 0$, we see that $\mathcal{X}$ is nonempty. Thus, the well-ordering of the set $\mathbb{N}$ implies that $\mathcal{X}$ has a unique least element d . We claim that $d = \gcd(m, n)$.

We first establish that d is a common divisor of m and n . When $m = 0$, the positive integer d divides 0. When $m \neq 0$, division with remainder establishes that there exists unique $q, r \in \mathbb{Z}$ such that $m = qd + r$ and $0 \leq r < d$. Since

$$r = m - qd = m - q(jm + kn) = (1 - qj)m + (-qk)n$$

and $r < d$, the defining property of d implies that $r = 0$, so d divides m . By symmetry, we also conclude that d divides n .

It remains to prove that every common divisor also divides d . Suppose that the integer e divides both m and n . There are integers u and v such that $m = ue$ and $n = ve$. We obtain

$$d = jm + kn = jue + kve = (ju + kv)e,$$

which establishes that e divides d . $\square$

The second requirement states that every common divisor k of m and n must divide d . Since Lemma 1.2.1 implies that $|k| \leq |d|$, we see that d is the ‘greatest’ common divisor.

Because every integer divides 0, there is no greatest common divisor of 0 and 0. For consistency with Lemma 1.2.6 and Theorem 1.2.7, we declare that $\gcd(0, 0) = 0$.

The history of the equation $jm + kn = \gcd(m, n)$ is more complicated and interesting than one might guess; see [Andrew Granville’s](#) preprint: [It is not “Bézout’s identity”](#).

1.4 Exercises

1.4.1 Problem. Determine which of the following statements are true. If a statement is false, provide a counterexample and, if possible, salvage it by modifying the statement so that it becomes true.

- i. Every binary relations that is reflexive and transitive is an equivalence relations.
- ii. Every equivalence relations is reflexive and transitive.
- iii. The equality relations on a set is the finest equivalence relation on that set.
- iv. Any two equivalence classes are either disjoint or equal.
- v. Every partition of a set arises from some equivalence relation.
- vi. If a binary relation has the property that every element is related to at least one element, then it is reflexive.
- vii. For all $k \in \mathbb{N}$ and all $(m, n) \in \mathbb{N}^2$, we have $(m, n) \simeq (m + k, n + k)$.
- viii. Every integer has infinitely many distinct representations in $\mathbb{N}^2$.
- ix. In division with remainder, the remainder r is allowed to be negative as long as $|r| < |n|$.
- x. When $m = 0$ and $n \neq 0$, the quotient $m // n$ is 0 and the remainder $m \% n$ is 0.
- xi. The remainder of m upon division by n is the unique integer closed to rational number m/n .
- xii. The last nonzero remainder produced by the Euclidean algorithm is the greatest common divisor.
- xiii. Replacing the pair (m, n) by $(n, m - n)$ preserves the greatest common divisor.
- xiv. The sequence of quotients in the Euclidean algorithm is unique.
- xv. For all $m, n \in \mathbb{Z}$, we have $\gcd(m, n) = \gcd(|m|, |n|)$.
- xvi. If $jm + kn = 1$ for some $j, k \in \mathbb{Z}$, then $\gcd(m, n) = 1$.

1.4.2 Problem. Given a function $\varphi: \mathcal{X} \rightarrow \mathcal{Y}$, show that ‘having the same image’ under φ defines an equivalence relation on $\mathcal{X}$.

1.4.3 Problem. Define a binary relation on the set $\mathbb{R}$ of real numbers as follows: for all $x, y \in \mathbb{R}$, we say $x \sim y$ if there exists $k \in \mathbb{Z}$ such that $x - y = 2k\pi$. Verify that this is an equivalence relation. Describe the set of equivalence classes. Are addition and multiplication well-defined on the quotient set $\mathbb{R}/\sim$?

1.4.4 Problem. The canonical total ordering $\leq$ on the integers $\mathbb{Z}$ is defined as follows. For all $m, n \in \mathbb{Z}$, we declare that $m \leq n$ or $n \geq m$ if $n - m$ is a nonnegative integer.

- i. For all $m \in \mathbb{Z}$, demonstrate that $m \leq m$.
- ii. When $k \leq m$ and $m \leq n$, establish that $k \leq n$.
- iii. When $m \leq n$ and $n \leq m$, verify that $m = n$.
- iv. For all $m, n \in \mathbb{Z}$, show that $m \leq n$ or $m \geq n$.

1.4.5 Problem. Let k, m , and n be integers.

- i. When $m \leq n$, demonstrate that $m + k \leq n + k$.
- ii. When $k > 0$ and $m \leq n$, establish that $km \leq kn$.
- iii. When $k < 0$ and $m \leq n$, establish that $km \geq kn$.

1.4.6 Problem. The *absolute value* function $|\cdot|: \mathbb{Z} \rightarrow \mathbb{N}$ is defined, for any integer m , by

$$|m| := \begin{cases} m & \text{if } m \geq 0, \\ -m & \text{if } m < 0. \end{cases}$$

- i. Let $n \in \mathbb{N}$. For all $m \in \mathbb{Z}$, prove that $-n \leq m \leq n$ if and only if $|m| \leq n$.
- ii. For all $m, n \in \mathbb{Z}$, show that $||n| - |m|| \leq |n + m| \leq |n| + |m|$.

1.4.7 Problem. Let k, m , and n be integers.

- i. Prove that $\gcd(km, kn) = |k| \gcd(m, n)$.
- ii. Prove that $\gcd(k, \gcd(m, n)) = \gcd(\gcd(k, m), n)$.

1.4.8 Problem. For all $m, n \in \mathbb{Z}$, a nonnegative integer $\ell := \text{lcm}(m, n)$ is a *least common multiple* of m and n if

(*common*) the integer ℓ is a multiple of both m and n , and

(*least*) any integer that is a multiple of m and n is also a multiple of ℓ .

For all positive integers m and n , prove that

$$\gcd(m, n) \text{lcm}(m, n) = mn.$$

1.4.9 Problem. Let k, m , and n be integers such that $m \neq 0$ or $n \neq 0$.

- i. Prove that $mx + ny = k$ has an integer solution if and only if k is a multiple of $\gcd(m, n)$.
- ii. Given an integer solution (x_0, y_0) to $mx + ny = k$, prove that all solutions have the form

$$x = x_0 + j \frac{\text{lcm}(m, n)}{m} \qquad y = y_0 - j \frac{\text{lcm}(m, n)}{n}$$

for some integer j .