1 Integers

Last Updated: 18 January 2023

The set of integers is the prototype for all rings. The word 'integer' comes from the Latin *integer* meaning untouched: the prefix "in" means 'not' and the root "tangere" means 'to touch'. This word was first used as a noun in 1571 by Thomas Digges (1546?–1595).

1.0 Negative Integers

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

How can we construct the set $\mathbb{Z}$ of integers from the set $\mathbb{N}$ of nonnegative integers? Except for zero, the additive inverse of a nonnegative integer is not a nonnegative integer. The integers address this deficiency by enlarging the set of numbers.

To construct the set $\mathbb{Z}$, we represent each integer by a pair (m_1, m_2) or nonnegative integers. However, some pairs represent the same integer. To formalize this idea, we introduce a relation on pairs of nonnegative integers.

Informally, the pair $(m_1, m_2) \in \mathbb{N} \times \mathbb{N}$ represents the difference $m_1 - m_2$.

Definition 1.0.0. Two pairs (m_1, m_2) and (n_1, n_2) of nonnegative integers satisfy $(m_1, m_2) \simeq (n_1, n_2)$ if $m_1 + n_2 = m_2 + n_1$.

Observe that $(m_1, m_2) \simeq (n_1, n_2)$ if and only if $m_1 + n_2 = m_2 + n_1$ or $m_1 - m_2 = n_1 - n_2$.

Lemma 1.0.1. *The binary relation $\simeq$ has the following three properties.*
Reflexivity: *For any pair (m_1, m_2) of nonnegative integers, we have $(m_1, m_2) \simeq (m_1, m_2)$.*
Symmetry: *For any two pairs (m_1, m_2) and (n_1, n_2) in $\mathbb{N} \times \mathbb{N}$, the relation $(m_1, m_2) \simeq (n_1, n_2)$ implies that $(n_1, n_2) \simeq (m_1, m_2)$.*
Transitivity: *For any three pairs (k_1, k_2), (m_1, m_2), and (n_1, n_2) in $\mathbb{N} \times \mathbb{N}$, the two relations $(k_1, k_2) \simeq (m_1, m_2)$ and $(m_1, m_2) \simeq (n_1, n_2)$ imply that $(k_1, k_2) \simeq (n_1, n_2)$.*

Proof.
Reflexivity: For any pair (m_1, m_2) in $\mathbb{N} \times \mathbb{N}$, we tautologically have $m_1 + m_2 = m_1 + m_2$, so $(m_1, m_2) \simeq (m_1, m_2)$.

Equality is reflexive.

Symmetry: For any two pairs (m_1, m_2) and (n_1, n_2) in $\mathbb{N} \times \mathbb{N}$, the relation $(m_1, m_2) \simeq (n_1, n_2)$ is equivalent to $m_1 + n_2 = m_2 + n_1$. It follows that $m_2 + n_1 = m_1 + n_2$, so $(n_1, n_2) \simeq (m_1, m_2)$.

Equality is symmetric.

Transitivity: For any three pairs (k_1, k_2), (m_1, m_2), and (n_1, n_2) in $\mathbb{N} \times \mathbb{N}$, the two relations $(k_1, k_2) \simeq (m_1, m_2)$ and $(m_1, m_2) \simeq (n_1, n_2)$ are equivalent to $k_1 + m_2 = k_2 + m_1$ and $m_1 + n_2 = m_2 + n_1$. Combining commutativity and associativity of addition with the cancellation law, we see that

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

implies that $k_1 + n_2 = k_2 + n_1$, so $(k_1, k_2) \simeq (n_1, n_2)$. □

Definition 1.0.2. The *set $\mathbb{Z}$ of integers* is the set of all equivalence classes in $\mathbb{N} \times \mathbb{N}$ under the relation $\simeq$.

The equivalence class in $\mathbb{Z} := (\mathbb{N} \times \mathbb{N}) / \simeq$ 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

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

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

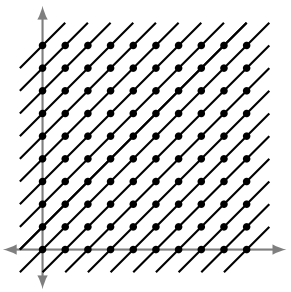

Figure 1.1: The equivalence classes in $\mathbb{N} \times \mathbb{N}$ as lines

The operations of addition and multiplication on the set $\mathbb{Z}$ of integers may be defined in terms of representatives. For any pairs (m_1, m_2) and (n_1, n_2) in $\mathbb{N} \times \mathbb{N}$, we declare that

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

However, we need to check that these operations do not depend on the choice of representatives. Consider four pairs (j_1, j_2), (k_1, k_2), (m_1, m_2), (n_1, n_2) in $\mathbb{N} \times \mathbb{N}$ such that $(j_1, j_2) \simeq (k_1, k_2)$ and $(m_1, m_2) \simeq (n_1, n_2)$. Commutativity and associativity for addition of nonnegative integers give

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

so $(j_1, j_2) + (m_1, n_1) \sim (k_1, k_2) + (n_1, n_2)$. Since commutativity and associativity for addition of nonnegative integers also give

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

cancelling the trailing mixed terms yields

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

so $(j_1, j_2)(m_1, m_2) \simeq (k_1, k_2)(n_1, n_2)$. It follows that addition and multiplication on $\mathbb{Z}$ is well-defined.

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

Theorem 1.0.3. *For any integers k, m, and n, we have*

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

Sketch of proof. One verifies these properties by direct computation with representatives using the relevant properties for addition and multiplication on the set $\mathbb{N}$. □

Corollary 1.0.4. *Every integer k has the additive inverse $(-1)\,k$.*

Proof. Suppose that the integer k is represented by the pair (m, n) of nonnegative integers. By definition, the product $(-1)\,k$ is represented by $(0,1)(m,n) = \big((0)m + (1)n, (0)n + (1)m\big) = (n,m)$ and the sum $k + (-1)k$ is represented by

$$(m,n) + (n,m) = (m+n, m+n) \simeq (0,0)$$

We conclude that $k + (-1)k = 0$. □

Remark 1.0.5. The map $\eta\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ defined, for any nonnegative integer n, by $\eta(n) := (n,0)$ gives rise to an injective map $\overline{\eta}\colon \mathbb{N} \to \mathbb{Z}$. Moreover, for any nonnegative integers m and n, we have

$$\eta(m+n) = (m+n, 0) = (m,0) + (n,0)\,,$$
$$\eta(m\,n) = (m\,n, 0) = (m,0)(n,0)\,.$$

Thus, the map $\overline{\eta}$ is compatible with addition and multiplication.

Exercises

Problem 1.0.6. The canonical ordering $\leqslant$ on the integers $\mathbb{Z}$ is defined as follows. For any two integers m and n, we declare that $m \leqslant n$ or $n \geqslant m$ if $n - m$ is a nonnegative integer.

(i) For any integer m, demonstrate that $m \leqslant m$.
(ii) When $k \leqslant m$ and $m \leqslant n$, establish that $k \leqslant n$.
(iii) When $m \leqslant n$ and $n \leqslant m$, verify that $m = n$.
(iv) For any two integers m and n, show that $m \leqslant n$ or $m \geqslant n$.

Problem 1.0.7. Let k, m, and n be integers.

(i) When $m \leqslant n$, demonstrate that $m + k \leqslant n + k$.
(ii) When $k > 0$ and $m \leqslant n$, establish that $k\,m \leqslant k\,n$.
(iii) When $k < 0$ and $m \leqslant n$, establish that $k\,m \geqslant k\,n$.

Problem 1.0.8. The *absolute value* function $|\bullet| : \mathbb{Z} \to \mathbb{N}$ is defined, for any integer m, by

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

(i) Let n be a nonnegative integer. For any integer m, prove that $-n \leqslant m \leqslant n$ if and only if $|m| \leqslant n$.
(ii) For any two integers m and n, show that

$$\big||n| - |m|\big| \leqslant |n+m| \leqslant |n| + |m|\ .$$

1.1 Division with Remainder

What is the division operation on integers? We start with the simplest case.

Definition 1.1.0. Let m and n be two integers. We say 'm *divides* n', 'm is a *divisor* of n', or 'n is *a multiple* of m' if there exists an integer k such that $n = km$.

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

Lemma 1.1.1. *Let m and n be integers with $n \neq 0$. When m divides n, we have $|m| \leqslant |n|$.*

Proof. As m divides n, there exists an integer k such that $n = km$. Both k and m are nonzero because n is nonzero. It follows that $|k| \geqslant 1$ and $|n| = |k|\,|m| \geqslant |m|$. □

Even when one integer fails to divide another, there exists a valuable division operation. Specifically, division with remainder (also known as Euclidean division) 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" strictly smaller than the absolute value of the divisor.

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

```
input:  m, n ∈ ℕ with n ≠ 0.
output: q, r ∈ ℕ such that
        m = q n + r and 0 ⩽ r < n.
Set (q, r) := (0, m);
While r ⩾ n do
   (q, r) = (q + 1, r − n);
Return (q, r).
```

Theorem 1.1.2. *Let n be a nonzero integer. For any integer m, there exists unique integers q and r such that $m = q\,n + r$ and $0 \leqslant r < |n|$.*

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

$$\mathcal{X} := \{m - k\,n \mid \text{there exists } k \in \mathbb{Z} \text{ such that } m - k\,n \geqslant 0\} \subseteq \mathbb{N}\,.$$

When $m \geqslant 0$, we have $m = m - 0(n) \in \mathcal{X}$. When $m < 0$, we have $m(1 - n) = m - m\,n \in \mathcal{X}$ because $1 - n \leqslant 0$. Since $\mathcal{X}$ is nonempty, the Well-Ordering Principle establishes that $\mathcal{X}$ contains a least element r. Hence, there exists an integer q such that $r = m - q\,n$ is smallest nonnegative integer of the form $m - k\,n$. By construction, we have $m = q\,n + r$ and $r \geqslant 0$. It remains to show that $r < n$ and to prove that q and r are the unique integers with these properties.

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

$$0 \leqslant r - n = (m - q\,n) - n = m - (q + 1)n\,.$$

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 $m = q\,n + r$, $0 \leqslant r < n$, $m = q'\,n + r'$, and $0 \leqslant r' < n$. The inequalities ensure that $|r' - r| < n$ and the equations give $(q - q')n = r' - r$. Assuming $r' - r \neq 0$, the integer n would divide $r' - r$ and Lemma 1.1.1 would show that $|r' - r| \geqslant |n|$. However, this would produce the contradiction $|n| \leqslant |r' - r| < n$. Hence, we deduce that $r' - r = 0$. Since $n \neq 0$, it also follows that $q - q' = 0$. □

We illustrate division with remainder with a few small examples:

$$\begin{aligned} 79 &= 2(32) + 15 \\ 982 &= 1(867) + 115 \\ 88\,278 &= 15(5\,803) + 1\,233 \\ 979\,010 &= 135(7\,209) + 5\,795 \\ 2\,633\,864 &= 8(313\,629) + 124\,832 \end{aligned}$$

Notation 1.1.3. In many programming languages, the remainder operator (or modulo operator) is denoted by $r = m \,\%\, n$. In few programming languages, the quotient operator (or floor division) is denoted by $q = m \mathbin{//} n$. In particular, we have

$$m = (m \mathbin{//} n)n + (m \,\%\, n)\,.$$

Definition 1.1.4. For any two integers m and n, a nonnegative integer $d := \gcd(m, n)$ is a *greatest common divisor* of m and n if

- the integer d divides both m and n, and
- any integer that divides both m and n also divides d.

The second requirement states that every common divisor k of m and n must divide d. Since Lemma 1.1.1 implies that $|k| \leqslant |d|$, we see that d is the 'greatest' common divisor.

Lemma 1.1.5. *For any nonzero integer m, we have* $\gcd(m, 0) = m$.

Proof. Since 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 $\gcd(m, 0) = m$. □

Because every integer divides 0, there is no greatest common divisor of 0 and 0. For consistency with Lemma 1.1.5 and Theorem 1.1.7, we declare that $\gcd(0, 0) = 0$.

There is an extremely inefficient method for computing greatest common divisors.

Problem 1.1.6. Determine $\gcd(165, 105)$.

Proof. We can list all divisors:
$165 : -165, -55, -33, -15, -11, -5, -3, -1, 1, 3, 5, 11, \underline{15}, 33, 55, 165$,
$105 : -105, -35, -21, -15, -7, -5, -3, -1, 1, 3, 5, 7, \underline{15}, 21, 35, 105$.
The largest integer on both lists is 15, so $\gcd(165, 105) = 15$. □

The existence and uniqueness of a greatest common divisor follows from a similar argument. Construct the finite list of the divisors for each integer and take the largest element appearing on both lists.

Greatest common divisors have another interpretation.

Theorem 1.1.7. *For any two integers m and n, there exists integers j and k such that* $\gcd(m, n) = j\,m + k\,n$. *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 not both zero. Consider the subset

$$\mathcal{X} := \{j\,m + k\,n \mid j \in \mathbb{Z}, k \in \mathbb{Z}, \text{ and } j\,m + k\,n > 0\} \subset \mathbb{N}.$$

As $(m)m + (n)n = m^2 + n^2 > 0$, we see that $\mathcal{X}$ is nonempty. Thus, the Well-Ordering Principle establishes that $\mathcal{X}$ has a unique least element d. We claim that $d = \gcd(m, n)$.

We first demonstrate that d is common divisor of m and n. When $m = 0$, the positive integer d divides 0. When $m \neq 0$, Theorem 1.1.2 establishes that there are unique integers q and r such that $m = q\,d + r$ and $0 \leqslant r < d$. Since

$$r = m - q\,d = m - q(j\,m + k\,n) = (1 - q\,j)m + (-q\,k)n$$

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 show that every common divisor also divides d. Suppose that the integer e divides both m and n. There exists integers u and v such that $m = u\,e$ and $n = v\,e$. We obtain

$$d = j\,m + k\,n = j\,u\,e + k\,v\,e = (j\,u + k\,v)e,$$

which proves that e divides d. □

Corollary 1.1.8. *For any two integers m and n, we have* $\gcd(m, n) = 1$ *if and only if* 1 *is an integer linear combination of m and n.*

Proof.

⇒: Suppose that $\gcd(m, n) = 1$. The first part of Theorem 1.1.7 implies that 1 is an integer linear combination of m and n.

⇐: Suppose that 1 is an integer linear combination of m and n. Because 1 is the smallest positive integer, the second part of Theorem 1.1.7 implies that 1 is the greatest common divisor of m and n. □

Exercises

Problem 1.1.9. Let k, m, and n be integers.

(i) Prove that $\gcd(k\,m, k\,n) = |k|\,\gcd(m, n)$.

(ii) Prove that $\gcd\big(k, \gcd(m, n)\big) = \gcd\big(\gcd(k, m), n\big)$.

Problem 1.1.10. For any two integers m and n, a nonnegative integer $\ell := \operatorname{lcm}(m, n)$ is a *least common multiple* of m and n if

- the integer ℓ is a multiple of both m and n, and
- any integer that is a multiple of m and n is also a multiple of ℓ.

For any two positive integers m and n, prove that

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

Problem 1.1.11. Let k, m, and n be three integers such that $m \neq 0$ or $n \neq 0$.

(i) Demonstrate that the equation $m\,x + n\,y = k$ 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 $m\,x + n\,y = k$, prove that all solutions have the form

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

for some integer j.

1.2 Fundamental Theorem of Arithmetic

What are the atoms or minimal elements for the multiplicative structure of the integers? We begin with a comparative notion.

Definition 1.2.0. Two integers m and n are *coprime* or *relatively prime* if $\gcd(m, n) = 1$.

Corollary 1.2.1. *Let ℓ, m, and n be integers. When $\gcd(\ell, m) = 1$ and k divides the product $m\,n$, the number ℓ divides n.*

Proof. Theorem 1.1.7 shows that there exists integers j and k such that $j\,\ell + k\,m = 1$. Distributivity, together with associativity and commutativity for integer multiplication, give

$$n = (1)n = (j\,\ell + k\,m)n = (j\,n)\ell + (m\,n)k\,.$$

Since ℓ divides the product $m\,n$, there is an integer i such that $m\,n = i\,\ell$. It follows that

$$n = (j\,n)\ell + (m\,n)k = (j\,n)\ell + (i\,\ell)k = (j\,n + i\,k)\ell\,,$$

so ℓ divides n. □

Before examining a couple formulations of minimality, we use division with remainder to obtain a much better algorithm for computing greatest common divisors. In particular, this approach avoids factorization.

Theorem 1.2.2 (Euclidean Algorithm)**.**

```
input:  Two integers m and n.
output: The greatest common divisor of m and n.
Set j := |m|;
Set k := |n|;
While j ≠ 0 do
   Set r := j % k;
   Set j := k;
   Set k := r;
Return k.
```

Proof. We first claim that $\gcd(m, n) = \gcd(n, m \,\%\, n)$. Set $q := m \mathbin{//} n$ and $r := m \,\%\, n$. Theorem 1.1.2 establishes that $m = q\,n + r$ and $0 \leqslant r < |n|$. It is enough to prove that the pairs (m, n) and (q, r) have the same common divisors.

Let e be a common divisor of m and n. Hence, there exists integers u and v such that $m = u\,e$ and $n = v\,e$. It follows that

$$r = m - q\,n = u\,e - q\,v\,e = (u - q\,v)e\,,$$

so e divides r. As e already divides n, we see that e is a common divisor of n and e. Conversely, let ℓ be a common divisor of n and r. There exists integers s and t such that $n = s\,\ell$ and $r = t\,\ell$. It follows that $m = q\,n + r = q\,s\,\ell + t\,\ell = (q\,s + t)\ell$, so ℓ divides m. As ℓ already divides m, we see that ℓ is a common divisor of m and n.

Finally, each step in the while loop replaces the pair (j, k) with the pair $(k, j \,\%\, k)$. Our first claim shows that replacement does not change the greatest common divisor. The algorithm terminates because sequence of remainders is decreasing and goes to zero in less than n steps. □

Problem 1.2.3. Compute the greatest common divisor of 21 837 and 2 088.

Solution. Since the Euclidean algorithm gives

$$\begin{aligned} 21\,837 &= 10(2\,088) + 957\,, \\ 2\,088 &= 2(957) + 174\,, \\ 957 &= 5(174) + 87\,, \\ 174 &= 2(87) + 0\,. \end{aligned}$$

we see that $\gcd(21\,837, 2\,088) = 87$. □

Definition 1.2.4. An integer p is *irreducible* if $p \neq \pm 1$ and the only divisors of p are ± 1 and $\pm p$. A nonzero integer, except for ± 1, is *reducible* (or *composite*) if it is not irreducible.

Remark 1.2.5. The *Sieve of Eratosthenes* provides a straightforward way to generate the list of irreducible positive integers. List the integers from 2 to n. The smallest entry 2 is prime. Cross out the multiplies of 2 from our list. The smallest remaining entry 3 is prime because it is not divisible by any smaller prime. Cross out the multiples of 3. Repeat.

Using this method, Table 1.1 lists the 25 irreducible positive integers less than 100.

The Greek polymath, Eratosthenes of Cyrene (276BCE–194BCE), is famous for his work on prime numbers and for measuring the diameter of the earth.

	$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	$\boxed{7}$	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	

Table 1.1: Irreducible positive integers less than 100

We record a simple consequence of irreducibility.

Lemma 1.2.6. *Let p be an irreducible integer. For any integer m that is not a multiple of p, we have* $\gcd(p, m) = 1$.

Proof. Suppose that d is a common divisor of p and m. We see that $d = \pm 1$ or $d = \pm p$ because d divides p and p is irreducible. Since d also divides m and p is not a divisor of m, we deduce that $d = \pm 1$. As $\gcd(p, m) \geqslant 0$, we conclude that $d = 1$. □

Definition 1.2.7. A integer p is *prime* if $p \neq \pm 1$ and p dividing the product $m\,n$ of two integers m and n implies that p divides m or p divides n.

In mathematics, the word 'or' is not exclusive. The definition allows for the possibility that p may divide both m and n.

Warning 1.2.8. The definition for a prime is unconventional. Most references do *not* include 0 as a prime integer. However, this choice does align with the prevailing terminology for ideals.

The next result recovers the standard definition.

Proposition 1.2.9. *A nonzero integer p is prime if and only if it is irreducible.*

Proof. When $p = \pm 1$, then p is neither irreducible nor prime, so the assertion holds. We may, thereby, assume that p is an integer other than 0 or ± 1.

⇒: Suppose that the integer p is prime. Consider a divisor d of p. Hence, there exists an integer q such that $p = q\,d$. As $(1)p = q\,d$, the integer p divides the product $q\,d$. By definition, we see that p divides q or p divides d.

- When p divides d, Lemma 1.1.1 establishes that $|d| \leqslant |p|$ and $|p| \leqslant |d|$, so $|d| = |p|$ and $d = \pm p$.
- When p divides q, there exists an integer k such that $q = k\,p$. It follows that $p = q\,d = k\,d\,p$ and $(1 - k\,d)p = 0$. As $p \neq 0$, we deduce that $1 - k\,d = 0$. Since $k\,d = 1$, the integer d divides 1 which implies $d = \pm 1$.

Therefore, we conclude that either $d = \pm p$ or $d = \pm 1$ which shows that p is irreducible.

⇐: Suppose that the integer p is irreducible. Assume that p divides a product $m\,n$ of integers and p does not divide m.

Lemma 1.2.6 shows that $\gcd(p, m) = 1$ and Corollary 1.2.1 shows that p divides n. Therefore, p is prime. □

We end by establishing that every integer is a unique product of primes.

Theorem 1.2.10 (Fundamental Theorem of Arithmetic)**.** *Any integer m may be written as $m = u\,p_1\,p_2 \cdots p_r$ where $u = \pm 1$, each p_j is a nonnegative prime integer, and $r \geqslant 0$. Moreover, this factorization is unique up to reordering the factors.*

Proof. It is enough to prove the statement for integers m greater than 1, because the factor u incorporates signs and (by our conventions) 0 is a nonnegative prime.

Existence: Consider the subset

$$\mathcal{X} := \{n \in \mathbb{Z} | n > 1 \text{ and } n \text{ is not a product of finitely many primes}\}.$$

Suppose that $\mathcal{X}$ is nonempty. The Well-Ordering Principle would establish that $\mathcal{X}$ contains a unique least element n. Since $n \in \mathcal{X}$, it would not be a product of primes, so n would not be a prime itself. Hence, there would exist integers j and k such that $n = j\,k$, $1 < j < n$, and $1 < k < n$. As n is the smallest integer in $\mathcal{X}$, we would deduce that $k \notin \mathcal{X}$ and $j \notin \mathcal{X}$. It would follows that k and j do have factorizations into primes. However, the product of this factorizations would be a factorization of n into primes which contradicts $n \in \mathcal{X}$. We conclude that $\mathcal{X} = \varnothing$ and every integer greater than 1 is a product of finitely many primes.q

Uniqueness: Consider the subset

$$\mathcal{Y} := \{n \in \mathbb{Z} \mid \text{the factorization of } n \text{ into primes is not unique}\}.$$

Suppose that $\mathcal{Y}$ is nonempty. The Well-Ordering Principle would establish that $\mathcal{Y}$ contains a unique least element n. Write two distinct factorizations for n:

$$n = p_1\,p_2 \cdots p_r = q_1\,q_2 \cdots q_s$$

where all p_i and q_j are positive primes. Both r and s are integers greater than 0 because $n \neq 1$. We are assuming that these factorizations are *not* the same up to reordering.

From the equation, we see that p_1 divides the product $q_1\,q_2 \cdots q_s$. Since p_1 is irreducible, it must divide one of the q_j. After relabeling the factors q_j, we may assume that p_1 divides q_1. As q_1 is prime, its divisors are ± 1 and $\pm q_1$. Becase p_1 is positive prime, it is not equal to ± 1 or $-q_1$, so $p_1 = q_1$. By cancelling the factors, we obtain $p_2\,p_3 \cdots p_r = q_2\,q_3 \cdots q_s$. Since this product is less than n our choice of n implies that this second factorization is unique up to reordering the primes. Hence, we deduce that $r - 1 = s - 1$ and $q_j = p_j$ for all $2 \leqslant j \leqslant r$ (up to reordering). However, this establishes that the two factorizations for n do coincide, contradicting our assumption. We conclude that $\mathcal{Y} = \varnothing$ and the factorizations are unique. □