Chapter 2

Sets and Numbers

Topics :

1. Sets
2. Operations on sets
3. The integers and division

Almost all mathematical objects (even numbers !) can be defined in terms of sets. In any mathematical study, one considers a set or sets of certain objects; sets of numbers are quite common. The theory that results from the intuitive definition of a set – the so-called *naive* set theory – leads to *paradoxes* (i.e., logical inconsistencies). These logical inconsistencies can be avoided by building the *axiomatic* set theory. However, all the sets considered in this course can be treated consistently from the "naive" point of view.

2.1 Sets

We think of a *set* as a collection of objects; these objects are called the *elements* (or *members*) of the set. We DO NOT attempt to define the words **collection** or **object** (and hence the term **set**), but we assume that if we have a set S, then there is some "rule" that determines whether a given object x is a member of S. We say that *a set is completely determined by its elements.*

NOTE : Membership in a set is an all-or-nothing situation. We cannot have a set S and an object x that belongs only partially to S. A given object is either a member of a set or it is not.

If A is a set and x is an object that belongs to A, we write $x \in A$. If x is not an element of A, then we write $x \notin A$.

NOTE : It is important to know that a set itself may also be an element of some other set. Mathematics is full of examples of sets of sets. A *line*, for instance, is a set of *points*; the set of all lines in the *plane* is a natural example of a set of sets (of points).

A basic relation between sets is that of *containment* (or *subsethood*).

2.1.1 DEFINITION. Let A and B be sets. We say that A is a **subset** of B, written $A \subseteq B$, provided every element of A is also an element of B. Simbolically:

$$\boxed{A \subseteq B \iff \forall x, \text{ if } x \in A \text{ then } x \in B.}$$

The phrases "A is contained in B" and "B contains A" are alternative ways of saying that "A is a subset of B".

NOTE : (1) We see that $A \subseteq B$ if and only if the quantification

$$\forall x \, (x \in A \to x \in B)$$

is TRUE.

(2) It follows from the definition of a subset that a set A is *not* a subset of a set B, written $A \not\subseteq B$, if and only if there is at least one element of A that is not an element of B. Simbolically :

$$\boxed{A \not\subseteq B \iff \exists x \text{ such that } x \in A \text{ and } x \notin B.}$$

(3) When we wish to emphasize that a set A is a subset of B but that $A \neq B$, we write $A \subset B$ and say that A is a **proper subset** of B.

2.1.2 DEFINITION. Let A and B be sets. We say that the sets A and B are **equal**, written $A = B$, provided every element of A is in B and every element of B is in A. Symbolically :

$$\boxed{A = B \iff A \subseteq B \quad \text{and} \quad B \subseteq A.}$$

NOTE : (1) *Two sets are equal if and only if they have the same elements.* More formally, $A = B$ if and only if the quantification

$$\forall x \, (x \in A \leftrightarrow x \in B)$$

is TRUE.

(2) To know that a set A equals a set B, we must know that $A \subseteq B$ and we must also know that $B \subseteq A$.

There are several ways to describe sets.
(i) One way is to *list* all the elements of the set, when it is possible. We use a notation where all elements of the set are listed between braces.

2.1.3 EXAMPLE. The set V of all vowels in the English alphabet can be written as

$$V = \{a, \, e, \, i, \, o, \, u\}.$$

2.1.4 EXAMPLE. The sets $\{a, b, c\}$, $\{a, c, b\}$ and $\{a, a, b, c\}$ are equal, since they have exactly the same elements, namely the symbols a, b and c.

NOTE : It does not matter in what order we list the objects nor does it matter if we repeat an object. All that matters is what objects are members of the set and what objects are not.

The unique set that has no members is called the **empty set**, and is denoted by the symbol $\emptyset$.

NOTE : The symbol $\emptyset$ is *not* the same as the Greek letter phi : ϕ or Φ.

Observe that

$$\emptyset \in \{\emptyset\} \quad \text{and} \quad \emptyset \subseteq \{\emptyset\}, \quad \text{but} \quad \emptyset \notin \emptyset\,.$$

It is important to distinguish clearly between the concepts of *set membership* ($\in$) and *set containment* ($\subseteq$). The notation $x \in A$ means that x is an element (member) of A. The notation $A \subseteq B$ means that every element of A is an element of B. Thus $\emptyset \subseteq \{1,2,3\}$ is TRUE, but $\emptyset \in \{1,2,3\}$ is FALSE.

NOTE : The difference between $\in$ and $\subseteq$ is analogous to the difference between x and $\{x\}$. The symbol x refers to some object (a number or whatever), and the notation $\{x\}$ means the set whose one and only one element is the object x. It is always *correct* to write $x \in \{x\}$, but it is *incorrect* to write $x = \{x\}$ or $x \subseteq \{x\}$.

Uppercase letters are usually used to denote sets. We have special symbols to denote sets of *numbers* :

$\mathbb{N}$ denotes the set of *natural* numbers $\{0,1,2,3,\dots\}$;

$\mathbb{Z}$ denotes the set of *integers*;

$\mathbb{Q}$ denotes the set of *rational* numbers;

$\mathbb{R}$ denotes the set of *real* numbers.

We will occasionally use the notation $\mathbb{Z}^+$ to denote the set of *positive integers* $\{1,2,3,\dots\}$. A natural number may be referred to as a *non-negative integer*.

We have

$$\mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}\,.$$

There are two popular ways of thinking about the set $\mathbb{R}$ of *real numbers* :

- as a *geometric* object, with its *points* as positions on a straight line – the **real line**;
- as an *algebraic* object, with its elements as numbers (expressed as *decimal expansions*, where if a number is irrational we think of longer and longer decimal expansions approximating it more and more closely) – the **real number system**.

Each of these intuitive ideas can be made precise (and actually lead to ways of constructing the real numbers from the rational numbers).

NOTE : (1) Although sets are usually used to group together elements with common properties, there is nothing that prevents a set from having seemingly unrelated elements. For instance, $\{\alpha, \text{Paris}, \text{Mike}, 102\}$ is the set containing the elements α, Paris, Mike, and 102.

(2) Sometimes the brace notation is used to describe a set without listing *all* its elements: some elements are listed, and then *ellipses* $(\dots)$ are used when the general pattern of the elements is obvious. For instance, the set of positive integers less than 102 can be denoted by $\{1, 2, 3, \dots, 102\}$.

(*ii*) Whenever we are given a set S, we can use **set-builder notation** to describe a subset of S. The form of this notation is

$$\{\, \text{dummy variable} \in S \,|\, \text{conditions} \,\}.$$

This is the set of all objects drawn from the set S and subject to the conditions specified. For example, we could write

$$A = \{n \in \mathbb{N} \,|\, n \text{ is prime and } n < 15\}$$

which would be read "A equals the set of all n belonging to $\mathbb{N}$ *such that* n is prime and n is less than 15". Thus $\{n \in \mathbb{N} \,|\, n \text{ is prime and } n < 15\}$ describes the set $\{2, 3, 5, 7, 11, 13\}$.

NOTE : In set-builder notation $\{x \in S \,|\, \dots\}$ is always read "The set of *all* x belonging to S *such that* $\dots$".

We have notation for certain special subsets of $\mathbb{R}$. We agree as usual that among real numbers

$\boxed{a < b}$ means "a is (strictly) less than b" or "$b - a$ is positive"

$\boxed{a \leq b}$ means "a is less than or equal to b" or "$b - a$ is non-negative".

Note that for any $a \in \mathbb{R}$, $a \leq a$. Then we define the **intervals** :

$$\begin{aligned}
[a, b] &:= \{x \in \mathbb{R} \,|\, a \leq x \leq b\}\,; \\
(a, b) &:= \{x \in \mathbb{R} \,|\, a \leq x < b\}\,; \\
(a, b] &:= \{x \in \mathbb{R} \,|\, a < x \leq b\}\,; \\
(a, b) &:= \{x \in \mathbb{R} \,|\, a < x < b\}.
\end{aligned}$$

When $b < a$, the definitions imply that all these sets equal $\emptyset$; if $a = b$, then $[a, b] = \{a\} = \{b\}$ and the rest are empty. By convention, the *half-unbounded* intervals are written similarly : if $a, b \in \mathbb{R}$, then

$$\begin{aligned}
[a, \infty) &:= \{x \in \mathbb{R} \,|\, a \leq x\}\,; \\
(-\infty, b] &:= \{x \in \mathbb{R} \,|\, x \leq b\}\,; \\
(a, \infty) &:= \{x \in \mathbb{R} \,|\, a < x\}\,; \\
(-\infty, b) &:= \{x \in \mathbb{R} \,|\, x < b\}
\end{aligned}$$

by definition, without thereby allowing the symbols $-\infty$ or ∞ as "numbers".

2.1.5 Example. Let $a, b \in \mathbb{R}$ such that $0 < a \leq b$. Then

$$a \leq \sqrt{ab} \leq \frac{a+b}{2} \leq b$$

with equality if and only if $a = b$.

Solution : Let $0 < a \leq b$. We have to prove three inequalities :

(1) $\sqrt{ab} - a = \sqrt{a}\left(\sqrt{b} - \sqrt{a}\right) \geq 0 \;\Rightarrow a \leq \sqrt{ab}\,.$

(2) $\frac{a+b}{2} - \sqrt{ab} = \frac{1}{2}\left(a + b - 2\sqrt{a}\cdot\sqrt{b}\right) = \frac{1}{2}\left(\sqrt{a} - \sqrt{b}\right)^2 \geq 0 \;\Rightarrow\; \sqrt{ab} \leq \frac{a+b}{2}\,.$

(3) $b - \frac{a+b}{2} = \frac{1}{2}(b - a) \geq 0 \;\Rightarrow\; \frac{a+b}{2} \leq b.$

The expressions $\sqrt{ab}$ and $\frac{a+b}{2}$ are called the **geometric mean** and the **arithmetic mean** (of the positive real numbers a and b), respectively.

NOTE : Inequality (2) has an interesting geometrical interpretation : *Among all rectangles with prescribed perimeter, the square is the one with largest area* (if $a+b=p$, then $ab \leq \left(\frac{p}{2}\right)^2$).

2.1.6 EXAMPLE. Let $a, b \in \mathbb{R}$ such that $a+b \geq 0$. Then the following inequality holds

$$\left(\frac{a+b}{2}\right)^3 \leq \frac{a^3+b^3}{2}$$

with equality if and only if $a = \pm b$.

SOLUTION : We have

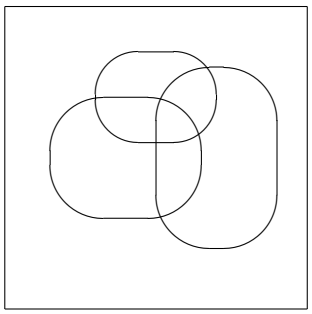
$$\begin{aligned}
\frac{a^3+b^3}{2} - \left(\frac{a+b}{2}\right)^3 &= \frac{1}{8}\left[4(a^3+b^3) - (a+b)^3\right] \\
&= \frac{1}{8}\left(4a^3+4b^3-a^3-b^3-3a^2b-3ab^2\right) \\
&= \frac{3}{8}\left(a^3-a^2b+b^3-ab^2\right) \\
&= \frac{3}{8}(a^2-b^2)(a-b) \\
&= \frac{3}{8}(a-b)^2(a+b) \geq 0
\end{aligned}$$

and hence

$$\left(\frac{a+b}{2}\right)^3 \leq \frac{a^3+b^3}{2}.$$

Clearly, we have equality if and only if $a-b=0$ or $a+b=0$; that is, $a = \pm b$.

(iii) Sets can also be represented graphically using **Venn diagrams**. In Venn diagrams the **universal set** $\mathcal{U}$, which contains all the objects under consideration, is represented by a rectangle. Inside this rectangle, circles or other geometrical figures are used to represent sets. Sometimes points are used to represent the particular elements of a set.



Venn diagram with three sets

Sets are used extensively in counting problems, and for such applications we need to discuss the "size" of sets.

2.1.7 Definition. Let S be a set. If there are exactly n distinct elements in S, where n is a natural number, we say that S is a **finite set** and that n is the **cardinality** of S. The cardinality of S is denoted by $|S|$.

2.1.8 Example. Let S be the set of letters in the English alphabet. Then $|S| = 26$.

2.1.9 Example. Since the empty set has no elements, it follows that $|\emptyset| = 0$.

2.1.10 Definition. A set is said to be **infinite** if it is not finite.

2.1.11 Example. The set $\mathbb{Z}^+$ of positive integers is infinite.

2.2 Operations on sets

Just as statements can be combined with logical connectives to produce new (compound) statements, and numbers can be added and multiplied to obtain new numbers, there are various operations we perform on sets. The most

basic set operations are *union* and *intersection*. Other operations are *difference*, *Cartesian product*, and *symmetric difference*; the latter is defined in the exercises.

It is safe to assume that all the sets under consideration are subsets of a fixed (large) *universal set* $\mathcal{U}$. Thus, for any set A,

$$\emptyset \subseteq A \subseteq \mathcal{U}.$$

2.2.1 DEFINITION. Let A and B be sets. The **union** of A and B, denoted by $A \cup B$, is the set of all objects that belong either to A or to B, or to both.

In set-builder notation,

$$\boxed{A \cup B := \{x \,|\, x \in A \text{ or } x \in B\}.}$$

2.2.2 EXAMPLE. What is the union of the sets $A = \{1, 2, 5\}$ and $B = \{1, 2, 4\}$?

SOLUTION : The union is $A \cup B = \{1, 2, 4, 5\}$.

2.2.3 DEFINITION. Let A and B be sets. The **intersection** of A and B, denoted by $A \cap B$, is the set of all objects that belong to both A and B.

In set-builder notation,

$$\boxed{A \cap B := \{x \,|\, x \in A \text{ and } x \in B\}.}$$

2.2.4 EXAMPLE. What is the intersection of the sets $A = \{1, 2, 5\}$ and $B = \{1, 2, 4\}$?

SOLUTION : The intersection is $A \cap B = \{1, 2\}$.

2.2.5 DEFINITION. Let A and B be sets. The **difference** of A and B, denoted by $A \setminus B$, is the set of all objects belonging to A, but not to B. The diference of A and B is also called the **complement of B relative to A**.

The complement of B relative to the universal set $\mathcal{U}$, denoted by B^c, is called the **complement** of B.

In set-builder notation,

$$\boxed{A \setminus B := \{x \,|\, x \in A \text{ and } x \notin B\}.}$$

It followes that

$$\emptyset^c = \mathcal{U} \quad \text{and} \quad \mathcal{U}^c = \emptyset.$$

Also, observe that (for any sets A and B)

$$A \setminus B = A \cap B^c.$$

2.2.6 Example. What is the difference of the sets $A = \{1, 2, 5\}$ and $B = \{1, 2, 4\}$?

Solution : The difference is $A \setminus B = \{5\}$. This is different from the difference $B \setminus A$, which is $\{4\}$.

We list now some important set identities. In this, A, B, and C are subsets of a universal set $\mathcal{U}$.

(1) $A \cap \mathcal{U} = A$ (identity) ;

(2) $A \cup \emptyset = A$ (identity) ;

(3) $A \cap \emptyset = \emptyset$ (domination) ;

(4) $A \cup \mathcal{U} = \mathcal{U}$ (domination) ;

(5) $(A^c)^c = A$ (complementation) ;

(6) $A \cap A = A$ (idempotency) ;

(7) $A \cup A = A$ (idempotency) ;

(8) $A \cap B = B \cap A$ (commutativity) ;

(9) $A \cup B = B \cup A$ (commutativity) ;

(10) $A \cap (B \cap C) = (A \cap B) \cap C$ (associativity) ;

(11) $A \cup (B \cup C) = (A \cup B) \cup C$ (associativity) ;

(12) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributivity) ;

(13) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributivity) ;

(14) $(A \cap B)^c = A^c \cup B^c$ (De Morgan's law) ;

(15) $(A \cup B)^c = A^c \cap B^c$ (De Morgan's law).

NOTE : There is a similarity between these set identities and the logical equivalences discussed in section **1.2**. In fact, the set identities given can be proved directly from the corresponding logical equivalences.

2.2.7 EXAMPLE. Prove that for any sets A and B

$$(A \cup B)^c = A^c \cap B^c.$$

SOLUTION : We have

$$x \in (A \cup B)^c \iff x \notin A \cup B \iff \neg(x \in A \cup B) \iff \neg(x \in A \vee x \in B) \iff$$

$$\neg(x \in A) \wedge \neg(x \in B) \iff x \notin A \wedge x \notin B \iff x \in A^c \wedge x \in B^c \iff x \in A^c \cap B^c.$$

Once a certain number of set properties have been established, new properties can be derived from them *algebraically*.

2.2.8 EXAMPLE. For all sets $A, B,$ and $C,$

$$(A \cup B) \setminus (C \setminus A) = A \cup (B \setminus C).$$

SOLUTION : We have

$$\begin{aligned}
(A \cup B) \setminus (C \setminus A) &= (A \cup B) \cap (C \setminus A)^c \\
&= (A \cup B) \cap (C \cap A^c)^c \\
&= (A \cup B) \cap ((A^c)^c \cup C^c) \\
&= (A \cup B) \cap (A \cup C^c) \\
&= A \cup (B \cap C^c) \\
&= A \cup (B \setminus C).
\end{aligned}$$

Set identities can also be proved using **membership tables**: we consider each combination of sets that an element can belong to and verify that elements in the same combinations of sets belong to both the sets in the identity; to indicate that an element *is* in an a set, the symbol **1** is used, whereas to indicate that an element is *not* in a set, the symbol **0** is used. (Note the similarity between the membership tables and truth tables; this is no coincidence !)

2.2.9 EXAMPLE. Use a membership table to show that (for all sets A, B, and C)

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

SOLUTION : The membership table is given below (it has eight rows).

A	B	C	$B \cap C$	$A \cup (B \cap C)$	$A \cup B$	$A \cup C$	$(A \cup B) \cap (A \cup C)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

It follows that the identity is valid.

Since the union and intersection of sets are associative operations, the sets $A \cup B \cup C$ and $A \cap B \cap C$ are well defined. We note that $A \cup B \cup C$ contains those objects that belong to at least one of the sets A, B, and C, and that $A \cap B \cap C$ contains those objects that belong to all of A, B, and C.

We can extend the union and intersection to n sets.

2.2.10 DEFINITION. Let $A_1, A_2, \ldots, A_n$ be a *collection* of sets. The **union** of A_1,

$A_2, \ldots, A_n$, denoted by $A_1 \cup A_2 \cup \cdots \cup A_n$, is the set that contains those elements that are members of at least one set in the collection.

In set-builder notation,

$$\boxed{A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i := \{x \,|\, \exists i \text{ such that } x \in A_i\}\,.}$$

2.2.11 DEFINITION. Let $A_1, A_2, \ldots, A_n$ be a *collection* of sets. The **intersection** of $A_1, A_2, \ldots, A_n$, denoted by $A_1 \cap A_2 \cap \cdots \cap A_n$, is the set that contains those elements that are members of all sets in the collection.

In set-builder notation,

$$\boxed{A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i := \{x \,|\, \forall i, \;\; x \in A_i\}\,.}$$

2.2.12 EXAMPLE. Let $A_i = \{i, i+1, i+2, \ldots\}, \quad i \in \{1, 2, \ldots, n\}$. Then

$$\bigcup_{i=1}^{n} A_i = \{1, 2, 3, \ldots\} \quad \text{and} \quad \bigcap_{i=1}^{n} A_i = \{n, n+1, n+2, \ldots\}.$$

2.2.13 DEFINITION. Let A and B be sets. The **Cartesian product** of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

In set-builder notation,

$$\boxed{A \times B := \{(a, b) \,|\, a \in A \text{ and } b \in B\}.}$$

2.2.14 EXAMPLE. What is the Cartesian product of the sets $A = \{1, 2, 3\}$ and $B = \{\alpha, \beta\}$?

SOLUTION : The Cartesian product is

$$A \times B = \{(1, \alpha), (1, \beta), (2, \alpha), (2, \beta), (3, \alpha), (3, \beta)\}.$$

NOTE : (1) The Cartesian products $A \times B$ and $B \times A$ are *not* equal, unless $A = \emptyset$ or $B = \emptyset$ (so that $A \times B = \emptyset$) or unless $A = B$.

(2) Since

$$(a, b) \in A \times B \quad \Longleftrightarrow \quad a \in A \text{ and } b \in B$$

we can use the Cartesian product set to describe the set of outcomes of performing one operation *and* then another. For example, an object has to be coloured by choosing one of the colours from the set $C = \{c_1, c_2, c_3\}$ and then numbered by choosing one of the numbers from the set $N = \{n_1, n_2\}$ then the set of all possible objects which result is represented by the set

$$C \times N = \{(c_i, n_j) \,|\, i \in \{1, 2, 3\},\ j \in \{1, 2\}\}.$$

The Cartesian product can easily be extended to n sets.

2.2.15 DEFINITION. Let $A_1, A_2, \ldots, A_n$ be sets. The **Cartesian product** of $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \cdots \times A_n$, is the set of all ordered n-**tuples** $(a_1, a_2, \ldots, a_n)$, where a_i belongs to A_i for $i \in \{1, 2, \ldots, n\}$.

In set-builder notation,

$$\boxed{A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i := \{(a_1, a_2, \ldots, a_n) \,|\, \forall i,\ \ a_i \in A_i\}\,.}$$

We write

$$A^2 := A \times A$$

and, in general,

$$A^n := \underbrace{A \times A \times \cdots \times A}_{n \text{ factors}}\,.$$

2.2.16 DEFINITION. Let S be a set. The **power set** of S, denoted by 2^S (or $\mathcal{P}(S)$), is the set of all subsets of S.

In set-builder notation,

$$\boxed{2^S := \{A \,|\, A \subseteq S\}.}$$

2.2.17 EXAMPLE. What is the power set of $S = \{1, 2, 3\}$?

SOLUTION : $2^S = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

2.3 The integers and division

The set of all *integers* is denoted by $\mathbb{Z}$. The mathematical theory of integers and their properties is called *number theory* (or sometimes, on traditional grounds, *arithmetic*).

Any two integers $a, b \in \mathbb{Z}$ can be *added* and *multiplied* : their *sum* $a + b$ and their *product* ab are well-defined integers. Addition and multiplication of integers are governed by certain laws. The most basic ones are the following :

$$a + b = b + a; \qquad ab = ba;$$
$$a + (b + c) = (a + b) + c; \qquad a(bc) = (ab)c;$$
$$a(b + c) = ab + ac.$$

NOTE : These fundamental arithmetic laws are very simple, and may seem obvious. But they might not be applicable to entities other than integers. However, these laws resemble some (but not all !) properties (laws) regarding logical propositions (w.r.t. disjuction and conjuction) or sets (w.r.t. union and intersection). For example, the addition of integers does not distributes w.r.t. the multiplication : in general, $a + bc \neq (a + b)(a + c)$.

The notion of *divisibility* is the central concept of number theory. Based on this concept, many important ideas (with far reaching applications) can be developed.

Divisibility

When one integer is devided by a second (nonzero) integer, the quotient may or may not be an integer. For example, $16 \div 4$ is an integer, whereas $15 \div 4$ is not.

We make the following definition.

2.3.1 DEFINITION. If $a, b \in \mathbb{Z}$ and $b \neq 0$, we say that a is **divisible** by b, denoted $a \vdots b$, provided there is an integer k such that $a = bk$. Simbolically,

$$\boxed{a \vdots b \iff a = bk \quad \text{for some } k \in \mathbb{Z}.}$$

Alternatively, we say that

- a is a **multiple** of b;
- b is a **divisor** of a;
- b is a **factor** of a;
- b **divides** a.

The (alternative) notation $b \mid a$ is read "b divides a".

2.3.2 EXAMPLE.

(a) Is 40 divisible by 8 ?

(b) Does 5 divide 120 ?

(c) Is 48 a multiple of -16 ?

(d) Does $7 \mid (-7)$?

SOLUTION : (a) Yes, $40 = 8{\cdot}5$. (b) Yes, $120 = 5{\cdot}24$. (c) Yes, $48 = 16{\cdot}(-3)$. (d) Yes, $-7 = 7 \cdot (-1)$.

2.3.3 EXAMPLE. If m is a nonzero integer, does m divide 0 ?

SOLUTION : Yes, because $0 = m \cdot 0$.

NOTE : We may express the fact that m is a nonzero integer, by writing $m \in \mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$.

2.3.4 EXAMPLE. Which integers divide 1 ?

SOLUTION : The only divisors of 1 are 1 and -1.

The following result is easy to prove.

2.3.5 PROPOSITION. *Let* $a, b, c \in \mathbb{Z}$. *Then*

1. *If* $a \vdots c$ *and* $b \vdots c$, *then* $(a+b) \vdots c$.
2. *If* $a \vdots b$, *then* $ac \vdots b$.
3. *If* $a \vdots b$ *and* $b \vdots c$, *then* $a \vdots c$.

Every positive integer greater than 1 is divisible by *at least* two integers, since a positive integer is divisible by 1 and by itself. Integers that have exactly two (different) positive integer factors are called *prime*.

2.3.6 DEFINITION. A positive integer $p > 1$ is called **prime** if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called **composite**.

2.3.7 EXAMPLE. The first few prime numbers are :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \cdots$$

They become progresively more sparse and are rather irregularly distributed.

NOTE : Attempts have been made to find simple arithmetical formulas that yield only primes, even though they may not give all of them. PIERRE DE FERMAT (1601-1665) made the fameous *conjecture* that *all numbers of the form*

$$F(n) = 2^{2^n} + 1$$

are prime. Indeed, for $n = 1, 2, 3, 4$ we obtain

$$\begin{aligned} F(1) &= 2^2 + 1 = 5 \\ F(2) &= 2^{2^2} + 1 = 17 \\ F(3) &= 2^{2^3} + 1 = 257 \\ F(4) &= 2^{2^4} + 1 = 65\,537 \end{aligned}$$

all prime numbers. But in 1732 LEONHARD EULER (1707-1783) discovered the factorization $2^{2^5} + 1 = 641 \cdot 6\,700\,417$; hence $F(5)$ is *not* prime.

Another remarkable and simple expression which produces many primes is

$$f(n) = n^2 - n + 41.$$

For $n = 1, 2, 3, \cdots, 40$, $f(n)$ is a prime number; but for $n = 41$, we have $f(n) = 41^2$, which is no longer a prime number.

On the whole, it has been a futile task to seek expressions of a simple type which produce only prime numbers. Even less promising is the attempt to find an algebraic formula which shall yield *all* the prime numbers.

Is the set of all such numbers *infinite*, or is there a largest prime number ? The answer was known to EUCLID and a proof (that the set of all prime numbers is infinite) will be given now. Only one additional fact is required.

2.3.8 LEMMA. *For any integer a and prime number p, if $p \,|\, a$, then $p \not| \,(a+1)$.*

PROOF : Suppose not. Suppose there exists an integer a and a prime number p such that

$$p \,|\, a \quad \text{and} \quad p \,|\, (a+1).$$

Then, by definition of divisibility, there exist integers k and ℓ so that

$$a = pk \quad \text{and} \quad a + 1 = p\ell.$$

It follows that

$$1 = (a+1) - a = pk - p\ell = p(k - \ell)$$

and so (since $k - \ell$ is an integer) $p \,|\, 1$. But the only divisors of 1 are 1 and -1. But p is prime, hence $p > 1$. This is a contradiction. (Hence the supposition is FALSE, and the proposition is TRUE.) □

NOTE : An implication $p \to q$ can be *proved* by showing that if p is TRUE, then q must also be TRUE. (This shows that the combination p TRUE and q FALSE never occurs.) A *proof* of this kind is called a **direct proof**.

Suppose that a contradiction can be *deduced* by assuming that q is not TRUE : the proposition $p \wedge \neg q \to \mathbf{C}$ is TRUE. We can see that

$$p \to q \iff (p \wedge \neg q \to \mathbf{C}) .$$

It follows that if p is TRUE, then q must also be TRUE. An *argument* of this type (for proving the implication $p \to q$) is called a **proof by contradiction**.

2.3.9 THEOREM. *The set of all prime numbers is infinite.*

PROOF : Suppose not. Suppose the set of all prime numbers is finite. (We must deduce a contradiction.) Then all the prime numbers can be listed, say, in ascending order :

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \cdots,\ p_n.$$

Consider the integer

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1.$$

Then $n > 1$ and so n is divisible by some prime number p : $p \,|\, n$. Also, since p is prime, p must equal one of the prime numbers $p_1, p_2, \cdots, p_n$. Thus

$$p \,|\, (p_1 \cdot p_2 \cdot p_3 \cdots p_n).$$

Then, by LEMMA 2.3.8, $p \not| \, (p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1)$. So $p \not| \, n$. This is a contradiction. (Hence the supposition is FALSE, and the theorem is TRUE.) □

The prime numbers are the building blocks of positive integers, as the following result shows. This result (also referred to as the *Unique Factorization Theorem*) says that any positive integer $n > 1$ is either a prime number or can be written as a product of prime numbers in a way that is unique except, perhaps, for the order of the factors.

2.3.10 THEOREM. (THE FUNDAMENTAL THEOREM OF ARITHMETIC) *Every positive integer $n > 1$ can be written uniquely as a product of prime numbers, where the prime factors are written in order of increasing size.*

Thus, for $n > 1$, there exist unique prime numbers $p_1 < p_2 < \cdots < p_k$ and unique positive integers $\alpha_1, \alpha_2 \cdots, \alpha_k$ such that

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k}.$$

2.3.11 EXAMPLE. Find the prime factorizations of the numbers $100, 999,$ and 2005.

SOLUTION : We have

$$\begin{aligned} 100 &= 2 \cdot 50 \\ &= 2 \cdot 2 \cdot 25 \\ &= 2^2 \cdot 5^2. \\ 999 &= 9 \cdot 111 \\ &= 3^2 \cdot 3 \cdot 37 \\ &= 3^3 \cdot 37. \\ 2005 &= 5 \cdot 401. \end{aligned}$$

NOTE : It is often important to know whether a given positive integer is prime. It can be shown that *a positive integer is a prime number if it is not divisible by any prime number less than or equal to its square root.* For example, the number 401 is prime because it is not divisible by any of the prime numbers 2,3,5,7,11,13,17 or 19.

An important *corollary* of THE FUNDAMENTAL THEOREM OF ARITHMETIC is the following :

2.3.12 PROPOSITION. *If a, b, p are positive integers and p is prime such that $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

SOLUTION : If p were a factor of neither a nor b, then then the product of the prime factorizations of a and b would yield a prime factorization of the integer ab *not containing* p. On the other hand, since p is assumed to be a factor of ab, there exists an integer k such that $ab = pk$. Hence the product of p by a prime factorization of k would yield a prime factorization of the

integer ab *containing* p, contrary to the fact that the prime factorization of ab is unique. □

2.3.13 EXAMPLE. If one has verified the fact that 13 is a divisor of $2\,652$, and the fact that $2\,652 = 6 \cdot 442$, one may conclude that 13 is a divisor of 442.

On the other hand, 6 is a factor of 240, and $240 = 15 \cdot 16$, but 6 is *not* a factor of either 15 or 16.

(This shows that the assumption that p is a prime number is an essential one.)

In order to find all the divisors (or factors) of any (positive integer) a we need only its prime decomposition

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}.$$

All the divisors of a are the numbers

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$$

where the β's are any integers satisfying the inequalities

$$0 \leq \beta_1 \leq \alpha_1, \quad 0 \leq \beta_2 \leq \alpha_2, \quad \cdots, \quad 0 \leq \beta_n \leq \alpha_n.$$

It follows that *the number of all different divisors of* a *(including the divisors* 1 *and* a*) is given by the product*

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1).$$

2.3.14 EXAMPLE. The positive integer $144 = 2^4 \cdot 3^2$ has $5 \cdot 3 = 15$ divisors. They are

$$1,\ 2,\ 4,\ 8,\ 16,\ 3,\ 6,\ 12,\ 24,\ 48,\ 9,\ 18,\ 36,\ 72,\ 144.$$

GCDs and LCMs

An integer may or may not be divisible by another. However, when an integer is divided by a positive integer, there always is a *quotient* and a *remainder*. The following result holds.

2.3.15 Theorem. (The Quotient-Remainder Theorem) *Given any integer a and positive integer d, there are unique integers q and r such that*

$$a = d \cdot q + r \quad \textit{and} \quad 0 \leq r < d.$$

In the equality above, d is called the **divisor**, a is called the **dividend**, q is called the **quotient**, and r is called the **remainder**.

2.3.16 Example. What are the quotient and the remainder when 82 is divided by 11 ?

Solution : We have

$$82 = 11 \cdot 7 + 5.$$

Hence the quotient (when 82 is divided by 11) is 7 and the remainder is 5.

2.3.17 Example. What are the quotient and the remainder when -43 is divided by 8 ?

Solution : We have

$$-43 = 8 \cdot (-6) + 5.$$

Hence the quotient (when -43 is divided by 8) is -6 and the remainder is 5. (Note that the remainder cannot be negative.)

2.3.18 Definition. Let a and b be two nonzero integers. The largest integer d such that $d \,|\, a$ and $d \,|\, b$ is called the **greatest common divisor** of a and b.

The greatest common divisor of a and b is denoted by $\mathsf{GCD}\,(a, b)$.

The GCD of two nonzero integers always exists because the set of common divisors of these integers is finite. One way to find the GCD of two integers is to find all the positive common divisors of both integers and then take the largest divisor.

2.3.19 EXAMPLE. Find the greatest common divisor of 48 and 64.

SOLUTION : The positive common divisors of 48 and 64 are

$$1, 2, 4, 8, \quad \text{and} \quad 16.$$

Hence $\mathsf{GCD}\,(48, 64) = 16$.

2.3.20 EXAMPLE. What is the GCD of 16 and 81 ?

SOLUTION : The integers 16 and 81 have no positive common divisors other than 1, so that $\mathsf{GCD}\,(16, 81) = 1$.

NOTE : Two integers who have no common positive divisors other than 1 are said to be **relatively prime**. Clearly, any two prime numbers are relatively prime.

Another way to find the GCD of two integers is to use the *prime factorizations* of these integers. Suppose that the prime factorizations of the nonzero integers a and b are :

$$a = p_1^{\alpha_1} \cdot p_1^{\alpha_2} \cdots p_n^{\alpha_n} \quad \text{and} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$$

where each exponent is a *nonnegative* integer and where all prime factors occuring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then $\mathsf{GCD}\,(a, b)$ is given by

$$\mathsf{GCD}\,(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_n^{\min(\alpha_n, \beta_n)}$$

where $\min(r, s)$ represents the *minimum* of the two numbers r and s.

2.3.21 EXAMPLE. Find the GCD of 200 and 360.

SOLUTION : The prime factorizations of 200 and 360 are

$$\begin{aligned} 200 &= 8 \cdot 25 \\ &= 2^3 \cdot 5^2, \\ 360 &= 4 \cdot 9 \cdot 10 \\ &= 2^3 \cdot 3^2 \cdot 5. \end{aligned}$$

Hence

$$\mathsf{GCD}\,(200, 360) = 2^{\min(3,3)} \cdot 3^{\min(0,2)} \cdot 5^{\min(2,1)} = 2^3 \cdot 3^0 \cdot 5^1 = 40.$$

Prime factorizations can also be used to find the *least commun multiple* of two integers.

2.3.22 DEFINITION. Let a and b be two positive integers. The smallest positive integer m such that $m \vdots a$ and $m \vdots b$ is called the **least common multiple** of a and b.

The least common multiple of a and b is denoted by $\mathsf{LCM}\,(a, b)$.

The LCM of two integers always exists because the set of integers divisible by both a and b is nonempty, and *every nonempty set of positive integers has a least element.* Suppose that the prime factorizations of a and b are as before. Then $\mathsf{LCM}\,(a, b)$ is given by

$$\mathsf{LCM}\,(a, b) = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdots p_n^{\max(\alpha_n,\beta_n)}$$

where $\max(r, s)$ represents the *maximum* of the two numbers r and s.

2.3.23 EXAMPLE. What is the least common multiple of $a = 2^2 \cdot 3^4 \cdot 5$ and $b = 2 \cdot 3^2 \cdot 7^2$?

SOLUTION : We have

$$\mathsf{LCM}\,(a, b) = 2^{\max(2,1)} \cdot 3^{\max(4,2)} \cdot 5^{\max(1,0)} \cdot 7^{\max(0,2)} = 2^2 \cdot 3^4 \cdot 5 \cdot 7^2.$$

There is an interesting relationship between the GCD and the LCM of two integers.

2.3.24 PROPOSITION. *Let a and b be positive integers. Then*

$$a \cdot b = \mathsf{GCD}\,(a, b) \cdot \mathsf{LCM}\,(a, b).$$

The Euclidean algorithm

The method for computing the GCD of two integers, using the prime factorization, is very inefficient. (The reason is that finding prime factorizations is a time-consuming process.) More efficient methods exist. The following *algorithm*, called the **Euclidean algorithm**, has been known since ancient times. It is based on the following facts :

- If r is a positive integer, then $\mathsf{GCD}\,(r, 0) = r$.
- If a, b, q, r are integers such that $a = b \cdot q + r$, then $\mathsf{GCD}\,(a, b) = \mathsf{GCD}\,(b, r)$.

The Euclid algorithm can be described as follows :

1. Let a and b be integers with $a > b \geq 0$.
2. To find the GCD of a and b, first check whether $b = 0$. If it is, then $\mathsf{GCD}\,(a, b) = a$. If it isn't, then put $r_0 = a$ and $r_1 = b$, and then apply successively the *Quotient-Remainder Theorem* :

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 && (0 \leq r_2 < r_1) \\ r_1 &= r_2 q_2 + r_3 && (0 \leq r_3 < r_2) \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n && (0 \leq r_n < r_{n-1}) \\ r_{n-1} &= r_n q_n. \end{aligned}$$

Eventually *a remainder of zero occurs in this sequence of successive divisions* (since a sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms).

3. It follows that

$$\begin{aligned} \mathsf{GCD}\,(a,b) &= \mathsf{GCD}\,(r_0,r_1) \\ &= \mathsf{GCD}\,(r_1,r_2) \\ &\vdots \\ &= \mathsf{GCD}\,(r_n,0) \\ &= r_n. \end{aligned}$$

Hence *the* $\mathsf{GCD}\,(a,b)$ *is the last nonzero remainder in the sequence of divisions.*

NOTE : It is always the case that the number of steps required in the Euclidean algorithm is at most five times the number of digits in the small number.

2.3.25 EXAMPLE. Calculate the GCD of 330 and 156 using the Euclidean algorithm.

SOLUTION : We have

$$\begin{aligned} 330 &= 156 \cdot 2 + 18 \\ 156 &= 18 \cdot 8 + 12 \\ 18 &= 12 \cdot 1 + 6 \\ 12 &= 6 \cdot 1 + 0. \end{aligned}$$

Hence

$$\mathsf{GCD}\,(330,156) = 6.$$

An extremely important property of $\mathsf{GCD}\,(a,b)$ can be derived from the Euclidean algorithm.

2.3.26 PROPOSITION. *If* a *and* b *are positive integers, then there exist integers* k *and* ℓ *such that*

$$\mathsf{GCD}\,(a,b) = ka + \ell b.$$

SOLUTION : As before, consider the sequence of successive divisions :

$$\begin{aligned} r_0 &= r_1q_1 + r_2 \\ r_1 &= r_2q_2 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n \\ r_{n-1} &= r_nq_n. \end{aligned}$$

From the first equation

$$r_2 = a - q_1b$$

so that r_2 can be written in the form $k_1a + \ell_1b$ (in this case $k_1 = 1$ and $\ell_1 = -q_1$).

From the next equation,

$$\begin{aligned} r_3 &= b - q_2r_2 \\ &= b - q_2(k_1a + \ell_1b) \\ &= (-q_2k_1)a + (1 - q_2\ell_1)b \\ &= k_2a + \ell_2b. \end{aligned}$$

Clearly this process can be repeated through the successive remainders $r_4, r_5, \cdots$ until we arrive at the representation

$$r_n = ka + \ell b$$

as was to be proved. □

2.3.27 EXAMPLE. Express $\mathsf{GCD}\,(61, 24)$ as a *linear combination* of 61 and 24 (i.e. in the form $k \cdot 61 + \ell \cdot 24$).

SOLUTION : We have

$$\begin{aligned} 61 &= 2 \cdot 24 + 13 \\ 24 &= 1 \cdot 13 + 11 \\ 13 &= 1 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

We have, from the first of these equations,

$$13 = 61 - 2 \cdot 24,$$

from the second,

$$11 = 24 - 13 = 24 - (61 - 2 \cdot 24) = -61 + 3 \cdot 24,$$

from the third,

$$2 = 13 - 11 = (61 - 2 \cdot 24) - (-61 + 3 \cdot 24) = 2 \cdot 61 - 5 \cdot 24,$$

and from the fourth,

$$1 = (-61 + 3 \cdot 24) - 5 \cdot (2 \cdot 61 - 5 \cdot 24) = -11 \cdot 61 + 28 \cdot 24.$$

NOTE : The fact that $d = \mathsf{GCD}\,(a, b)$ can always be written in the form

$$d = k \cdot a + \ell \cdot b$$

may be used to prove the FUNDAMENTAL THEOREM OF ARITHMETIC.

2.4 Exercises

Exercise 16 TRUE or FALSE ?

(a) $\emptyset = \{\emptyset\}$.

(b) $4 \in \{4\}$.

(c) $\{4\} \subseteq \{\{4\}\}$.

(d) $\emptyset \in \{4\}$.

(e) $\emptyset \subseteq \{4\}$.

(f) $[2, 4] \subseteq \mathbb{N}$.

(g) $\{2, 3, 4\} \subseteq \mathbb{Z}$.

(h) $\frac{1}{2} \in \{0, 1\}$.

Exercise 17 Let $a, b, c \in \mathbb{R}$. Prove that

$$a^2 + b^2 + c^2 \geq ab + bc + ca$$

with equality if and only if $a = b = c$.

Exercise 18 Let $a, b, a_1, a_2, b_1, b_2 \in \mathbb{R}$. Prove that :

(a) (**Mean inequalities**) If $0 < a \leq b$, then

$$a \leq \frac{2}{\frac{1}{a} + \frac{1}{b}} \leq \sqrt{ab} \leq \frac{a+b}{2} \leq \sqrt{\frac{a^2+b^2}{2}} \leq b$$

with equality if and only if $a = b$.

(b) (**Cauchy-Schwarz inequality**)

$$(a_1b_1 + a_2b_2)^2 \leq (a_1^2 + a_2^2)(b_1^2 + b_2^2)$$

with equality if and only if $a_1 = rb_1$ and $a_2 = rb_2 \quad (r \in \mathbb{R})$.

(c) (**Chebyshev inequality**) If $a_1 \leq a_2$ and $b_1 \leq b_2$, then

$$(a_1 + a_2)(b_1 + b_2) \leq 2(a_1b_1 + a_2b_2)$$

with equality if and only if $a_1 = a_2$ and $b_1 = b_2$.

NOTE : (1) The expressions $\frac{2}{\frac{1}{a}+\frac{1}{b}}$ and $\sqrt{\frac{a^2+b^2}{2}}$ are called the **harmonic mean** and the **quadratic mean** (of the positive real numbers a and b), respectively.

(2) All these inequalities (given here for the case $n = 2$) can be generalized.

Exercise 19 Find conditions on sets A and B to make each of the following propositions TRUE.

(a) $A \cup B = A$.

(b) $A \cap B = B$.

(c) $A \cup B = A \cap B$.

(d) $A \setminus B = \emptyset$.

(e) $A \setminus B = A$.

(f) $A \setminus B = B$.

(g) $A \setminus B = B \setminus A$.

Exercise 20 Can you conclude that $A = B$ if A, B and C are sets such that

(a) $A \cup C = B \cup C$?

(b) $A \cap C = B \cap C$?

(c) $A \cup C = B \cup C$ and $A \cap C = B \cap C$?

Exercise 21 The **symmetric difference** of A and B, denoted by $A \triangle B$, is the set containing those elements in either A or B, but not in both A and B; that is,

$$A \triangle B := (A \cup B) \setminus (A \cap B).$$

(a) Find the symmetric difference of $\{1, 2, 3\}$ and $\{2, 3, 4\}$.

(b) Show that

i. $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

ii. $A \triangle A = \emptyset$.

iii. $A \triangle \emptyset = A$.

iv. $A \triangle B = B \triangle A$.

v. $(A \triangle B) \triangle C = A \triangle (B \triangle C)$

(c) What can you say about the sets A and B if $A \triangle B = A$?

Exercise 22 TRUE or FALSE ?

(a) If A, B are finite sets, then $| A \times B | = | A | \cdot | B |$.

(b) If A, B are finite sets, then $| A \setminus B | = | A | - | B |$.

(c) If A, B are finite sets, then $| A \cup B | = | A | + | B |$.

(d) If A, B are finite sets, then $| 2^A | = 2^{|A|}$.

(e) If A, B are sets, and $(5, 6) \notin A \times B$, then $5 \notin A$ and $6 \notin B$.

(f) If A, B are sets, and $5 \notin A$, then $(5, 6) \notin A \times B$.

(g) If A, B are sets, and $(A \times B) \cap (B \times A) \neq \emptyset$, then $A \cap B \neq \emptyset$.

(h) If A, B are sets, and $A \cap B \neq \emptyset$, then $(A \times B) \cap (B \times A) \neq \emptyset$.

If the statement is FALSE, give a counterexample.

Exercise 23 Let A, B, and C be sets. Show that :

(a) $(A \setminus B) \cap (A \cap B) = \emptyset$.

(b) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

(c) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

(d) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

(e) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.

Exercise 24 Prove the following statements.

(a) If a is a nonzero integer, then

$$1 \,|\, a \quad \text{and} \quad a \,|\, 0.$$

(b) If $a, b,$ and c are integers such that $a \,|\, b$, then $a \,|\, bc$.

(c) If $a, b,$ and c are integers such that $a \,|\, b$ and $b \,|\, c$, then $a \,|\, c$.

(d) If $a, b, c,$ and d are integers such that $a \,|\, c$ and $b \,|\, d$, then $ab \,|\, cd$.

(e) If $a, b,$ and c are integers such that $ac \,|\, bc$, then $a \,|\, b$.

Exercise 25 Are the following integers prime ?

(a) 93.

(b) 101.

(c) 301.

(d) 1001.

Exercise 26 In each of the following cases, what are the quotient and remainder ?

(a) 19 is divided by 7.

(b) -101 is divided by 11.

(c) 1001 is divided by 13.

(d) 0 is divided by 23.

(e) -1 is divided by 5.

Exercise 27 Find the prime factorization of each of the following.

(a) 39.

(b) 81.

(c) 101.

(d) 289.

(e) 899.

Exercise 28 Use the Euclidean algorithm to find

(a) $\mathsf{GCD}\,(12, 18)$.

(b) $\mathsf{GCD}\,(111, 201)$.

(c) $\mathsf{GCD}\,(1001, 1331)$.

(d) $\mathsf{GCD}\,(123, 4321)$.

Exercise 29 Express the GCD of each of the following pairs of integers as a linear combination of these integers.

(a) 10, 11.

(b) 21, 44.

(c) 36, 48.

(d) 34, 55.

(e) 117, 213.

(f) 0, 223.

Exercise 30 TRUE or FALSE ?

(a) If a and b are integers such that $a \vdots b$ and $b \vdots a$, then $a = b$.

(b) If $a, b,$ and c are positive integers such that $a \mid bc$, then $a \mid c$.

(c) The integers which leave a remainder 1 when divided by 2 and also leave a remainder 1 when divided by 3 are those and only those of the form $6k + 1$, where $k \in \mathbb{Z}$.