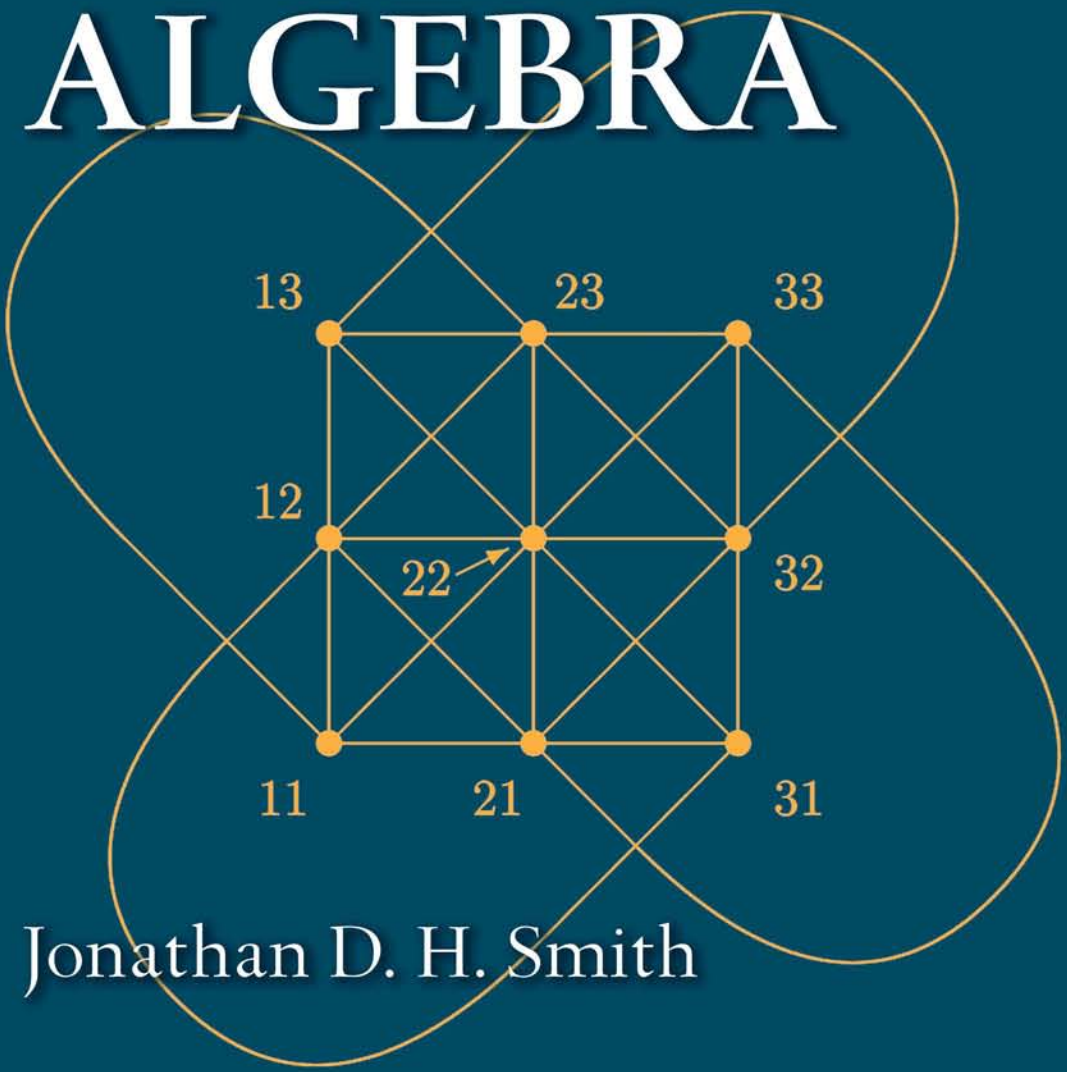
TEXTBOOKS in MATHEMATICS

INTRODUCTION TO ABSTRACT ALGEBRA



Jonathan D. H. Smith

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

INTRODUCTION TO ABSTRACT ALGEBRA

TEXTBOOKS in MATHEMATICS

Series Editor: Denny Gulick

PUBLISHED TITLES

COMPLEX VARIABLES: A PHYSICAL APPROACH WITH APPLICATIONS AND MATLAB®
Steven G. Krantz

INTRODUCTION TO ABSTRACT ALGEBRA
Jonathan D. H. Smith

LINEAR ALBEBRA: A FIRST COURSE WITH APPLICATIONS
Larry E. Knop

FORTHCOMING TITLES

ENCOUNTERS WITH CHAOS AND FRACTALS
Denny Gulick

TEXTBOOKS in MATHEMATICS

INTRODUCTION TO ABSTRACT ALGEBRA

Jonathan D. H. Smith

Iowa State University

Ames, Iowa, U.S.A.

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20131121

International Standard Book Number-13: 978-1-4200-6372-1 (eBook - PDF)

Contents

Preface

This book is designed as an introduction to "abstract" algebra, particularly for students who have already seen a little calculus, as well as vectors and matrices in 2 or 3 dimensions. The emphasis is not placed on abstraction for its own sake, or on the axiomatic method. Rather, the intention is to present algebra as the main tool underlying discrete mathematics and the digital world, much as calculus was accepted as the main tool for continuous mathematics and the analog world.

Traditionally, treatments of algebra at this level have faced a dilemma: groups first or rings first? Presenting rings first immediately offers familiar concepts such as polynomials, and builds on intuition gained from working with the integers. On the other hand, the axioms for groups are less complex than the axioms for rings. Moreover, group techniques, such as quotients by normal subgroups, underlie ring techniques such as quotients by ideals. The dilemma is resolved by emphasizing semigroups and monoids along with groups. Semigroups and monoids are steps up to groups, while rings have both a group structure and a semigroup or monoid structure.

The first three chapters work at the concrete level: numbers, functions, and equivalence. Semigroups of functions and groups of permutations appear early. Functional composition, cycle notation for permutations, and matrix notation for linear functions provide techniques for practical computation, avoiding less direct methods such as generators and relations or table look-up. Equivalence relations are used to introduce rational numbers and modular arithmetic. They also enable the First Isomorphism Theorem to be presented at the set level, without the requirement for any group structure. If time is short (say just one quarter), the first three chapters alone may be used as a quick introduction to algebra, sufficient to exhibit irrational numbers or to gain a taste of cryptography.

Abstract groups and monoids are presented in the fourth chapter. The examples include orthogonal groups and stochastic matrices, while concepts such as Lagrange's Theorem and groups of units of monoids are covered. The fifth chapter then deals with homomorphisms, leading to Cayley's Theorem reducing abstract groups to concrete groups of permutations. Rings form the topic of the sixth chapter, while integral domains and fields follow in the seventh. The first six or seven chapters provide basic coverage of abstract algebra, suitable for a one-semester or two-quarter course.

Subsequent chapters deal with slightly more advanced topics, suitable for a second semester or third quarter. Chapter 8 delves deeper into the theory

of rings and fields, while modules — particularly vector spaces and abelian groups — form the subject of Chapter 9. Chapter 10 is devoted to group theory, and Chapter 11 gives an introduction to quasigroups.

The final four chapters are essentially independent of each other, so that instructors have the freedom to choose which topics they wish to emphasize. In particular, the treatment of fields in Chapter 8 does not make use of any of the concepts of linear algebra, such as vector space, basis, or dimension, which are covered in Chapter 9. For a one-semester introduction to groups, one could replace Chapter 6 with Chapter 10, using the field of integers modulo a prime in the examples that call for a finite field.

Each chapter includes a range of exercises, of varying difficulty. Chapter notes point out variations in notation and approach, or list the names of mathematicians that are used in the terminology. No biographical sketches are given, since libraries and the Internet can offer much more detail as required.

A special feature of the book is the inclusion of the "Study Projects" at the end of each chapter. The use of these projects is at the instructor's discretion. Some of them may be incorporated into the main presentation, offering typical applications or extensions of the algebraic topics. Some are coherent series of exercises, that could be assigned along with the other problems, or used for extra credit. Some projects are suitable for group study by students, occasionally involving some outside research.

I have benefited from many discussions with my students and colleagues about algebra, its presentation and application. Specific acknowledgments are due to Mark Ciecior, Dan Nguyen, Jessica Schuring, Dr. Sungyell Song, Shibi Vasudevan, and anonymous referees for helpful comments on a preliminary version of the book. The original impetus for the project came from Bob Stern at Taylor & Francis. I am grateful to him, and the publishing staff, for bringing it to fruition.

Chapter 1

NUMBERS

Algebra begins as the art of working with numbers. The *integers* are the whole numbers, positive, negative, and zero. Put together, they form the set

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\} \tag{1.1}$$

(the letter $\mathbb{Z}$ coming from the German word Zahlen, meaning "numbers"). The *natural numbers* are the nonnegative integers, including zero. They are "natural" because they are the possible numbers of elements in a finite set. For example, 4 is the number of elements of the set

$$\{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\} \tag{1.2}$$

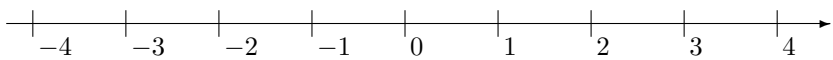
of suits in a deck of cards, while 13 is the number of elements of the set

$$\{\mathrm{A}\heartsuit, \mathrm{K}\heartsuit, \mathrm{Q}\heartsuit, \mathrm{J}\heartsuit, 10\heartsuit, 9\heartsuit, 8\heartsuit, 7\heartsuit, 6\heartsuit, 5\heartsuit, 4\heartsuit, 3\heartsuit, 2\heartsuit\} \tag{1.3}$$

of cards in the suit $\heartsuit$ of hearts. Note that 0 is the number of elements in the empty set $\varnothing$ or $\{\ \}$. The natural numbers form the set

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}\,. \tag{1.4}$$

Another set of numbers familiar from calculus is the set $\mathbb{R}$ of *real numbers*, like -17, $\sqrt{2} = 1.41421\dots$, $e = 2.71828\dots$, $\pi = 3.14159\dots$, and so on. It is hard to display the set of real numbers as a list of elements between braces, like the sets (1.1)–(1.4) above. Instead, the set $\mathbb{R}$ is pictured as the *real line*



(like an axis in the graph of a function). Pictures like this are useful as geometric visualizations of real numbers. At times similar pictures can even be useful for natural numbers or integers, since these numbers also happen to be real numbers.

1.1 Ordering numbers

In calculus, order relations between real numbers are crucial, for instance when we want to find the maximum value of a function over a certain range.

Recall that $x < y$ (read "x less than y") means $y - x$ is positive, while $x \leq y$ (read "x less than or equal to y") means that $y - x$ is nonnegative. We can also write $y > x$ ("x greater than y") instead of $x < y$, or $y \geq x$ ("x greater than or equal to y") instead of $x \leq y$. In the real line picture, with the positive numbers going off to the right, the relation $x < y$ becomes an arrow $x \longrightarrow y$. It is often helpful to signify the relation $x \leq y$ with an arrow from x to y, without requiring the arrow to go horizontally from left to right.

Since algebra also needs to work with order relations between numbers, it is important to know the rules for manipulating them. The first rule is called *reflexivity*:

$$x \leq x \tag{1.5}$$

for any real (or integral, or natural) number x. This particular rule doesn't seem to be saying very much, but it often serves as a place-holder. The second rule is *transitivity*:

$$\big(\ x \leq y \quad \text{and} \quad y \leq z\ \big) \quad \text{implies} \quad x \leq z \tag{1.6}$$

for any real (or integral, or natural) numbers x, y, and z. If Xavier can't beat Yerkes, and Yerkes can't beat Zandor, then Xavier can't beat Zandor either. Why does (1.6) hold? Well, if $x \leq y$ and $y \leq z$, the quantities $y - x$ and $z - y$ are nonnegative. In that case, so is their sum $z - x$, meaning that $x \leq z$. Transitivity makes a natural arrow picture:

... "completing the triangle." The final rule for the order relation is the one that yields conclusions of proofs, when you want to show that two numbers are actually equal:

$$\big(\ x \leq y \quad \text{and} \quad y \leq x\ \big) \quad \text{implies} \quad x = y \tag{1.7}$$

for real numbers x and y. This rule is called *antisymmetry*. If Xavier can't beat Yerkes, and Yerkes can't beat Xavier either, then Xavier and Yerkes will tie.

Rules for an order relation

(R)	**Reflexivity:**	$x \leq x$				
(T)	**Transitivity:**	$x \leq y$	and	$y \leq z$	imply	$x \leq z$
(A)	**Antisymmetry:**	$x \leq y$	and	$y \leq x$	imply	$x = y$

As an illustration of the use of the rules, here's a proposition with its proof.

PROPOSITION 1.1 **(Squeezing.)**
Suppose x, y, and z are real numbers. If $x \le y \le z \le x$, then $x = z$.

PROOF Since $x \le y \le z$, transitivity shows that $x \le z$. But also $z \le x$, so antisymmetry gives $x = z$. □

1.2 The Well-Ordering Principle

Compare (1.1) with (1.4). The elements of $\mathbb{Z}$ in (1.1) stretch off arbitrarily far to the left inside the braces: There is no smallest integer. In a version of the schoolyard game "My Dad earns more than your Dad," consider two players trying to name the smaller integer. Whatever number the first player names, say $-10,000,000$, the second player can always choose $-10,000,001$ or something even more negative. With the natural numbers, the situation is different. It is summarized by the following statement, the so-called

Well-Ordering Principle:

Each nonempty subset S of $\mathbb{N}$ has a least element $\inf S$.

(Compare Exercise 7. The mathematical notation $\inf S$ stands for the *infimum* of S.) Of course, the principle is only required for infinite subsets S. For finite nonempty subsets S, the least element $\inf S$, in this case often denoted as the *minimum* $\min S$, can be located easily (Project 2).

Example 1.2 **(An application of the Well-Ordering Principle.)**
Suppose $S = \{n \in \mathbb{N} \mid 10^n < \frac{1}{2}n^n\}$, the set of natural numbers n for which the power 10^n is less than half the power n^n. The set S is nonempty, indeed infinite, since as n increases beyond 10, the power n^n grows faster than 10^n. (Formally, $\lim_{n\to\infty}(\frac{1}{2}n^n/10^n) = \infty$.) The Well-Ordering Principle guarantees that S has a least element $\inf S$. You are invited to find it in Exercise 5. □

In one of its main applications, the Well-Ordering Principle underwrites the techniques known as *recursion* and *mathematical induction*. For example, consider the definition of the *factorial* $n!$ of a natural number n. This quantity is usually defined recursively as follows:

$$0! = 1\,, \qquad (n+1)! = (n+1)\cdot n!$$

How can we be sure that the definition is complete, that it will not leave a quantity such as 50001200! undefined?

For generality, consider a property $P(n)$ of a natural number n, say the property that $n!$ is defined by the given recursive procedure.

- The **Induction Basis** is the statement that the property $P(0)$ holds.
- The **Induction Step** is the statement that truth of the property $P(n)$ implies the truth of the property $P(n+1)$.
- The **Principle of Induction** states: The Induction Basis and Induction Step together guarantee that $P(n)$ holds for all natural numbers n.

To justify the Principle of Induction, suppose that it goes wrong. In other words, the set

$$S = \{n \mid P(n) \text{ is false } \}$$

is nonempty. By the Well-Ordering Principle, the set S has a least element s. The Induction Basis shows that s cannot be 0. Thus $s > 0$, and $s-1$ is a natural number. Since $s-1$ does not lie in S, the property $P(s-1)$ holds. The Induction Step then gives the contradiction that $P(s)$ is true. Thus the Principle of Induction cannot go wrong.

Example 1.3 **(A model proof by induction.)**
Let $P(n)$ be the statement that the identity

$$1^2 + 2^2 + 3^2 + \ldots + (n-1)^2 + n^2 = \frac{n(n+1)(2n+1)}{6} \tag{1.8}$$

holds for a natural number n. As Induction Basis, note that (1.8) reduces to the triviality $0 = 0$ for $n = 0$, so $P(0)$ is true. For the Induction Step, suppose that $P(n)$ is true, so that (1.8) holds as written. Then

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \ldots + (n-1)^2 + n^2 + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)(2n^2+7n+6)}{6} \\ &= \frac{(n+1)(n+2)\big(2(n+1)+1\big)}{6}, \end{aligned}$$

so that $P(n+1)$ is true. This proves (1.8) by induction. □

1.3 Divisibility

The set $\mathbb{Z}$ of integers is a subset of the set $\mathbb{R}$ of real numbers; so integers can certainly be compared using the order relation $\leq$ for real numbers. However, in many cases a different relation between integers is more relevant. This is the relation of *divisibility*. Given two integers m and n, the integer m is said to be a *multiple* of n if there is an integer r such that $m = r \cdot n$. For example, 946 is a multiple of 11, since $946 = 86 \cdot 11$. Even integers are the multiples of 2. Zero is a multiple of every integer. Turning the relationship around, an integer n is said to *divide* an integer m, or to be a *divisor* of m, if m is a multiple of n. Summarizing,

$$\boxed{n \text{ divides } m} \quad \text{is equivalent to} \quad \boxed{m \text{ is a multiple of } n}. \tag{1.9}$$

The statement "n divides m" is written symbolically as $n \mid m$.

It is useful to compare the two equivalent concepts of (1.9). Divisibility is most convenient for formulating mathematical claims. On the other hand, it is generally easier to prove those claims by working with the corresponding equation $m = r \cdot n$ from the relation of being a multiple. As an example, consider the proof that the divisibility relation $\mid$ on $\mathbb{Z}$ shares the reflexivity (R) and transitivity (T) properties of the relation $\leq$ on $\mathbb{R}$ (page 2).

PROPOSITION 1.4 **(Divisibility on $\mathbb{Z}$ is reflexive and transitive.)** *Let m, n, and p be integers. Then:*

(R) $m \mid m$;

(T) $\big(\ m \mid n$ *and* $n \mid p\ \big)$ *implies* $m \mid p$.

PROOF (R) For each integer m, the equation $m = 1 \cdot m$ holds, so m is a multiple of m.

(T) Since $m \mid n$, there is an integer r with $n = rm$. Since $n \mid p$, there is an integer s with $p = sn$. Then

$$p = sn = s(rm) = (sr)m$$

is a multiple of m, so $m \mid p$. ∎

However, the relation $\mid$ on $\mathbb{Z}$ is not antisymmetric. For example, $5 \mid -5$ since $-5 = (-1) \cdot 5$, and $-5 \mid 5$ since $5 = (-1) \cdot (-5)$. Nevertheless, $5 \neq -5$. The situation changes when we restrict ourselves to natural numbers. We regain all three properties: reflexivity (R), transitivity (T), and antisymmetry (A).

***PROPOSITION 1.5* (Divisibility on $\mathbb{N}$ is an order relation.)**
Let m, n, and p be natural numbers. Then:

(R) $m \mid m$;

(T) $\big(\ m \mid n$ *and* $n \mid p\ \big)$ *implies* $m \mid p$;

(A) $\big(\ m \mid n$ *and* $n \mid m\ \big)$ *implies* $m = n$.

The proof of Proposition 1.5 is assigned as Exercise 14. The proposition means that divisibility relations between natural numbers may be displayed with arrow diagrams, just like the order relations between real numbers. For example, the set

$$\{1, 2, 3, 4, 6, 12\}$$

of divisors of 12 is exhibited in Figure 1.1. The diagram explicitly displays divisibilities such as $3 \mid 6$ with arrows: $3 \longrightarrow 6$. Other relations, such as $3 \mid 12$ or $4 \mid 4$, are implicit from the transitivity and reflexivity guaranteed by Proposition 1.5.

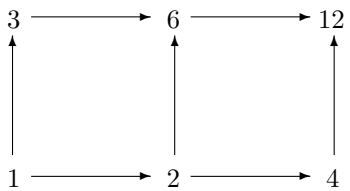


FIGURE 1.1: The positive divisors of 12.

1.4 The Division Algorithm

To check whether a positive integer d divides a given integer a (positive, negative, or zero), a formal procedure known as the *Division Algorithm* is available. Given the

`input` : a `positive integer` d (the *divisor*) and (1.10)

an `integer` a (the *dividend*), (1.11)

the Division Algorithm (Figure 1.2) produces the

`output` : an `integer` q (the *quotient*) and (1.12)

an `integer` r (the *remainder*), (1.13)

satisfying the following:

$$a = dq + r\,; \tag{1.14}$$

$$0 \leq r < d\,. \tag{1.15}$$

For example, given the divisor 5 and dividend 37, the algorithm produces 7 as the quotient and 2 as the remainder: $37 = 5 \cdot 7 + 2$, with $0 \leq 2 < 5$. Given divisor 5 and dividend -42, it produces $-42 = 5 \cdot (-9) + 3$, with $0 \leq 3 < 5$. In general, the dividend a is a multiple of the divisor d if and only if the remainder r is zero.

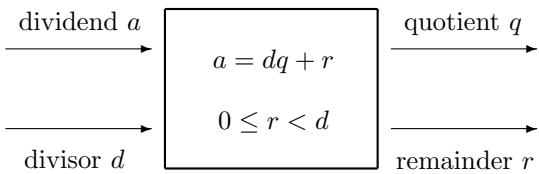


FIGURE 1.2: The Division Algorithm.

The word *dividend* in (1.11) means "the thing that is to be divided," like the profits of a company being divided among the shareholders. The word *quotient* in (1.12) is Latin for "How many times?" (the divisor d has to be added to itself to approach or equal the dividend). Then the remainder r is what is left after subtracting q times the divisor d from the dividend a.

The following proposition, with its proof, is a guarantee that the Division Algorithm will always perform as claimed. The proof relies on the use of the Well-Ordering Principle as presented in Section 1.2.

PROPOSITION 1.6

Given a dividend a as in (1.11)*, and a divisor d as in* (1.10)*, there is a unique quotient q as in* (1.12) *and a unique remainder r as in* (1.13)*, such that the equation* (1.14) *and inequalities* (1.15) *hold.*

PROOF Define a subset S of $\mathbb{N}$ by

$$S = \{a - dk \mid k \in \mathbb{Z},\ a - dk \geq 0\} \tag{1.16}$$

— the set all integers of the form $a - dk$ in which k is an element of the set $\mathbb{Z}$ of integers, and such that the inequality $a - dk \geq 0$ is satisfied.

Claim 1: The set S is nonempty.

If $a \geq 0$, then $a - d \cdot 0 = a$ is an element of S. Now d is a positive integer, so $d - 1 \geq 0$. Then if $a < 0$, we have $a - da = (-a)(d-1) \geq 0$, as a product of two nonnegative integers. Thus $a - da$ is an element of S in this case.

With Claim 1 established, we can appeal to the Well-Ordering Principle. It tells us that the nonempty subset S of $\mathbb{N}$ has a least element $\inf S$. Set

$$r = \inf S\,. \tag{1.17}$$

Since r is an element of S, we have $0 \leq r$, the left-hand inequality in (1.15). And again since r is an element of S, we know that it is of the form $r = a - dk$ for some integer k. Set the quotient q to be the integer with

$$r = a - dq\,. \tag{1.18}$$

Adding dq to both sides of this equation yields (1.14).

Claim 2: $r < d$.

Could Claim 2 possibly be false? Could it happen that $r \geq d$? Well, if so, $r - d$ is still a natural number. But by (1.18),

$$r - d = a - d(q+1)\,,$$

so $r - d$ would be a member of S strictly less than r. That would contradict (1.17), so the assumption that led to the contradiction, namely $r \geq d$, must be false. This shows that Claim 2 must be true, and verifies the right-hand inequality in (1.15).

Claim 3: The integers q and r satisfying (1.14) and (1.15) are unique.

Suppose $a = dq' + r'$ for integers q' and r' with $0 \leq r' < d$. Now $r' < r$ cannot be true, for otherwise we would have $0 \leq r' = a - dq'$ as an element of S less than r, the least element of S. Conversely, $r < r'$ cannot be true either, for then we would have $q > q'$, i.e., $(q - q') > 0$ and $(q - q') \geq 1$, with

$$r' = r + (r' - r) = r + \big((a - dq') - (a - dq)\big) = r + d(q - q') \geq d\,,$$

in contradiction to $r' < d$. Thus $r = r'$ and $q = q'$. ∎

1.5 Greatest common divisors

Let a and b be nonzero integers. A positive integer c is said to be a *common divisor* of a and b if it divides both a and b:

$$c \mid a \text{ and } c \mid b\,.$$

For example, consider the divisors of 72 displayed in Figure 1.3. It is apparent that 4 is a common divisor of 24 and 36.

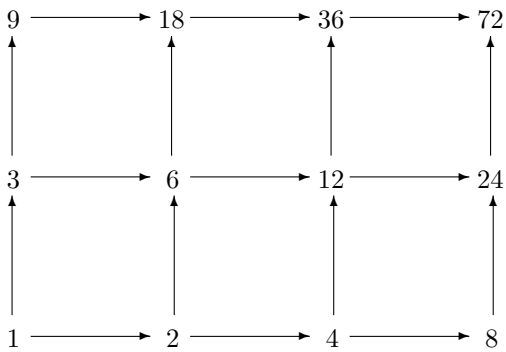


FIGURE 1.3: The positive divisors of 72.

There are other common divisors of 24 and 36, such as 2 and 12.

DEFINITION 1.7 **(Greatest common divisor, relatively prime.)** *Let a and b be nonzero integers.*

(a) *A positive integer d is the* greatest common divisor *(GCD) of a and b if*

- *d is a common divisor of a and b, and*
- *if c is a common divisor of a and b, then $c \leq d$.*

(b) *The integers a and b are said to be* relatively prime *or* coprime *if their greatest common divisor is* 1.

For instance, 12 is the greatest common divisor of 24 and 36. The numbers 8 and 9 are relatively prime. Note that 1 is coprime to every nonzero integer.

Why should the greatest common divisor of two nonzero integers a and b be guaranteed to exist? Well, the set of common divisors of a and b is a finite set

S, the intersection of the finite sets of positive divisors of a and b. (Compare Exercise 11.) The greatest common divisor is then just the maximum element of the finite set S. Since each pair a, b of nonzero integers has a uniquely defined greatest common divisor, we may use a functional notation

$$\gcd(a, b)$$

to denote that number. For example, $\gcd(24, 36) = 12$. Note that

$$\gcd(a, a) = |a|\,, \tag{1.19}$$

$$\gcd(b, a) = \gcd(a, b)\,, \tag{1.20}$$

and

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b) \tag{1.21}$$

for nonzero integers a and b (compare Exercise 26).

The defining properties of the greatest common divisor of a pair of nonzero integers a and b may be summarized as follows:

$d = \gcd(a, b)$ if and only if:

- $d \mid a$ and $d \mid b$; (1.22)
- $\big(\ c \mid a$ and $c \mid b\ \big)$ implies $c \le d$. (1.23)

1.6 The Euclidean Algorithm

Given nonzero integers a and b, how can we compute $\gcd(a, b)$? By (1.21), it is sufficient to consider the case where a and b are both positive. By (1.19), it is sufficient to consider the case where a and b are distinct. And finally, by (1.20), it is sufficient to consider the case where $a > b$. Then for positive integers $a > b$, the positive integer $\gcd(a, b)$ is produced by the *Euclidean Algorithm*.

In fact, the Euclidean Algorithm is capable of more. Borrowing terminology from matrix theory or linear algebra, define a real number z to be an *integral linear combination* of real numbers x and y if it can be expressed in the form

$$z = lx + my \tag{1.24}$$

with integer coefficients l and m. Much of the significance of integral linear combinations resides in the following simple result, whose proof is assigned as Exercise 27.

PROPOSITION 1.8 **(Common divisor divides linear combination.)** *A common divisor c of integers n and p is a divisor of each integral linear combination $ln + mp$ of n and p.*

The **Euclidean Algorithm** not only produces $\gcd(a,b)$, but if required may also be used to exhibit $\gcd(a,b)$ as an integral linear combination of a and b. Given integers $a > b > 0$, the algorithm works with a strictly decreasing sequence

$$r_{-1} > r_0 > r_1 > r_2 > \cdots > r_k > r_{k+1} = 0 \tag{1.25}$$

of natural numbers. Following the initial specification

$$r_{-1} = a \quad \text{and} \quad r_0 = b\,,$$

the natural numbers (1.25) are produced by a series of steps. For $0 \le i \le k$, Step (i) applies the Division Algorithm with r_{i-1} as the dividend and r_i as the divisor:

$$r_{i-1} = q_{i+1} r_i + r_{i+1}\,, \tag{1.26}$$

obtaining r_{i+1} as the remainder with $r_i > r_{i+1} \ge 0$ (and some integer q_{i+1} as the quotient). The Euclidean Algorithm makes its last call to the Division Algorithm in Step (k), obtaining the remainder $r_{k+1} = 0$. At that time the greatest common divisor $\gcd(a,b)$ is output as r_k, the last nonzero remainder in the list (1.25).

Why is $r_k = \gcd(a,b)$, and how is r_k produced as a linear combination of a and b.? To answer these questions, it is helpful to rewrite (1.26) as the matrix equation

$$\begin{bmatrix} r_{i-1} \\ r_i \end{bmatrix} = \begin{bmatrix} q_{i+1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix} \tag{1.27}$$

holding for $0 \le i \le k$. (Compare Section 2.3, page 28, for a review of matrix multiplication.) Note that (1.27) is an equality between 2-dimensional column vectors with integral entries. Equality of the bottom entries is trivial, while (1.26) is the equality between the top entries. Now

$$\begin{bmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{bmatrix} \begin{bmatrix} q_{i+1} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} q_{i+1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{bmatrix},$$

so (1.27) is equivalent to the matrix equation

$$\begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{bmatrix} \begin{bmatrix} r_{i-1} \\ r_i \end{bmatrix} \tag{1.28}$$

for $0 \le i \le k$. Repeated use of (1.28) gives

$$\begin{bmatrix} r_k \\ r_{k+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \begin{bmatrix} r_{-1} \\ r_0 \end{bmatrix} = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \begin{bmatrix} r_{-1} \\ r_0 \end{bmatrix}$$

for integers s and t (computed by multiplying the 2×2 matrices in the middle term), so r_k is expressed as the integral linear combination

$$r_k = s r_{-1} + t r_0 = sa + tb \tag{1.29}$$

of a and b. By Proposition 1.8, any common divisor c of a and b is a divisor of r_k, confirming that r_k satisfies the requirement (1.23) for the greatest common divisor of a and b. Finally, repeated use of (1.27) gives

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} r_{-1} \\ r_0 \end{bmatrix} = \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} q_{k+1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_k \\ r_{k+1} \end{bmatrix} = \begin{bmatrix} s' & t' \\ u' & v' \end{bmatrix} \begin{bmatrix} r_k \\ 0 \end{bmatrix}$$

for integers s', t', u', and v', so that $a = s'r_k$ and $b = u'r_k$. This means that $r_k \mid a$ and $r_k \mid b$. Thus r_k satisfies the requirement (1.22) for the greatest common divisor of a and b.

Now we know that $r_k = \gcd(a, b)$, the import of the equation (1.29) may be recorded for future reference as follows. (Compare Exercise 28.)

***PROPOSITION 1.9* (GCD as an integral linear combination.)**
Let a and b be nonzero integers. Then the greatest common divisor $\gcd(a, b)$ *may be expressed as an integral linear combination of a and b.*

***Example 1.10* (A run of the Euclidean Algorithm.)**
Consider the determination of $\gcd(7, 5)$ with the Euclidean Algorithm. The calls to the Division Algorithm are as follows:

$$\begin{aligned} &\text{Step (0)}: && 7 = 1 \cdot 5 \;+\; 2 \\ &\text{Step (1)}: && 5 = 2 \cdot 2 \;+\; 1 \\ &\text{Step (2)}: && 2 = 2 \cdot 1 \;+\; 0 \end{aligned}$$

Thus $\gcd(7, 5)$ emerges as 1, the remainder from the penultimate Step (1). The matrix equations (1.27) become

$$\begin{bmatrix} 7 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 5 \\ 2 \end{bmatrix}, \qquad \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \qquad \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

The matrix equations (1.28) become

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \qquad \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 5 \\ 2 \end{bmatrix}, \qquad \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 7 \\ 5 \end{bmatrix}.$$

Thus

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 7 \\ 5 \end{bmatrix} = \begin{bmatrix} -2 & 3 \\ 5 & -7 \end{bmatrix} \begin{bmatrix} 7 \\ 5 \end{bmatrix},$$

whence $\gcd(7, 5) = 1 = (-2) \cdot 7 + 3 \cdot 5$. □

1.7 Primes and irreducibles

The positive number 35 can be reduced to a product $5 \cdot 7$ of smaller positive numbers 5 and 7. On the other hand, neither 5 nor 7 can be reduced further. In fact, if $5 = a \cdot b$ for positive integers a and b, then $a = 1$ and $b = 5$ or $a = 5$ and $b = 1$. We define a positive integer p to be *irreducible* if $p > 1$ and

$$0 < d \mid p \quad \text{implies} \quad \big(d = 1 \text{ or } d = p \big) \tag{1.30}$$

for integers d. Irreducibility is an "internal" or "local" property of a positive integer p, only involving the finite set of positive divisors of p.

Now look outwards rather than inwards. The positive number 35 may divide a product, without necessarily dividing any of the factors in that product. For example, 35 divides $7 \cdot 10$, but 35 does not divide 7 or 10. On the other hand, 5 divides the product $7 \cdot 10$, and then 5 divides the factor 10 in the product. We define a positive integer p to be *prime* if $p > 1$ and

$$p \mid a \cdot b \quad \text{implies} \quad \big(p \mid a \ \text{ or } \ p \mid b \big) \tag{1.31}$$

for any integers a and b. Primality may be considered as an "external" or "global" property of a positive integer p, since it involves arbitrary integers a and b. The two properties are summarized as follows:

Properties of an integer $p > 1$:

(internal)	**irreducible:**	$0 < d \mid p$	implies	$\big(d = 1 \text{ or } d = p \big)$
(external)	**prime:**	$p \mid a \cdot b$	implies	$\big(p \mid a \ \text{ or } \ p \mid b \big)$

It is a feature of the integers that the internal concept of irreducibility agrees with the external concept of primality.

PROPOSITION 1.11 **("Prime" ≡ "irreducible" for integers.)** *Let $p > 1$ be an integer.*

(a) *If p is prime, then it is irreducible.*

(b) *If p is irreducible, then it is prime.*

PROOF (a): Suppose p is prime and $0 < d \mid p$, say $p = d'd$ for some positive integer d'. Then $p \mid d'd$. Since p is prime, it follows that $p \mid d'$ or $p \mid d$. In the latter case, $d \mid p$ and $p \mid d$, so $d = p$ by antisymmetry. In the former case, the same argument (replacing d by d') shows $d' = p$. Then $d = 1$.

(b): Suppose p is irreducible and $p \mid a \cdot b$, say $ab = pk$ for some integer k. Suppose p does not divide a. It will be shown that $p \mid b$. Since p is irreducible, its only positive divisors are 1 and p. Thus $\gcd(p, a) = 1$, for $\gcd(p, a) = p$ would mean $p \mid a$. Using Proposition 1.9, write $\gcd(p, a)$ as an integral linear combination

$$1 = lp + ma$$

of p and a. Postmultiplying by b gives

$$\begin{aligned} b &= lpb + mab \\ &= lpb + mpk = p(lb + mk)\,, \end{aligned}$$

so that $p \mid b$ as required. □

With Proposition 1.11 proved, prime numbers (as in Figure 1.4) may be characterized equally well by either the irreducibility (1.30) or the primality (1.31). (See the Notes to this section on page 23.)

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	161	191	193	197	199	211	223	227	229

FIGURE 1.4: The first 50 prime numbers.

There is a traditional adjective for numbers which are not prime:

***DEFINITION 1.12* (Composite numbers.)** *An integer n is said to be* composite *if $n > 1$, but n is not prime.*

Thus a number $n > 1$ is composite if it is not irreducible, i.e., if it has a nontrivial factorization $n = a \cdot b$ with integers $1 < a < n$ and $1 < b < n$.

1.8 The Fundamental Theorem of Arithmetic

In Figure 1.3, the number 72 is displayed as the product $72 = 8 \cdot 9 = 2^3 \cdot 3^2 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$ of prime numbers. The latter product may be written with the

factors in various orders, such as $72 = 2 \cdot 3 \cdot 2 \cdot 2 \cdot 3$ or $72 = 2 \cdot 3 \cdot 2 \cdot 3 \cdot 2$. But to within such reorderings of the prime factors, the factorization is unique. The *Fundamental Theorem of Arithmetic* states that every integer greater than 1 has a factorization as a product of primes, unique up to reordering of the factors.

The existence part of the theorem is stated and proved as follows.

THEOREM 1.13 **(Existence of factorizations.)**
Each integer $n > 1$ may be expressed as a product of prime numbers.

PROOF Let B be the set of integers $n > 1$ which cannot be expressed as a product of primes. If the theorem is false, then B is nonempty. In that case, the Well-Ordering Principle says that B has a least element b. Since the integer b lies in the set B, it is not itself prime (or irreducible), so it has divisors g_1 and g_2 with

$$b = g_1 g_2 \tag{1.32}$$

and $1 < g_1, g_2 < b$. Since the divisors g_1 and g_2 are strictly less than b, the least element of B, they are expressible as products of primes. But then (1.32) expresses the integer b as a product of primes, contradicting its status as a member of B. Since falsehood of the theorem leads to an inevitable contradiction, we conclude that the theorem is true. □

Implicit in the proof of Theorem 1.13 is a method, however slow, to produce the factorization of a given integer larger than 1 as a product of primes. For example, consider $b = 500$, which factorizes as $b = g_1 g_2$ with $g_1 = 50$ and $g_2 = 10$. Then $g_1 = 5 \cdot 10 = 5 \cdot 2 \cdot 5$ and $g_2 = 2 \cdot 5$, so $500 = 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5$. If b is less friendly, e.g., $b = 281957$, then one has to try dividing b in turn by successive primes $p = 2, 3, 5, 7, 11, \ldots$ up to $\sqrt{b}$ (compare Exercise 36).

We now state the uniqueness half of the fundamental theorem.

THEOREM 1.14 **(Uniqueness of factorization.)**
Suppose that $p_1, p_2, \ldots, p_r$ and $q_1, q_2 \ldots, q_s$ are primes. Then if

$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s \,, \tag{1.33}$$

$r = s$, and each p_i on the left hand side of (1.33) appears as a q_j on the right hand side of (1.33).

To prove Theorem 1.14, we will use a subsidiary result, a "lemma."

LEMMA 1.15
Suppose that $p_1, q_1, q_2, \ldots, q_s$ are primes. Then if

$$p_1 \mid q_1 \cdot q_2 \cdot \ldots \cdot q_s \,, \tag{1.34}$$

there is some $1 \leq j \leq s$ *such that* $p_1 = q_j$.

PROOF Suppose that the lemma is false. Let S be the set of natural numbers s for which there are primes $p_1, q_1, q_2, \ldots, q_s$ with (1.34) holding, but where p_1 does not appear as any q_j with $1 \leq j \leq s$. Since the lemma is false, the set S is nonempty, and thus has a least element s. Consider $p_1, q_1, q_2, \ldots, q_s$ as in (1.34) for this integer s. Now p_1 does not divide the product $q_1 \cdot q_2 \cdot \ldots \cdot q_{s-1}$, for then the minimality of s in S would mean that p_1 shows up among $q_1, q_2, \ldots, q_{s-1}$. Since p_1 is prime, and (1.34) holds, it follows that $p_1 \mid q_s$. Since $1 < p_1$ and q_s is irreducible, $p_1 = q_s$, in contradiction to the assumption. Thus the lemma is true after all. ∎

To complete the proof of Theorem 1.14, suppose (1.33) holds. Then

$$p_1 \mid q_1 \cdot q_2 \cdot \ldots \cdot q_s \,.$$

By Lemma 1.15, there is some $1 \leq j \leq s$ such that $p_1 = q_j$. Then

$$p_2 \cdot p_3 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_s \,.$$

By Lemma 1.15, p_2 cancels with some q_k from the right-hand side. Continuing in this fashion, the p_i on the left of (1.33) are paired off with the q_j on the right. In particular, the number r of factors on the left-hand side of (1.33) agrees with the number s of factors on the right.

The Fundamental Theorem of Arithmetic makes a connection between the two order relations $\leq$ and $\mid$ on the set $\mathbb{N}$ of natural numbers. Specifically, for distinct primes $p_1, p_2, \ldots, p_r$ and natural numbers $e_1, f_1, e_2, f_2, \ldots, e_r, f_r$,

$$p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r} \mid p_1^{f_1} \cdot p_2^{f_2} \cdot \ldots \cdot p_r^{f_r} \text{ if and only if } e_1 \leq f_1, \ \ldots, \ e_r \leq f_r.$$

We conclude with an application of this idea.

***DEFINITION 1.16* (Least common multiple.)** *Let* a *and* b *be nonzero integers. The* least common multiple $\operatorname{lcm}(a, b)$ *of* a *and* b *is the minimum element of the set* $S = \{m \mid m > 0\,,\ a \mid m\,,\ b \mid m\}$ *of positive common multiples of* a *and* b.

Write $\max\{e, f\}$ for the maximum of integers e and f. The Fundamental Theorem of Arithmetic yields the following result. Its proof is assigned as Exercise 39.

***PROPOSITION 1.17* (Computing the least common multiple.)** *Let* $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ *and* $b = p_1^{f_1} \cdot p_2^{f_2} \cdot \ldots \cdot p_r^{f_r}$ *for distinct primes* $p_1, p_2, \ldots, p_r$, *and natural numbers* $e_1, f_1, e_2, f_2, \ldots, e_r, f_r$. *Then*

$$\operatorname{lcm}(a, b) = p_1^{\max\{e_1, f_1\}} \cdot p_2^{\max\{e_2, f_2\}} \cdot \ldots \cdot p_r^{\max\{e_r, f_r\}} \,.$$

1.9 Exercises

1. Suppose x, y, and z are real numbers. If $x \leq y \leq z \leq x$, give a formal proof that $y = z$ by use of transitivity and antisymmetry.

2. Suppose that $x_0, x_1, \ldots, x_n$ are real numbers, with $x_0 \leq x_1 \leq \cdots \leq x_n$. If $x_n \leq x_0$, show that $x_0 = x_r$ for $1 \leq r \leq n$.

3. Why is (1.7) true?

4. Why is (1.5) true?

5. Find the least element $\inf S$ of the set S from Example 1.2.

6. Find the smallest integer n for which $2^n < n!$.

7. Let S be a nonempty subset of $\mathbb{N}$. Let s be an element of S. The intersection $\{0, 1, \ldots, s-1\} \cap S$ denotes the set of elements of S less than s.

   (a) If the intersection $\{0, 1, \ldots, s-1\} \cap S$ is empty, show that $\inf S = s$.

   (b) If the intersection $\{0, 1, \ldots, s-1\} \cap S$ is nonempty, show that $\inf S = \min(\{0, 1, \ldots, s-1\} \cap S)$.

8. Prove
$$1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$
for natural numbers n.

9. (a) Prove
$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \tag{1.35}$$
for natural numbers n by induction.

   (b) Can you prove (1.35) directly, without using induction?

10. Prove $n < 2^n$ for natural numbers n.

11. Let m be a nonzero integer.

    (a) Show that $n \mid m$ implies $|n| \leq |m|$. (In words: each divisor of a nonzero integer is no greater than that integer in absolute value.)

    (b) If you are uncomfortable with absolute values, show instead that $n \mid m$ implies $n^2 \leq m^2$.

    (c) Conclude that the set of divisors of m is finite.

12. Show that every integer divides zero.

13. There are 36 inches in a yard, and 100 centimeters in a meter.

    (a) In how many ways can a piece of wood a yard long be divided into equal pieces whose length is an integral number of inches?

    (b) In how many ways can a piece of wood a meter long be divided into equal pieces whose length is an integral number of centimeters?

14. Prove Proposition 1.5. [Hint: To prove the antisymmetry (A) that does not hold for divisibility on $\mathbb{Z}$, consider the solutions x of the equation $x^2 = 1$ in $\mathbb{Z}$ and $\mathbb{N}$.]

15. Describe the divisibility relation $|$ on the set $\mathbb{R}$ of real numbers.

16. Consider running the Division Algorithm on the inputs $a = 1$ and $d = 0$.

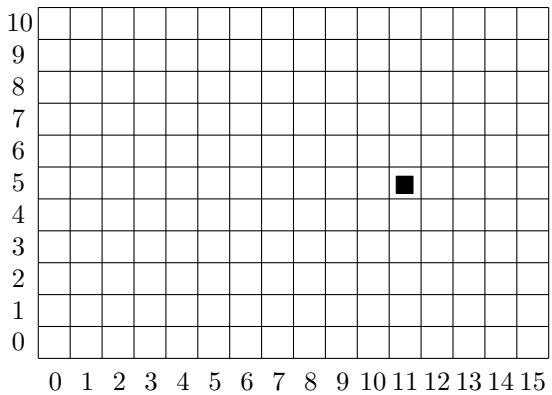
    (a) For the set S of (1.16), what is $\inf S$?

    (b) Show that a unique remainder r is obtained, but that the quotient q is not unique.

    (c) Is Proposition 1.6 contradicted?

17. Let d be a positive odd number. Show that for each integer a, there are unique integers q and r such that $a = dq + r$ with $|r| < d/2$. In other words, each integer a can be approximated by a multiple of d to within an error of less than $d/2$.

18. Consider the 16×11 rectangular array of 176 pixels in a display.



    The pixels are located by their coordinates in the array, so that the bottom left pixel has coordinates $(0, 0)$, and the top right pixel has coordinates $(15, 10)$. The pixels are addressed by the numbers from 0 to 175. The address of the pixel with coordinates (q, r) is

$$a = 11q + r\,.$$

(a) What is the address of the pixel with the black square?

(b) What are the coordinates of the pixel with address 106?

19. Let $d > 1$ be a fixed integer, known as the *base*. To represent a given positive integer n as a sequence $n = n_k n_{k-1} \dots n_2 n_1$ of digits in base d, with $0 \leq n_i < d$ for $1 \leq i \leq k$, consider the following algorithm:

    (a) Initialize with $q_0 = n$ and $i = 1$;

    (b) At Step (i), obtain $q_{i-1} = q_i d + n_i$ with the Division Algorithm;

    (c) Stop at Step (k) when $q_k = 0$;

    (d) Otherwise, replace i by $i + 1$ and return to (b).

    Show that $n = n_k d^{k-1} + n_{k-1} d^{k-2} + \ldots + n_2 d + n_1$.

20. Express the base 10 number 3817 as a *hexadecimal* (base 16) number. Use $A = 10$, $B = 11$, $C = 12$, $D = 13$, $E = 14$, $F = 15$ for the digits above 9.

21. In a certain state, persons under age 21 are not allowed into bars that serve intoxicating beverages. If 21 were read as an *octal* number (to base 8), what would be the minimum age (to the usual base 10) of persons allowed into bars?

22. In Figure 1.3:

    (a) Identify the set of positive divisors of 18.

    (b) Identify the set of positive divisors of 24.

    (c) Identify the set S of common divisors of 18 and 24.

    (d) Identify $\gcd(18, 24)$ as the largest element of the set S.

23. Find all pairs of relatively prime positive integers less than 10.

24. Show that 1 is the only positive integer that is relatively prime to every positive integer.

25. In a gearbox, gear wheel A meshes with gear wheel B. The two rotate together many times. Gear wheel A has a teeth, and gear wheel B has b teeth. Show that each tooth of A meshes with each tooth of B at some time if and only if a and b are relatively prime.

26. Prove the equalities (1.19), (1.20), and (1.21).

27. Prove Proposition 1.8.

28. Without appealing to the discussion of the Euclidean Algorithm, give a direct proof of Proposition 1.9. [Hint: Applying the Well-Ordering Principle, show that $\gcd(a, b)$ is the smallest member of the set S of positive, integral linear combinations of a and b.]

29. Let c be a positive common divisor of two nonzero integers a and b.
    (a) Show that c divides $\gcd(a, b)$.
    (b) Show that $\gcd(a, b)/c = \gcd(a/c, b/c)$.

30. For nonzero integers a, b, and c, with $c > 0$, show that $\gcd(ac, bc) = \gcd(a, b) \cdot c$.

31. Let a and b be distinct nonzero integers. Show that the greatest common divisor $\gcd(a, b)$ can be expressed in infinitely many distinct ways as an integral linear combination $\gcd(a, b) = la + mb$ of a and b.

32. Use the Euclidean Algorithm to determine $\gcd(109, 60)$, and to express it as an integral linear combination of 109 and 60.

33. Show that $2n + 1$ and $3n + 1$ are coprime for all natural numbers n.

34. Show that the Euclidean Algorithm will make at most b calls to the Division Algorithm when it computes $\gcd(a, b)$ with $a > b > 0$.

35. (a) In how many ways can 72 be expressed as an *ordered* product of three twos and two threes?
    (b) Interpret each such expression $72 = p_1p_2p_3p_4p_5$ (with $p_i = 2$ or 3) as a walk from 1 to 72 along the path

$$1 \to p_1 \to p_1p_2 \to p_1p_2p_3 \to p_1p_2p_3p_4 \to p_1p_2p_3p_4p_5 = 72$$

    in Figure 1.3.
    (c) Conversely, show that each path from 1 to 72, following the arrows at each step, determines an ordered factorization.

36. (a) Show that a composite number b has a prime divisor p with $p \leq \sqrt{b}$.
    (b) Conclude that an integer n is prime if it is not divisible by any prime less than $\sqrt{n}$.

37. Factorize $b = 281957$ as a product of primes.

38. Can you prove that $n^2 - n + 41$ is prime for each natural number n?

39. Prove Proposition 1.17.

40. For positive integers a and b, show that an integer is a multiple of both a and b if and only if it is a multiple of $\operatorname{lcm}(a, b)$.

41. Use the Fundamental Theorem of Arithmetic to obtain a formula for $\gcd(a, d)$, similar to the formula for $\operatorname{lcm}(a, b)$ given in Proposition 1.17.

42. For nonzero integers a, b, and c, show that $\gcd(a, bc) = 1$ if and only if both $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

43. For positive integers a and b, prove $a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$. [Hint: For natural numbers e and f, prove $e + f = \min\{e,f\} + \max\{e,f\}$.]

44. (a) Give an example of prime numbers p_1, p_2 and natural numbers e_1, f_1, e_2, f_2 such that

$$\operatorname{lcm}\left(p_1^{e_1}p_2^{e_2}, p_1^{f_1}p_2^{f_2}\right) \neq p_1^{\max\{e_1,f_1\}} \cdot p_2^{\max\{e_2,f_2\}}.$$

(b) Why does this not contradict Proposition 1.17?

45. (a) Let $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_r$ be the first r primes. Show that

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$$

is not divisible by any of $p_1, p_2, \ldots, p_r$.

(b) Applying Theorem 1.13 to n, deduce that there is a prime number p_s with $p_r < p_s \leq n$.

(c) Conclude that there is an infinite number of primes.

46. Let n be a positive integer. A positive integer d is said to be a *unitary divisor* of n if d divides n, and $\gcd(d, n/d) = 1$. In this case, n is said to be a unitary multiple of d.

(a) Determine the unitary divisors of 72 and 1200.

(b) Determine the least common unitary multiple of 18 and 45.

(c) Show that there is no least common unitary multiple of 3 and 9.

47. Consider a world in which the only positive numbers are the numbers

$$1, 5, 9, 13, 17, 21, 25, 29, \ldots \tag{1.36}$$

of the form $4r + 1$ for r in $\mathbb{N}$. Suppose that the numbers are only multiplied, not added.

(a) Show that the product of two numbers from the list (1.36) also appears in the list.

(b) Show that the numbers below 25 in the list (1.36) are irreducible within this alternative world.

(c) Show that 9 divides $21 \cdot 21$, but 9 does not divide 21.

(d) Conclude that in this world, the property of being prime is distinct from the property of being irreducible.

1.10 Study projects

1. For a sport competition of your choice (say one season of a particular league), determine whether the transitivity rule (1.6) and antisymmetry rule (1.7) apply.

2. Consider the problem of finding the minimum $\min S$ of a finite set S of natural numbers with n elements. Design a procedure to do this with just $n-1$ comparisons between pairs of elements from S. As inspiration, look at the brackets for a single-elimination sport competition in a league with n members. (Compare Figure 1.5 for the case $n = 6$.)

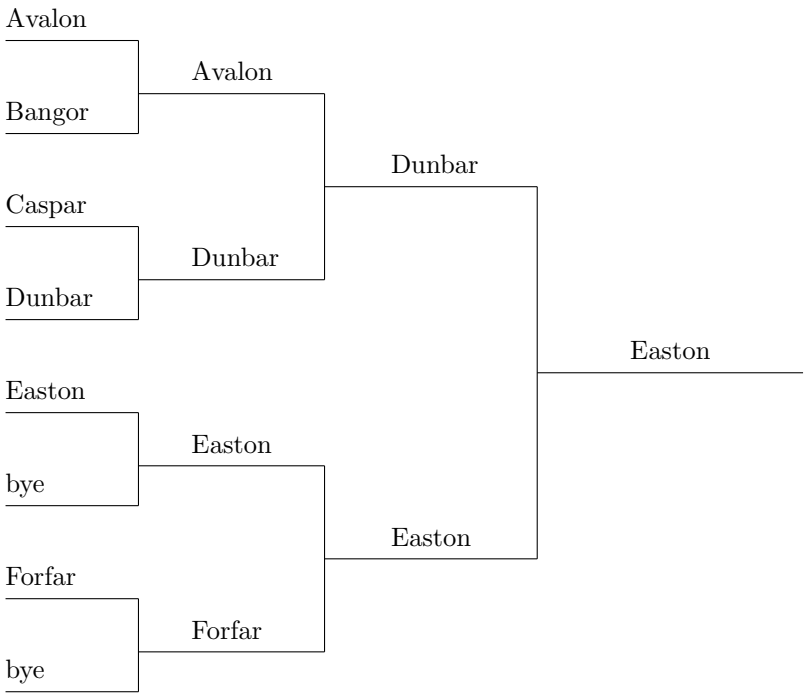


FIGURE 1.5: Brackets for a competition.

3. The number 946 is a multiple of 11. Also, the difference between the respective sums $9 + 6$ and 4 of the odd-placed and even-placed digits of 946 is (a multiple of) 11. Is this just a coincidence, or can you extend the observation to derive a quick way of recognizing multiples of 11?