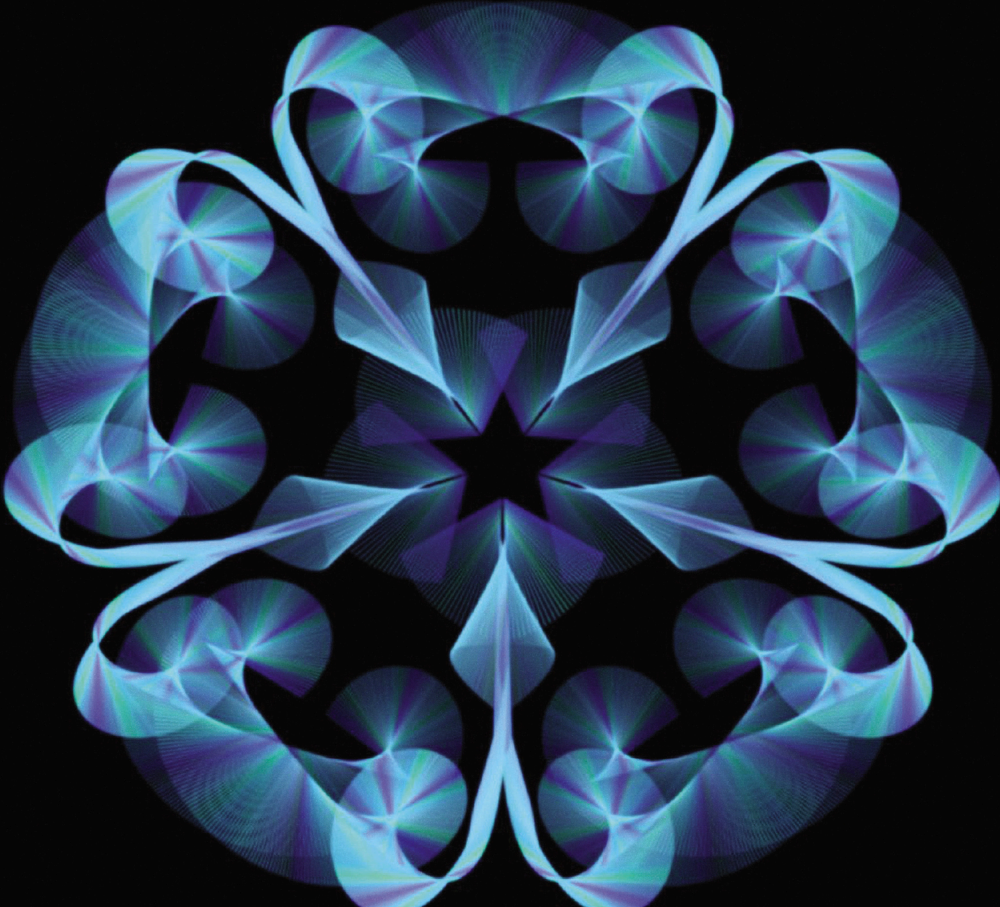
Joseph A. Gallian

CONTEMPORARY ABSTRACT ALGEBRA

Ninth Edition



Notations

(The number after the item indicates the page where the notation is defined.)

SET THEORY

$\cap_{i\in I} S_i$	intersection of sets S_i, $i \in I$
$\cup_{i\in I} S_i$	union of sets S_i, $i \in I$
$[a]$	$\{x \in S \mid x \sim a\}$, equivalence class of S containing a, 18
$\lvert s \rvert$	number of elements in the set of S

SPECIAL SETS

Z	integers, additive groups of integers, ring of integers
Q	rational numbers, field of rational numbers
Q^+	multiplicative group of positive rational numbers
F^*	set of nonzero elements of F
$\mathbf{R}$	real numbers, field of real numbers
$\mathbf{R}^+$	multiplicative group of positive real numbers
$\mathbf{C}$	complex numbers

FUNCTIONS AND ARITHMETIC

f^{-1}	inverse of the function f
$t \mid s$	t divides s, 3
$t \nmid s$	t does not divide s, 3
$\gcd(a, b)$	greatest common divisor of the integers a and b, 4
$\text{lcm}(a, b)$	least common multiple of the integers a and b, 6
$\lvert a + b \rvert$	$\sqrt{a^2 + b^2}$, 13
$\phi(a)$	image of a under ϕ, 20
$\phi: A \to B$	mapping of A to B, 21
gf, $\alpha\beta$	composite function, 21

ALGEBRAIC SYSTEMS

D_4	group of symmetries of a square, dihedral group of order 8, 33
D_n	dihedral group of order $2n$, 34
e	identity element, 43
Z_n	group $\{0, 1, \ldots, n - 1\}$ under addition modulo n, 44
$\det A$	the determinant of A, 45
$U(n)$	group of units modulo n (that is, the set of integers less than n and relatively prime to n under multiplication modulo n), 46
$\mathbf{R}^n$	$\{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in \mathbf{R}\}$, 47
$SL(2, F)$	group of 2×2 matrices over F with determinant 1, 47
$GL(2, F)$	2×2 matrices of nonzero determinants with coefficients from the field F (the general linear group), 48
g^{-1}	multiplicative inverse of g, 51
$-g$	additive inverse of g, 51
$\lvert G \rvert$	order of the group G, 60
$\lvert g \rvert$	order of the element g, 60
$H \leq G$	subgroup inclusion, 61
$H < G$	subgroup $H \neq G$, 61
$\langle a \rangle$	$\{a^n \mid n \in Z\}$, cyclic group generated by a, 65
$Z(G)$	$\{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$, the center of G, 66

$C(a)$	$\{g \in G \mid ga = ag\}$, the centralizer of a in G, 68
$\langle S \rangle$	subgroup generated by the set S, 71
$C(H)$	$\{x \in G \mid xh = hx$ for all $h \in H\}$, the centralizer of H, 71
$\phi(n)$	Euler phi function of n, 83
S_n	group of one-to-one functions from $\{1, 2, \ldots, n\}$ to itself, 95
A_n	alternating group of degree n, 95
$G \approx \overline{G}$	G and $\overline{G}$ are isomorphic, 121
ϕ_a	mapping given by $\phi_a(x) = axa^{-1}$ for all x, 128
$\mathrm{Aut}(G)$	group of automorphisms of the group G, 129
$\mathrm{Inn}(G)$	group of inner automorphisms of G, 129
aH	$\{ah \mid h \in H\}$, 138
aHa^{-1}	$\{aha^{-1} \mid h \in H\}$, 138
$\lvert G:H \rvert$	the index of H in G, 142
HK	$\{hk \mid h \in H, k \in K\}$, 144
$\mathrm{stab}_G(i)$	$\{\phi \in G \mid \phi(i) = i\}$, the stabilizer of i under the permutation group G, 146
$\mathrm{orb}_G(i)$	$\{\phi(i) \mid \phi \in G\}$, the orbit of i under the permutation group G, 146
$G_1 \oplus G_2 \oplus \cdots \oplus G_n$	external direct product of groups $G_1, G_2, \ldots, G_n$, 156
$U_k(n)$	$\{x \in U(n) \mid x \bmod k = 1\}$, 160
$H \triangleleft G$	H is a normal subgroup of G, 174
G/H	factor group, 176
$H \times K$	internal direct product of H and K, 183
$H_1 \times H_2 \times \cdots \times H_n$	internal direct product of $H_1, \ldots, H_n$, 184
$\mathrm{Ker}\,\phi$	kernel of the homomorphism ϕ, 194
$\phi^{-1}(g')$	inverse image of g' under ϕ, 196
$\phi^{-1}(\overline{K})$	inverse image of $\overline{K}$ under ϕ, 197
$Z[x]$	ring of polynomials with integer coefficients, 228
$M_2(Z)$	ring of all 2×2 matrices with integer entries, 228
$R_1 \oplus R_2 \oplus \cdots \oplus R_n$	direct sum of rings, 229
nZ	ring of multiples of n, 231
$Z[i]$	ring of Gaussian integers, 231
$U(R)$	group of units of the ring R, 233
$\mathrm{char}\,R$	characteristic of R, 240
$\langle a \rangle$	principal ideal generated by a, 250
$\langle a_1, a_2, \ldots, a_n \rangle$	ideal generated by $a_1, a_2, \ldots, a_n$, 250
R/A	factor ring, 250
$A + B$	sum of ideals A and B, 256
AB	product of ideals A and B, 257
$\mathrm{Ann}(A)$	annihilator of A, 258
$N(A)$	nil radical of A, 258
$F(x)$	field of quotients of $F[x]$, 269
$R[x]$	ring of polynomials over R, 276
$\deg f(x)$	degree of the polynomial, 278
$\Phi_p(x)$	pth cyclotomic polynomial, 294
$M_2(Q)$	ring of 2×2 matrices over Q, 330
$\langle v_1, v_2, \ldots, v_n \rangle$	subspace spanned by $v_1, v_2, \ldots, v_n$, 331
$F(a_1, a_2, \ldots, a_n)$	extension of F by $a_1, a_2, \ldots, a_n$, 341

$f'(x)$	the derivative of $f(x)$, 346
$[E:F]$	degree of E over F, 356
$\mathrm{GF}(p^n)$	Galois field of order p^n, 368
$\mathrm{GF}(p^n)^*$	nonzero elements of $\mathrm{GF}(p^n)$, 369
$\mathrm{cl}(a)$	$\{xax^{-1} \mid x \in G\}$, the conjugacy class of a, 387
n_p	the number of Sylow p-subgroups of a group, 393
$W(S)$	set of all words from S, 424
$\langle a_1, a_2, \ldots, a_n \mid w_1 = w_2 = \cdots = w_t \rangle$	group with generators $a_1, a_2, \ldots, a_n$ and relations $w_1 = w_2 = \cdots = w_t$, 426
Q_4	quarternions, 430
Q_6	dicyclic group of order 12, 430
D_∞	infinite dihedral group, 431
$\mathrm{fix}(\phi)$	$\{i \in S \mid \phi(i) = i\}$, elements fixed by ϕ, 474
$\mathrm{Cay}(S:G)$	Cayley digraph of the group G with generating set S, 482
$k * (a, b, \ldots, c)$	concatenation of k copies of $(a, b, \ldots, c)$, 490
(n, k)	linear code, k-dimensional subspace of F^n, 508
F^n	$F \oplus F \oplus \cdots \oplus F$, direct product of n copies of the field F, 508
$d(u, v)$	Hamming distance between vectors u and v, 509
$\mathrm{wt}(u)$	the number of nonzero components of the vector u (the Hamming weight of u), 509
$\mathrm{Gal}(E/F)$	the automorphism group of E fixing F, 531
E_H	fixed field of H, 531
$\Phi_n(x)$	nth cyclotomic polynomial, 548

Contemporary Abstract Algebra

Contemporary Abstract Algebra

NINTH EDITION

Joseph A. Gallian

University of Minnesota Duluth

CENGAGE Learning®

Australia • Brazil • Mexico • Singapore • United Kingdom • United States

This is an electronic version of the print textbook. Due to electronic rights restrictions, some third party content may be suppressed. Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. The publisher reserves the right to remove content from this title at any time if subsequent rights restrictions require it. For valuable information on pricing, previous editions, changes to current editions, and alternate formats, please visit www.cengage.com/highered to search by ISBN#, author, title, or keyword for materials in your areas of interest.

Important Notice: Media content referenced within the product description or the product text may not be available in the eBook version.

CENGAGE Learning

Contemporary Abstract Algebra, Ninth Edition
Joseph A. Gallian

Product Director: Terry Boyle

Product Manager: Richard Stratton

Content Developer: Spencer Arritt

Product Assistant: Kathryn Schrumpf

Marketing Manager: Ana Albinson

Sr. Content Project Manager: Tanya Nigh

Art Director: Vernon Boes

Manufacturing Planner: Doug Bertke

Production Service and Compositor: Lumina Datamatics Inc.

Photo and Text Researcher: Lumina Datamatics Inc.

Text Designer: Diane Beasley

Cover Designer: Terri Wright Design

Cover image: Complex Flows by Anne Burns

Library of Congress Control Number: 2015954307

ISBN: 978-1-305-65796-0

Cengage Learning
20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com.**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

To learn more about Cengage Learning Solutions, visit **www.cengage.com.**

Purchase any of our products at your local college store or at our preferred online store **www.cengagebrain.com.**

Printed in the United States of America
Print Number: 01 Print Year: 2015

In memory of my brother.

Contents

Preface

Set your pace to a stroll. Stop whenever you want. Interrupt, jump back and forth, I won't mind. This book should be as easy as laughter. It is stuffed with small things to take away. Please help yourself.

Willis Goth Regier, *In Praise of Flattery, 2007*

Although I wrote the first edition of this book more than thirty years ago, my goals for it remain the same. I want students to receive a solid introduction to the traditional topics. I want readers to come away with the view that abstract algebra is a contemporary subject–that its concepts and methodologies are being used by working mathematicians, computer scientists, physicists, and chemists. I want students to see the connections between abstract algebra and number theory and geometry. I want students to be able to do computations and to write proofs. I want students to enjoy reading the book. And I want convey to the reader my enthusiasm for this beautiful subject.

Educational research has shown that an effective way of learning mathematics is to interweave worked-out examples and practice problems. Thus, I have made examples and exercises the heart of the book. The examples elucidate the definitions, theorems, and proof techniques. The exercises facilitate understanding, provide insight, and develop the ability of the students to do proofs. There is a large number of exercises ranging from straight forward to difficult and enough at each level so that instructors have plenty to choose from that are most appropriate for their students. The exercises often foreshadow definitions, concepts, and theorems to come. Many exercises focus on special cases and ask the reader to generalize. Generalizing is a skill that students should develop but rarely do. Even if an instructor chooses not to spend class time on the applications in the book, I feel that having them there demonstrates to students the utility of the theory.

Changes for the ninth edition include new exercises, new examples, new biographies, new quotes, new appliactions, and a freshening of the historical notes and biographies from the 8th edition. These changes accentuate and enhance the hallmark features that have made previous editions of the book a comprehensive, lively, and engaging introduction to the subject:

- Extensive coverage of groups, rings, and fields, plus a variety of non-traditional special topics
- A good mixture of more nearly 1700 computational and theoretical exercises appearing in each chapter that synthesize concepts from multiple chapters
- Back-of-the-book skeleton solutions and hints to the odd-numbered exercises
- Worked-out examples– totaling more than 300–ranging from routine computations to quite challenging
- Computer exercises that utilize interactive software available on my website that stress guessing and making conjectures
- A large number of applications from scientific and computing fields, as well as from everyday life
- Numerous historical notes and biographies that spotlight the people and events behind the mathematics
- Motivational and humorous quotations.
- More than 275 figures, photographs, tables, and reproductions of currency that honor mathematicians
- Annotated suggested readings for interesting further exploration of topics.

Cengage's book companion site www.cengage.com/math/gallian includes an instructor's solution manual with detailed solutions for all exercises and other resources. The website www.d.umn.edu/~jgallian also offers a wealth of additional online resources supporting the book, including:

- True/false questions with comments
- Flash cards
- Essays on learning abstract algebra, doing proofs, and reasons why abstract algebra is a valuable subject to learn
- Links to abstract algebra-related websites and software packages and much, much more.

Additionally, Cengage offers a Student Solutions Manual, available for purchase separately, with detailed solutions to the odd-numbered exercises in the book (ISBN13: 978-1-305-65797-7; ISBN10: 1-305-65797-7)

I wish to thank Roger Lipsett for serving as accuracy checker and my UMD colleague Robert McFarland for giving me a number of exercises that are in this edition. I am indebted to Spencer Arritt, Content Developer at Cengage Learning, for his excellent work on this edition. My appreciation also goes to Richard Stratton, Kate Schrumpf, Christina Ciaramella, Nick Barrows, Brittani Morgan, and Tanya Nigh from Cengage. Finally, I am grateful for the help of Manoj Chander and the composition work of the whole team at Lumina Datamatics.

Contemporary Abstract Algebra

PART 1

Integers and Equivalence Relations

For online student resources, visit this textbook's website at www.CengageBrain.com

0 Preliminaries

When we see it [modular arithmetic] for the first time, it looks so abstract that it seems impossible something like this could have any real-world applications.

Edward Frenkel, *Love and Math: The Heart of Hidden Reality*

The whole of science is nothing more than a refinement of everyday thinking.

Albert Einstein, *Physics and Reality*

Properties of Integers

Much of abstract algebra involves properties of integers and sets. In this chapter we collect the properties we need for future reference.

An important property of the integers, which we will often use, is the so-called Well Ordering Principle. Since this property cannot be proved from the usual properties of arithmetic, we will take it as an axiom.

Well Ordering Principle

Every nonempty set of positive integers contains a smallest member.

The concept of divisibility plays a fundamental role in the theory of numbers. We say a nonzero integer t is a *divisor* of an integer s if there is an integer u such that $s = tu$. In this case, we write $t \mid s$ (read "t divides s"). When t is not a divisor of s, we write $t \nmid s$. A *prime* is a positive integer greater than 1 whose only positive divisors are 1 and itself. We say an integer s is a *multiple* of an integer t if there is an integer u such that $s = tu$ or, equivalently, if t is a divisor of s.

As our first application of the Well Ordering Principle, we establish a fundamental property of integers that we will use often.

Theorem 0.1 Division Algorithm

Let a and b be integers with $b > 0$. Then there exist unique integers q and r with the property that $a = bq + r$, where $0 \leq r < b$.

PROOF We begin with the existence portion of the theorem. Consider the set $S = \{a - bk \mid k \text{ is an integer and } a - bk \geq 0\}$. If $0 \in S$, then b divides a and we may obtain the desired result with $q = a/b$ and $r = 0$. Now assume $0 \notin S$. Since S is nonempty [if $a > 0$, $a - b \cdot 0 \in S$; if $a < 0$, $a - b(2a) = a(1 - 2b) \in S$; $a \neq 0$ since $0 \notin S$], we may apply the Well Ordering Principle to conclude that S has a smallest member, say $r = a - bq$. Then $a = bq + r$ and $r \geq 0$, so all that remains to be proved is that $r < b$.

If $r \geq b$, then $a - b(q + 1) = a - bq - b = r - b \geq 0$, so that $a - b(q + 1) \in S$. But $a - b(q + 1) < a - bq$, and $a - bq$ is the *smallest* member of S. So, $r < b$.

To establish the uniqueness of q and r, let us suppose that there are integers q, q', r, and r' such that

$$a = bq + r, \quad 0 \leq r < b, \quad \text{and} \quad a = bq' + r', \quad 0 \leq r' < b.$$

For convenience, we may also suppose that $r' \geq r$. Then $bq + r = bq' + r'$ and $b(q - q') = r' - r$. So, b divides $r' - r$ and $0 \leq r' - r \leq r' < b$. It follows that $r' - r = 0$, and therefore $r' = r$ and $q = q'$. ▮

The integer q in the division algorithm is called the *quotient* upon dividing a by b; the integer r is called the *remainder* upon dividing a by b.

▮ **EXAMPLE 1** For $a = 17$ and $b = 5$, the division algorithm gives $17 = 5 \cdot 3 + 2$; for $a = -23$ and $b = 6$, the division algorithm gives $-23 = 6(-4) + 1$. ▮

Definitions Greatest Common Divisor, Relatively Prime Integers

The *greatest common divisor* of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by gcd(a, b). When gcd(a, b) = 1, we say a and b are *relatively prime*.

The following property of the greatest common divisor of two integers plays a critical role in abstract algebra. The proof provides an application of the division algorithm and our second application of the Well Ordering Principle.

▮ Theorem 0.2 GCD Is a Linear Combination

For any nonzero integers a and b, there exist integers s and t such that gcd(a, b) = as + bt. Moreover, gcd(a, b) is the smallest positive integer of the form as + bt.

PROOF Consider the set $S = \{am + bn \mid m, n \text{ are integers and } am + bn > 0\}$. Since S is obviously nonempty (if some choice of m and

n makes $am + bn < 0$, then replace m and n by $-m$ and $-n$), the Well Ordering Principle asserts that S has a smallest member, say, $d = as + bt$. We claim that $d = \gcd(a, b)$. To verify this claim, use the division algorithm to write $a = dq + r$, where $0 \leq r < d$. If $r > 0$, then $r = a - dq = a - (as + bt)q = a - asq - btq = a(1 - sq) + b(-tq) \in S$, contradicting the fact that d is the smallest member of S. So, $r = 0$ and d divides a. Analogously (or, better yet, by symmetry), d divides b as well. This proves that d is a common divisor of a and b. Now suppose d' is another common divisor of a and b and write $a = d'h$ and $b = d'k$. Then $d = as + bt = (d'h)s + (d'k)t = d'(hs + kt)$, so that d' is a divisor of d. Thus, among all common divisors of a and b, d is the greatest. ■

The special case of Theorem 0.2 when a and b are relatively prime is so important in abstract algebra that we single it out as a corollary.

Corollary

If a and b are relatively prime, then there exist integers s and t such that $as + bt = 1$.

EXAMPLE 2 $\gcd(4, 15) = 1$; $\gcd(4, 10) = 2$; $\gcd(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) = 2 \cdot 3^2$. Note that 4 and 15 are relatively prime, whereas 4 and 10 are not. Also, $4 \cdot 4 + 15(-1) = 1$ and $4(-2) + 10 \cdot 1 = 2$. ■

The next lemma is frequently used. It appeared in Euclid's *Elements*.

Euclid's Lemma $p \mid ab$ Implies $p \mid a$ or $p \mid b$

If p is a prime that divides ab, then p divides a or p divides b.

PROOF Suppose p is a prime that divides ab but does not divide a. We must show that p divides b. Since p does not divide a, there are integers s and t such that $1 = as + pt$. Then $b = abs + ptb$, and since p divides the right-hand side of this equation, p also divides b. ■

Note that Euclid's Lemma may fail when p is not a prime, since $6 \mid (4 \cdot 3)$ but $6 \nmid 4$ and $6 \nmid 3$.

Our next property shows that the primes are the building blocks for all integers. We will often use this property without explicitly saying so.

Theorem 0.3 Fundamental Theorem of Arithmetic

Every integer greater than 1 *is a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if $n = p_1p_2 \cdots p_r$ and $n = q_1q_2 \cdots q_s$, where the p's and q's are primes, then $r = s$ and, after renumbering the q's, we have $p_i = q_i$ for all i.*

We will prove the existence portion of Theorem 0.3 later in this chapter (Example 11). The uniqueness portion is a consequence of Euclid's Lemma (Exercise 31).

Another concept that frequently arises is that of the least common multiple of two integers.

Definition Least Common Multiple

The *least common multiple* of two nonzero integers *a* and *b* is the smallest positive integer that is a multiple of both *a* and *b*. We will denote this integer by lcm(*a*, *b*).

We leave it as an exercise (Exercise 10) to prove that every common multiple of *a* and *b* is a multiple of lcm(*a*, *b*).

EXAMPLE 3 $\text{lcm}(4, 6) = 12$; $\text{lcm}(4, 8) = 8$; $\text{lcm}(10, 12) = 60$; $\text{lcm}(6, 5) = 30$; $\text{lcm}(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) = 2^2 \cdot 3^3 \cdot 5 \cdot 7^2$. ∎

Modular Arithmetic

Another application of the division algorithm that will be important to us is modular arithmetic. Modular arithmetic is an abstraction of a method of counting that you often use. For example, if it is now September, what month will it be 25 months from now? Of course, the answer is October, but the interesting fact is that you didn't arrive at the answer by starting with September and counting off 25 months. Instead, without even thinking about it, you simply observed that $25 = 2 \cdot 12 + 1$, and you added 1 month to September. Similarly, if it is now Wednesday, you know that in 23 days it will be Friday. This time, you arrived at your answer by noting that $23 = 7 \cdot 3 + 2$, so you added 2 days to Wednesday instead of counting off 23 days. If your electricity is off for 26 hours, you must advance your clock 2 hours, since $26 = 2 \cdot 12 + 2$. Surprisingly, this simple idea has numerous important applications in mathematics and computer science. You will see a few of them in this section. The following notation is convenient.

When $a = qn + r$, where q is the quotient and r is the remainder upon dividing a by n, we write $a \bmod n = r$. Thus,

$$\begin{aligned}
3 \bmod 2 &= 1 \text{ since } 3 = 1 \cdot 2 + 1,\\
6 \bmod 2 &= 0 \text{ since } 6 = 3 \cdot 2 + 0,\\
11 \bmod 3 &= 2 \text{ since } 11 = 3 \cdot 3 + 2,\\
62 \bmod 85 &= 62 \text{ since } 62 = 0 \cdot 85 + 62,\\
-2 \bmod 15 &= 13 \text{ since } -2 = (-1)15 + 13.
\end{aligned}$$

In general, if a and b are integers and n is a positive integer, then $a \bmod n = b \bmod n$ if and only if n divides $a - b$ (Exercise 7).

In our applications, we will use addition and multiplication mod n. When you wish to compute $ab \bmod n$ or $(a + b) \bmod n$, and a or b is greater than n, it is easier to "mod first." For example, to compute $(27 \cdot 36) \bmod 11$, we note that $27 \bmod 11 = 5$ and $36 \bmod 11 = 3$, so $(27 \cdot 36) \bmod 11 = (5 \cdot 3) \bmod 11 = 4$. (See Exercise 9.)

Modular arithmetic is often used in assigning an extra digit to identification numbers for the purpose of detecting forgery or errors. We present two such applications.

▮ EXAMPLE 4 The United States Postal Service money order shown in Figure 0.1 has an identification number consisting of 10 digits together with an extra digit called a *check*. The check digit is the 10-digit number modulo 9. Thus, the number 3953988164 has the check digit 2, since

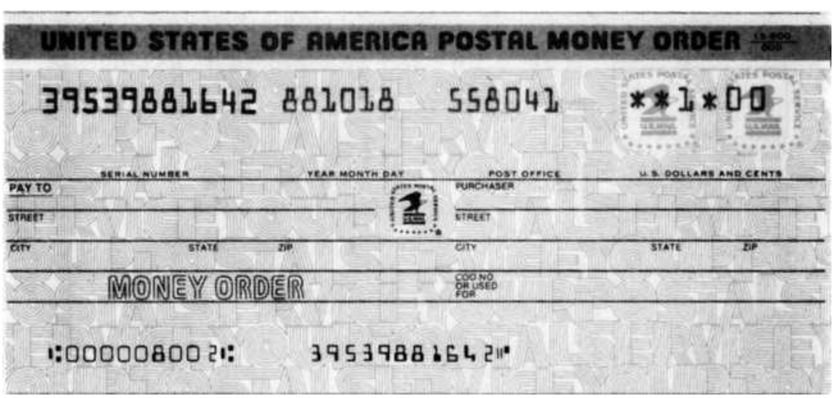


Figure 0.1

3953988164 mod 9 = 2.† If the number 39539881642 were incorrectly entered into a computer (programmed to calculate the check digit) as, say, 39559881642 (an error in the fourth position), the machine would calculate the check digit as 4, whereas the entered check digit would be 2. Thus, the error would be detected. ∎

∎ **EXAMPLE 5** Airline companies, the United Parcel Service, and the rental-car companies Avis and National use the mod 7 values of identification numbers to assign check digits. Thus, the identification number 00121373147367 (see Figure 0.2) has the check digit 3 appended

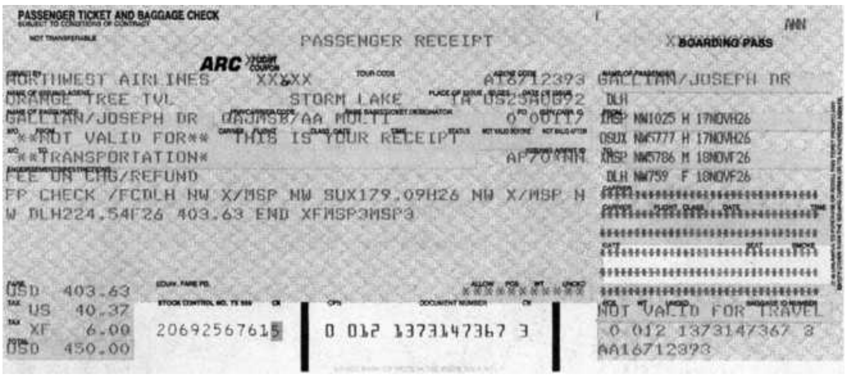


Figure 0.2

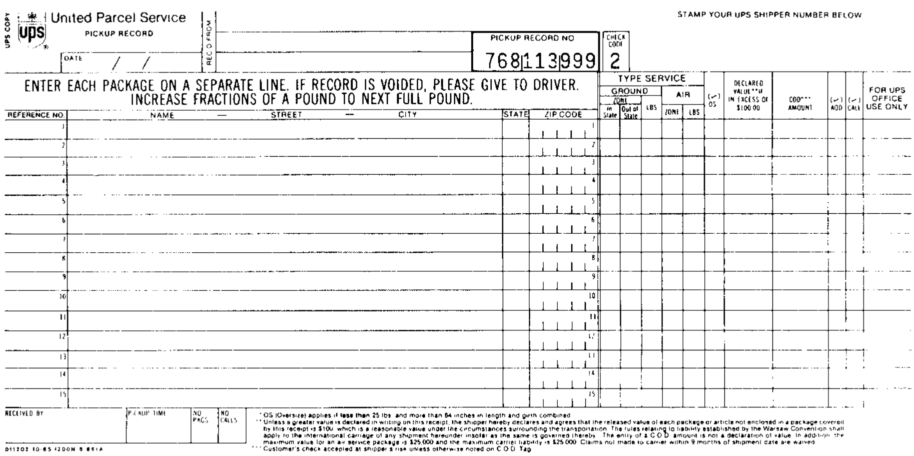


Figure 0.3

---

†The value of N mod 9 is easy to compute with a calculator. If $N = 9q + r$, where r is the remainder upon dividing N by 9, then on a calculator screen $N \div 9$ appears as $q.rrrrr\ldots$, so the first decimal digit is the check digit. For example, $3953988164 \div 9 = 439332018.222$, so 2 is the check digit. If N has too many digits for your calculator, replace N by the sum of its digits and divide that number by 9. Thus, 3953988164 mod 9 = 56 mod 9 = 2. The value of 3953988164 mod 9 can also be computed by searching Google for "3953988164 mod 9."

to it because 121373147367 mod 7 = 3. Similarly, the UPS pickup record number 768113999, shown in Figure 0.3, has the check digit 2 appended to it. ▮

The methods used by the Postal Service and the airline companies do not detect all single-digit errors (see Exercises 41 and 45). However, detection of all single-digit errors, as well as nearly all errors involving the transposition of two adjacent digits, is easily achieved. One method that does this is the one used to assign the so-called Universal Product Code (UPC) to most retail items (see Figure 0.4). A UPC identification number has 12 digits. The first six digits identify the manufacturer, the next five identify the product, and the last is a check. (For many items, the 12th digit is not printed, but it is always bar-coded.) In Figure 0.4, the check digit is 8.

Figure 0.4

To explain how the check digit is calculated, it is convenient to introduce the dot product notation for two k-tuples:

$$(a_1, a_2, \ldots, a_k) \cdot (w_1, w_2, \ldots, w_k) = a_1w_1 + a_2w_2 + \cdots + a_kw_k.$$

An item with the UPC identification number $a_1a_2 \cdots a_{12}$ satisfies the condition

$$(a_1, a_2, \ldots, a_{12}) \cdot (3, 1, 3, 1, \ldots, 3, 1) \bmod 10 = 0.$$

To verify that the number in Figure 0.4 satisfies this condition, we calculate

$$\begin{aligned}(0 \cdot 3 + 2 \cdot 1 + 1 \cdot 3 + 0 \cdot 1 + 0 \cdot 3 + 0 \cdot 1 + 6 \cdot 3 + 5 \cdot 1 \\ + 8 \cdot 3 + 9 \cdot 1 + 7 \cdot 3 + 8 \cdot 1) \bmod 10 = 90 \bmod 10 = 0.\end{aligned}$$

The fixed k-tuple used in the calculation of check digits is called the *weighting vector.*

Now suppose a single error is made in entering the number in Figure 0.4 into a computer. Say, for instance, that 021000958978 is