

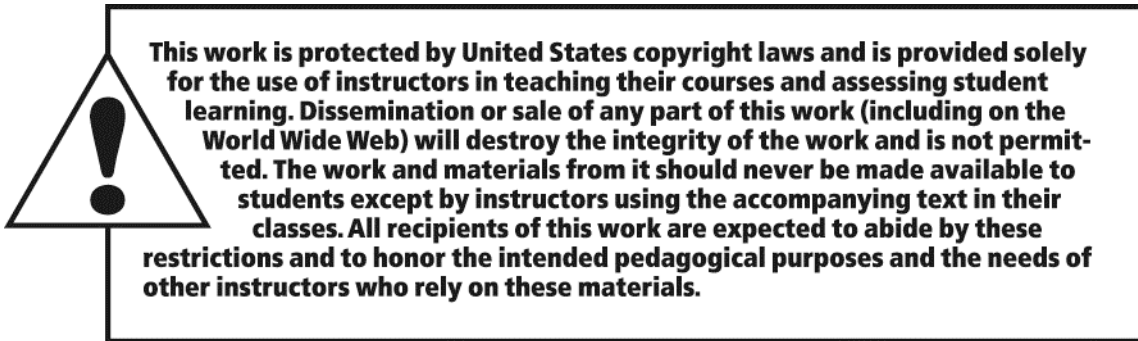
ONLINE
INSTRUCTOR'S
SOLUTIONS MANUAL

ELEMENTARY NUMBER THEORY
AND ITS APPLICATIONS
SIXTH EDITION

Kenneth Rosen
Monmouth University

Addison-Wesley
is an imprint of

PEARSON



The author and publisher of this book have used their best efforts in preparing this book. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness. The author and publisher make no warranty of any kind, expressed or implied, with regard to these programs or the documentation contained in this book. The author and publisher shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of these programs.

Reproduced by Pearson Addison-Wesley from electronic files supplied by the author.

Copyright © 2011, 2005, 2000 Pearson Education, Inc.
Publishing as Addison-Wesley, 75 Arlington Street, Boston, MA 02116.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. Printed in the United States of America.

ISBN-13: 978-0-321-53801-7
ISBN-10: 0-321-53801-3

Addison-Wesley
is an imprint of



www.pearsonhighered.com

Contents

1

| | |
|--|-----|
| Chapter 1. The Integers | 1 |
| 1.1. Numbers and Sequences | 1 |
| 1.2. Sums and Products | 7 |
| 1.3. Mathematical Induction | 10 |
| 1.4. The Fibonacci Numbers | 14 |
| 1.5. Divisibility | 19 |
| Chapter 2. Integer Representations and Operations | 25 |
| 2.1. Representations of Integers | 25 |
| 2.2. Computer Operations with Integers | 29 |
| 2.3. Complexity and Integer Operations | 31 |
| Chapter 3. Primes and Greatest Common Divisors | 35 |
| 3.1. Prime Numbers | 35 |
| 3.2. The Distribution of Primes | 38 |
| 3.3. Greatest Common Divisors and their Properties | 44 |
| 3.4. The Euclidean Algorithm | 49 |
| 3.5. The Fundamental Theorem of Arithmetic | 53 |
| 3.6. Factorization Methods and the Fermat Numbers | 63 |
| 3.7. Linear Diophantine Equations | 66 |
| Chapter 4. Congruences | 71 |
| 4.1. Introduction to Congruences | 71 |
| 4.2. Linear Congruences | 78 |
| 4.3. The Chinese Remainder Theorem | 82 |
| 4.4. Solving Polynomial Congruences | 86 |
| 4.5. Systems of Linear Congruences | 89 |
| 4.6. Factoring Using the Pollard Rho Method | 91 |
| Chapter 5. Applications of Congruences | 93 |
| 5.1. Divisibility Tests | 93 |
| 5.2. The Perpetual Calendar | 98 |
| 5.3. Round-Robin Tournaments | 101 |
| 5.4. Hashing Functions | 103 |
| 5.5. Check Digits | 104 |
| Chapter 6. Some Special Congruences | 111 |
| 6.1. Wilson's Theorem and Fermat's Little Theorem | 111 |
| 6.2. Pseudoprimes | 115 |
| 6.3. Euler's Theorem | 117 |
| Chapter 7. Multiplicative Functions | 121 |
| 7.1. The Euler Phi-Function | 121 |
| 7.2. The Sum and Number of Divisors | 127 |
| 7.3. Perfect Numbers and Mersenne Primes | 133 |
| 7.4. Möbius Inversion | 137 |
| 7.5. Partitions | 141 |

| | |
|---|-----|
| Chapter 8. Cryptology | 151 |
| 8.1. Character Ciphers | 151 |
| 8.2. Block and Stream Ciphers | 152 |
| 8.3. Exponentiation Ciphers | 158 |
| 8.4. Public Key Cryptography | 159 |
| 8.5. Knapsack Ciphers | 161 |
| 8.6. Cryptographic Protocols and Applications | 162 |
| Chapter 9. Primitive Roots | 165 |
| 9.1. The Order of an Integer and Primitive Roots | 165 |
| 9.2. Primitive Roots for Primes | 168 |
| 9.3. The Existence of Primitive Roots | 171 |
| 9.4. Discrete Logarithms and Index Arithmetic | 173 |
| 9.5. Primality Tests Using Orders of Integers and Primitive Roots | 176 |
| 9.6. Universal Exponents | 178 |
| Chapter 10. Applications of Primitive Roots and the Order of an Integer | 181 |
| 10.1. Pseudorandom Numbers | 181 |
| 10.2. The ElGamal Cryptosystem | 183 |
| 10.3. An Application to the Splicing of Telephone Cables | 184 |
| Chapter 11. Quadratic Residues | 187 |
| 11.1. Quadratic Residues and Nonresidues | 187 |
| 11.2. The Law of Quadratic Reciprocity | 194 |
| 11.3. The Jacobi Symbol | 199 |
| 11.4. Euler Pseudoprimes | 202 |
| 11.5. Zero-Knowledge Proofs | 203 |
| Chapter 12. Decimal Fractions and Continued Fractions | 205 |
| 12.1. Decimal Fractions | 205 |
| 12.2. Finite Continued Fractions | 208 |
| 12.3. Infinite Continued Fractions | 212 |
| 12.4. Periodic Continued Fractions | 214 |
| 12.5. Factoring Using Continued Fractions | 218 |
| Chapter 13. Some Nonlinear Diophantine Equations | 221 |
| 13.1. Pythagorean Triples | 221 |
| 13.2. Fermat's Last Theorem | 224 |
| 13.3. Sums of Squares | 227 |
| 13.4. Pell's Equation | 230 |
| 13.5. Congruent Numbers | 231 |
| Chapter 14. The Gaussian Integers | 239 |
| 14.1. Gaussian Integers and Gaussian Primes | 239 |
| 14.2. Greatest Common Divisors and Unique Factorization | 247 |
| 14.3. Gaussian Integers and Sums of Squares | 256 |
| Appendix A. Axioms for the Set of Integers | 261 |
| Appendix B. Binomial Coefficients | 263 |

CHAPTER 1

The Integers

1.1. Numbers and Sequences

- 1.1.1. a.** The set of integers greater than 3 is well-ordered. Every subset of this set is also a subset of the set of positive integers, and hence must have a least element.
- b.** The set of even positive integers is well-ordered. Every subset of this set is also a subset of the set of positive integers, and hence must have a least element.
- c.** The set of positive rational numbers is not well-ordered. This set does not have a least element. If a/b were the least positive rational number then $a/(b+a)$ would be a smaller positive rational number, which is a contradiction.
- d.** The set of positive rational numbers of the form $a/2$ is well-ordered. Consider a subset of numbers of this form. The set of numerators of the numbers in this subset is a subset of the set of positive integers, so it must have a least element b . Then $b/2$ is the least element of the subset.
- e.** The set of nonnegative rational numbers is not well-ordered. The set of positive rational numbers is a subset with no least element, as shown in part c.
- 1.1.2.** Let S be the set of all positive integers of the form $a - bk$. S is not empty because $a - b(-1) = a + b$ is a positive integer. Then the well-ordering principle implies that S has a least element, which is the number we're looking for.
- 1.1.3.** Suppose that x and y are rational numbers. Then $x = a/b$ and $y = c/d$, where a, b, c , and d are integers with $b \neq 0$ and $d \neq 0$. Then $xy = (a/b) \cdot (c/d) = ac/bd$ and $x + y = a/b + c/d = (ad + bc)/bd$ where $bd \neq 0$. Because both $x + y$ and xy are ratios of integers, they are both rational.
- 1.1.4. a.** Suppose that x is rational and y is irrational. Then there exist integers a and b such that $x = \frac{a}{b}$ where a and b are integers with $b \neq 0$. Suppose that $x + y$ is rational. Then there exist integers c and d with $d \neq 0$ such that $x + y = \frac{c}{d}$. This implies that $y = (x + y) - x = (c/d) - (a/b) = (ad - bc)/bd$, which means that y is rational, a contradiction. Hence $x + y$ is irrational.
- b.** This is false. A counterexample is given by $\sqrt{2} + (-\sqrt{2}) = 0$.
- c.** This is false. A counterexample is given by $0 \cdot \sqrt{2} = 0$.
- d.** This is false. A counterexample is given by $\sqrt{2} \cdot \sqrt{2} = 2$.
- 1.1.5.** Suppose that $\sqrt{3}$ were rational. Then there would exist positive integers a and b with $\sqrt{3} = a/b$. Consequently, the set $S = \{k\sqrt{3} \mid k \text{ and } k\sqrt{3} \text{ are positive integers}\}$ is nonempty because $a = b\sqrt{3}$. Therefore, by the well-ordering property, S has a smallest element, say $s = t\sqrt{3}$. We have $s\sqrt{3} - s = s\sqrt{3} - t\sqrt{3} = (s - t)\sqrt{3}$. Because $s\sqrt{3} = 3t$ and s are both integers, $s\sqrt{3} - s = (s - t)\sqrt{3}$ must also be an integer. Furthermore, it is positive, because $s\sqrt{3} - s = s(\sqrt{3} - 1)$ and $\sqrt{3} > 1$. It is less than s because $s = t\sqrt{3}$, $s\sqrt{3} = 3t$, and $\sqrt{3} < 3$. This contradicts the choice of s as the smallest positive integer in S . It follows that $\sqrt{3}$ is irrational.

- 1.1.6.** Let S be a set of negative integers. Then the set $T = \{-s : s \in S\}$ is a set of positive integers. By the well-ordering principle, T has a least element t_0 . We prove that $-t_0$ is a greatest element of S . First note that because $t_0 \in T$, then $t_0 = -s_0$ for some $s_0 \in S$. Then $-t_0 = s_0 \in S$. Second, if $s \in S$, then $-s \in T$, so $t_0 \leq -s$. Multiplying by -1 yields $s \leq -t_0$. Because the choice of s was arbitrary, we see that $-t_0$ is greater than or equal to every element of S .
- 1.1.7. a.** Because $0 \leq 1/4 < 1$, we have $[1/4] = 0$.
- b.** Because $-1 \leq -3/4 < 0$, we have $[-3/4] = -1$.
- c.** Because $3 \leq 22/7 < 4$, we have $[22/7] = 3$.
- d.** Because $-2 \leq -2 < -1$, we have $[-2] = -2$.
- e.** We compute $[1/2 + [1/2]] = [1/2 + 0] = [1/2] = 0$.
- f.** We compute $[-3 + [-1/2]] = [-3 - 1] = [-4] = -4$.
- 1.1.8. a.** Because $-1 \leq -1/4 < 0$, we have $[-1/4] = -1$.
- b.** Because $-4 \leq -22/7 < -3$, we have $[-22/7] = -4$.
- c.** Because $1 \leq 5/4 < 2$, we have $[5/4] = 1$.
- d.** We compute $[[1/2]] = [0] = 0$.
- e.** We compute $[3/2 + [-3/2]] = [1 + (-2)] = [-1] = -1$.
- f.** We compute $[3 - [1/2]] = [3 - 0] = [3] = 3$.
- 1.1.9. a.** Because $[8/5] = 1$, we have $\{8/5\} = 8/5 - [8/5] = 8/5 - 1 = 3/5$.
- b.** Because $[1/7] = 0$, we have $\{1/7\} = 1/7 - [1/7] = 1/7 - 0 = 1/7$.
- c.** Because $[-11/4] = -3$, we have $\{-11/4\} = -11/4 - [-11/4] = -11/4 - (-3) = 1/4$.
- d.** Because $[7] = 7$, we have $\{7\} = 7 - [7] = 7 - 7 = 0$.
- 1.1.10. a.** Because $[-8/5] = -2$, we have $\{-8/5\} = -8/5 - [-8/5] = -8/5 - (-2) = 2/5$.
- b.** Because $[22/7] = 3$, we have $\{22/7\} = 22/7 - [22/7] = 22/7 - 3 = 1/7$.
- c.** Because $[-1] = -1$, we have $\{-1\} = -1 - [-1] = -1 - (-1) = 0$.
- d.** Because $[-1/3] = -1$, we have $\{-1/3\} = -1/3 - [-1/3] = -1/3 - (-1) = 2/3$.
- 1.1.11.** If x is an integer, then $[x] + [-x] = x - x = 0$. Otherwise, $x = z + r$, where z is an integer and r is a real number with $0 < r < 1$. In this case, $[x] + [-x] = [z + r] + [-z - r] = z + (-z - 1) = -1$.
- 1.1.12.** Let $x = [x] + r$ where $0 \leq r < 1$. We consider two cases. First suppose that $r < \frac{1}{2}$. Then $x + \frac{1}{2} = [x] + (r + \frac{1}{2}) < [x] + 1$ because $r + \frac{1}{2} < 1$. It follows that $[x + \frac{1}{2}] = [x]$. Also $2x = 2[x] + 2r < 2[x] + 1$ because $2r < 1$. Hence $[2x] = 2[x]$. It follows that $[x] + [x + \frac{1}{2}] = [2x]$. Next suppose that $\frac{1}{2} \leq r < 1$. Then $[x] + 1 \leq x + (r + \frac{1}{2}) < [x] + 2$, so that $[x + \frac{1}{2}] = [x] + 1$. Also $2[x] + 1 \leq 2[x] + 2r = 2([x] + r) = 2x < 2[x] + 2$ so that $[2x] = 2[x] + 1$. It follows that $[x] + [x + \frac{1}{2}] = [x] + [x] + 1 = 2[x] + 1 = [2x]$.

1.1.13. We have $[x] \leq x$ and $[y] \leq y$. Adding these two inequalities gives $[x] + [y] \leq x + y$. Hence $[x + y] \geq [x] + [y] = [x] + [y]$.

1.1.14. Let $x = a + r$ and $y = b + s$, where a and b are integers and r and s are real numbers such that $0 \leq r, s < 1$. By Exercise 14, $[2x] + [2y] = [x] + [x + \frac{1}{2}] + [y] + [y + \frac{1}{2}]$. We now need to show that $[x + \frac{1}{2}] + [y + \frac{1}{2}] \geq [x + y]$. Suppose $0 \leq r, s < \frac{1}{2}$. Then $[x + \frac{1}{2}] + [y + \frac{1}{2}] = a + b + [r + \frac{1}{2}] + [s + \frac{1}{2}] = a + b$, and $[x + y] = a + b + [r + s] = a + b$, as desired. Suppose that $\frac{1}{2} \leq r, s < 1$. Then $[x + \frac{1}{2}] + [y + \frac{1}{2}] = a + b + [r + \frac{1}{2}] + [s + \frac{1}{2}] = a + b + 2$, and $[x + y] = a + b + [r + s] = a + b + 1$, as desired. Suppose that $0 \leq r < \frac{1}{2} \leq s < 1$. Then $[x + \frac{1}{2}] + [y + \frac{1}{2}] = a + b + 1$, and $[x + y] \leq a + b + 1$.

1.1.15. Let $x = a + r$ and $y = b + s$, where a and b are integers and r and s are real numbers such that $0 \leq r, s < 1$. Then $[xy] = [ab + as + br + sr] = ab + [as + br + sr]$, whereas $[x][y] = ab$. Thus we have $[xy] \geq [x][y]$ when x and y are both positive. If x and y are both negative, then $[xy] \leq [x][y]$. If one of x and y is positive and the other negative, then the inequality could go either direction. For examples take $x = -1.5, y = 5$ and $x = -1, y = 5.5$. In the first case we have $[-1.5 \cdot 5] = [-7.5] = -8 > [-1.5][5] = -2 \cdot 5 = -10$. In the second case we have $[-1 \cdot 5.5] = [-5.5] = -6 < [-1][5.5] = -1 \cdot 5 = -5$.

1.1.16. If x is an integer then $-[-x] = -(-x) = x$, which certainly is the least integer greater than or equal to x . Let $x = a + r$, where a is an integer and $0 < r < 1$. Then $-[-x] = -[-a - r] = -(-a + [-r]) = a - [-r] = a + 1$, as desired.

1.1.17. Let $x = [x] + r$. Because $0 \leq r < 1$, $x + \frac{1}{2} = [x] + r + \frac{1}{2}$. If $r < \frac{1}{2}$, then $[x]$ is the integer nearest to x and $[x + \frac{1}{2}] = [x]$ because $[x] \leq x + \frac{1}{2} = [x] + r + \frac{1}{2} < [x] + 1$. If $r \geq \frac{1}{2}$, then $[x] + 1$ is the integer nearest to x (choosing this integer if x is midway between $[x]$ and $[x + 1]$) and $[x + \frac{1}{2}] = [x] + 1$ because $[x] + 1 \leq x + r + \frac{1}{2} < [x] + 2$.

1.1.18. Let $y = x + n$. Then $[y] = [x] + n$, because n is an integer. Therefore the problem is equivalent to proving that $[y/m] = ([y]/m)$ which was done in Example 1.34.

1.1.19. Let $x = k + \epsilon$ where k is an integer and $0 \leq \epsilon < 1$. Further, let $k = a^2 + b$, where a is the largest integer such that $a^2 \leq k$. Then $a^2 \leq k = a^2 + b \leq x = a^2 + b + \epsilon < (a + 1)^2$. Then $[\sqrt{x}] = a$ and $[\sqrt{[x]}] = [\sqrt{k}] = a$ also, proving the theorem.

1.1.20. Let $x = k + \epsilon$ where k is an integer and $0 \leq \epsilon < 1$. Choose w from $0, 1, 2, \dots, m - 1$ such that $w/m \leq \epsilon < (w + 1)/m$. Then $w \leq m\epsilon < w + 1$. Then $[mx] = [mk + m\epsilon] = mk + [m\epsilon] = mk + w$. On the other hand, the same inequality gives us $(w + j)/m \leq \epsilon + j/m < (w + 1 + j)/m$, for any integer $j = 0, 1, 2, \dots, m - 1$. Note that this implies $[\epsilon + j/m] = [(w + j)/m]$ which is either 0 or 1 for j in this range. Indeed, it equals 1 precisely when $w + j \geq m$, which happens for exactly w values of j in this range. Now we compute $\sum_{j=0}^{m-1} [x + j/m] = \sum_{j=0}^{m-1} [k + \epsilon + j/m] = \sum_{j=0}^{m-1} k + [\epsilon + j/m] = mk + \sum_{j=0}^{m-1} [(w + j)/m] = mk + \sum_{j=m-w}^{m-1} 1 = mk + w$ which is the same as the value above.

1.1.21. a. Because the difference between any two consecutive terms of this sequence is 8, we may compute the n th term by adding 8 to the first term $n - 1$ times. That is, $a_n = 3 + (n - 1)8 = 8n - 5$.

b. For each n , we have $a_n - a_{n-1} = 2^{n-1}$, so we may compute the n th term of this sequence by adding all the powers of 2, up to the $(n - 1)$ th, to the first term. Hence $a_n = 5 + 2 + 2^2 + 2^3 + \dots + 2^{n-1} = 5 + 2^n - 2 = 2^n + 3$.

c. The n th term of this sequence appears to be zero, unless n is a perfect square, in which case the term is 1. If n is not a perfect square, then $[\sqrt{n}] < \sqrt{n}$, where $[x]$ represents the greatest integer function. If n is a perfect square, then $[\sqrt{n}] = \sqrt{n}$. Therefore, $[[\sqrt{n}]/\sqrt{n}]$ equals 1 if n is a perfect square and 0 otherwise, as desired.

d. This is a Fibonacci-like sequence, with $a_n = a_{n-1} + a_{n-2}$, for $n \geq 3$, and $a_1 = 1$, and $a_2 = 3$.

- 1.1.22. a. Each term given is 3 times the preceding term, so we conjecture that the n th term is the first term multiplied by 3, $n - 1$ times. So $a_n = 2 \cdot 3^{n-1}$.
- b. In this sequence, $a_n = 0$ if n is a multiple of 3, and equals 1 otherwise. Let $[x]$ represent the greatest integer function. Because $[n/3] < n/3$ when n is not a multiple of 3 and $[n/3] = n/3$ when n is a multiple of 3, we have that $a_n = 1 - [n/3]/(n/3)$.
- c. If we look at the difference of successive terms, we have the sequence 1, 1, 2, 2, 3, 3, ... So if n is odd, say $n = 2k + 1$, then a_n is obtained by adding $1 + 1 + 2 + 2 + 3 + 3 + \dots + k + k = 2t_k$ to the first term, which is 1. (Here t_k stands for the k th triangular number.) So if n is odd, then $a_n = 1 + 2t_k$ where $k = (n - 1)/2$. If n is even, say $n = 2k$, then $a_n = a_{2k+1} - k = 1 - k + 2t_k$.
- d. This is a Fibonacci-like sequence, with $a_n = a_{n-1} + 2a_{n-2}$, for $n \geq 3$, and $a_1 = 3$, and $a_2 = 5$.
- 1.1.23. Three possible answers are $a_n = 2^{n-1}$, $a_n = (n^2 - n + 2)/2$, and $a_n = a_{n-1} + 2a_{n-2}$.
- 1.1.24. Three possible answers are $a_n = a_{n-1}a_{n-2}$, $a_n = a_{n-1} + 2n - 3$, and $a_n =$ the number of letters in the n th word of the sentence "If our answer is correct we will join the Antidisestablishmentarianism Society and boldly state that 'If our answer is correct we will join the Antidisestablishmentarianism Society and boldly state....'"
- 1.1.25. This set is exactly the sequence $a_n = n - 100$, and hence is countable.
- 1.1.26. The function $f(n) = 5n$ is a one-to-one correspondence between this set and the set of integers, which is known to be countable.
- 1.1.27. One way to show this is to imitate the proof that the set of rational numbers is countable, replacing a/b with $a + b\sqrt{2}$. Another way is to consider the function $f(a + b\sqrt{2}) = 2^a 3^b$ which is a one-to-one map of this set into the rational numbers, which is known to be countable.
- 1.1.28. Let A and B be two countable sets. If one or both of the sets are finite, say A is finite, then the listing $a_1, a_2, \dots, a_n, b_1, b_2, \dots$, where any b_i which is also in A is deleted from the list, demonstrates the countability of $A \cup B$. If both sets are infinite, then each can be represented as a sequence: $A = \{a_1, a_2, \dots\}$, and $B = \{b_1, b_2, \dots\}$. Consider the listing $a_1, b_1, a_2, b_2, a_3, b_3, \dots$ and form a new sequence c_i as follows. Let $c_1 = a_1$. Given that c_n is determined, let c_{n+1} be the next element in the listing which is different from each c_i with $i = 1, 2, \dots, n$. Then this sequence is exactly the elements of $A \cup B$, which is therefore countable.
- 1.1.29. Suppose $\{A_i\}$ is a countable collection of countable sets. Then each A_i can be represented by a sequence, as follows:

$$\begin{array}{rcl} A_1 & = & a_{11} \quad a_{12} \quad a_{13} \quad \dots \\ A_2 & = & a_{21} \quad a_{22} \quad a_{23} \quad \dots \\ A_3 & = & a_{31} \quad a_{32} \quad a_{33} \quad \dots \\ & & \vdots \end{array}$$

Consider the listing $a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \dots$, in which we first list the elements with subscripts adding to 2, then the elements with subscripts adding to 3 and so on. Further, we order the elements with subscripts adding to k in order of the first subscript. Form a new sequence c_i as follows. Let $c_1 = a_{11}$. Given that c_n is determined, let c_{n+1} be the next element in the listing which is different from each c_i with $i = 1, 2, \dots, n$. Then this sequence is exactly the elements of $\bigcup_{i=1}^{\infty} A_i$, which is therefore countable.

- 1.1.30. a. Note that $\sqrt{2} \approx 1.4 = 7/5$, so we might guess that $\sqrt{2} - 7/5 \approx 0$. If we multiply through by 5 we expect that $5\sqrt{2} - 7$ should be small, and its value is approximately 0.071 which is much less than $1/8 = 0.125$. So we may take $a = 5 \leq 8$ and $b = 7$.

- b. As in part a., note that $\sqrt[3]{2} = 1.2599 \dots \approx 1.25 = 5/4$, so we investigate $4\sqrt[3]{2} - 5 = 0.039 \dots \leq 1/8$. So we may take $a = 4 \leq 8$ and $b = 5$.
- c. Because we know that $\pi \approx 22/7$ we investigate $|7\pi - 22| = 0.0088 \dots \leq 1/8$. So we may take $a = 7 \leq 8$ and $b = 22$.
- d. Because $e \approx 2.75 = 11/4$ we investigate $|4e - 11| = 0.126 \dots$, which is too large. A closer approximation to e is 2.718. We consider the decimal expansions of the multiples of $1/7$ and find that $5/7 = .714 \dots$, so $e \approx 19/7$. Therefore we investigate $|7e - 19| = 0.027 \leq 1/8$. So we may take $a = 7 \leq 8$ and $b = 19$.
- 1.1.31. a. Note that $\sqrt{3} = 1.73 \approx 7/4$, so we might guess that $\sqrt{3} - 7/4 \approx 0$. If we multiply through by 4 we find that $|4\sqrt{3} - 7| = 0.07 \dots < 1/10$. So we may take $a = 4 \leq 10$ and $b = 7$.
- b. It is helpful to keep the decimal expansions of the multiples of $1/7$ in mind in these exercises. Here $\sqrt[3]{3} = 1.442 \dots$ and $3/7 = 0.428 \dots$ so that we have $\sqrt[3]{3} \approx 10/7$. Then, as in part a., we investigate $|7\sqrt[3]{3} - 10| = 0.095 \dots < 1/10$. So we may take $a = 7 \leq 10$ and $b = 10$.
- c. Because $\pi^2 = 9.869 \dots$ and $6/7 = 0.857 \dots$, we have that $\pi^2 \approx 69/7$, so we compute $|7\pi^2 - 69| = 0.087 \dots < 1/10$. So we may take $a = 7 \leq 10$ and $b = 69$.
- d. Because $e^3 = 20.0855 \dots$ we may take $a = 1$ and $b = 20$ to get $|1e^3 - 20| = 0.855 \dots < 1/10$.
- 1.1.32. For $j = 0, 1, 2, \dots, n+1$, consider the $n+2$ numbers $\{j\alpha\}$, which all lie in the interval $0 \leq \{j\alpha\} < 1$. We can partition this interval into the $n+1$ subintervals $(k-1)/(n+1) \leq x < k/(n+1)$ for $k = 1, \dots, n+1$. Because we have $n+2$ numbers and only $n+1$ intervals, by the pigeonhole principle, some interval must contain at least two of the numbers. So there exist integers r and s such that $0 \leq r < s \leq n+1$ and $|\{r\alpha\} - \{s\alpha\}| \leq 1/(n+1)$. Let $a = s - r$ and $b = [s\alpha] - [r\alpha]$. Because $0 \leq r < s \leq n+1$, we have $1 \leq a \leq n$. Also, $|a\alpha - b| = |(s-r)\alpha - ([s\alpha] - [r\alpha])| = |(s\alpha - [s\alpha]) - (r\alpha - [r\alpha])| = |\{s\alpha\} - \{r\alpha\}| < 1/(n+1)$. Therefore, a and b have the desired properties.
- 1.1.33. The number α must lie in some interval of the form $r/k \leq \alpha < (r+1)/k$. If we divide this interval into equal halves, then α must lie in one of the halves, so either $r/k \leq \alpha < (2r+1)/2k$ or $(2r+1)/2k \leq \alpha < (r+1)/k$. In the first case we have $|\alpha - r/k| < 1/2k$, so we take $u = r$. In the second case we have $|\alpha - (r+1)/k| < 1/2k$, so we take $u = r+1$.
- 1.1.34. Suppose that there are only finitely many positive integers q_1, q_2, \dots, q_n with corresponding integers p_1, p_2, \dots, p_n such that $|\alpha - p_i/q_i| < 1/q_i^2$. Because α is irrational, $|\alpha - p_i/q_i|$ is positive for every i , and so is $|q_i\alpha - p_i|$ so we may choose an integer N so large that $|q_i\alpha - p_i| > 1/N$ for all i . By Dirichlet's Approximation Theorem, there exist integers r and s with $1 \leq s \leq N$ such that $|s\alpha - r| < 1/N < 1/s$, so that $|\alpha - r/s| < 1/s^2$, and s is not one of the q_i . Therefore, we have another solution to the inequality. So no finite list of solutions can be complete, and we conclude that there must be an infinite number of solutions.
- 1.1.35. First we have $|\sqrt{2} - 1/1| = 0.414 \dots < 1/1^2$. Second, Exercise 30, part a., gives us $|\sqrt{2} - 7/5| < 1/50 < 1/5^2$. Third, observing that $3/7 = 0.428 \dots$ leads us to try $|\sqrt{2} - 10/7| = 0.014 \dots < 1/7^2 = 0.0204 \dots$. Fourth, observing that $5/12 = 0.4166 \dots$ leads us to try $|\sqrt{2} - 17/12| = 0.00245 \dots < 1/12^2 = 0.00694 \dots$.
- 1.1.36. First we have $|\sqrt[3]{5} - 1/1| = 0.7099 \dots < 1/1^2$. Second, $|\sqrt[3]{5} - 5/3| = 0.04 \dots < 1/3^2$. Third, because $\sqrt[3]{5} = 1.7099 \dots$, we try $|\sqrt[3]{5} - 17/10| = 0.0099 \dots < 1/10^2$. Likewise, we get a fourth rational number with $|\sqrt[3]{5} - 171/100| = 0.000024 \dots < 1/100^2$. Fifth, consideration of multiples of $1/7$ leads to $|\sqrt[3]{5} - 12/7| = 0.0043 \dots < 1/7^2$.
- 1.1.37. We may assume that b and q are positive. Note that if $q > b$, we have $|p/q - a/b| = |pb - aq|/qb \geq 1/qb > 1/q^2$. Therefore, solutions to the inequality must have $1 \leq q \leq b$. For a given q , there can be only finitely many p such that the distance between the rational numbers a/b and p/q is less than $1/q^2$.

(indeed there is at most one.) Therefore there are only finitely many p/q satisfying the inequality.

- 1.1.38. a.** Because $n2$ is an integer for all n , so is $[n2]$, so the first ten terms of the spectrum sequence are 2, 4, 6, 8, 10, 12, 14, 16, 18, 20.
- b.** The sequence for $n\sqrt{2}$, rounded, is 1.414, 2.828, 4.242, 5.656, 7.071, 8.485, 9.899, 11.314, 12.728, 14.142. When we apply the floor function to these numbers we get 1, 2, 4, 5, 7, 8, 9, 11, 12, 14 for the spectrum sequence.
- c.** The sequence for $n(2 + \sqrt{2})$, rounded, is 3.414, 6.828, 10.24, 13.66, 17.07, 20.48, 23.90, 27.31, 30.73, 34.14. When we apply the floor function to these numbers we get 3, 6, 10, 13, 17, 20, 23, 27, 30, 34, for the spectrum sequence.
- d.** The sequence for $n\pi$, rounded is 2.718, 5.436, 8.155, 10.87, 13.59, 16.31, 19.03, 21.75, 24.46, 27.18. When we apply the floor function to these numbers we get 2, 5, 8, 10, 13, 16, 19, 21, 24, 27, for the spectrum sequence.
- e.** The sequence for $n(1 + \sqrt{5})/2$, rounded, is 1.618, 3.236, 4.854, 6.472, 8.090, 9.708, 11.33, 12.94, 14.56, 16.18. When we apply the floor function to these numbers we get 1, 3, 4, 6, 8, 9, 11, 12, 14, 16 for the spectrum sequence.
- 1.1.39. a.** Because $n3$ is an integer for all n , so is $[n3]$, so the first ten terms of the spectrum sequence are 3, 6, 9, 12, 15, 18, 21, 24, 27, 30.
- b.** The sequence for $n\sqrt{3}$, rounded, is 1.732, 3.464, 5.196, 6.928, 8.660, 10.39, 12.12, 13.86, 15.59, 17.32. When we apply the floor function to these numbers we get 1, 3, 5, 6, 8, 10, 12, 13, 15, 17 for the spectrum sequence.
- c.** The sequence for $n(3 + \sqrt{3})/2$, rounded, is 2.366, 4.732, 7.098, 9.464, 11.83, 14.20, 16.56, 18.93, 21.29, 23.66. When we apply the floor function to these numbers we get 2, 4, 7, 9, 11, 14, 16, 18, 21, 23 for the spectrum sequence.
- d.** The sequence for $n\pi$, rounded is 3.142, 6.283, 9.425, 12.57, 15.71, 18.85, 21.99, 25.13, 28.27, 31.42. When we apply the floor function to these numbers we get 3, 6, 9, 12, 15, 18, 21, 25, 28, 31, for the spectrum sequence.
- 1.1.40.** Because $\alpha \neq \beta$, their decimal expansions must be different. If they differ in digits that are to the left of the decimal point, then $[\alpha] \neq [\beta]$, so certainly the spectrum sequences are different. Otherwise, suppose that they differ in the k th position to the right of the decimal. Then $[10^k\alpha] \neq [10^k\beta]$, and so the spectrum sequences will again differ.
- 1.1.41.** Assume that $1/\alpha + 1/\beta = 1$. Note first that for all integers n and m , $m\alpha \neq n\beta$, for otherwise, we solve the equations $m\alpha = n\beta$ and $1/\alpha + 1/\beta = 1$ and get rational solutions for α and β , a contradiction. Therefore the sequences $m\alpha$ and $n\beta$ are disjoint.
- For an integer k , define $N(k)$ to be the number of elements of the sequences $m\alpha$ and $n\beta$ which are less than k . Now $m\alpha < k$ if and only if $m < k/\alpha$, so there are exactly $[k/\alpha]$ members of the sequence $m\alpha$ less than k . Likewise, there are exactly $[k/\beta]$ members of the sequence $n\beta$ less than k . So we have $N(k) = [k/\alpha] + [k/\beta]$. By definition of the greatest integer function, we have $k/\alpha - 1 < [k/\alpha] < k/\alpha$ and $k/\beta - 1 < [k/\beta] < k/\beta$, where the inequalities are strict because the numbers are irrational. If we add these inequalities we get $k/\alpha + k/\beta - 2 < N(k) < k/\alpha + k/\beta$ which simplifies to $k - 2 < N(k) < k$. Because $N(k)$ is an integer, we conclude that $N(k) = k - 1$. This shows that there is exactly one member of the union of the sequences $m\alpha$ and $n\beta$ in each interval of the form $k - 1 \leq x < k$, and therefore, when we apply the floor function to each member, exactly one will take on the value k .
- Conversely, suppose that α and β are irrational numbers such that $1/\alpha + 1/\beta \neq 1$. If $1/\alpha + 1/\gamma = 1$ then we know from the first part of the theorem that the spectrum sequences for α and γ partition the positive integers. By Exercise 40, we know that the spectrum sequences for β and γ are different, so the