Complete Solutions Manual

Abstract Algebra
An Introduction

THIRD EDITION

Thomas W. Hungerford
St. Louis University

Prepared by

Roger Lipsett

BROOKS/COLE
CENGAGE Learning

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

BROOKS/COLE
CENGAGE Learning

For product information and technology assistance, contact us at **Cengage Learning Customer & Sales Support, 1-800-354-9706**

For permission to use material from this text or product, submit all requests online at **www.cengage.com/permissions**
Further permissions questions can be emailed to **permissionrequest@cengage.com**

ISBN-13: 978-1-133-61123-3
ISBN-10: 1-133-61123-0

Brooks/Cole
20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **www.cengage.com/global**

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

To learn more about Brooks/Cole, visit **www.cengage.com/brookscole**

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
1 2 3 4 5 6 7 17 16 15 14 13

CONTENTS

Chapter 1

Arithmetic in $\mathbb{Z}$ Revisited

1.1 The Division Algorithm

1. (a) $q = 4$, $r = 1$. (b) $q = 0$, $r = 0$. (c) $q = -5$, $r = 3$.

2. (a) $q = -9$, $r = 3$. (b) $q = 15$, $r = 17$. (c) $q = 117$, $r = 11$.

3. (a) $q = 6$, $r = 19$. (b) $q = -9$, $r = 54$. (c) $q = 62720$, $r = 92$.

4. (a) $q = 15021$, $r = 132$. (b) $q = -14940$, $r = 335$. (c) $q = 39763$, $r = 3997$.

5. Suppose $a = bq + r$, with $0 \le r < b$. Multiplying this equation through by c gives $ac = (bc)q + rc$. Further, since $0 \le r < b$, it follows that $0 \le rc < bc$. Thus this equation expresses ac as a multiple of bc plus a remainder between 0 and $bc - 1$. Since by Theorem 1.1 this representation is unique, it must be that q is the quotient and rc the remainder on dividing ac by bc.

6. When q is divided by c, the quotient is k, so that $q = ck$. Thus $a = bq + r = b(ck) + r = (bc)k + r$. Further, since $0 \le r < b$, it follows (since $c \ge 1$) than $0 \le r < bc$. Thus $a = (bc)k + r$ is the unique representation with $0 \le r < bc$, so that the quotient is indeed k.

7. Answered in the text.

8. Any integer n can be divided by 4 with remainder r equal to 0, 1, 2 or 3. Then either $n = 4k$, $4k + 1$, $4k + 2$ or $4k + 3$, where k is the quotient. If $n = 4k$ or $4k + 2$ then n is even. Therefore if n is odd then $n = 4k + 1$ or $4k + 3$.

9. We know that every integer a is of the form $3q$, $3q + 1$ or $3q + 2$ for some q. In the last case $a^3 = (3q + 2)^3 = 27q^3 + 54q^2 + 36q + 8 = 9k + 8$ where $k = 3q^3 + 6q^2 + 4q$. Other cases are similar.

10. Suppose $a = nq + r$ where $0 \le r < n$ and $c = nq' + r'$ where $0 < r' < n$. If $r = r'$ then $a - c = n(q - q')$ and $k = q - q'$ is an integer. Conversely, given $a - c = nk$ we can substitute to find: $(r - r') = n(k - q + q')$. Suppose $r \ge r'$ (the other case is similar). The given inequalities imply that $0 \le (r - r') < n$ and it follows that $0 \le (k - q + q') < 1$ and we conclude that $k - q + q' = 0$. Therefore $r - r' = 0$, so that $r = r'$ as claimed.

11. Given integers a and c with $c \neq 0$. Apply Theorem 1.1 with $b = |c|$ to get $a = |c| \cdot q_0 + r$ where $0 \leq r < |c|$. Let $q = q_0$ if $c > 0$ and $q = -q_0$ if $c < 0$. Then $a = cq + r$ as claimed. The uniqueness is proved as in Theorem 1.1.

1.2 Divisibility

1. (a) 8. (b) 6. (c) 1. (d) 11. (e) 9. (f) 17. (g) 592. (h) 6.

2. If $b \mid a$ then $a = bx$ for some integer x. Then $a = (-b)(-x)$ so that $(-b) \mid a$. The converse follows similarly.

3. Answered in the text.

4. (a) Given $b = ax$ and $c = ay$ for some integers x, y, we find $b + c = ax + ay = a(x + y)$. Since $x + y$ is an integer, conclude that $a \mid (b + c)$.
   (b) Given x and y as above we find $br + ct = (ax)r + (ay)t = a(xr + yt)$ using the associative and distributive laws. Since $xr + yt$ is an integer we conclude that $a \mid (br + ct)$.

5. Since $a \mid b$, we have $b = ak$ for some integer k, and $a \neq 0$. Since $b \mid a$, we have $a = bl$ for some integer l, and $b \neq 0$. Thus $a = bl = (ak)l = a(kl)$. Since $a \neq 0$, divide through by a to get $1 = kl$. But this means that $k = \pm 1$ and $l = \pm 1$, so that $a = \pm\, b$.

6. Given $b = ax$ and $d = cy$ for some integers x, y, we have $bd = (ax)(cy) = (ac)(xy)$. Then $ac \mid bd$ because xy is an integer.

7. Clearly $(a, 0)$ is at most $|a|$ since no integer larger than $|a|$ divides a. But also $|a| \mid a$, and $|a| \mid 0$ since any nonzero integer divides 0. Hence $|a|$ is the gcd of a and 0.

8. If $d = (n, n + 1)$ then $d \mid n$ and $d \mid (n + 1)$. Since $(n + 1) - n = 1$ we conclude that $d \mid 1$. (Apply Exercise 4(b).) This implies $d = 1$, since $d > 0$.

9. No, ab need not divide c. For one example, note that $4 \mid 12$ and $6 \mid 12$, but $4 \cdot 6 = 24$ does not divide 12.

10. Since $a \mid a$ and $a \mid 0$ we have $a \mid (a, 0)$. If $(a, 0) = 1$ then $a \mid 1$ forcing $a = \pm 1$.

11. (a) 1 or 2 (b) 1, 2, 3 or 6. Generally if $d = (n, n + c)$ then $d \mid n$ and $d \mid (n + c)$. Since c is a linear combination of n and n+c, conclude that $d \mid c$.

12. (a) False. (ab, a) is always at least a since $a \mid ab$ and $a \mid a$.
    (b) False. For example, $(2, 3) = 1$ and $(2, 9) = 1$, but $(3, 9) = 3$.
    (c) False. For example, let $a = 2$, $b = 3$, and $c = 9$. Then $(2, 3) = 1 = (2, 9)$, but $(2 \cdot 3, 9) = 3$.

13. (a) Suppose $c \mid a$ and $c \mid b$. Write $a = ck$ and $b = cl$. Then $a = bq + r$ can be rewritten $ck = (cl)q + r$, so that $r = ck - clq = c(k - lq)$. Thus $c \mid r$ as well, so that c is a common divisor of b and r.

(b) Suppose $c \mid b$ and $c \mid r$. Write $b = ck$ and $r = cl$, and substitute into $a = bq + r$ to get $a = ckq + cl = c(kq + l)$. Thus $c \mid a$, so that c is a common divisor of a and b.

(c) Since (a, b) is a common divisor of a and b, it is also a common divisor of b and r, by part (a). If (a, b) is not the greatest common divisor (b, r) of b and r, then $(a, b) > (b, r)$. Now, consider (b, r). By part (b), this is also a common divisor of (a, b), but it is less than (a, b). This is a contradiction. Thus $(a, b) = (b, r)$.

14. By Theorem 1.3, the smallest positive integer in the set S of all linear combinations of a and b is exactly $(a,\ b)$.

(*a*) $(6,\ 15) = 3$ (*b*) $(12,\ 17)=1$.

15. (a) This is a calculation.

(b) At the first step, for example, by Exercise 13 we have $(a, b) = (524, 148) = (148, 80) = (b, r)$. The same applies at each of the remaining steps. So at the final step, we have $(8, 4) = (4, 0)$; putting this string of equalities together gives

$$(524, 148) = (148, 80) = (80, 68) = (68, 12) = (12, 8) = (8, 4) = (4, 0).$$

But by Example 4, $(4, 0) = 4$, so that $(524, 148) = 4$.

(c) $1003 = 56 \cdot 17 + 51$, $56 = 51 \cdot 1 + 5$, $51 = 5 \cdot 10 + 1$, $5 = 1 \cdot 5 + 0$. Thus $(1003, 56) = (1, 0) = 1$.

(d) $322 = 148 \cdot 2 + 26$, $148 = 26 \cdot 5 + 18$, $26 = 18 \cdot 1 + 8$, $18 = 8 \cdot 2 + 2$, $8 = 2 \cdot 4 + 0$, so that $(322, 148) = (2, 0) = 2$.

(e) $5858 = 1436 \cdot 4 + 114$, $1436 = 114 \cdot 12 + 68$, $114 = 68 \cdot 1 + 46$, $68 = 46 \cdot 1 + 22$, $46 = 22 \cdot 2 + 2$, $22 = 2 \cdot 11 + 0$, so that $(5858, 1436) = (2, 0) = 2$.

(f) $68 = 148 - (524 - 148 \cdot 3) = -524 + 148 \cdot 4$.

(g) $12 = 80 - 68 \cdot 1 = (524 - 148 \cdot 3) - (-524 + 148 \cdot 4) \cdot 1 = 524 \cdot 2 - 148 \cdot 7$.

(h) $8 = 68 - 12 \cdot 5 = (-524 + 148 \cdot 4) - (524 \cdot 2 - 148 \cdot 7) \cdot 5 = -524 \cdot 11 + 148 \cdot 39$.

(i) $4 = 12 - 8 = (524 \cdot 2 - 148 \cdot 7) - (-524 \cdot 11 + 148 \cdot 39) = 524 \cdot 13 - 148 \cdot 46$.

(j) Working the computation backwards gives $1 = 1003 \cdot 11 - 56 \cdot 197$.

16. Let $a = da_1$ and $b = db_1$. Then a_1 and b_1 are integers and we are to prove: $(a_1,\ b_1) = 1$. By Theorem 1.3 there exist integers u, v such that $au + bv = d$. Substituting and cancelling we find that $a_1u + b_1v = 1$. Therefore any common divisor of a_1 and b_1 must also divide this linear combination, so it divides 1. Hence $(a_1,\ b_1) = 1$.

17. Since $b \mid c$, we know that $c = bt$ for some integer t. Thus $a \mid c$ means that $a \mid bt$. But then Theorem 1.4 tells us, since $(a, b) = 1$, that $a \mid t$. Multiplying both sides by b gives $ab \mid bt = c$.

18. Let $d = (a,\ b)$ so there exist integers $x,\ y$ with $ax + by = d$. Note that $cd \mid (ca,\ cb)$ since cd divides ca and cb. Also $cd = cax + cby$ so that $(ca,\ cb) \mid cd$. Since these quantities are positive we get $cd = (ca,\ cd)$.

19. Let $d = (a,\ b)$. Since $b + c = aw$ for some integer w, we know c is a linear combination of a and b so that $d \mid c$. But then $d \mid (b, c) = 1$ forcing $d = 1$. Similarly $(a, c) = 1$.

20. Let $d = (a, b)$ and $e = (a, b + at)$. Since $b + at$ is a linear combination of a and b, $d \mid (b + at)$ so that $d \mid e$. Similarly since $b = a(-t) + (b + at)$ is a linear combination of a and $b + at$ we know $e \mid b$ so that $e \mid d$. Therefore $d = e$.

21. Answered in the text.

22. Let $d = (a, b, c)$. Claim: $(a, d) = 1$. [Proof: (a, d) divides d so it also divides c. Then $(a, d) \mid (a, c) = 1$ so that $(a, d) = 1$.] Similarly $(b, d) = 1$. But $d \mid ab$ and $(a, d) = 1$ so that Theorem 1.5 implies that $d \mid$ b. Therefore $d = (b. d) = 1$.

23. Define the powers b^n recursively as follows: $b^1 = b$ and for every $n \geq 1$, $b^{n+1} = b \cdot b^n$. By hypothesis $(a, b^1) = 1$. Given $k \geq 1$, assume that $(a, b^k) = 1$. Then $(a, b^{k+1}) = (a, b \cdot b^k) = 1$ by Exercise 24. This proves that $(a, b^n) = 1$ for every $n \geq 1$.

24. Let $d = (a, b)$. If $ax + by = c$ for some integers x, y then c is a linear combination of a and b so that $d \mid c$. Conversely suppose c is given with $d \mid$ c, say $c = dw$ for an integer w. By Theorem 1.3 there exist integers u, v with $d = au + bv$. Then $c = dw = auw + bvw$ and we use $x = uw$ and $y = vw$ to solve the equation.

25. (a) Given $au + bv = 1$ suppose $d = (a, b)$. Then $d \mid a$ and $d \mid b$ so that d divides the linear combination $au + bv = 1$. Therefore $d = 1$.
    (b) There are many examples. For instance if $a = b = d = u = v = 1$ then $(a, b) = (1, 1) = 1$ while $d = au + bv = 1 + 1 = 2$.

26. Let $d = (a, b)$ and express $a = da_1$ and $b = db_1$ for integers a_1, b_1. By Exercise 16, $(a_1, b_1) = 1$. Since $a \mid c$ we have $c = au = da_1u$ for some integer u. Similarly $c = bv = db_1v$ for some integer v. Then $a_1u = c/d = b_1V$ and Theorem 1.5 implies that $a_1 \mid v$ so that $v = a_1w$ for some integer w. Then $c = da_1b_1w$ so that $cd = d^2a_1b_1w = abw$ and $ab \mid cd$.

27. Answered in the text.

28. Suppose the integer consists of the digits $a_na_{n-1}\dots a_1a_0$. Then the number is equal to

$$\sum_{k=0}^{n} a_k 10^k = \sum_{k=0}^{n} a_k(10^k - 1) + \sum_{k=0}^{n} a_k.$$

Now, the first term consists of terms with factors of the form $10^k - 1$, all of which are of the form $999\dots99$, which are divisible by 3, so that the first term is always divisible by 3. Thus $\sum_{k=0}^{n} a_k 10^k$ is divisible by 3 if and only if the second term $\sum_{k=0}^{n} a_k$ is divisible by 3. But this is the sum of the digits.

29. This is almost identical to Exercise 28. Suppose the integer consists of the digits $a_na_{n-1}\dots a_1a_0$. Then the number is equal to

$$\sum_{k=0}^{n} a_k 10^k = \sum_{k=0}^{n} a_k(10^k - 1) + \sum_{k=0}^{n} a_k.$$

Now, the first term consists of terms with factors of the form $10^k - 1$, all of which are of the form $999\dots99$, which are divisible by 9, so that the first term is always divisible by 9. Thus $\sum_{k=0}^{n} a_k 10^k$ is divisible by 9 if and only if the second term $\sum_{k=0}^{n} a_k$ is divisible by 9. But this is the sum of the digits.

30. Let $S = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : x_1\ x_2, \ldots, x$ are integers$\}$. As in the proof of Theorem 1.3, S does contain some positive elements (for if $a_i \neq 0$ then $a_i^2 \in S$ is positive). By the Well Ordering Axiom this set S contains a smallest positive element, which we call t. Suppose $t = a_1u_1 + a_2u_2 + \cdots + a_nu_n$ for some integers u_i.
Claim. $t = d$. The first step is to show that $t \mid a_1$. By the division algorithm there exist integers q and r such that $a_1 = tq + r$ with $0 \leq r < t$. Then $r = a_1 - tq = a_1(1 - u_1q) + a_2(-u_2q) + \cdots + a_n(-u_nq)$ is an element of S. Since $r < t$ (the smallest positive element of S), we know r is not positive. Since $r \geq 0$ the only possibility is $r = 0$. Therefore $a_1 = tq$ and $t \mid a_1$. Similarly we have $t \mid a_j$ for each j, and t is a common divisor of $a_1, a_2, \cdots, a_n$. Then $t \leq d$ by definition.

On the other hand d divides each a_i so d divides every integer linear combination of $a_1, a_2, \cdots, a_n$. In particular, $d \mid t$. Since $t > 0$ this implies that $d \leq t$ and therefore $d = t$.

31. (a) $[6, 10] = 30$; $[4, 5, 6, 10] = 60$; $[20, 42] = 420$, and $[2, 3, 14, 36, 42] = 252$.

(b) Suppose $a_i \mid t$ for $i = 1, 2, \ldots, k$, and let $m = [a_1, a_2, \ldots, a_k]$. Then we can write $t = mq + r$ with $0 \leq r < m$. For each i, $a_i \mid t$ by assumption, and $a_i \mid m$ since m is a common multiple of the a_i. Thus $a_i \mid (t - mq) = r$. Since $a_i \mid r$ for each i, we see that r is a common multiple of the a_i. But m is the smallest positive integer that is a common multiple of the a_i; since $0 \leq r < m$, the only possibility is that $r = 0$ so that $t = mq$. Thus any common multiple of the a_i is a multiple of the least common multiple.

32. First suppose that $t = [a, b]$. Then by definition of the least common multiple, t is a multiple of both a and b, so that $t \mid a$ and $t \mid b$. If $a \mid c$ and $b \mid c$, then c is also a common multiple of a and b, so by Exercise 31, it is a multiple of t so that $t \mid c$.

Conversely, suppose that t satisfies the conditions (i) and (ii). Then since $a \mid t$ and $b \mid t$, we see that t is a common multiple of a and b. Choose any other common multiple c, so that $a \mid c$ and $b \mid c$. Then by condition (ii), we have $t \mid c$, so that $t \leq c$. It follows that t is the least common multiple of a and b.

33. Let $d = (a, b)$, and write $a = da_1$ and $b = db_1$. Write $m = \frac{ab}{d} = \frac{da_1db_1}{d} = da_1b_1$. Since a and b are both positive, so is m, and since $m = da_1b_1 = (da_1)b_1 = ab_1$ and $m = da_1b_1 = (db_1)a_1 = ba_1$, we see that m is a common multiple of a and b. Suppose now that k is a positive integer with $a \mid k$ and $b \mid k$. Then $k = au = bv$, so that $k = da_1u = db_1v$. Thus $\frac{k}{d} = a_1u = b_1v$. By Exercise 16, $(a_1, b_1) = 1$, so that $a_1 \mid v$, say $v = a_1w$. Then $k = db_1v = db_1a_1w = mw$, so that $m \mid k$. Thus $m \leq k$. It follows that m is the least common multiple. But by construction, $m = \frac{ab}{(a,b)} = \frac{ab}{d}$.

34. (a) Let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, it follows that $d \mid (a + b)$ and $d \mid (a - b)$, so that d is a common divisor of $a + b$ and $a - b$. Hence it is a divisor of the greatest common divisor, so that $d = (a, b) \mid (a + b, a - b)$.

(b) We already know that $(a, b) \mid (a+b, a-b)$. Now suppose that $d = (a+b, a-b)$. Then $a+b = dt$ and $a - b = du$, so that $2a = d(t + u)$. Since a is even and b is odd, d must be odd. Since $d \mid 2a$, it follows that $d \mid a$. Similarly, $2b = d(t - u)$, so by the same argument, $d \mid b$. Thus d is a common divisor of a and b, so that $d \mid (a, b)$. Thus $(a, b) = (a + b, a - b)$.

(c) Suppose that $d = (a + b, a - b)$. Then $a + b = dt$ and $a - b = du$, so that $2a = d(t + u)$. Since a and b are both odd, $a + b$ and $a - b$ are both even, so that d is even. Thus $a = \frac{d}{2}(t + u)$, so that $\frac{d}{2} \mid a$. Similarly, $\frac{d}{2} \mid b$, so that $\frac{d}{2} = \frac{(a+b,a-b)}{2} \mid (a, b) \mid (a + b, a - b)$. Thus $(a, b) = \frac{(a+b,a-b)}{2}$ or $(a, b) = (a + b, a - b)$. But since (a, b) is odd and $(a + b, a - b)$ is even, we must have $\frac{(a+b,a-b)}{2} = (a, b)$, or $2(a, b) = (a + b, a - b)$.

1.3 Primes and Unique Factorization

1. (a) $2^4 \cdot 3^2 \cdot 5 \cdot 7$.
   (b) $-5 \cdot 7 \cdot 67$.
   (c) $2 \cdot 5 \cdot 4567$.
   (d) $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$.

2. (a) Since $2^5 - 1 = 31$, and $\sqrt{31} < 6$, we need only check divisibility by the primes 2, 3, and 5. Since none of those divides 31, it is prime.
   (b) Since $2^7 - 1 = 127$, and $\sqrt{127} < 12$, we need only check divisibility by the primes 2, 3, 5, 7, and 11. Since none of those divides 127, it is prime.
   (c) $2^{11} - 1 = 2047 = 23 \cdot 89$.

3. They are all prime.

4. The pairs are $\{3,5\}$, $\{5,7\}$, $\{11,13\}$, $\{17,19\}$, $\{29,31\}$, $\{41,43\}$, $\{59,61\}$, $\{71,73\}$, $\{101,103\}$, $\{107,109\}$, $\{137,139\}$, $\{149,151\}$, $\{179,181\}$, $\{191,193\}$, $\{197,199\}$.

5. (a) Answered in the text. These divisors can be listed as $2^j \cdot 3^k$ for $0 \le j \le s$ and $0 \le k \le t$.
   (b) The number of divisors equals $(r+1)(s+1)(t+1)$.

6. The possible remainders on dividing a number by 10 are $0, 1, 2, \dots, 9$. If the remainder on dividing p by 10 is 0, 2, 4, 6, or 8, then p is even; since $p > 2$, p is divisible by 2 in addition to 1 and itself and cannot be prime. If the remainder is 5, then since $p > 5$, p is divisible by 5 in addition to 1 and itself and cannot be prime. That leaves as possible remainders only 1, 3, 7, and 9.

7. Since $p \mid (a + bc)$ and $p \mid a$, we have $a = pk$ and $a + bc = pl$, so that $pk + bc = pl$ and thus $bc = p(l - k)$. Thus $p \mid bc$. By Theorem 1.5, either $p \mid b$ or $p \mid c$ (or both).

8. (a) As polynomials,
   $$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$
   (b) Since $2^{2n} \cdot 3^n - 1 = (2^2 \cdot 3)^n - 1 = 12^n - 1$, by part (a), $12^n - 1$ is divisible by $12 - 1 = 11$.

9. If p is a prime and $p = rs$ then by the definition r, s must lie in $\{1, -1, p, -p\}$. Then either $r = \pm 1$ or $r = \pm p$ and $s = p/r = \pm 1$, Conversely if p is not a prime then it has a divisor r not in $\{1, -1, p, -p\}$. Then $p = rs$ for some integer s. If s equals ± 1 or $\pm p$ then $r = p/s$ would equal $\pm p$ or $+1$, contrary to assumption. This r, s provides an example where the given statement fails.

10. Assume first that $p > 0$. If p is a prime then (a, p) is a positive divisor of p, so that $(a, p) = 1$ or p. If $(a, p) = p$ then $p \mid a$. Conversely if p is not a prime it has a divisor d other than ± 1 and $\pm p$. We may change signs to assume $d > 0$. Then $(p, d) = d \neq 1$. Also $p \nmid d$ since otherwise $p \mid d$ and $d = p$ implies $d = p$. Then $a = d$ provides an example where the required statement fails. Finally if $p < 0$ apply the argument above to $-p$.

11. Since $p \mid a - b$ and $p \mid c - d$, also $p \mid (a - b) + (c - d) = (a + c) - (b + d)$. Thus p is a divisor of $(a + c) - (b + d)$; the fact that p is prime means that it is a prime divisor.

12. Since $n > 1$ Theorem 1.10 implies that n equals a product of primes. We can pull out minus signs to see that n = $p_1\ p_2\ \ldots\ p_r$ where each p_i is a positive prime. Re-ordering these primes if necessary, to assume $p_1 \le p_2 \le \ldots \le p_r$. For the uniqueness, suppose there is another factorization $n = q_1\, q_2 \ldots q_s$ for some positive primes q_i with $q_1 \le q_2 \ldots \le q_s$. By theorem 1.11 we know that $r = s$ and the p_i's are just a re-arrangement of the q_is. Then p_1 is the smallest of the p_i's, so it also equals the smallest of the q_i's and therefore $p_1 = q_1$. We can argue similarly that $p_2 = q_2, \ldots, p_r = q_r$. (This last step should really be done by a formal proof invoking the Well Ordering Axiom.)

13. By Theorem 1.8, the Fundamental Theorem of Arithmetic, every integer except 0 and ± 1 can be written as a product of primes, and the representation is unique up to order and the signs of the primes. Since in our case $n > 1$ is positive and we wish to use positive primes, the representation is unique up to order. So write $n = q_1\, q_2 \ldots q_s$ where each $q_i > 0$ is prime. Let $p_1, p_2, \ldots, p_r$ be the distinct primes in the list. Collect together all the occurrences of each p_i, giving r_i copies of p_i, i.e. $p_i^{r_i}$.

14. Suppose $d \mid p$ so that $p = dt$ for some integer t. The hypothesis then implies that $p \mid d$ or $p \mid t$. If $p \mid d$ then (applying Exercise 1.2.5) $d = \pm p$. Similarly if $p \mid t$ then, since we know that $t \mid p$, we get $t = +p$, and therefore $d = \pm 1$.

15. Apply Corollary 1.9 in the case $a_1 = a_2 = \cdots = a_n$ to see that if $p \mid a^n$ then $p \mid a$. Then $a = pu$ for some integer u, so that $a^n = p^n u^n$ and $p^n \mid a^n$.

16. Generally, $p \mid a$ and $p \mid b$ if and only if $p \mid (a, b)$, as in Corollary 1.4. Then the Exercise is equivalent to: $(a, b) = 1$ if and only if there is no prime p such that $p \mid (a, b)$. This follows using Theorem 1.10.

17. First suppose u, v are integers with $(u, v) = 1$. <u>Claim</u>. $(u^2, v^2) = 1$. For suppose p is a prime such that $p \mid u^2$ and $p \mid v^2$. Then $p \mid u$ and $p \mid v$ (using Theorem 1.8), contrary to the hypothesis $(u, v) = 1$. Then no such prime exists and the Claim follows by Exercise 8.
Given $(a, b) = p$ write $a = pa_1$ and $b = pb_1$. Then $(a_1, b_1) = 1$ by Exercise 1.2.16. Then $(a^2, b^2) = (p^2 {a_1}^2, p^2 {b_1}^2) = p^2({a_1}^2, {b_1}^2)$, using Exercise 1.2.18. By the Claim we conclude that $(a^2, b^2) = p^2$.

18. The choices $p = 2$, $a = b = 0$, $c = d = 1$ provide a counterexample to (a) and (b).
(c) Since $p \mid (a^2 + b^2) - a{\cdot}a = b^2$, conclude that $p \mid b$ by Theorem 1.8.

19. If $r_i \le s_i$ for every i, then

$$b = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k} = p_1^{r_1} p_1^{s_1 - r_1} p_2^{r_2} p_2^{s_2 - r_2} \ldots p_k^{r_k} p_k^{s_k - r_k} = (p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}) \cdot \left(p_1^{s_1 - r_1} p_2^{s_2 - r_2} \ldots p_k^{s_2 - r_k}\right)$$
$$= a \cdot \left(p_1^{s_1 - r_1} p_2^{s_2 - r_2} \ldots p_k^{s_2 - r_k}\right).$$

Since each $s_i - r_i \ge 0$, the second factor above is an integer, so that $a \mid b$.

Now suppose $a \mid b$, and consider $p_i^{r_i}$. Since this is composed of factors only of p_i, it must divide $p_i^{s_i}$, since $p_i \nmid p_j$ for $i \ne j$. Thus $p_i^{r_i} \mid p_i^{s_i}$. Clearly this holds if $r_i \le s_i$, and also clearly it does not hold if $r_i > s_i$, since then $p_i^{r_i} > p_i^{s_i}$.

20. (a) The positive divisors of a are the numbers $d = p_1^{m1}p_2^{m2}\cdots p_k^{mk}$ where the exponents m_i satisfy $0 \le m_j \le r_j$ for each $j = 1, 2,,.., k$. This follows from unique factorization. If d also divides b we have $0 \le m_j \le s_j$ for each $i = 1, 2,... k$. Since $n_j = \min\{r_i, s_i\}$ we see that the positive common divisors of a and b are exactly those numbers $d = p_1^{m1}p_2^{m2} \cdots p_k^{mk}$ where $0 \le m_j \le n_j$ for each $j = 1, 2,..., k$. Then (a, b) is the largest among these common divisors, so it equals $p_1^{n1}p_2^{n2}\cdots p_k^{nk}$.
(b) For $[a, b]$ a similar argument can be given, or we can apply Exercise 1.2.31, noting that $\max\{r, s\} = r + s - \min\{r, s\}$ for any positive numbers r, s.

21. Answered in the text.

22. If every r_i is even it is easy to see that n is a perfect square. Conversely suppose n is a square. First consider the special case $n = p^r$ is a power of a prime. If $p^r = m^2$ is a square, consider the prime factorization of m. By the uniqueness (Theorem 1.11), p is the only prime that can occur, so m $= p^s$ for some s, and $p^r = m^2 = p^{2s}$. Then $r = 2s'$ is even. Now for the general case, suppose $n = m^2$ is *a* perfect square. If some r_i is odd, express $n = p_i^{ri} \cdot k$ where k is the product of the other primes involved in n.
Then p_i^{ri} and k are relatively prime and Exercise 13 implies that p_i^{ri} is a perfect square. By the special case, r_i. is even.

23. Suppose $a = p_1^{r_1}p_2^{r_2}\ldots p_k^{r_k}$ and $b = p_1^{s_1}p_2^{s_2}\ldots p_k^{s_k}$ where the p_i are distinct positive primes and $r_i \ge 0$, $s_i \ge 0$. Then $a^2 = p_1^{2r_1}p_2^{2r_2}\ldots p_k^{2r_k}$ and $b^2 = p_1^{2s_1}p_2^{2s_2}\ldots p_k^{2s_k}$. Then using Exercise 19 (twice), we have $a \mid b$ if and only if $r_i \le s_i$ for each i if and only if $2r_i \le 2s_i$ for each i if and only if $a^2 \mid b^2$.

24. This is almost identical to the previous exercise. If $n > 0$ is an integer, suppose $a = p_1^{r_1}p_2^{r_2}\ldots p_k^{r_k}$ and $b = p_1^{s_1}p_2^{s_2}\ldots p_k^{s_k}$ where the p_i are distinct positive primes and $r_i \ge 0$, $s_i \ge 0$. Then $a^n = p_1^{nr_1}p_2^{nr_2}\ldots p_k^{nr_k}$ and $b^2 = p_1^{ns_1}p_2^{ns_2}\ldots p_k^{ns_k}$. Then using Exercise 19 (twice), we have $a \mid b$ if and only if $r_i \le s_i$ for each i if and only if $nr_i \le ns_i$ for each i if and only if $a^n \mid b^n$.

25. The binomial coefficient $\binom{p}{k}$ is

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p\cdot(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}.$$

Now, the numerator is clearly divisible by p. The denominator, however, consists of a product of integers all of which are less than p. Since p is prime, none of those integers (except 1) divide p, so the product cannot have a factor of p (to make this more precise, you may wish to write the denominator as a product of primes and note that p cannot appear in the list).

26. Claim: Each $A_k = (n + 1)! + k$ is composite, for $k = 2, 3,. .. , n + 1$. Proof. Since $k \le n + 1$ we have $k \mid (n + 1)!$ and therefore $k \mid A_k$. Then A_k is composite since $I < k < A_k$.

27. By the division algorithm $p = 6k + r$ where $0 \le r < 6$. Since $p > 3$ is prime it is not divisible by 2 or 3, and we must have $r = 1$ or 5. If $p = 6k + 1$ then $p^2 = 36k^2 + 12k + 1$ and $p^2 + 2 = 36k^2 + 12k + 3$ is a multiple of 3. Similarly if $p = 6k + 5$ then $p^2 + 2 = 36k^2 + 60k + 27$ is a multiple of 3. So in each case, $p^2 + 2$ is composite.

28. The sums in question are: $1 + 2 + 4 + \cdots + 2^n$. When $n = 7$ the sum is $255 = 3{\cdot}5{\cdot}17$ and when $n = 8$ the sum is $511 = 7{\cdot}73$. Therefore the assertion is false. The interested reader can verify that this sum equals $2^{n+1} - 1$. These numbers are related to the "Mersenne primes".

29. This assertion follows immediately from the Fundamental Theorem 1.11.

30. (a) If $a^2 = 2b^2$ for positive integers a, b, compare the prime factorizations on both sides. The power of 2 occurring in the factorization of a^2 must be even (since it is a square). The power of 2 occurring in $2b^2$ must be odd. By the uniqueness of factorizations (The Fundamental Theorem) these powers of 2 must be equal, a contradiction.
(b) If $\sqrt{2}$ is rational it can be expressed as a fraction $\frac{a}{b}$ for some positive integers a, b. Clearing denominators and squaring leads to: $a^2 = 2b^2$, and part (a) applies.

31. The argument in Exercise 20 applies. More generally see Exercise 27 below.

32. Suppose all the primes can be put in a finite list $p_1, p_2, \cdots, p_k$ and consider $N = p_1 p_2 \ldots p_k + 1$. None of these p_i can divide N (since 1 can be expressed as a linear combination of p_i and N). But $N > 1$ so N must have some prime factor p. (Theorem 1.10). This p is a prime number not equal to any of the primes in our list, contrary to hypothesis.

33. Suppose n is composite, and write $n = rs$ where $1 < r, s < n$. Then, as you can see by multiplying it out,

$$2^n - 1 = (2^r - 1)\left(2^{s(r-1)} + 2^{s(r-2)} + 2^{s(r-3)} + \cdots + 2^s + 1\right).$$

Since $r > 1$, it follows that $2^r > 1$. Since $s > 1$, we see that $2^s + 1 > 1$, so that the second factor must also be greater than 1. So $2^n - 1$ has been written as the product of two integers greater than one, so it cannot be prime.

34. Proof: Since $n > 2$ we know that $n! - 1 > 1$ so it has some prime factor p. If $p \le n$ then $p \mid n!$, contrary to the fact that $p \mid n!$. Therefore $n < p < n!$.

35. We sketch the proof (b). Suppose $a > 0$ (What if $a < 0$?), $r^n = a$ and $r = u/v$ where u, v are integers and $v > 0$. Then $u^n = av^n$. If p is a prime let k be the exponent of p occurring in a (that is: $p^k \mid a$ and $p^{k+1} \nmid a$). The exponents of p occurring in u^n and in v^n must be multiples of n, so unique factorization implies k is a multiple of n. Putting all the primes together we conclude that $a = b^n$ for some integer b.

36. If p is a prime > 3 then $2 \nmid p$ and $3 \nmid p$, so by Exercise 1.2.34 we know $24 \mid p^2 - 1$. Similarly $24 \mid (q^2 - 1)$ so that $p^2 - q^2 = (p^2 - 1) - (q^2 - 1)$ is a multiple of 24.

Chapter 2

Congruence in $\mathbb{Z}$ and Modular Arithmetic

2.1 Congruence and Congruence Classes

1. (a) $2^{5-1} = 2^4 = 16 \equiv 1 \pmod 5$. (b) $4^{7-1} = 4^6 = 4096 \equiv 1 \pmod 7$.
   (c) $3^{11-1} = 3^{10} = 59049 \equiv 1 \pmod{11}$.

2. (a) Use Theorems 2.1 and 2.2: $6k + 5 \equiv 6.1 + 5 \equiv 11 \equiv 3 \pmod 4$.
   (b) $2r + 3s \equiv 2.3 + 3.(-7) \equiv -15 \equiv 5 \pmod{10}$.

3. (a) Computing the checksum gives

$$10 \cdot 3 + 9 \cdot 5 + 8 \cdot 4 + 7 \cdot 0 + 6 \cdot 9 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 1 + 2 \cdot 8 + 1 \cdot 9$$
$$= 30 + 45 + 32 + 54 + 20 + 3 + 16 + 9 = 209.$$

   Since $209 = 11 \cdot 19$, we see that $209 \equiv 0 \pmod{11}$, so that this could be a valid ISBN number.

   (b) Computing the checksum gives

$$10 \cdot 0 + 9 \cdot 0 + 8 \cdot 3 + 7 \cdot 1 + 6 \cdot 1 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 5 + 2 \cdot 9 + 1 \cdot 5$$
$$= 24 + 7 + 6 + 20 + 15 + 18 + 5 = 95.$$

   Since $95 = 11 \cdot 8 + 7$, we see that $95 \equiv 7 \pmod{11}$, so that this could not be a valid ISBN number.

   (c) Computing the checksum gives

$$10 \cdot 0 + 9 \cdot 3 + 8 \cdot 8 + 7 \cdot 5 + 6 \cdot 4 + 5 \cdot 9 + 4 \cdot 5 + 3 \cdot 9 + 2 \cdot 6 + 1 \cdot 10$$
$$= 27 + 64 + 35 + 24 + 45 + 20 + 27 + 12 + 10 = 264.$$

   Since $264 = 11 \cdot 24$, we see that $264 \equiv 0 \pmod{11}$, so that this could be a valid ISBN number.