Contents

1 Appendix

2 Hints to Problems
  Chapter 1 Hints .......................................................... 3
  Chapter 2 Hints .......................................................... 8
  Chapter 3 Hints .......................................................... 10
  Chapter 4 Hints .......................................................... 15
  Chapter 5 Hints .......................................................... 18
  Chapter 6 Hints .......................................................... 22
  Chapter 7 Hints .......................................................... 25
  Chapter 8 Hints .......................................................... 32
  Chapter 9 Hints .......................................................... 36
  Chapter 10 Hints .......................................................... 40
  Chapter 11 Hints .......................................................... 45
  Chapter 12 Hints .......................................................... 51
  Chapter 13 Hints .......................................................... 58
  Chapter 14 Hints .......................................................... 69
  Chapter 15 Hints .......................................................... 75
  Appendix Hints ......................................................... 82
Chapter 1

Appendix

TO BE INCLUDED
Chapter 2

Hints to Problems
CHAPTER 2. HINTS TO PROBLEMS

Section 1.1

1a. Try a few different options.
1b. Try a few different options.
1c. Use the Pythagorean theorem and substitute a in place of b.

3. Use the relationship between $m$ and $n$ given in section 1.1.

5a. Use the Pythagorean Theorem.
5b. Use the Pythagorean theorem along with the diagram of the tiles in the section.
5c. Use the Pythagorean theorem along with the diagram of the tiles in the section.

7. The dean’s decree can be carried out if and only if

$$(1 + \sqrt{2})N = \sqrt{2}M \iff \frac{1 + \sqrt{2}}{\sqrt{2}} = \frac{M}{N}$$

where $N$ is the number of octagonal tiles and $M$ is the number of triangular tiles. Show that the left hand side of the equation is not rational.

9a. Look at the geometric figures in this section to see how triangular and square numbers are determined.
9b. Decompose two to three different square numbers into triangles to come up with a general answer.

11a. $d$ is the hypotenuse of a right triangle. The edge of the box with length $l$, and the diagonal of the $h \times w$ rectangle form the other two sides of the triangle.
11ci. Let $\alpha$ be the factor by which you must increase the side length. Using your equation from part a, write an expression for the diagonal in terms of $\alpha$ and $x$. Set this equal to twice the diagonal length. Now solve for alpha.
11cii. Let $\alpha$ be the factor by which you must increase the side length. Find the volume of the cube in terms of $\alpha$ and $x$. Set this equal to twice the volume. Now solve for alpha.
Section 1.2

1a. Use the definition of $i$ along with rules of multiplication of positive and negative numbers.

1b. Consider the general form of a complex number, $a + bi$. Square this number and equate to -4. Expand the square into its full form using FOIL and compare the real and imaginary parts.

1c. Use the general form of a complex number, $a + bi$. Square this number and equate to -4. Expand the square into its full form using FOIL and compare the real and imaginary parts.

3. Use the definitions of natural numbers, integers, rational numbers, real numbers and complex numbers given earlier in the section.

5. Since 7 cannot be divided by 1, multiply by the dividend by 10 and incorporate a decimal point into the quotient. This will enable you to proceed with long division.

7. Use the fact that every integer is divisible by 1.

9. Rewrite $0.999...$ as $\frac{9}{10} + (\frac{9}{10})(\frac{1}{10}) + (\frac{9}{10})(\frac{1}{10})^2 + ...$

Section 1.3

1. Consider the definition of hypothesis and conclusion given in the beginning of this section to solve each part of this question.

3. Consider the definition of hypothesis and conclusion given in the beginning of this section.

5. Use the definition of an odd integer.

7. Use the definition of an odd integer and an even integer.

9. Use the fact that $n$ is an integer, coupled with the hint given in the question.

11a. Use the definition of a rational number.

11b. Use the definition of a rational number.

13. Use the definition of a rational number and an indirect proof.

15. Use an indirect proof.

17a. Start with $x_1 = x_2$. Then substitute these into the algebraic relation given in the question and proceed.
17b. Start with $y_1 = y_2$. Then substitute these into the equation given in the question and use your knowledge of algebra to proceed.

19. Consider $(x - y) + (x + y)$.

21. What is the least number of friends a guest can have? What is the greatest number of friends a guest can have? Use an indirect proof.

23. Let $x$ be an arbitrary real number. Then the reciprocal of $x$ is $1/x$. Assume that $x + 1/x < 2$ and find a contradiction. (This is an indirect proof).

Section 1.4

1. Try dividing both numbers by some simple fractions until you get an integer answer for both sets of quotients.

3a. Remember that $\sqrt{2}$ is irrational from Section 1.1.

3b. Remember that $\sqrt{2}$ is irrational from Section 1.1.

5. Follow the proof of Theorem 1.4.1

7. Follow the proof of Theorem 1.4.1. As you go along you must also prove that if $n^3$ is even then $n$ is even.

9. Rearrange the terms in the equation so that $a$ and $c$ are on one side and both terms with $\sqrt{2}$ are on the other. Use a proof by contradiction.

11. Use the definition of commensurable.

13. Use an indirect proof and the answer to exercise 7.

Section 1.5

1a. Try this formula on the first few integers.

1b. Try this formula on the first few integers.

1c. Try this formula on the first few integers.

3a. Provide a counterexample.

3b. Use the properties of even numbers to determine the answer.
3c. Provide a counterexample.
3d. Provide a counterexample.
3e. Provide a counterexample.
3f. Use the properties of even numbers to determine the answer.
5. Use the technique of negation from this section.
7a. Use the definition of a positive integer.
7b. Use the definition of a negative integer.
7c. Work with \( n = 0 \).
9. Construct \( p \) and \( q \) using the given equations.
11. Use a proof by contradiction.
13. Provide a counterexample.
Section 2.1

7a. Let \( P(n) = \frac{n(n+1)}{2} \). Rewrite \( P(k+1) \) in terms of \( P(k) \).

7b. Let \( P(n) = \frac{n(n+1)(n+2)}{6} \). Rewrite \( P(k+1) \) in terms of \( P(k) \).

9. Use induction. Don’t forget to use the inductive hypothesis when looking into \( P(k+1) \). Then use algebra to get it into the form of \( (k+1) (2(k+1) + 1) \).

11. Use induction. Don’t forget to use the inductive hypothesis when looking into \( P(k+1) \). Then use algebra to get it into the proper form.

13. If using induction to prove, let your hypothesis be that \( k! \leq k^k \).

15. Utilizing the result from exercise 14 along with some simple algebra, the result is easily obtained. Alternatively, induction can be used as before.

17. Play the game for the given values of \( n \). A formula will arise fairly easily.

19. Use the formula you obtained in 17 and proved in 18.

21. Let \( P(n) = \frac{n^3 - n}{6} \). Rewrite \( P(k+1) \) in terms of \( P(k) \) and notice that \( k \) or \( k+1 \) must be even.

23. Consider the case when \( k + 1 = 2 \).

25. When looking at \( P(k+1) \), try ignoring one of the lines and then applying the inductive hypothesis. Then put the line back in, and see what you can do next.

27. Notice that a \( 2^{k+1} \times 2^{k+1} \) checkerboard can be divided into four \( 2^k \times 2^k \) boards. Try re-orienting some of the boards after using the inductive hypothesis.

Section 2.2

7c. Use strong induction and the fact that the Base Case \( (n = 1, 2) \) is given by the definition of \( G_1 \) and \( G_2 \).

9. Similar to Exercise 7c, it just requires more algebraic simplification after substitution.

15. By the way the game works, there will always be two heaps at the beginning of someone’s turn. So you can always eat a heap. What does this imply about possible loss methods?

17. Use the fact that the sum of two odd numbers must be even. If you begin with at least 1 even heap, split this heap into two heaps both with an odd number of peanuts. If your opponent can still win, she is forced to split a heap that has an odd number of peanuts.
Section 2.3

3. Notice that the ratio does not depend on the scale of the diagram, so you can set any part of it to any value you wish.

5. Use induction. Remember: odd + odd = even, etc.

7. Use induction. Remember: $a^x \cdot a^y = a^{x+y}$.

11. Use induction.

13. Use induction and consider $F_{k+2}^2 - F_{k+1}F_{k+3}$.

15a. For any real number $x$, if $|x| < 1$ then $x^n < x$ for $n \geq 1$.

15b. Use the result from part a.

Section 2.4

1. Since $\varphi$ is between 1 and 2, its fractional part is $\varphi - 1$. Similarly, since $\varphi$ is between $-1$ and 0, its fractional part is $-\varphi$.

9. Use the expressions you have obtained for $\varphi^n$ and $\varphi^n$ in exercises 6d and 8a. [You will have to prove 6d is true in exercise 10. 8a can be proven in a similar manner.]

11. What happens if you square the expression?
Section 3.1

1. a. False  b. True  c. False  d. True  e. True  f. False  
g. True  h. True  i. False  j. True  k. False  l. True

3. ±1, ±2, ±4, ±5, ±10, ±20.

5. ±1, ±2, ±4

7. ±1, ±2, ±4

9. If $c = 0$, then $a$ and $b$ can be anything and we still have $ac|bc$. For example, let $a = 5$ and $b = 3$. Then $a \nmid b$ but $ac = bc = 0$ so $ac|bc$.

11. If $a|1$, then there exists some $k \in \mathbb{Z}$ such that $ak = 1$. Now try looking at this with absolute values.

13. $a|b$ implies some $k \in \mathbb{Z}$ such that $ak = b$. What about $b|c$? Can we put these things together?

15. If $a|b$ and $b|a$, then there exist $j, k \in \mathbb{Z}$ such that $a = bj$ and $b = ak$. Thus, $a = bj = akj$. This gives us two possible cases, one of which says something about the value of $a$ and the other tells us the value of $kj$.

17. (a) If $d|x$, then there exists some $k \in \mathbb{Z}$ such that $dk = x$. Where can we substitute this new expression for $x$? What will that tell us?  
(b) If $d|x$ and $d|y$, then there exist $j, k \in \mathbb{Z}$ such that $dj = x$ and $dk = y$. Where can we substitute these new expression? What will we be able to show from that?

19. How would you get rid of the $b$ from $(b + c)$? Look at what you did; can you use the linear combination lemma along those lines?

21. Who said brute force doesn’t solve things?

23. (a) What numbers above have an odd number of positive divisors? They are 1, 4, 9, 16, 25. Look familiar?  
(b) Divisors of positive integers tend to come in pairs. Why is this? Well, if $j|n$, then there is some $k \in \mathbb{Z}$ such that $jk = n$. But that means $k|n$ as well. So how can we have an odd number of divisors if our divisors come in pairs?

25. By the problem statement, we have that $\frac{1}{a} + \frac{1}{b} = k$ for some $k \in \mathbb{N}$. What can we multiply both sides by to get rid of the fractions? By using algebra, will we be able to say anything about what $a$ divides? what $b$ divides? What will these facts imply?

27. (a) How can you factor $x^2 + 3x + 2$?
(b) Remember that you can factor out negative numbers as well.

(c) Find a counter-example.

(d) Every integer is even or odd. Which one is \((x^2 + x)\)? Can we look at \(x\)? What does \(x^2 + x\) factor to? Remember that multiplying any number by an even number will make the product even.

**Section 3.2**

1. Look just underneath Definition 3.2.2.

3. \((3, 5), (5, 7), (11, 13), (17, 19), \text{ and many, many more.}\)

5. (a) \(-2, -3, \text{ and } -47.\)

(b) You know that \(b \in \mathbb{N}, b = 0, \text{ or } -b \in \mathbb{N}\) by trichotomy. Furthermore, \(b \neq 0\) since it’s prime. Try tackling each case on its own and look at the relations between the old definition and the new one. Finally, note that if \(b\) is prime by the new definition, \(-b\) must be as well.

7. Use the Linear Combination Lemma.

9. Think in terms of the factors that make up \(a\) and \(b\).

11. Clearly you can make all the composite numbers since they’re all already in your basket. But what would it mean if you could make a prime out of composite numbers?

13. By Goldbach’s conjecture, you can make any even number. Now what are some relations between the evens and the odds. How do you make odds out of evens?

15. Factor \(n^3 + 1\) into the product of two polynomials. Then show that it does not meet the definition of a prime number.

17. Use prime factorization: \(n = p_1^{a_1} \cdots p_m^{a_m}\) where each \(p_i < n\). Now look at the two cases of where \(m \geq 2\) and \(m = 1\) and think about how a factorial works.

19. Consider the case when \(n\) is even and when \(n\) is odd separately. In each case, find a composite integer \(a\) such that \(n\) can be written as \((n - a) + a.\)

21. (a) Factor \(a^n - 1\) into the product of two polynomials. Then use the fact that \(a^n - 1\) is prime.

(b) Use a proof by contradiction.
23. Use brute force linear combinations at first to get a feel for the problem in (a), (b), and (c). Once you get to (d) and (e) though, you’ll need something more elegant. For (d), begin by writing out all the numbers that you can sum to using just 6 and 9. Then all the numbers you can sum to using exactly one 20 along with 6’s and 9’s. Continue to move your number of 20’s up until you have covered all of the numbers past a certain point. Figure out how to adapt this method for part (e).

Section 3.3

1. Follow the method given earlier in the section, and remember you only have to cross out primes below \(\sqrt{288} \approx 16.97\). Once finished, you can check your answer by using the internet.

3. To solve this problem, you’ll need to find the number of primes between 8.58 \cdot 10^9 and 8.59 \cdot 10^9. You can do this by using the approximation \(\pi(n) \approx \frac{n}{\log n}\) and then looking at the difference between the two results.

5. Try looking at \(40^2 + 40 + 41\) and \(41^2 + 41 + 41\). Can you factor these in such a way to illustrate compositeness?

7. The first composite number is \(h(80)\).

9. For (a) and (b), it’s probably easiest to choose small numbers. For part (c), use the Linear Combination Lemma.

11. (a) Let \(k = p_1 \cdots p_n + 1\). From the proof of Theorem 3.3.1, \(k\) cannot contain any prime factor \(p_i\) such that \(i \leq n\).
   (b) Recall that \(2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1\).
   (c) Let \(x\) be an element of \(\mathbb{N}\). Define \(r = \log_2(\log_2(x))\). Now consider \(p_r\). (Note that \(r\) may not be a natural number. Consider the case when \(r\) is an element of \(\mathbb{N}\) and when \(r\) is not an element of \(\mathbb{N}\) separately.)

13. (a) Use the fact that if an integer \(d\) divides some number \(n\), then \(d\) cannot divide \(n + 1\).
   (b) Use a proof by contradiction. Consider \(p_n!\) where \(p_n\) is the greatest prime.

15. Let \(a \in \mathbb{N}\) and consider the expression \(a! + n\). Under what conditions will the expression be composite (think in terms of the Linear Combination Lemma).

17. (a) Use the basic properties of exponents to rewrite \(F(n) - 1\) in terms of \(F(m) - 1\) raised to some power. Then use what you know about binomial expansions to find a contradiction.
   (b) Every Fermat number can be factored into primes. However, by the above, we know no factor can appear in multiple Fermat numbers. Now use the fact that there are infinitely many Fermat numbers.
Section 3.4

1. (a) 11, (b) 7, (c) 3, (d) 99, (e) 1, (f) 2, (g) 1, (h) 11, (i) 1, (j) 3, (k) 1.

3. Think of the primes as building blocks.

5. Find a counter-example.

7. Use the definition of a prime number.

9. Show that \( a \) fulfills the definition of the \( \gcd \) by showing that any common divisor \( d \) is less than or equal to \( a \).

11. Let \( d = \gcd(a, b) = \text{lcm}(a, b) \). Then \( d|a \) and \( d|b \). Also, \( a|d \) and \( b|d \). What does this tell us in terms of absolute values?

13. Use Lemma 3.4.4.

15. It suffices to show that \( S \) is nonempty.

17. Ah, brute force: is there anything it can’t solve?

19. \( \gcd(k, \text{lcm}(a, b)) \).

21. \( \gcd(a, b, c) \).

23. Let \( m = \text{lcm}(a, b) \), then \( ka|km \) and \( kb|km \), so \( km \) is a common multiple of \( ka \) and \( kb \). Now use contradiction to show that no \( n < km \) can be a common multiple. Notice that \( ka|n \) implies that \( k|n \).

25. Prove by induction and use the recurrence relation of the Fibonacci numbers.

Section 3.5

1. (a) 85 = 4 \cdot 19 + 9, (b) 132 = 11 \cdot 12 + 0, (c) 573 = 3 \cdot 191 + 0, (d) \(-45 = -7 \cdot 7 + 4\), (e) \(90 = 1 \cdot 89 + 1\), (f) 0 = 0 \cdot 17 + 0.

3. 0, 1, 2, 3, 4, 5.

5. (a) Clearly 3 and 5 are both in \( S \). (b) 1. (c) If 1 is in the set, we can take multiples of the combination used to produce it, and make any natural number we want. (d) See (c).

7. Try \( a = b = x = 2 \).

9. If \( b < 0 \), then \( 0 \leq r < b \) implies \( 0 < 0 \)!
11. Use transitivity of division.

13. Let \( x = -|a| \).

15. Divide \( n \) by 3. There are only three possibilities for the remainder: 0, 1, and 2. Work with these three cases.

17. Use the Division Theorem to divide \( n \) by 5.

19. Other than 2, no prime can be even. Thus, any prime must be of the form \( 4k + 1 \) or \( 4k + 3 \).
   For (e), compute \( p^2 - 1 \) for each of these two possibilities.

21. Use the result from Exercise 18e.

23. \( (2345)_8 = (1642)_9 \).

25. Let \( n = r_kb^k + \ldots + r_1b^1 + r_0b^0 \). Then \( n + 1 = r_kb^k + \ldots + r_1b^1 + (r_0 + 1)b^0 \). There are two cases to consider: \( r_0 + 1 < b \) and \( r_0 + 1 = b \). In the latter case, find the smallest \( r_i \) such that \( r_i + 1 < b \).

27. I. Since \( a \neq 0 \), either \( a \) or \( -a \) is greater than 0.
   II. Since \( d \in S \), we have \( d = ax + by \) for some \( x, y \in \mathbb{Z} \).
   III. Use the Division Theorem to write \( b = qd + r \) and then show that \( r \) must equal 0.

29. (a) Let \( a = 4k + 1 \) and \( b = 4j + 1 \). Multiply \( a \) and \( b \), and then use algebraic manipulation.
   (b) Use a proof by induction.
   (c) Consider the set of prime factors of \( n = 4k + 3 \) and use the result from part (b).

Section 3.6

1. (a) 11, (b) 7, (c) 5

3. (a) 3, (b) \( \frac{\text{lcm}(50, b)}{50} \), (c) 12

5. (a) 1.3, (b) 3.8, (c) The greatest common measure of three real numbers \( x, y \) and \( z \) is the largest real number \( f \) such that \( x = n \cdot f \), \( y = m \cdot f \) and \( z = q \cdot f \) where \( n, m \) and \( q \) are integers, (d) \( 3\sqrt{2} \).
Section 4.1

1. \[150 = 2 \cdot 54 + 42,\]
   \[54 = 1 \cdot 42 + 12,\]
   \[42 = 3 \cdot 12 + 6,\]
   \[12 = 2 \cdot 6 + 0.\]

3. (a) 5 steps:
   \[19 = 1 \cdot 11 + 8\]
   \[11 = 1 \cdot 8 + 3\]
   \[8 = 2 \cdot 3 + 2\]
   \[3 = 1 \cdot 2 + 1\]
   \[2 = 2 \cdot 1 + 0\]

   (b) 3 steps:
   \[124 = 3 \cdot 36 + 16\]
   \[36 = 2 \cdot 16 + 4\]
   \[16 = 4 \cdot 4 + 0\]

   (c) 2 steps:
   \[55,029 = 4 \cdot 13,753 + 17\]
   \[13,753 = 809 \cdot 17 + 0\]

   (d) 3 steps:
   \[1,111,111 = 100 \cdot 11,111 + 11\]
   \[11,111 = 1010 \cdot 11 + 1\]
   \[11 = 11 \cdot 1 + 0\]

5. Any pair such that the remainder will evenly divide the quotient works.

7. The algorithm takes two steps.

   \[7k + 14 = 2(3k + 6) + k + 2\]
   \[3k + 6 = 3(k + 2) + 0.\]

9. (a) Write \(r_1\) as a linear combination of \(a\) and \(b\).

   (b) Solve for \(r_2\). Now write \(r_2\) as a linear combination of \(a\) and \(b\).

   (c) Think in terms of induction.
11. Think in terms of contradiction and make sure to double-check your hypothesis.

13. Hmmm. Those numbers from the above two exercises sure look like they’re being made in the same way that Fibonacci numbers get made...

15.

17.

**Section 4.2**

1. (a) 1, (b) 3, (c) 2, (d) 36, (e) 17, (f) 1.

3. The algorithm will cycle down through all of the Fibonacci numbers beneath the pair you start with.

5. Hopefully you know how to write computer programs...

7. (a) 40, (b) 29.

9. Apply the Euclidean Algorithm to \(a\) and \(b\). Now consider the resulting array of equations. What do you see when you multiply all of those equations by \(k\)?

11. (a) 4,785 steps, (b) About half a second, (c) Since \(a\) has 1,000 digits, \(\sqrt{a}\) will have 500.

13. First, notice that we have:

\[
gcd(F_m, F_{m+n}) = gcd(F_m, F_m F_{n+1} + F_{m-1} F_n) \\
= gcd(F_m, F_{m-1} F_n) \text{ since } F_m | F_m F_{n+1}. \\
= gcd(F_m, F_n) \text{ since } gcd(F_m, F_{m-1}) = 1.
\]

Now show that for any \(q, r \in \mathbb{N}\), \(gcd(F_{qm+r}, F_m) = gcd(F_r, F_m)\). Finally, with this piece of information, apply the Euclidean algorithm on the Fibonacci index numbers.

**Section 4.3**

1. \[
\begin{align*}
\frac{19}{14} &= 2 \cdot \frac{1}{2} + \frac{5}{14} \\
\frac{1}{2} &= 7 \cdot \frac{1}{14} + \frac{1}{2} \\
\frac{5}{3} &= 2 \cdot \frac{2}{14} + \frac{1}{3} \\
\frac{2}{5} &= 2 \cdot \frac{1}{14} + 0.
\end{align*}
\]
3. In general, the “gcd” — the smallest square needed to fill the rectangle — of \( \frac{a}{10} \) and \( \frac{b}{4} \) is \( \gcd(a, b) \).

5. Follow the method used for a \( \sqrt{2} \times 1 \) rectangle. Continue to compare sides until you find a pair that are similar.

7. Can you show that this rectangle is similar to one where the sides are integers?

9. Can you show that \( CEF \) is an isosceles triangle?

11. By assumption, we know that \( AB \) and \( AC \) are multiples of \( \delta \). Can you show that \( EF \) is a linear combination of those two sides?

13. Consider that \( s_1 = s_2 + d_2 \).
Section 5.1

1. (a) Let $x$ be the length of Diophantus’ life in years. Then from the problem we have $x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4$.

(b) From (a) we can deduce that Diophantus lived until he was 84, he spent 14 years as a boy, he grew a beard at 21, he married at 33, his son was born when he was 38 and he was 80 when his son died.

3. \{..., (−11, 8), (−4, 3), (10, −7), (17, −12), ...\}. In general, $(3+7k, −2−5k)$ is an integral solution for all $k \in \mathbb{Z}$.

5. Solutions are of the form $(-1 + 3t, 1 − 2t)$ for integers $t$.

7. $7X + 3Y = 1$. It passes through all points of the form $(-2 + 3t, 5 + 7t)$.

9. Use a proof by contradiction. Follow the proof of Theorem 5.1.1.

11. Notice: $3|21$, $3|51$, and $3|12$. If a solution did exist, what would that imply by the Linear Combination Lemma?


15. $X = 3, Y = 2$.

17. Re-arrange to get $X^2 = 2 + 5Y$. Thus $2 + 5Y \geq 0$, so the right side will always end in either a 2 or a 7. Are there any perfect squares that end in a 2 or a 7?

19. Plug $ax$, $ay$ and $az$ into the Pythagorean Theorem.

21. Just use a value of $n$ that will fail to match your examples.

Section 5.2

1. (a) $(−1, 3)$ is a solution, for example.

(b) The given solution corresponds to a diagram with a potato and one 11 lb brick on one side of the scale, and three 4 lb bricks on the other.

(c) $81 = 7 \cdot 11 + 4$ so $4 = 81 − 7 \cdot 11$.

(d) $1 = (−1)11 + 3 \cdot 4 = (−1)11 + 3(81 − 7 \cdot 11) = 3 \cdot 81 + (−22)11$ so $(3, −22)$ is a solution to $81X + 11Y = 1$. In terms of the potato problem, three 81 lb bricks balances twenty two 11 lb bricks plus a 1 lb potato.
1. \( 97 = 4 \cdot 23 + 5, \)
   \[ 23 = 4 \cdot 5 + 3. \]
   \[ 5 = 1 \cdot 3 + 2. \]
   \[ 3 = 1 \cdot 2 + 1. \]
   Thus, \( 1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2(23 - 4 \cdot 5) - 5 = 2 \cdot 23 - 9 \cdot 5 = 2 \cdot 23 - 9(97 - 4 \cdot 23) = 38 \cdot 23 - 9 \cdot 97, \) so \((38, -9)\) is a solution.

5. \( 500 = 1 \cdot 423 + 77, \)
   \[ 423 = 5 \cdot 77 + 38, \]
   \[ 77 = 2 \cdot 38 + 1. \]
   Thus, \( 1 = 77 - 2 \cdot 38 = 77 - 2(423 - 5 \cdot 77) = 11 \cdot 77 - 2 \cdot 423 = 11(500 - 423) - 2 \cdot 423 = 11 \cdot 500 - 13 \cdot 423, \) so \((11, -13)\) is a solution.

7. The method gives \((-2, -1)\) as a solution.

9. 35 and 49 have a common factor of 7, so there is no solution.

11. Begin with the fact that \(47x_0 + 6y_0 = 1,\) then use the substitution \(6 = 100 - 2 \cdot 47.\)

13. By Theorem 5.1.2, for the Diophantine equation to have a solution, we know \(\gcd(a, a+2) = 1.\)
   Combine this with using the Euclidean Algorithm.

15. Notice that \(0 \leq r < b\) and \(\gcd(a, b) = \gcd(b, r).\)

**Section 5.3**

1. \(\gcd(91, 21) = 7.\)
   (a) No solution.
   (b) Has a solution.
   (c) No solution.
   (d) Has a solution.
   (e) Has a solution.
   (f) No solution.

3. No solution since \(\gcd(22, 111) = 11 \nmid 1.\)

5. \((-60, 70).\)

7. No solution since \(\gcd(24, 36) = 12 \nmid 18.\)

9. \((22, 11).\)
11. Use Theorem 5.3.2.

13. Use Theorem 5.3.2.

15. (a) Use the methods previously outlined in the chapter.
      (b) Use the solution to the Diophantine equation $7X + 24Y = 2$.
      (c) Use the solution to the Diophantine equation $73X + 55Y = 1$.
      (d) Use the solution to the Diophantine equation $15X + 41Y = 3$.

17. From Exercise 16, you can show that $\gcd(\gcd(a, b), c) \leq \gcd(a, b, c)$. To show that $\gcd(a, b, c) \leq \gcd(\gcd(a, b), c)$, think in terms of linear combinations and their relation to the gcd.

19. Given that $\gcd(63, 28) = 7$, we can find the solution $(-26, 13, -1)$.

21. Use the result from Exercise 17.

23. Use the result from Exercise 21.

25. For the $\Rightarrow$ direction, suppose that there exist $x, y \in \mathbb{N}$ such that $s + xa = t + yb$ and figure out a way to apply Theorem 5.3.2. For the $\Leftarrow$ direction, suppose $\gcd(a, b) \mid (t - s)$. Apply Theorem 5.3.2, and work with what this gives you.

**Section 5.4**

1. a) $X, Y = -4, 7$
      b) $(-4 + 11k, 7 - 19k)$

3. a) $X, Y = 964, -481$
      b) $(964 + 2411k, -481 - 1203k)$

5. $\gcd(1155, 29393) = 7 > 1$, so there is no solution.

7. $\gcd(429, 242) = 11 > 1$, so there is no solution.

9. a) $X, Y = -23, -81$ using previous Exercise.
      b) $(-23 + 48k, -81 + 169k)$

      b) $(-40 + 66k, 24 - 39k)$

13. a) $X, Y = -5000, 4000$.
      b) $(-5000 + 99k, 4000 - 81k)$
15. a) \(X, Y = 650, -300\)
   
b) \((650 + 106k, -300 - 49k)\)

17. Notice that equation (9) and equation (10) differ by \(k = 25\).

19. (a) Find an answer that is not in \(S\)
    
    (b) You can’t apply a theorem unless you meet its “if”-requirement.

21. If \(p\) is prime and \(p|d\), then \(p|a\), so \(p \nmid b\). Thus \(\gcd(b, d) = 1\).

23. Since \(\gcd(a, b) = 1\), if \(p|b\), then \(p \nmid a\).

25. Look at the set of solutions \(S\) from Theorem 5.4.1.

27. Same as above.

29. A solution is positive if \(cx - bk > 0\) and \(cy + ak > 0\). Use these inequalities and the fact that \(c > abn\) to find \(n\) values of \(k\) that give a positive solution.

31. (a) \(4 \cdot 5 + 2 \cdot 7 = 34\).

   (b) Use brute force.

   (c) 23.

   (d) Let \(k\) be the largest number of chicken nuggets you cannot buy. Show that \(k + 1, k + 2, k + 3, k + 4\) and \(k + 5\) can all be written as \(5X + 7Y\). Now show how any number \(n > k\) can be derived from these five consecutive numbers.
Section 6.1

1.(a) $2^4 \cdot 3^3 \cdot 5$
(b) $7^3$
(c) $2^{10}$
(d) $2^3 \cdot 5^3$
(e) $2^2 \cdot 3^2$
(f) $5^3 \cdot 17$

3. Use $2^{2n} - 1 = (2^n - 1)(2^n + 1)$.

5. Use $p! = p(p-1)!$ and the definition of a prime number to show that $(p-1)!$ does not contain any factor of $p$.

7. Use induction on $r$ by setting $a = a_1...a_{r-1}$, $b = a_r$ and applying proposition 6.1.2.

9.(a) First show that it is equal to the number of factors of 5 in 100!. Find this number by counting the numbers between 1 and 100 which are divisible by 5 and $25=5^2$.

(b) Follow (a).

11. Use proposition 6.1.3.

13. Use the fundamental theorem of arithmetic to show that $b$ must have a factor of 5.

15. Use lemma 3.1.3.

17. For the first part, use the fact that $n$ is not squarefree if and only if there is a prime $p$ such that $p^2 | n$. For the second part, use the fundamental theorem of arithmetic.

19. Use a proof by contradiction. If $\gcd(a^2, b^2) = k \neq 1$, then there is a prime $p$ such that $p|a^2$ and $p|b^2$. Use exercise 11 to show $\gcd(a, b) \neq 1$.

21. Write $p^2 - q^2 = (p-q)(p+q)$. Using this factorization show that $p^2 - q^2$ is divisible by 4 and 3 hence by 12.

23. Show that $p = 3k + 2$ for some odd number $k$. Then $p + (p + 2) = 6(k + 1)$ is divisible by 12.
Section 6.2

1. (a) 8.
   (b) 5.
   (c) 6.
   (d) 16.
   (e) 9.
   (f) 101.
   (g) 130.
   (h) 10201.

3. (a) $5^3 \cdot 7^6 \cdot 13$.
   (b) $2^9 \cdot 3^2 \cdot 5^4 \cdot 7^2 \cdot 13^3 \cdot 17^2 \cdot 29$.

5. 2, 3, 5.

7. 6, 8, 10.

9. (a) 91 years.
   (b) 119 years.
   (c) 1547 years.
   (d) 42 more years.

11. Write $a = 5a_1$ and $b = 5b_1$. Then deduce that $\gcd(a_1, b_1) = 1$ and $\text{lcm}(a_1, b_1) = a_1b_1 = 108$. Apply the FTA to find all possible pairs $(a_1, b_1)$.

13. Follow the proof of proposition 6.2.9.

15. Follow the proof of theorem 6.2.7.

17. Set $a = 30$, $c = 24$ and find $b$.

19. Show that $\gcd(b, c) = 24, \gcd(a, c) = 84$ imply that 4 is a factor of $\gcd(a, b)$. Hence the answer is no.

21. Follow the proof of lemma 6.2.8.
23. Use the FTA and proposition 6.2.3.

25. Follow theorem 6.2.7 and use exercise 21.

27. If \( x = \frac{a}{b} \) (where \( a, b \) are integers and satisfy \( \gcd(a, b) = 1 \)) is a solution, then \( a^n = -b(c_{n-1}a^{n-1} + c_{n-2}a^{n-2}b + \cdots + c_0b^{n-1}) \). So \( b|a^n \). Show that \( x \) must be an integer.

29. Use the fact that \( n \) is a perfect square if and only if the number of prime factors \( p \) in \( n \) is even.

31. Follow the proof of proposition 6.2.4.

33. \( abc \).

35. \( \text{lcm}(a, b, c) \).
Section 7.1

1.(a) $17 - (-163) = 4 \cdot 45$
(b) $617 - 1 = 7 \cdot 88$
(c) $-17 - (-71) = 6 \cdot 9$
(d) $192 - 0 = 24 \cdot 8$

3.(a) $36 = 2(13) + 10 = 10 \pmod{13}$.
(b) $15 = 5(3) + 0 = 0 \pmod{3}$.
(c) $5 \ast 12 = 60 = 8(7) + 4 = 4 \pmod{7}$.

5. The congruence classes are: {$\ldots, -4, 0, 4, 8, \ldots$}, {$\ldots, -3, 1, 5, 9, \ldots$}, {$\ldots, -2, 2, 6, 10, \ldots$}, and {$\ldots, -1, 3, 7, 11, \ldots$}.

7.(a) It is the congruence class of $15 \pmod{20}$:
{$\ldots, -25, -5, 15, 35, 55, 75, \ldots$}
(b) It is the congruence class of $0 \pmod{9}$:
{$\ldots, -27, -18, -9, 0, 9, 18, \ldots$}
(c) It is the congruence class of $37 \pmod{35}$, which is the same as the congruent class of $2 \pmod{35}$:
{$\ldots, -68, -33, 2, 37, 72, \ldots$}

9.(a) $75 - 5 = 70$, so $m|70$. The numbers $m > 1$ that divide 70 are 2, 5, 10, 7, 14, 35, and 70.
(b) $100 - (-1) = 101$, so $m|101$. 101 is prime, so $m = 101$ is the only possible modulus.
(c) $15 - (-5) = 20$, so $m|20$. The numbers $m > 1$ that divide 20 are 2, 4, 5, 10, and 20.
(d) $-46 - 3 = -49$, so $m| -49$. The numbers $m > 1$ that divide $-49$ are 7 and 49.

11. Use definition 7.1.1.

13. Use proposition 7.1.2 and lemma 3.1.3.

15. Use proposition 7.1.2.

17. Use the symmetry property of theorem 7.1.6.

19.(a) It is an equivalence relation.
(b) It is not symmetric.

(c) It is an equivalence relation.

(d) It is not symmetric.

(e) It is an equivalence relation.

(f) It is an equivalence relation.

(g) It does not have any properties of equivalence relations.

(h) It is an equivalence relation.

(i) It is not reflexive and transitive.

(j) It is not transitive.

(k) It is not reflexive and transitive.

(l) It is an equivalence relation.

21.(a) 19 j).

(b) 19 d).

(c) Consider the following relation on real numbers, $x \sim y$ if $xy \neq 0$. Show that it is both symmetric and transitive but not reflexive because $0 \sim 0$ is not valid.

23. Show that if two equivalence classes have a nonempty intersection, then they are equal.
25. (a) \((1, 1), (1, 3), (3, 1), (3, 3), (2, 2), (2, 4), (4, 2), (4, 4), (5, 5)\).

(b) For example, \(P_1 = \{1\}, P_2 = \{2\}, P_3 = \{3\}, P_4 = \{4\}, P_5 = \{5\}\). The ordered pairs are \((1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\).

27. \(R_1 = \{(1, 1), (2, 2), (3, 3), (1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 2)\}, R_2 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}, R_3 = \{(1, 1), (2, 2), (3, 3), (1, 3), (3, 1)\}, R_4 = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}, R_5 = \{(1, 1), (2, 2), (3, 3)\}.

Section 7.2

1. (a) \(4 + 3 = 7 \equiv 2 \pmod{7}\).

(b) \(1 + 5 = 6\).

(c) \(1 + 3 = 4\).

(d) \(5 + 5 = 10 \equiv 3 \pmod{7}\).

3. (a) \(6 + 8 + 1 + 6 + 5 + 4 = 30 \equiv 3 \pmod{9}\).

(b) \(6 + 8 + 8 + 4 + 5 = 31 \equiv 4 \pmod{9}\).

(c) \(8 + 4 + 9 + 7 + 1 + 8 + 3 + 2 + 3 + 1 + 3 + 2 + 5 + 6 = 62 \equiv 8 \pmod{9}\).

(d) \(1 + 1 + 8 + 7 + 5 + 8 + 9 + 5 + 7 + 3 + 4 + 2 + 5 = 65 \equiv 2 \pmod{9}\).

(e) \(3 + 4 + 8 + 2 = 17 \equiv 2 \pmod{9}\).

5. (a) 6.

(b) 6.

(c) 6.

(d) 0.

(e) 7.

7. (a) 2.

(b) 1.

(c) 1 and 6.

(d) There does not exist such a number.
CHAPTER 2. HINTS TO PROBLEMS

9. \(63! = 61! \times 62 \times 63 \mod 71 = (-9) \times (-8) \mod 71 = 1 \mod 71\). This means that \(63! \equiv 61! \mod 71\), because they only differ multiplicatively by 1.

11. Use theorem 7.1.2.

13. Use theorem 7.2.1.

15. Use theorem 7.2.1 with \(r = s = -1\).

17. Note that the last two digits of \(d - e\) are zero hence it is divisible by 100.

19. (a) Note that multiplying a number by 10 change the last digit to zero.

(b) Note that multiplying a number by 5 change the last digit to 0 or 5.

21. Use \(d = d_{n-1}d_{n-2}...d_3d_2d_1d_0 \equiv d_2d_1d_0 \mod 8\).

23. Use the test for divisibility by 9 (corollary 7.2.3.).

25. No. Use the test for divisibility by 11.

27. (a) Use \(F_{80} = F_{79} + F_{78}\) and theorem 7.2.1.

(b) \(1, 1, 2, 0, 2, 1, 0, 1, 1, \ldots\) from here it repeats.

(c) \(1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, \ldots\) from here it repeats.

(d) \(1, 1, 2, 3, 5, 2, 1, 3, 4, 1, 5, 0, 5, 5, 4, 3, 1, 4, 5, 3, 2, 5, 1, 0, 1, 1, \ldots\) from here it repeats.

(e) Note that the Fibonacci sequence modulo 6 repeats after 24 terms, and the Fibonacci sequence modulo 4 repeats after 6 terms, so it will also repeat after 24 terms. Conclude that after 24 terms the Fibonacci sequence will be equal modulo 12 as well.

(f) Note that if two numbers reduced modulo \(m\) repeat right next to each other then the sequence is periodic and there are only \(m\) equivalence classes.

(g) Use (f) and note that if \(F_{k+2} \equiv F_{k+p+2} \mod m\) and \(F_{k+1} \equiv F_{k+p+1} \mod m\) then \(F_k \equiv F_{k+p} \mod m\).

29. (a) Show that \(d = d_{m-1}d_{m-2}...d_3d_2d_1d_0 \equiv d_{n-1}d_{n-2}...d_3d_2d_1d_0 \mod 2^n\). Note that \(d - d_{n-1}d_{n-2}...d_3d_2d_1d_0\) is divisible by \(10^n\).

(b) \(2^6\).

(c) Show that \(d = d_{m-1}d_{m-2}...d_3d_2d_1d_0 \equiv d_{n-1}d_{n-2}...d_3d_2d_1d_0 \mod 5^n\). Note that \(d - d_{n-1}d_{n-2}...d_3d_2d_1d_0\) is divisible by \(10^n\).
31. Reduce $10^n$ modulo 13 and follow method 7.2.4 to obtain $d = d_{n-1}\ldots d_7d_6d_5d_4d_3d_2d_1d_0 = d_0 + 10d_1 + 100d_2 + \ldots + 10^{n-1}d_{n-1} \equiv d_0 - 3d_1 - 4d_2 - d_3 + 3d_4 + 4d_5 + d_6 - 3d_7\ldots \pmod{13}$.

33. First note that 645 = 3*5*43. Using $2^2 = 1 \pmod{3}$, $2^2 = -1 \pmod{5}$ and $2^7 = -1 \pmod{43}$ show that $2^{14} = 1 \pmod{645}$. Finally since 14|644 conclude that $2^{644} - 1 = 0 \pmod{645}$.

Section 7.3

1. (a) 4.
   (b) 2.
   (c) 0.

3. (a) 0.
   (b) 4.
   (c) 8.

5. (a) 8.
   (b) 3.
   (c) 8.

7. (a) 78945612390, for example.
   (b) Any transposition within the first 10 digits will produce a valid number, e.g. 79845612390.
   (c) Interchanging the last digit with a different digit among the first ten will produce an invalid number, e.g. 78945612309.

9. Show that if the i-th digit is $x$ originally but replaced by $y$ by mistake then $i(x - y)$ is divisible by 11 and deduce that $x = y$.

Section 7.4

1. Any $x \equiv 9 \pmod{10}$ is a solution.

3. Any $x \equiv 159 \pmod{175}$ is a solution.

5. There is no solution.
7. (a) We would have to solve the equation $8x - 10y = 1$, but 1 is not divisible by 2.

(b) We would have to solve the equation $169x - 325y = 40$, but 40 is not divisible by 13.

9. (a) 8.

(b) 6.

(c) 26.

11. (a) No. For example take $s = 0, t = 140$.

(b) Yes. Note that $lcm(20, 35) = 140$.

(c) Yes.

13. $x \equiv 8 \pmod{15}$ is the only solution.

15. $x \equiv 50 \pmod{52}$ is the only solution.

17. There are two non-congruent solutions: $x \equiv 7 \pmod{30}$ and $x \equiv 22 \pmod{30}$.

19. Show that if $x_0$ is a solution then $y$ is a solution if and only if $y - x_0$ is divisible by $d$.

21. Follow the proof of theorem 7.4.1 and use theorem 5.4.2.

23. Show that among possibilities $(1, 3, 4), (1, 3, 9), (1, 8, 4), (1, 8, 9), (7, 3, 4), (7, 3, 9)$

    $(7, 8, 4), (7, 8, 9)$, there are only six different possibilities for the value of $x$ modulo $m$.

25. (a) Use theorem 7.4.2.

(b) Take $k$ and $l$ to be the reductions of $s$ modulo $a$ and $b$, respectively.

27. Any $x \equiv 5566 \pmod{10626}$ is a solution.

29. Show that there is no solution.

31. Note that in both cases, you need to solve a system of congruences!

33. Write the corresponding system of congruences to obtain that the number of soldiers in the company must be $2101 \pmod{2310}$.

35. Use induction on $r$. 

Section 7.5

1. Monday.
3. Tuesday.
5. Sunday.
7. Tuesday.
9. Follow example 3.
13. Show that they have the same doomsday and are not a leap year.

17. (a) 365.2425
   (b) 11,582
   (c) 365.24225

Section 7.6

1. (a) \( T = 3, \ V = 0, \ H = 145 \).
   (b) \( T = 12, \ V = 9, \ H = 109 \).
   (c) \( T = 4, \ V = 3, \ H = 303 \).
3. (a) 11,111.
   (b) 4,745.
   (c) 4941.

5. Show that we need to solve \( x \equiv 19 \pmod{20} \) and \( x \equiv 10 \pmod{365} \) which has no solution so the date never occurs.

7. Day 6 on wheel 1, day 27 on wheel 2, and day 380 on wheel 3.

9. (a) \( 249, 271a + 81, 872b + 303, 366c, \) reduced modulo 317,254.
   (b) \( 249, 271 * 3 + 81, 872 * 19 + 303, 366 * 100 \equiv 280, 073 \pmod{317254} \).
8.1

1. \( \mathbb{Z}_2 \)

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>·</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

3. \( \mathbb{Z}_4 \)

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>·</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
</tr>
</tbody>
</table>

5. \( \mathbb{Z}_{10} \)

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>·</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>8</td>
<td>5</td>
<td>2</td>
<td>9</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

7. a. \( x = 1 \)

b. \( x = 2 \)

c. \( x = 1 \)
d. \( x = 0 \)
e. \( x = 1 \) or \( 2 \)
f. no solutions

9. a. \( x = 2 \)
b. \( x = 3 \)
c. \( x = 4 \)
d. \( x = 1 \)
e. no solutions
f. \( x = 2 \) or \( 3 \)

11. commutativity.

13. Consider the multiplicative table of \( \mathbb{Z}_6 \).

8.2

1. \( \mathcal{A} = \{ x \in \mathbb{Z} | x = 11k + 4 \text{ where } k \in \mathbb{Z} \} \). So
   \( \mathcal{A} = \{ \ldots, -18, -7, 4, 15, 26, \ldots \} \).

3. a. \( -8 = 12 \).
   
b. \( -5 = 15 \).
   
c. \( -2 = 18 \).

5. \( 0, 1, 3, 4, 9, 10, 12 \).

7. \( x = 0, 2, 3, 5 \).

9. Show that it does not contain the additive identity element.

11. Use the corresponding properties of the ring of integers, \( \mathbb{Z} \).

13. Use theorem 8.2.4.

15. Expand \((\pi + \bar{b})^2\) using ring properties of \( \mathbb{Z}_n \).

17. If it was well-defined then \( \bar{0} \ast \bar{0} = \bar{\pi} \ast \bar{\pi} \) which is not correct!

19. This operation is not well-defined. For example in \( \mathbb{Z}_5 \), \( \bar{1} = \bar{5} \), but \( \bar{3} \ast \bar{1} = \bar{3} \) and \( \bar{3} \ast \bar{5} = \bar{4} \).
CHAPTER 2. HINTS TO PROBLEMS

8.3

1. (a) $\overline{44}$
   (b) $\overline{675}$
   (c) Does not exist.
   (d) $\overline{161}$

3. (a) $\overline{x} = \overline{7}$
   (b) $\overline{x} = \overline{9}$
   (c) $\overline{x} = \overline{5}$

5. (a) $\overline{x} = \overline{16}$
   (b) $\overline{x} = \overline{17}$

7. (a) $\overline{-1}$
   (b) $\overline{-1}$
   (c) $\overline{0}$
   (d) $\overline{0}$

9. Use theorem 8.3.3.

11. Use Euclid’s Lemma (5.3.2).

13. (a) Multiples of the gcd$(a, n)$.
   (b) Show that $\overline{b}$ appears in the row of $\overline{a}$ if and only if the Diophantine equation $ax + ny = b$ has a solution.
   (c) $\overline{n \mod \text{gcd}(a,n)}$ distinct elements.

15. The commutativity property.

17. Expand the left-hand side using ring properties of $\mathbb{Z}_n$.

8.4

1. The two-letter blocks I_ LO VE _M AT H_ are represented by the numbers 927 1215 2205 2713 120 827. These encrypt to the ciphertext 2270 2558 821 1329 1463 2170.

3. NUMBER THEORY IS USEFUL FOR ENCIIPHERING MESSAGES.
5. The encrypted message is 44262 114078 45575 176179 214668 113662 113662 45462 26177 274771 25272 76184

7. The encrypted message is 1731366464 2636605374 1110082937 1827377175 2649526464 1433606470 1111213647 2024425664 404113655 413273736 1104253148

8.5

1. The encrypted message is 1797 1699 2397 1298 588 1155 2632 2577 2597

3. GEOLOGY ROCKS

5. (a) The encrypted message is 2025 1671 2617 117 944 1859 1843 908
   (b) Use the Euclidean Algorithm to find integers $x$ and $y$ so that $5x + 2727y = 1$. You’ll find that $x = 1091$, so this is the inverse of 5 modulo 2727.
   (c) THEY KNOW TOO MUCH

7. The end of the message reads “...STEAL AWAY TOGETHER.”

9. If it is not one-to-one then two distinct letters or blocks of letters could encrypt to the same code and so there would be no way to decrypt the message.
CHAPTER 2. HINTS TO PROBLEMS

9.1

1. Fermat’s Little Theorem tells us that \(43^{38} \pmod{37} \equiv 43^2 \cdot 43^{36} \equiv 43^2 \cdot 1\). Since \(43 \equiv 6 \pmod{37}\), we get \(43^{38} \pmod{37} \equiv 36\).

3. \(2^{12} \equiv 1 \pmod{13}\), so \(8^4 = (2^3)^4 \equiv 1 \pmod{13}\). Since 98 is 96 + 2, \(8^{98} \equiv 8^{96} \cdot 8^2 \equiv 1 \cdot 8^2 \pmod{13} \equiv 64 \equiv 12 \pmod{13}\).

5. \(26 \equiv 0 \pmod{13}\). So \(26^{1000} \pmod{13} \equiv 0\).

7. (a) 6, 12, 18. All multiples of 6 will work.
(b) 1, 7, 13, .... They are all of the form \(6k + 1\) for some integer \(k\).
(c) 2, 8, 14. They are all of the form \(6k + 2\) for some integer \(k\).

9. (a) Statement: If \(a \equiv b \pmod{p}\), then \(a^n \equiv b^n \pmod{p}\). To prove it use theorem 7.2.1.
(b) Statement: If \(m \equiv n \pmod{p - 1}\), then \(a^m \equiv a^n \pmod{p}\). To prove it write \(m = n + k(p - 1)\) for some integer \(k\).

11. (a) The number 119 is not prime, so we cannot apply Fermat’s Little Theorem.
(b) \(4^{129} \equiv 1 \pmod{7}\).
(c) \(4^{129} \equiv 4 \pmod{17}\).
(d) Use the Chinese Remainder Theorem.

13. Use Fermat’s Little Therem.

15. Consider two different cases namely \(p|a\) and \((p, a) = 1\).

17. (a) Use Fermat’s Little Theorem.
(b) Consider two different cases namely \(n\) is odd and \(n\) is even.
(c) Use Fermat’s Little Theorem to reduce \(n^7\) modulo 3.
(d) Use (a),(b) and (c).

19. Use theorem 8.2.4.

21. Use Fermat’s little theorem and exercise 9.

9.2

1. (a) \(1, 2, 3, 4\).
(b) \(1, 5\).
3. (a) $656 = 2^4 \cdot 41$, so $\phi(656) = 40 \cdot 2^3 = 320$.
   (b) $2905 = 5 \cdot 7 \cdot 83$, so $\phi(2905) = 4 \cdot 6 \cdot 82 = 1968$.
   (c) $27720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$, so $\phi(27720) = 2^2 \cdot (2 \cdot 3) \cdot 4 \cdot 6 \cdot 10 = 5760$.
   (d) $10^{100} = 2^{100} \cdot 5^{100}$, so $\phi(10^{100}) = (2^{99}) \cdot (4 \cdot 5^{99})$.

5. It seems that $\sum_{d | m, d > 0} \phi(d) = m - 1$.
   (a) 8
   (b) 11
   (c) 19

7. (a) The general formula of $\phi(p_1^{a_1} \cdots p_k^{a_k})$ is
   $$(p_1 - 1)p_1^{a_1 - 1} \cdots (p_k - 1)p_k^{a_k - 1}.$$  
   From this, we get $\phi(p^a) = (p - 1)p^{a-1}$.
   (b) $\phi(3^4) = (3 - 1)3^{4-1} = 54$.

9. Note that either $n = 2^k$ or there is a prime $p > 2$ dividing $n$. Use formula 9.2.8 in each case.

11. If $\phi(m) = 98$, then for any prime factor $p$ of $m$ we have $p - 1 | 98$. Prove by contradiction.

13. Use definition 9.2.5.

15. (a) For $p = 2$: Reduced resides: $1, 3$; $\phi(2^2) = 2$
   For $p = 3$: Reduced resides: $1, 2, 4, 5, 7, 8$; $\phi(3^2) = 6$
   For $p = 5$: Reduced resides: $1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24$; $\phi(5^2) = 20$. The formula is $p(p - 1)$.
   (b) Show that the only integers $0 < a < p^2$ which $(a, p^2) \neq 1$ are $p, 2p, 3p, ..., (p - 1)p$.
   (c) Show that the only integers $0 < a < p^2$ which $(a, p^2) \neq 1$ are $p, 2p, 3p, ..., (p^k - 1)p$.

17. Use lemma (9.2.8) to show $\phi(2^{2k+1})$ is a perfect square for any $k$.

19. Use formula 9.2.8 and proposition 6.2.3.

21. (a) Consider the prime factorizations of $a, m$ and $n$.
   (b) Show that the numbers $a$ in the range $0, \ldots, mn - 1$ such that $a \equiv b \pmod{m}$ are
   $\{b, b + m, \ldots, b + m(n - 1)\}$ which modulo $n$ are $\{0, 1, \ldots, n - 1\}$. From this conclude that
   $s_b = \phi(n)$.
   (c) Show that for any number $a$ in the range $0, \ldots, mn - 1$ such that $a \equiv b \pmod{m}$, we have
   $(a, m) \neq 1$. Use (a) to show that $(a, mn) = 1$ hence $s_b = 0$.
   (d) Show that for any number $a$ in the range $0, \ldots, mn - 1$ such that $(a, mn) = 1$ there is a
   unique $b$ in the range $0, \ldots, m - 1$ such that $a \equiv b \pmod{m}$ and then use (b).
   (e) Use (b), (c) and (d).
23. Use Lemma 9.2.8 to show that
\[ \phi \left( \left( p_1^{a_1} \right) \left( p_2^{a_2} \right) \cdots \left( p_k^{a_k} \right) \right) = \phi \left( p_1^{a_1} \right) \cdot \phi \left( \left( p_2^{a_2} \right) \cdots \left( p_k^{a_k} \right) \right). \]
Then use exercise 15c to derive the formula.

25. (a) \( p(m - \phi(m)) \).
(b) \( m \).
(c) Count the number of elements counted both in (a) and (b) to show that there are \( p(m - \phi(m)) + \phi(m) \) numbers not relatively prime to \( pm \).
(d) Use (c) and the definition of \( \phi(pm) \).

9.3

1. \( \phi(33) = 2 \cdot 10 = 20. \) \( 7^{21} \equiv 7^{20} \cdot 7 \equiv 7 \pmod{33} \).

3. \( \phi(13) = 12. \) \( 5^{14} \equiv 5^{12} \cdot 5^2 \equiv 5^2 \equiv 12 \pmod{13} \).

5. \( \phi(108) = 36. \) \( 217^{73} \equiv 1^{72} \cdot 1 \equiv 1 \pmod{108} \).

7. \( \bar{a} \).

9. \( \bar{60} \).

11. \( \phi(30) = 24. \) So, we need only to find \( 12^5 \) \( \pmod{35} \). Using successive squaring, this is \( 17 \).

13. Use theorem 8.2.4.

15. Use \( 123^{456} \equiv 3^{456} \pmod{10} \).

17. (a) Multiply the equation by the multiplicative inverse of 13 to obtain a simpler equation.
    (b) Multiply the equation by the multiplicative inverse of 5 to obtain a simpler equation.
    (c) Multiply the equation by the multiplicative inverse of 10 to obtain a simpler equation.

19. First reduce \( 5^{64} \) modulo \( \phi(12) = 4 \), then raise the 7 to that result.

21. Reduce \( 3^{27} \) modulo 64.

9.4

1. 11, 01, 16, 28, 06, 23

3. The exponents should be relatively prime to \( \phi(p) \).
   (a) \( \phi(2819) = 2818 = 1409 \cdot 2 \).
   (b) \( \phi(2729) = 2728 = 2^3 \cdot 11 \cdot 31 \).
5. (a) \( p - 1 = 2896 \), and \( \gcd(2317, 2896) = 1 \). So it is a valid encryption scheme.
   (b) \( d = 5 \).
   (c) The deciphered message is I HAVE PLANS

7. (a) 28 09 09 23
   (b) We cannot find a multiplicative inverse of 18 modulo 28.
   (c) The encryption exponent must be relatively prime to \( p - 1 \).

9. The encrypted message is 167 167 1745, so the encryption scheme must not have been valid.

9.5

1. (a) \( n = 2747 \).
   (b) \( \phi(n) = 2640 \).
   (c) Only exponents relatively prime to 2640 will work. Of the ones listed, these are: 7, 49, and 91.

3. \( d = 55 \).

5. \( n = 2881 \), so we encipher by raising to the 5th power modulo 2881. The ciphered message is:
   578 846 2743 2111 1373

7. \( n = 2867 \), so we encipher by raising to the 7th power modulo 2867. The ciphered message is:
   895 958

9. (a) \( d = 11 \).
   (b) FOOD

11. (a) We need the multiplicative inverse of 7 modulo \( \phi(pq) = 2760 \). It is 1183.
    (b) AWAY WE GO

13. (a) BROKEN
    (b) They would have to make it much harder to factor \( n \) into primes. Perhaps they could choose \( p \) and \( q \) to be very large.

15. Yes the algorithm would still work, assuming that all of the prime factors of the modulus are big enough that the message will be relatively prime to the it. The only difference would be the formula for \( \phi(n) \).
10.1

1. Corollary 10.1.4 tells us that any element of $\mathbb{Z}_{29}$ have an order that divides $p - 1 = 28$. So, the possible orders of any element of $\mathbb{Z}_{29}$ are 1, 2, 4, 7, 14, and 28.

3. (a) $\text{ord}_{15}(4) = 2$.
   (b) $\text{ord}_{15}(7) = 4$.
   (c) $\text{ord}_{20}(7) = 4$.

5. Use Euler’s Theorem and proposition 10.1.4.

7. Use exercise 7 to show that $\text{ord}(a) = \phi(m)$.

9. (a) $\text{ord}_7(2) = 3$.
    (b) $\text{ord}_{15}(2) = 4$.

11. Show that $\text{ord}(a^t)|s$ and $\text{ord}(a)|\text{ord}(a^t)t$ and conclude that $\text{ord}(a^t) = s$.

13. First show that $\left(\frac{a^j}{\overline{a}^j}\right)^{\gcd(s,j)} = 1$. Now suppose that $k = \text{ord}(\overline{a}^j)$ and that $k < s/\gcd(s,j)$. Use 10.1.3 to derive a contradiction.

15. (a) $\text{ord}(8) = 12$.
   (b) $\text{ord}(32) = 36$.

17. (a) The number of perfect inside shuffles required to return a deck with $2n$ cards to its original order is equal to the number of perfect outside shuffles required to return a deck with $2(n + 1)$ cards to its original order.
   (b) The number of inside shuffles necessary to return a deck with $2n$ cards to its original order is $\text{ord}_{2n+1}(2)$.

19. Completely backwards.

21. $\text{ord}_{13}(12) = 2$, $\text{ord}_{13}(8) = 4$, $\text{ord}_{13}(8 \cdot 12) = 4$.

23. $\text{ord}_{13}(2) = 12$, $\text{ord}_{13}(6) = 12$, $\text{ord}_{13}(2 \cdot 6) = 2$.

25. Observe that $x^2 - y^2 = (x + y)(x - y)$ and use Euclid’s Lemma (5.4.2).

27. For the first part use Exercise 11. For the second part use the definition of $\text{ord}_n(a)$.

29. We apply the proposition to get the factors $\gcd(a^{r/2} \pm 1, n)$.

31. (a) There is only one prime factor: 3.
    (b) Use Proposition 10.1.3 to show that $\text{ord}_r(2) \mid p$ and conclude that $\text{ord}_r(2) = p$.
    (c) Show that $\text{ord}_r(2) \mid r - 1$ and use (b).
10.2

1. (a) \( x = 0, 2, 3, \) or \( 5. \)
   (b) \( x = 0, 1, 2, 3, 4 \) or \( 5. \)

3. Note that \( x = 3 \) is a solution to all of the equations. (a) \( x = 3 \) or 4.
   (b) \( x = 3, 5, \) or 6.
   (c) \( x = 3 \) or 4.
   (d) \( x = 3. \)

5. The modulus was not prime, which is a requirement of Theorem 10.2.1.

7. (a) Use Fermat’s Little theorem to show that every reduced residue must satisfy at least one of them. Then show that no reduced residue can satisfy both equations. (b) If \( a^8 = 1, \) then \( \text{ord}(a) \) must divide 8. So it is either 1, 2, 4, or 8.
   (c) Show that \( \text{ord}(a) = 16 \) using the fact that \( \text{ord}(a) \) must divide 16.

9. (a) \( \overline{4}. \)
   (b) Yes, \( \pm \overline{2} = \overline{2}, \overline{3}. \)
   (c) \( \overline{x} = (-8 + 2)(\overline{2})^{-1} = \overline{5} \cdot \overline{6} = \overline{8}, \) and \( \overline{x} = (-8 - 2)(\overline{2})^{-1} = \overline{1} \cdot \overline{6} = \overline{6}. \)

11. (a) \( \overline{12}. \)
   (b) Yes, \( \pm \overline{5} = \overline{5}, \overline{8}. \)
   (c) \( \overline{x} = (-9 + 5)(\overline{2})^{-1} = \overline{9} \cdot \overline{7} = \overline{11}, \) and \( \overline{x} = (-9 - 5)(\overline{2})^{-1} = \overline{12} \cdot \overline{7} = \overline{6}. \)

13. Show that we can write the equation in the form \( (\overline{x} + \frac{\overline{b}}{\overline{2}})^2 = \overline{\frac{b^2 - 4ac}{4a^2}}. \) Use this to show that there is a solution if and only if there is \( \overline{x} \) such that \( \overline{s}^2 = \overline{d} \) and if \( \overline{s}^2 = \overline{d} \) solve the equation.

15. (a) \( x = \overline{1}, \overline{2}. \)
   (b) \( x = \overline{0}, \overline{2}. \)
   (c) Use the Chinese Remainder Theorem to replace the equation by the following systems of congruences:
   \[\begin{align*}
x &\equiv 1 \pmod{5} \text{ and } x \equiv 0 \pmod{7} \\
x &\equiv 1 \pmod{5} \text{ and } x \equiv 3 \pmod{7} \\
x &\equiv 2 \pmod{5} \text{ and } x \equiv 0 \pmod{7} \\
x &\equiv 2 \pmod{5} \text{ and } x \equiv 3 \pmod{7}
\end{align*}\]
   The solutions are \( x \equiv 7, 17, 21, \) or 31 \( \pmod{35}. \)
10.3

1. First note that $3^1 \equiv 3 \pmod{7}$, $3^2 \equiv 2 \pmod{7}$, and $3^3 \equiv 6 \pmod{7}$. So we must have that ord$(3) = 6$ modulo 7, and 3 is a primitive root. We know then that $3^j$ will be a primitive root for any $j$ such that gcd$(j, 6) = 1$. This gives $3^1 = 3$, $3^5 \equiv 5 \pmod{7}$. Since $\phi(6) = 2$, we expect only two primitive roots, so this is a complete list.

3. First note that $3^1 \equiv 3 \pmod{17}$, $3^2 \equiv 9 \pmod{17}$, $3^4 \equiv 13 \pmod{17}$, and $3^8 \equiv 16 \pmod{17}$. So we must have that ord$(3) = 16$ modulo 17, and 3 is a primitive root. We know then that $3^j$ will be a primitive root for any $j$ such that gcd$(j, 16) = 1$. This gives $3^1 = 3$, $3^3 \equiv 10 \pmod{17}$, $3^5 \equiv 5 \pmod{17}$, $3^7 \equiv 11 \pmod{17}$, $3^9 \equiv 14 \pmod{17}$, $3^{11} \equiv 7 \pmod{17}$, $3^{13} \equiv 12 \pmod{17}$, and $3^{15} \equiv 6 \pmod{17}$. Since $\phi(16) = 8$, we expect eight primitive roots, so this is a complete list.

5. No. Use Exercise 1.

7. Note that $\pi$ must divide $p - 1$, and the only number greater than $\frac{p-1}{2}$ that divides $p - 1$ is $p - 1$ itself.

9. Try number 3.

11. Show that if ord$(\pi) < p - 1$ then there are at most ord$(\pi)$ distinct powers of $\pi$.

13. Let $\pi$ be a primitive root modulo $p$. Show that all elements of order $d$ are the elements of the form $\pi^{k(p-1)}$ where $k < d$ is relatively prime to $d$ which are exactly $\phi(d)$ elements.

15. (a) Note that $\phi(6) = 2$.
   (b) Note that $\phi(10) = 4$.

17. (a) Note that $\phi(15) = 8$. Show that the order of any reduced residue divides 4.
   (b) Note that $\phi(8) = 4$ and the reduced residues are 1, 3, 5, 7 which have orders different than 8.

19. (a) Note that $\frac{n}{p^r}$ has at least one prime factor.
   (b) Use the Euler function and the fact that $n$ has at least two distinct prime factor.
   (c) This follows from (b) similarly as in Exercise 18(a).
   (d) Use the Chinese Remainder Theorem.
   (e) Use (d).

21. (a) Use induction. The base case $s = 3$ was shown in Exercise 17(b). Assume the result for some arbitrary $s \geq 3$. Let $a \in \mathbb{Z}$. Then $a^{2^{-s-2}} \equiv 1 \pmod{2^s}$.
   Hence, $a^{2^{s-2}} = k2^s + 1$. Using Squaring, show that $a^{2^{s-1}} \equiv 1 \pmod{2^{s+1}}$.
   (b) Use (a).
23. (a) Since \( \gcd(m, 2) = 1 \), we have \( \phi(2m) = (2 - 1)\phi(m) = \phi(m) \).
(b) 10 cannot be a primitive root modulo 94 since it is not a reduced residue modulo 94.
(c) 57.
(d) Let \( \pi \) be a primitive root modulo \( m \). Then either \( \pi \) or \( \pi + m \) is odd. WLOG assume that \( \pi \) is odd. Prove that \( \pi \) is a primitive root modulo \( 2m \).

10.4

1. (a) 4
   (b) 7

3. (a) 13
   (b) 15

5. 14

7. The key step is to find a prime of the form \( p = 2q + 1 \), with \( q \) prime. This can be done by searching for 30 digit primes \( r \) and then checking if \( 2r + 1 \) is prime and checking if \( (r - 1)/2 \) is prime. One such possible combination is \( p = 833814642651690461148175665347 \), \( q = 416907321325845230574087832673 \). Once you have primes of this form, it is easy to check for primitive roots since the order of an element modulo \( q \) must be 1, 2, \( p \) or \( 2p \). For the primes above, \( a = 2 \) is a primitive root.

9. Using \( x_0 = 326916 \), the first 10 pseudorandom numbers generated are 874071, 113, 12, 0, 0, 0, 0, ...  
   We see this as follows.
   \( (326916)^2 = 106874071056 \)
   \( (874071)^2 = 764000113041 \)
   \( (000113)^2 = 12769 = 000000012769 \)
   \( (000012)^2 = 144 = 00000000144 \)
   \( (000000)^2 = 0 \), and this is going to continue producing 0's.

11. Using \( x_0 = 971582 \), the first 10 pseudorandom numbers generated are 971582, 971582, ...
   The period is one.

13. (a) 5, 0, 1, 3, 7, 4, 9, 8, 6, 2, 5, ... The period is 10.
   (b) 5, 5, ... The period is 1.
15. (a) Note that \( a^r \equiv 1 \pmod{m} \).
    (b) Prove by contradiction. If \( x_i \equiv x_j \pmod{m} \) for \( i < j \leq r \), then show that \( \text{ord}_m(a) \leq j - i < r \), a contradiction.

17. Apply geometric series to \( d_1 \cdots d_r = d_1 \cdots d_r 10^{-r} + d_1 \cdots d_r 10^{-2r} + \cdots \).

19. (a) Use \( 9^{p-1} = (3^2)^{p-1} = 3^{p-1} \equiv 1 \pmod{p} \) to show that 9 is only a primitive root for \( p = 2 \).
    (b) Given any perfect square \( a = b^2 \), use \( a^{p-1} = (b^2)^{p-1} = b^{p-1} \equiv 1 \pmod{p} \) to show that \( a \) can only be a primitive root for \( p = 2 \).
    (c) Note that for any prime, \( p \), \( (-1)^2 = 1 \equiv 1 \pmod{p} \) and \( (-1)^1 = -1 \equiv p - 1 \pmod{p} \). Conclude that \(-1\) is a primitive root for exactly two primes, namely 2 and 3.

21. It is a multiple of \( m \).

23. Letting \( a_k = x_k^2 - x_{k-1} x_{k+1} \) we find \( a_1 = 81 - 48 = 33 \) and \( a_2 = 55 \). Conclude that \( m = 11 \) and \( \overline{a} = 7 \).

25. To multiply 5 by 11 modulo 13 using the wheel, do the following: place the 1 of the inner wheel so it lines up with the 5 of the outer wheel. Then look on the inner wheel for the 11. The number that lines up with it will be the product. (In this case, 3.)

27. Begin by finding a primitive root of \( \mathbb{Z}_{17} \). In Example 3 of Section 10.3, we are told that \( \overline{3} \) is a primitive root, so we will use that. Now we look at the ordered set \( \{ \overline{3}^0, \overline{3}^1, \overline{3}^2, \ldots, \overline{3}^{16} \} \). This equals \( \{ 1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6 \} \). Now arrange these around an inner/outer wheel pattern and you will have a wheel for multiplication modulo 17.
11.1

1. Yes. $4^2 = 3$.

3. $1, 2, 4, 8, 5, 13, 15, 16$.

5. $\left( \frac{2}{p} \right) = 1$

7. $\left( \frac{27}{17} \right) = 1$

9. $\left( \frac{4}{17} \right) = 1$

11. $\left( \frac{11}{17} \right) = -1$

13. $\left( \frac{-5}{17} \right) = -1$

15. $\left( \frac{-1}{p} \right) = 1$ for $p = 5, 13, 17$. $\left( \frac{-1}{p} \right) = -1$ for $p = 3, 7, 11, 19$.

17. (a) $\left( \frac{4}{101} \right) = 1$.

(b) Since $a$ is a perfect square, there exists a $b$ such that $b^2 = a$ and $p$ does not divide $b$. Then $\overline{b^2} = \overline{a} \neq 0$ is $\mathbb{Z}_p$ and hence $\left( \frac{a}{p} \right) = 1$ by definition of the Legendre symbol.

19. Use definition of the Legendre symbol.

21. Give a proof by contradiction. Suppose that $x^2 \equiv ab \pmod{p}$ and $y^2 \equiv a \pmod{p}$. Let $z$ be some multiplicative inverse of $y$ modulo $p$. Then show that $(zx)^2 \equiv b \pmod{p}$, a contradiction.

23. To prove it, consider the following different cases. (a) At least one of the two elements is 0. (b) Both elements are quadratic residues. (c) One element is a quadratic residue and the other is a quadratic nonresidue. (d) Both elements are quadratic residues. To prove (a), use the definition of the Legendre symbol. To prove (b) use exercise 11.1.20. To prove (c), use exercise 11.1.21. Finally to prove (d) use exercise 11.1.22.

25. Note that $59 \equiv 3 \pmod{4}$. Show that if $n$ is a perfect square then 3 is a quadratic residue modulo 4 which is not valid, hence $n$ is not a perfect square.

27. The values of $\left( \frac{p}{5} \right)$ read $-1, 1, -1, -1, 1, -1$.

The values of $\left( \frac{a}{p} \right)$ read $-1, 1, -1, -1, 1, -1$.

29. (a) There is agreement when at least one of the primes is equivalent to 1 modulo 4. Otherwise they disagree.

(b) It turns out that $\left( \frac{p}{q} \right) = \left( \frac{q}{p} \right)$ either $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$. Otherwise $\left( \frac{p}{q} \right) = -\left( \frac{q}{p} \right)$. This will be proven later in the chapter.
31. (a) The cubic residues modulo 5 are 1, 2, 3, and 4. The cubic residues modulo 7 are 1 and 6. The cubic residues modulo 11 are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10. The cubic residues modulo 13 are 1, 5, 8, and 12.
(b) The number of cubic residues modulo $p$ is $\frac{p-1}{3}$ if $p \equiv 1$ modulo 3. If $p \equiv 2$ modulo 3, then the number of cubic residues modulo $p$ is $p - 1$. If $p \equiv 0$ modulo 3, then $p = 3$ and it is easy to see that there are 2 cubic residues.
(c) Let $\bar{a}$ be a cubic residue. Then there exists an $x$ such that $x^3 = \bar{a}$ and there exists a unique $y$ such that $xy = 1$. Thus, $x^3y^3 = \bar{a}y^3 = 1$. So we have that $(xy)^3 = 1$. Use proposition 10.2.2 to complete the proof.

11.2

1. (a) $\left(\frac{-1}{47}\right) = -1$
   (b) $\left(\frac{-1}{101}\right) = 1$
   (c) $\left(\frac{1000003}{5075009}\right) = -1$
   (d) $\left(\frac{1000003}{5075009}\right) = 1$

3. (a) $\left(\frac{31}{67}\right) = -1$
   (b) $\left(\frac{-1}{67}\right) = -1$
   (c) $\left(\frac{-31}{67}\right) = (\frac{-1}{67}) \cdot (\frac{31}{23}) = -1 \cdot -1 = 1$

5. (a) $\left(\frac{a}{7}\right) = -1$
   (b) $\left(\frac{-a}{7}\right) = 1$

7. First show that $\frac{p-1}{2}$ is odd (respectively even) if and only if $p \equiv 3 \pmod{4}$ (respectively $p \equiv 1 \pmod{4}$). Use this to finish the proof.

9. (a) We have $\bar{a}^2 = \frac{a^2}{p} \neq 0$ in $\mathbb{Z}_p$ which by the definition of the Legendre symbol we obtain $\left(\frac{a^2}{p}\right) = 1$.
   (b) Use $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{p}\right)$
   (c) First note that $\left(\frac{a^2}{p}\right) = (a^2)^{\frac{p-1}{2}} = a^{p-1}$. Then Use Fermat’s Little Theorem.

11. First show that it is true for $p = 7$. For $p \geq 11$ note that $1^2 = 1$, $2^2 = 4$, and $3^2 = 9$ are all quadratic residues. Since $\left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{10}{p}\right)$, conclude that at least one of the numbers 2, 5, 10 is a quadratic residue modulo $p$. Show that this completes the proof.
11.3

1. \((\frac{3}{7}) = 1\)
2. \((\frac{7}{11}) = -1\)
3. \((\frac{5}{37}) = -1\)
4. \((\frac{3}{11}) = 1\)

9. Use the Law of Quadratic Reciprocity to show that \(p = 2\) or \(p \equiv \pm 1 \pmod{12}\).

11. Use the Law of Quadratic Reciprocity to show that \(p = 2\), or \(p \equiv \pm 1, \pm 3, \) or \(\pm 9 \pmod{28}\).

13. (a) Write \(a\) as a product of powers of primes. That is, \(a = s_1^{k_1} \cdot s_2^{k_2} \cdots s_n^{k_n}\) for \(s_l\) prime and \(n \geq 0\) and \(k_i \geq 1\). Note that since \(p \equiv q \pmod{s_l}\), we have \((\frac{p}{s_l}) = (\frac{q}{s_l})\) for all \(l\). Use the Law of Quadratic reciprocity to prove \((\frac{a}{p}) = (\frac{a}{q})\) in both cases.

(b) CASE 1: Let \(p \equiv q \pmod{4}\). So there exists \(a \in \mathbb{Z}\) such that \(4a = p - q\). So \(p \equiv q \pmod{4a}\) and we can thus use \(a\) in the Euler form \((\frac{a}{p}) = (\frac{a}{q})\). Now show that \((\frac{p}{q}) = (\frac{4a+q}{q}) = (\frac{4a}{q}) = (\frac{a}{q})\). Use this to prove the Law of Quadratic Reciprocity in this case.

CASE 2: Let \(p \equiv -q \pmod{4}\). Use a proof similar to the first case.

11.4

1. In all three cases, \((\frac{2}{5}) = -1\).
2. In all three cases, \((\frac{2}{7}) = -1\).
3. In all three cases, \((\frac{4}{11}) = 1\).
4. In both cases, \((\frac{2}{11}) = -1\).
5. (a) -1
   (b) -1
   (c) -1
6. \((\frac{18}{101}) = -1\)

13. Show that \((\frac{-1}{55}) = -1\) and deduce that the answer is No.
15. Yes.

17. Use the fact that the Legendre symbol can only have the values 1 and $-1$.

19. Use theorem 11.4.3.

21. (a) $g = 2 \implies \left( \frac{3}{11} \right) = 1$
(b) $g = 2 \implies \left( \frac{3}{17} \right) = 1 \quad g = 4 \implies \left( \frac{3}{23} \right) = 1$
(c) $g = \left\lfloor \frac{p-1}{3} \right\rfloor - \left\lfloor \frac{p-1}{6} \right\rfloor$
(d) $p \equiv \pm 1 \pmod{12}$

11.5

1. (a) 1
   (b) -1

3. (a) 20
   (b) 1

5. (a) 21
   (b) -1

7. 1

9. -1 for all a, b, c, d

11. (a) Figure
    (b) 3
    (c) -1

13. (a) Figure
    (b) 9
    (c) -1

15. (a) Figure
    (b) 7
    (c) 3
    (d) 6

17. (a) Figure
    (b) 12
    (c) 7
    (d) 8
19. Using the rectangle whose diagonal is the diagonal of $P$, we can see geometrically that the number of lattice points on the rectangle is $\frac{(a+1)(b+1)}{2}$. When divided into half by its diagonal, each triangle shares gcd$(a,b) + 1$ lattice points. Use this to finish the proof.

21. Let $p$ be a prime number. Let $n = \frac{p-1}{2}$. Let $q_k$ be the quotient and $r_k$ be the remainder when $2k$ is divided by $p$ for $1 \leq k \leq n$. We get the following equations:

\[
\begin{align*}
2 \cdot 1 &= q_1 \cdot p + r_1 \\
2 \cdot 2 &= q_2 \cdot p + r_2 \\
&\vdots \\
2 \cdot n &= q_n \cdot p + r_n
\end{align*}
\]

Show that $T(2,p) = 0$ and $q_k = 0$ for all $k$, so $2(1 + \cdots + n) = r_1 + \cdots + r_n$. Define $s_k$ as in this section and conclude that $g \equiv (s_1 + \cdots + s_n) \pmod{2}$, where $g$ is the number of $k$’s for which $r_k$ is a negative residue. Use theorem 11.4.1 and Gauss’s Lemma to finish the proof.

11.6

1. \[
\begin{align*}
\left(\frac{22}{37}\right) &= \left(\frac{2}{37}\right) \cdot \left(\frac{11}{37}\right) \\
&= -1 \cdot \left(\frac{37}{11}\right) \\
&= -\left(\frac{4}{11}\right) \\
&= -1
\end{align*}
\]

3. \[
\begin{align*}
\left(\frac{590}{733}\right) &= \left(\frac{2}{733}\right) \cdot \left(\frac{5}{733}\right) \cdot \left(\frac{59}{733}\right) \\
&= -1 \cdot \left(\frac{733}{5}\right) \cdot \left(\frac{733}{59}\right) \\
&= -1 \cdot \left(\frac{3}{5}\right) \cdot \left(\frac{25}{59}\right) \\
&= -1 \cdot -1 \cdot 1 \\
&= 1
\end{align*}
\]
5. (a) \( T(3, q) = \left\lfloor \frac{q-1}{3} \right\rfloor - \left\lfloor \frac{q-1}{6} \right\rfloor \)
(b) \( T(q, 3) = \left\lfloor \frac{q}{3} \right\rfloor \)
(c) Prove it in two different cases, namely \( 3|q - 1 \) and \( 3|q - 2 \).

7. Use the law of quadratic reciprocity for \( p \) and \( q = 2p + 1 \).

9. Use definitions of Jacobi and Legendre symbols.

11. Use definition of Jacobi symbol and the fact when \( p \) is prime then \( p|a - b \) implies \( \left( \frac{a}{p} \right) = \left( \frac{b}{p} \right) \).

13. (a) Note that \( p_i - 1 \) is even.
(b) Show that \( n = p_1^{k_1} \cdots p_n^{k_n} \equiv (1 + k_1(p_1 - 1)) + \cdots + (1 + k_m(p_m - 1)) \) (mod 4) \( \equiv 1 + k_1(p_1 - 1) + \cdots + k_m(p_m - 1) \) (mod 4).
(c) Note that both sides in the congruence of (b) are even.
(d) Use Euler’s Identity (11.2.2).

15. Use the Euler’s identity and law of quadratic reciprocity.

17. First prove that if \( x \) is odd then \( x^2 \equiv 1 \) (mod 8). Use this to prove that \( x^2 \equiv a \) (mod \( 2^m \)) can not have any solutions if \( a \not\equiv 1 \) (mod 8).
Now use induction on \( m \) to show that if \( a \equiv 1 \) (mod \( 2^m \)), then there are exactly four solutions. Prove the theorem directly for \( m = 3 \).
Next, suppose that \( a \equiv 1 \) (mod 8) and \( x^2 \equiv a \) (mod \( 2^m \)) has exactly four solutions. Prove that if \( x \) is a solution in (mod \( 2^m \)), then \( x + 2^{m-1} \) is also a solution and deduce that the four solutions of \( x^2 \equiv a \) (mod \( 2^m \)) look like \( x_1, y_1 = x_1 + 2^{m-1} \) and \( x_2, y_2 = x_2 + 2^{m-1} \).
Now show that one of \( x_1 \) and \( y_1 \) must solve \( x^2 \equiv a \) (mod \( 2^{m+1} \)) and similarly for \( x_2 \) and \( y_2 \). Deduce from this that there are at least four solutions for \( x^2 \equiv a \) (mod \( 2^{m+1} \)).
Using the fact that the solutions of \( x^2 \equiv a \) (mod \( 2^{m+1} \)) are also solutions \( x^2 \equiv a \) (mod \( 2^m \)), prove that there are exactly four solutions for \( x^2 \equiv a \) (mod \( 2^{m+1} \)).
12.1

1. Use successive squaring: \(2^{246} \equiv 2^{27+2^6+2^7+2^4+2^2+2} \equiv 61 \cdot 55 \cdot 139 \cdot 81 \cdot 16 \cdot 4 \equiv 220 \pmod{247}\).

   We can conclude that 247 is composite by Fermat’s Little Theorem. We call 2 a witness to the fact that 247 is composite.

3. \(2^{38} \equiv 4 \pmod{39}\). Hence 39 is composite.

5. \(13^{20} \equiv 1 \pmod{21}\) and \(16^{20} \equiv 4 \pmod{21}\). Hence, 21 is composite.

7. \(3^{90} \equiv 1 \pmod{91}\). But \(2^{90} \equiv 64 \pmod{91}\) shows that 91 is in fact composite.

9. \(2^{670} \equiv 353 \pmod{671}\) shows that 671 is composite.

11. \(6^{501000} \equiv 1 \pmod{501001}\). \(2^{501000} \equiv 1 \pmod{501001}\). \(11^{501000} \equiv 1 \pmod{501001}\). You can conclude nothing about 501001. You may suspect, however, that 501001 is prime.

13. (a) 67
   (b) No. By Fermat’s Little Theorem.
   (c) No. By the definition of Carmichael numbers.

15. Use the definition of a Carmichael number.

17. Show that \(n\) is not squarefree hence it is not a Carmichael number.

19. Show that \(n\) is not squarefree.

21. Show that \((n-1)^{n-1} \equiv 1 \pmod{n}\) if \(n\) is odd and \((n-1)^{n-1} \equiv -1 \pmod{n}\) if \(n\) is even.

23. Suppose that \(gcd(a,n) = g \neq 1\). Then show that if \(a^{n-1} \equiv k \pmod{n}\) then \(k|q\) hence \(k\) cannot be 1 which means that \(a\) is a Fermat witness for \(n\).

25. Note that the formula can be written as \(n-1 - A\) where \(A\) is the number of solutions to the congruence \(\alpha^{n-1} \equiv 1 \pmod{n}\). Show that \(A\) is equal to Show that \(A\) is equal to the number of solutions to \(\alpha^{n-1} \equiv 1 \pmod{p_1}\), multiplied by \(\alpha^{n-1} \equiv 1 \pmod{p_2}\), multiplied by \(\ldots\), multiplied by \(\alpha^{n-1} \equiv 1 \pmod{p_s}\). Finally Conclude that \(A = gcd(n-1,p_1-1) \cdot gcd(n-1,p_2-1) \cdots gcd(n-1,p_s-1)\).

27. If \(s = rn\), then show that \(2^s - 1 = (2^r - 1)(2^{r(n-1)} + 2^{r(n-2)} + \ldots + 2^r + 1)\).
CHAPTER 2. HINTS TO PROBLEMS

12.2

1. At least 108.

3. At least 1560.

5. (a) Yes. \( n \) could be a Carmichael number.
   (b) Use theorem 12.2.3.

7. Let \( n = 121k \). Use inequality (10) with \( p = 11 \) to show that there will be at most \( \frac{10}{171}n \) non-witnesses.

9. Note that \( \frac{1}{4}(n - 1) - \frac{2}{9}n = \frac{n - 9}{36} \). Now use \( n \geq p^2 \geq 9 \) to show that \( \frac{2}{9}n \leq \frac{1}{4}(n - 1) \).

11. For example, let \( p = q = 5 \). Then \( n = 25 \) and \( p - 1 = q - 1 = 4 \) divides \( n - 1 = 24 \).

13. (a) Note that \( n' \) and \( p^2 \) are relatively prime.
   (b) Use \( y \equiv x + p \pmod{p^2} \), to prove (6) and (7) and to prove (8) use the fact that \( x \) and \( n \) are relatively prime.

15. (a) 1105.
    (b) 1105 = 5 \cdot 13 \cdot 17. Factors less than these whose product is greater than 561 can be shown to not be Carmichael numbers.

17. Show that \( \text{ord}_p(a)|\text{ord}_{p^2}(a) \) for any \( a \).

19. Let \( n = p^2 \). Raise both sides of the congruence \( a^{p - 1} \equiv b^{p - 1} \pmod{p^2} \) to the \( p + 1^{st} \) power and use Lemma 12.2.2.

21. By problem 18, the order of \( a \) is either \( p - 1 \) or \( p^2 - 1 \). If the order of \( a \) is not \( p^2 - 1 \), then use problem 20 to show that the order of \( a + p \) is \( p^2 - 1 \).

12.3

1. 217 is composite.

3. (a) 340 = 2 \cdot 5 \cdot 34
   (b) 148 = 2 \cdot 37
   (c) 560 = 2^4 \cdot 35
   (d) 1058 = 2 \cdot 529

5. \( 4^7 \equiv 4 \pmod{15} \) and \( 4^14 \equiv 1 \pmod{15} \) shows that 4 is a Miller-Rabin witness for 15.

7. \( 14^7 \equiv 14 \pmod{15} \) and \( 14^{14} \equiv 1 \pmod{15} \) shows that 14 is a Miller-Rabin witness for 15.
9. None. 7 is prime.

11. 3 is not a witness to the compositeness of 149 by either test.


15. Composite by Miller-Rabin Test.

17. Prove that $1^q \equiv 1 \pmod{n}$ and $(n - 1)^q \equiv 1$ or $-1 \pmod{n}$ for any $n, q$.

19. Note that the successive square roots of $a_{n-1}^{\frac{n-1}{2}}$ will never be equivalent to 1 or -1.

21. Note that we do not need to factorize $n$. We only need to keep dividing by 2 until some odd number is reached.

23. (a) Show that $(a^{2^{k-1}q+1})(a^{2^{k-2}q+1}) \cdots (a^{q}+1)(a^{q}+1) = l^k$ where $l \in \mathbb{N}$. Thus we only need to determine which term is divisible by $l$, and then whatever is left are all factors of $n$. If none of the factors determined in this manner are prime factors, just keep repeating this process one the factors until the prime factors are determined.

(b) If $n$ is a Carmichael number, then find a Miller-Rabin witness $a$. If $a$ is not Fermat witness, then we can simply follow the procedure described in part (a). If $a$ is a Fermat witness, then it shares a common factor with $n$. If $a$ is prime, then we have found a factor of $n$. If $a$ is composite and difficult to factor, then we can find a Miller-Rabin witness for $a$ and keep repeating this process and the process in $a$ until we have factors for $a$ and thus have determined a factor for $n$.

25. 100 percent.

27. (a) $\left(\frac{1}{4}\right)^{100} \approx 0.622 \times 10^{-60}$.

(b) $P(C)$ and $P(-C)$ have nothing to do with how many times the Miller-Rabin test is run and $P(M \mid -C)$ is always 1.

(c) $\frac{\log(10^{200}) - 1}{\log(10^{200}) + 4^{100} - 1} \approx 2.86 \times 10^{-58}$.

12.4

1. (a) For $m = 1$, there is 1 solution. For $m = 2$ there are 2 solutions. For $m = 3$, there is 1 solution. For $m = 4$, there are 4 solutions. For $m = 5$, there are no solutions.

(b) For $m = 1$, there is 1 solution. For $m = 2$, there are 2 solutions. For $m = 3$, there is 1 solution. For $m = 4$ there are no solutions. For $m = 5$ there are no solutions.
3. (a) For $m = 1$, there is 1 solution. For $m = 2$ there are 2 solutions. For $m = 3$, there is 1 solution. For $m = 4$, there are 2 solutions. For $m = 5$, there are 5 solutions. For $m = 6$, there are 2 solutions. For $m = 7$, there is 1 solution. For $m = 8$, there are 2 solutions. For $m = 9$, there is 1 solution. For $m = 10$, there are 10 solutions. For $m = 11$, there is 1 solution.
(b) For $m = 1$, there is 1 solution. For $m = 2$ there are 0 solutions. For $m = 3$, there is 1 solution. For $m = 4$, there are 0 solutions. For $m = 5$, there are 5 solutions. For $m = 6$, there are 0 solutions. For $m = 7$, there is 1 solution. For $m = 8$, there are 0 solutions. For $m = 9$, there is 1 solution. For $m = 10$, there are 0 solutions. For $m = 11$, there is 1 solution.

5. (a) 25.
(b) 25.

7. (a) 25.
(b) 25.

9. $\bar{x}^m$ has only 1 value modulo $p$ for any $\bar{x}$, and $-1 \equiv 1 \pmod{p}$ only when $p = 2$.

11. For example, the equation $\bar{x}^4 \pmod{13}$ has 4 solutions which is greater than $\frac{p-1}{4} = \frac{12}{4} = 3$.

13. Then $m$ is allowed to equal $\frac{p-1}{2}$ which means that there are $\frac{p-1}{2}$ solutions.

15. (a) $p = 13$, $m = 3$.
(b) $p = 13$, $m = 5$.

17. (a) Use Lemma 12.4.1.
(b) Consider the example in the section, $\mathbb{Z}_{13}$. Of all the rows where $m$ is odd, the rows of 3 and 9 have the most 1’s in them, and each row only has 3, or $\frac{13-1}{2}$.

12.5

1. (a) $340 = 2^4 \cdot 85$
(b) From left to right, the first row reads 10, 1 and the second row reads 1, 1.
(c) No.
(d) Yes, since non of the congruences hold in both moduli, non hold modulus 341.

3. $n - 1 = 2^3$. $8 \equiv -1 \pmod{9}$ which means 8 is a misleader to the compositeness of 9.

5. $n - 1 = 2^6$. Since $8^2 \equiv -1 \pmod{5}$, $8^2 \equiv -1 \pmod{13}$ and $65 = 5 \cdot 13$, $8 \equiv -1 \pmod{65}$ by lemma 12.5.1., which means 8 is a misleader to the compositeness of 65.

7. It’s not a misleader since $n - 1 = 2 \cdot 49$ and $10^{49} \equiv 10 \pmod{99}$ and $10^{98} \equiv 1 \pmod{99}$. Thus none of the congruences in the Miller-Rabin test are satisfied.
9. In $\mathbb{Z}_2$, $1 \equiv -1$.

11. Use Observation 12.5.1 and Lemma 12.5.2.

<table>
<thead>
<tr>
<th>Congruence</th>
<th>Equation</th>
<th>Solutions per Prime</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C[-1]$</td>
<td>$x^{31575} = 1$</td>
<td>[5, 15, 25]</td>
<td>1875</td>
</tr>
<tr>
<td>$C[0]$</td>
<td>$x^{31575} = -1$</td>
<td>[5, 15, 25]</td>
<td>1875</td>
</tr>
<tr>
<td>$C[1]$</td>
<td>$x^{63150} = -1$</td>
<td>[10, 30, 50]</td>
<td>15000</td>
</tr>
<tr>
<td>$C[2]$</td>
<td>$x^{126300} = -1$</td>
<td>[20, 0, 0]</td>
<td>0</td>
</tr>
</tbody>
</table>

(a) There are 5 solutions to $C[-1]$.
(b) There are 1875 total solutions to $C[-1]$.
(c) There are 18750 total misleaders.

13. Let $P = \{p_1, p_2, \ldots, p_s\}$. Then we have

$$\prod_P \gcd(q, p_j - 1) + \sum_{i=0}^{k-1} \left\{ \prod_P \gcd(2^i q, p_j - 1) \right\} \text{ if } t > i$$

15. 11 is prime: Take $a = 7$. Use $10 = 5 \cdot 2$.

5 is prime: Take $a = 3$. Use $4 = 2^2$.

3 is prime: Take $a = 2$. Use $2 = 2$.

71 is prime: Take $a = 7$. Use $70 = 2 \cdot 5 \cdot 7$.

5 is prime: Take $a = 3$. Use $4 = 2^2$.

7 is prime: Take $a = 3$. Use $6 = 2 \cdot 3$.

3 is prime: Take $a = 2$. Use $2 = 2$.

5 is prime: Take $a = 2$. Use $4 = 2^2$.

11 is prime: Take $a = 2$. Use $10 = 2 \cdot 5$.

5 is prime: Take $a = 2$. Use $4 = 2^2$. 

17. Let $P = \{p_1, p_2, \ldots, p_s\}$. Then we have

$$\prod_P \gcd(q, p_j - 1) + \sum_{i=0}^{k-1} \left\{ \prod_P \gcd(2^i q, p_j - 1) \right\} \text{ if } t > i$$
43 is prime: Take $a = 3$. Use $42 = 2 \cdot 3 \cdot 7$.

3 is prime: Take $a = 2$. Use $2 = 2$.

7 is prime: Take $a = 3$. Use $6 = 2 \cdot 3$.

3 is prime: Take $a = 2$. Use $2 = 2$.

223 is prime: Take $a = 2$. Use $222 = 2 \cdot 3 \cdot 37$.

3 is prime: Take $a = 2$. Use $2 = 2$.

37 is prime: Take $a = 2$. Use $36 = 2^2 \cdot 3^2$.

3 is prime: Take $a = 2$. Use $2 = 2$.

7. Line 1: (i) $7^{238} \equiv 1 \pmod{239}$. (ii) $7^{119} \equiv 238 \pmod{239}$, $7^{34} \equiv 24 \pmod{239}$, $7^{14} \equiv 211 \pmod{239}$.

Line 2: (i) $3^6 \equiv 1 \pmod{7}$. (ii) $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$

Line 3: (i) $2^2 \equiv 1 \pmod{3}$. (ii) Since $q = 1$, this condition holds.

Line 4: (i) $3^{16} \equiv 1 \pmod{17}$. (ii) $3^8 \equiv 16 \pmod{17}$.

9. (a) Show that $ord_n(a) = n - 1$ and then use Lemma 12.6.2.

(b) Thus the converse is not true. For example take $n = 5$ and $a = 4$.

11. $L(5) = 1$, $L(7) = 2$, $L(71) = 4$.

13. Use induction and properties of logarithms.

15. Use theorem 12.6.3 and note that 2 is the only prime factor of $F_n - 1$.

17. The $\Leftarrow$ part is just like exercise 15. The $\Rightarrow$ part is just like exercise 16 except that instead of doing things modulo 12 in part a, use modulo 10.

12.7

1. (a) $40x + 41$
   (b) 3
   (c) No.
   (d) Composite.

3. (a) $x^2 + 1$
   (b) $11x^2 + 10x + 1$
   (c) Yes.
(d) This is not enough information since we have only checked for \( a = 1 \) and we need to check for all \( a \leq \sqrt{\log_2(5)} \approx 4.02 \).

5. (a) \( 88573x + 88674 \).
   (b) \( x + 2 \)
   (c) Yes.
   (d) This is not enough information since we have only checked for \( a = 2 \) and we need to check for all \( a \leq \sqrt{\log_2(11)} \approx 4.9 \).

7. (a) 557496
   (b) Need to check \( \sqrt{r} \cdot \log_2(n) \approx 6776 \) values.
   (c) Maximum possible degree of polynomial is the largest possible remainder: \( r - 1 = 6678 \).

9. Note that \( \binom{n}{q} = \frac{n!}{q!(n-q)!} = \frac{n(n-1)\ldots(n-q+1)}{q!} \) and the only term in the numerator divisible by \( q \) is \( n \).
CHAPTER 2. HINTS TO PROBLEMS

13.1

1. See Figure 2.1

3. (a) \(-28 + 10i\)
   (b) \(6 + 2i\)
   (c) \(10 + 20i\)
   (d) \(a^2 + b^2\)

5. (a) The multiplicative inverse of \(5 + 7i\) is 
   \[
   \frac{1}{5+7i} = \frac{1}{5+7i} \cdot \frac{5-7i}{5-7i} = \frac{5-7i}{25+49} = \frac{5}{74} - \frac{7}{74}i.
   \]
   (b) Multiplying the two numbers together gives us \((5 + 7i)(\frac{5-7i}{74}) = \frac{74}{74} = 1\). Thus, the two
   are multiplicative inverses.

7. Use identity \(a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2)(c^2 + d^2)\) where \(a, b, c, d\) are integers.

9. (a) \(-b\).
   (b) \(a\).
   (c) Note that \(i(a + bi) = -b + ia\).

11. If \(z \cdot w_1 = z \cdot w_2 = 1\), then \(w_1 = (w_2z)w_1 = w_2(zw_1) = w_2\).

13. If \(1 = (a + bi)(1 + i)\) where \(a, b\) are integers, then by multiplying show that \(a - b = 1\) and
   \(a + b = 0\). Show that these equations have no integer solutions.

15. Use definition 13.1.2 to prove each property.

17. (a) Possibilities are \(\pm 1 \pm 4i\) and \(\pm 4 \pm i\).
   (b) This is impossible, since 11 can’t be written as the sum of two squares.
   (c) Possibilities are \(\pm 5, \pm 5i, \pm 3 \pm 4i, \pm 4 \pm 3i\).
   (d) This is impossible, since 21 can’t be written as a sum of two squares.

13.2

1. We know that \(N(5 + 6i) = 25 + 36 = 61\). Since 61 is prime in \(\mathbb{Z}\), then by lemma 13.2.6, \(5 + 6i\)
   is prime in the Gaussian integers.

3. The factors are \(\pm 1, \pm i, \pm 2, \pm 3, \pm 2i, \pm 3i, \pm 6, \pm 6i, \pm 1 \pm i, \text{ and } \pm 3 + \pm 3i\).

5. Suppose \(z\) is a common factor of \(2 + 5i\) and \(3 + 2i\). Then since the norm is multiplicative,
   \(N(z) | N(2 + 5i) = 29\) and \(N(z) | N(3 + 2i) = 13\). The greatest common divisor of 29 and 13
   is 1, so we have \(N(z) = 1\), and hence \(z\) is a unit. Therefore, \(2 + 5i\) and \(3 + 2i\) are relatively
   prime.
Figure 2.1: Diagram for problem 13.1.1
7. (a) $\pm 1$.
   (b) Every nonzero element of $\mathbb{Q}$ is a unit.
   (c) Every integer relatively prime to 10 is a unit in $\mathbb{Z}_{10}$.
   (d) All integers relatively prime to $n$ are units in $\mathbb{Z}_n$.

9. Use $n = (a + bi)(a - bi)$.

11. $i(-i) = 1$, $(-1)(-1) = 1$ and clearly $1 \cdot 1 = 1$. So $\pm 1, \pm i$ are all units.

13. Since $d \mid x$ we have $ad = x$ and similarly we can write $bd = y$. Therefore we have $mx + ny = mad + nbd = (ma + nb)d$. This implies $d \mid mx + ny$.

15. Suppose that $N(z) = p$, for $p$ prime in $\mathbb{Z}$, but that $z$ is not prime in $\mathbb{Z}[i]$. Then $z = a \cdot b$. Then $p = N(z) = N(ab) = N(a) \cdot N(b)$, use problems 12 and 13 to show that $a$ or $b$ must be a unit and therefore $z$ is prime.

17. (a) If $d \mid a$ and $d \mid b$ then show that $N(d) \mid N(a)$ and $N(d) \mid N(b)$, hence $N(d) = 1$. Deduce that $d$ is a unit.
   (b) The converse statement is that if $\gcd(a, b) = 1$, then $\gcd(N(a), N(b)) = 1$. This statement is false. For example, take $a = 1 + 2i$ and $b = 2 + i$.

19. (a) $46 = 2 \cdot 23$ and so is prime.
   $48 = 6 \cdot 8$ and so is not prime.
   (b) The prime elements are those of the form $4n + 2$ where $n$ is a nonnegative integer.
   (c) If $a = 2^m m \in S$ where $m$ is odd then, $a = 2 \ldots 2 \cdot (2m)$. Show that each factor is prime.
   (d) Consider 60. $60 = 2 \cdot 30$ and $60 = 6 \cdot 10$. Also $180 = 6 \cdot 30 = 18 \cdot 10$.

21. $N(z) = 1$. See observation 13.2.4.

23. If they were the same up to order or multiplication by units, then either $N(1 + \sqrt{-5}) = N(2)$ or $N(3)$ which is not possible.

### 13.3

1. (a) $q b + r = (-1 + 2i)(4 + 2i) + (-1 + i) = -4 - 2i + 8i - 4 - 1 + i = -9 + 7i = a$
   (b) $N(r) = 1^2 + 1^2 = 2 < 20 = 4^2 + 2^2 = N(b)$

3. (a) In figure 2.2, $b = 3i$.
   (b) Given the diagram, we can choose any of $i, 2i, -1 + i, -1 + 2i$ as possible quotients. These give remainder norms of 2, 5, 5, and 8 respectively and these are all smaller than $N(3i) = 9$, so all four options work and all possible solutions are $q = i, r = -1 - i; q = 2i, r = 2 - i; q = -1 + i, r = -1 + 2i$; and $q = -1 + 2i, r = 2 + 2i$. 
5. Using the algebraic method we get \( q = -2i \) and \( r = 1 + i \).

7. Using the algebraic method we get \( q = -7 - 3i \) and \( r = 2 + 2i \).

9. Using the algebraic method we get \( q = -4 + 2i \) and \( r = -i \).

For the geometric method, we use figure 2.3 to see that we can choose any of \(-3 + i, -3 + 2i, -4 + i, -4 + 2i\) as quotients. All of these give remainders with \( N(r) = 1 < 2 = N(1 - i) \), so all four options work and any of the answers \( q = -3 + i, r = i; q = -3 + 2i, r = -1; q = -4 + i, r = 1 \) and \( q = -4 + 2i, r = -i \).

11. (a) See figure 2.5.

(b) 0, 1, 2, \( i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i \). These are the points inside one square, including one vertex (since they all have remainder of 0) and two edges.

13. It is true if \( b \neq 0 \). To prove it write \( b = ad \) and use the properties of norms.

15. Prove that \( \frac{a}{b} = \frac{su + tv}{u^2 + v^2} + \frac{tu - sv}{u^2 + v^2}i \) and conclude that the real and imaginary parts of \( \frac{a}{b} \) are rational.

17. Note that if \( z = \frac{a}{b} = z_1 + z_2i \) then there exist \( n_1, n_2 \in \mathbb{Z} \) such that \( |z_1 - n_1| \leq \frac{1}{2} \) and \( |z_2 - n_2| \leq \frac{1}{2} \). Now let \( n = n_1 + n_2i \) and prove that \( |z - n| = |(z_1 - n_1) + (z_2 - n_2)i| \leq \sqrt{2} \).

19. (a) Let \( a, b \in \mathbb{Z} \) with \( b \neq 0 \). Then there exist \( q, r \in \mathbb{Z} \) such that \( a = qb + r \) and \( |r| < |b| \).

(b) The two possible answers are \( q = 3, r = 2 \) and \( q = 4, r = -3 \).

(c) The two possible answers are \( q = -3, r = 2 \) and \( q = -4, r = -3 \).

21. Use that fact that after each step, the norm of the remainder must be strictly less than the norm of the remainder in the previous step.

23. Two possible ways are

\[
\begin{align*}
5 + 20i &= (1 + i)(11 + 3i) + (-3 + 6i) \\
11 + 3i &= -2i(-3 + 6i) + (-1 - 3i) \\
-3 + 6i &= (-1 - i)(-1 - 3i) + (-1 + 2i) \\
-1 - 3i &= (-1 + i)(-1 + 2i) + 0
\end{align*}
\]

and

\[
\begin{align*}
5 + 20i &= (1 + 2i)(11 + 3i) - 5i \\
11 + 3i &= (-1 + 2i)(-5i) + (1 - 2i) \\
-5i &= (2 - i)(1 - 2i) + 0.
\end{align*}
\]

25. The pairs \(-2 + 5i, 1 + i, 6 + 3i, 3 + i, 1 + 2i, 16 - 5i, 17 + 37i\) are all relatively prime.
13.4

1. (a) Two other factorizations are \( 5 = (-2 - i)(-2 + i) \) and \( 5 = (1 - 2i)(1 + 2i) \).
   (b) This is not a contradiction because they are all the same factorization up to units as can be seen in the following equations:
   \(-1(2 + i) = -2 - i, \; i(2 + i) = -1 + 2i, \; -i(2 + i) = 1 - 2i, \; -1(2 - i) = -2 + i, \; i(2 - i) = 1 + 2i \) and \(-i(2 - i) = -1 - 2i.\) Unique factorization says that if you multiply a factorization by units, then it is still the same factorization.

3. \((1 - i)(2 + i)(2 + 3i)\)

5. \(2 - 5i\) is prime.

7. Use Theorem 13.3.3 to show that there exist \(X, Y \in \mathbb{Z}[i]\) such that \(mX + dY = 1\). Multiplying through by \(n\) we get \(n = nmX + ndY\). Use this to prove \(d|n\).

9. Note that a common divisor, \(d\) of \(q\) and \(a\) must divide both \(q\) and \(a\).

11. Use induction on \(N(z)\).

13. Use the properties of norm.

15. (a) First prove that if \(z = z_1z_2\) then \(z^* = z_1^*z_2^*\). Use this to prove (a).
   (b) Note that \(u\) can only be \(1, -1, i, -i\). Consider different cases according to what \(u\) is.

17. Note that \(2\) is prime in \(\mathbb{Z}[\sqrt{-5}]\) and \(2|6\), but \(2\) does not divide \(1 + \sqrt{-5}\) or \(1 - \sqrt{-5}\).

13.5

1. For all of the numbers in this problem, we will use Theorem 13.5.5. Since they are all integers, then their norms are squares in \(\mathbb{Z}\) and therefore conditions one and two do not hold. Thus, they are prime if they are congruent to 3 modulo 4 and not prime if they are congruent to 1 modulo 4 where the unit mentioned in condition 3 is 1. 
   (a) \(29 \equiv 1 \pmod{4}\) so it is not prime in \(\mathbb{Z}[i]\).
   (b) \(31 \equiv 3 \pmod{4}\) so it is prime in \(\mathbb{Z}[i]\).
   (c) \(563 \equiv 3 \pmod{4}\) so it is prime in \(\mathbb{Z}[i]\).
   (d) \(1009 \equiv 1 \pmod{4}\) so it is not prime in \(\mathbb{Z}[i]\).
   (e) \(2011 \equiv 3 \pmod{4}\) so it is prime in \(\mathbb{Z}[i]\).
   (f) \(2^61 - 1 \equiv 3 \pmod{4}\) so it is prime in \(\mathbb{Z}[i]\).

3. \(N(z) = 2: (1 + i), \; N(z) = 3: \emptyset, \; N(z) = 4: \emptyset, \; N(z) = 5: (2 + i), \; N(z) = 6: \emptyset, \; N(z) = 7: \emptyset, \; N(z) = 8: \emptyset, \; N(z) = 9: \{3\}, \; N(z) = 10: \emptyset, \; N(z) = 11: \emptyset, \; N(z) = 12: \emptyset.

5. Use that fact that the only quadratic residues \((\bmod 8)\) are 0, 1, and 4.
7. Use the contrapositive of Theorem 13.5.3 and Corollary 13.5.2.

9. Note that by Theorem 13.5.5 \( p \) is not prime in \( \mathbb{Z}[i] \). SO \( p = zw \) where \( z, w \in \mathbb{Z}[i] \) are not units. Use properties of norm to show that \( N(z) = N(w) = p \). Finally show that \( z \) and \( w \) must be prime in \( \mathbb{Z}[i] \).

11. For statements (i) and (ii), use Lemma 13.2.6. For statement (iii) use Theorem 13.5.4.

13. (a) Note that \( N(2) = 4 \). Use the exact same logic of Exercise 13.5.9 and arrive at the conclusion that \( N(z) = 2 \). By Exercise 13.5.3, we have that \( z = u \cdot (1 + i) \), where \( u \) is a unit.

(b) See Exercise 13.5.9.

(c) Use Corollary 13.5.2.

13.6

1. (a) \( 4^2 + 5^2 \)

(b) \( 3^2 + 3^2 \)

(c) Not possible. Note that 21 factors uniquely as \( 3 \cdot 7 \) in \( \mathbb{Z}[i] \). If \( a^2 + b^2 = 3 \cdot 7 \), we would have \((a - bi)(a + bi) = 3 \cdot 7 \). Since 3 and 7 are prime in \( \mathbb{Z}[i] \), we would have \( 3|(a - bi) \) or \( 3|(a + bi) \), and similarly for 7. But this would say that \( 3|a \) and \( 3|b \) and likewise for 7. This would mean that 21|\( a \) and 21|\( b \), but then \( a \) and \( b \) are too large to satisfy \( N(a + bi) = 21 \).

3. Using Theorem 13.6.1, these primes are the sum of two squares if and only if they are congruent to 1 modulo 4.

(a) \( 149 \equiv 1 \mod 4 \) so it can be written as a sum of two squares.

(b) \( 151 \equiv 3 \mod 4 \) so it can not be written as a sum of two squares.

(c) \( 91711 \equiv 11 \equiv 3 \mod 4 \) so it can not be written as a sum of two squares.

(d) \( 10,000,019 \equiv 19 \equiv 3 \mod 4 \) so it can not be written as a sum of two squares.

(e) \( 23,456,789 \equiv 89 \equiv 1 \mod 4 \) so it can be written as a sum of two squares.

(f) \( 10^{200} + 357 = 100 \cdot 10^{198} + 357 \equiv 57 \equiv 1 \mod 4 \) so it can be written as a sum of two squares.

5. In each case, we don’t count it as “different” to change the sign of \( a \) and \( b \) or to switch their order. (a) one way (it’s a 1 mod 4 prime): \( 15^2 + 2^2 \)

(b) 2 ways: \( 10^2 + 5^2 \) and \( 11^2 + 2^2 \)

(c) no ways (it’s a 3 mod 4 prime)

7. Note that \( u \) must be \( 1, -1, i \) or \( i \).

9. First, prove that the product of two SOTSes is also a SOTS. Use the identity \( a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (bc - ad)^2 \).
Next note that the number 2 and any prime congruent to 1 modulo 4 can be written as a sum of squares. Also, any prime \( p \) raised to an even power, say \( 2i \) is also a sum of squares as \( p^{2i} = (p^i)^2 + 0^2 \).

3 modulo 4 is raised to an even power in the factorization of \( n \) into primes.

11. (a) \( x^2 \equiv \left( \frac{a^{p-1}}{4} \right)^2 \equiv a^{\frac{p-1}{2}} \equiv -1 \) (mod \( p \)).

(b) From Chapter 11, we know that for any \( a \neq 0 \), there is a \( \frac{1}{2} \) chance that \( a^{\frac{p-1}{2}} \equiv -1 \) (mod \( p \)) (this is due to Euler’s Identity [11.2.2] and the fact that exactly half of the nonzero elements are quadratic residues). Thus if we randomly choose a few \( a \)'s, chances are that one of them will work.

13. First notice that for both of the cases, we can use Euler’s Identity with Theorem 11.4.3 to see that \( 2^{\frac{p-1}{2}} \equiv -1 \) (mod \( p \)). In each case, set \( x = 2^{\frac{p-1}{2}} \) (mod \( p \)) and look at the Gaussian gcd of \( x + i \) and \( p \) with a computer program. (a) 8675309 = 422² + 2915². (b) 10¹⁰² + 117 = 453995475299019885990121049201972823439835907751721² + 8910039889969187988422937466998175100083².

15. By the Fundamental Theorem of Gaussian Arithmetic, it is enough to show that our factorization contains only primes and units and that its product is \( n \). Using Theorem 13.5.5, show that all the factors are prime.

17. Show that it is equal to the number of the non-negative integer solutions of \( f_1 + g_1 = b_1, \ldots, f_r + g_r = b_r \) which is equal to \( (b_1 + 1)(b_2 + 1) \cdots (b_r + 1) \).
Figure 2.2: Diagram for problem 13.3.3 where $b = 3i$.
Figure 2.3: Diagram for problem 13.3.9 with $b = 1 - i$. 
Figure 2.4: Diagram for problem 13.3.10 with $b = 5 + 7i$. 
图 2.5：问题 13.3.11 中的图示，其中 $b = 3$. 
14.1

1. [2, 3, 4, 2]
2. [4, 10, 7, 5]
3. \( \frac{74}{31} \)
4. \[0, 9, 9, 9\] = 82
5. [4, 10, 7, 5]
6. \[1, 1, 1, 1\] = \( \frac{8}{5} \)
7. \[2, 3, 4, 2\]
8. \[3, 10, 7, 5\]
9. \[1, 1, 1, 1\] = \( \frac{8}{5} \)
10. \[4, 8, 8, 8, 8, \ldots\]
11. \[6, 3, 1, 1, 7, 2, \ldots\]
12. \( F_{k+1} + F_k = [a_1, a_2, \ldots, a_k] = [1, 1, \ldots, 1] \)

14.2

1. [3, 6]
2. [3, 3, 6]
3. [4, 8, 8, 8, 8, 8, \ldots]
4. [6, 3, 1, 1, 7, 2, \ldots]
5. \( e - 1 = [1, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots] \). The pattern continues by adding 4 each time.
6. \( e - 1 = [0, 1, 6, 10, 14, 22, \ldots] \). The pattern continues by adding 4 each time.
7. \( e - 1 = [0, 2, 6, 10, 14, 22, \ldots] \). The pattern continues by adding 4 each time.
8. \( e^{1/2} = [1, 1, 1, 1, 5, 1, 1, 9, 1, 1, 13, 1, 1, 17, \ldots] \). The pattern continues by 1, 1 add 4.
9. \( e^{1/3} = [1, 2, 1, 1, 8, 1, 1, 14, 1, 1, 20, 1, 1, 26, \ldots] \). The pattern continues by 1, 1 add 6.
10. \( x = 4 + \frac{1}{2 + \frac{1}{x}} \). So after some algebra we get \( x^2 - 4x - 2 = 0 \), which leads to \( x = 2 + \sqrt{6} \) as the only positive root of the polynomial.
11. \( \alpha = \frac{1 + \sqrt{5}}{2} \)
12. \( \alpha = \frac{-7 + \sqrt{53}}{2} \)
17. \( \alpha = \frac{5 + \sqrt{35}}{2} \)

19. \( \alpha = \frac{-1 + \sqrt{15}}{2} = [1, \frac{3}{2}, 3] \)

21. We can calculate backwards to find that \([2, 2, 4] = \sqrt{6}\).

23. Use induction and the definition of \([a_1, \ldots, a_n]\).

25. Note that if \( \alpha = [a_1, a_2, \ldots] = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}} \) then \( \frac{1}{\alpha} = 0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}} = [0, a_1, a_2, \ldots] \).

27. (a) 2 and 5
(b) \( \Rightarrow \)
Use the fact that if \( \frac{a}{b} \) has a terminating decimal expansion, then \( \frac{a}{b} = \frac{k}{10^n} \) for some integers \( k \) and \( n \).

\( \Leftarrow \)
Suppose \( b = 2^m5^n \). If \( m \leq n \), then we may write \( \frac{a}{b} = \frac{2^{m-n}a}{2^m5^n} \), which gives a terminating decimal expansion for \( \frac{a}{b} \). If \( n < m \), the proof is similar.

(c) In base 12, a fraction written in lowest terms, \( \frac{a}{b} \), has a terminating expansion if and only if the denominator \( b \) contains only factors of 2 and 3.

29. (a) The base case is \( m = 0 \) for which we have \( [S(x)] = S(x) \) is a rational linear functional. So suppose the result holds for all continued fractions with \( m \) terms before the \( S(x) \). Then for any \( b_1, \ldots, b_{m+1} \) use \( [b_1, \ldots, b_{m+1}, S(x)] = b_1 + \frac{1}{[b_2, \ldots, b_{m+1}, S(x)]} \) to show that \( b_1, \ldots, b_{m+1} \) use \( [b_1, \ldots, b_{m+1}, S(x)] \) is a rational linear function.
(b) We have \( D = [b_1, \ldots, b_m] = [b_1, \ldots, b_m, [b_1, \ldots, b_m]] = [b_1, \ldots, b_m, D] \). Use (a) to write the right side of this equation as \( \frac{aD+b}{cD+d} \) and show that \( cD^2 + (d-a)D - b = 0 \).
(c) Give a proof by induction and use the following identities

\[
[a_1, \ldots, a_n, \frac{a\sqrt{b} + c}{d}] = 1 + \frac{1}{[a_2, \ldots, a_n, \frac{a\sqrt{b} + c}{d}]} = 1 + \frac{1}{e\sqrt{f} + g} = 1 + \frac{h}{e\sqrt{f} + g} = 1 + \frac{h(g - e\sqrt{f})}{(g - e\sqrt{f})(g + e\sqrt{f})} = 1 + \frac{hg - he\sqrt{f}}{g^2 - e^2f} = \frac{e\sqrt{f} + g}{h} \text{ by induction hypothesis.}
\]
### 14.3

| convergent $r_n$ | error = $|\theta - r_n|$ |
|------------------|-----------------------------|
| continued fraction = simple fraction = decimal | decimal $\approx \frac{1}{3}$ |
| [1] | $1 = 1$ | 0.618033... $\approx \frac{1}{1}$ |
| [1, 1] | $2 = 2$ | 0.381966... $\approx \frac{1}{2}$ |
| [1, 1, 1] | $\frac{3}{2} = 1.5$ | 0.1180339888... $\approx \frac{1}{3}$ |
| [1, 1, 1, 1] | $\frac{4}{3} = 1.6666...$ | 0.0486326... $\approx \frac{1}{4}$ |
| [1, 1, 1, 1, 1] | $\frac{5}{3} = 1.6$ | 0.018034... $\approx \frac{1}{5}$ |
| [1, 1, 1, 1, 1, 1] | $\frac{6}{4} = 1.5$ | 0.006966... $\approx \frac{1}{6}$ |
| [1, 1, 1, 1, 1, 1, 1] | $\frac{7}{4} = 1.619...$ | 0.0010136... $\approx \frac{1}{7}$ |

(b) In table above.

(c) They are alternately $-2$ and $1$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$r_n = \frac{h_n}{k_n}$</th>
<th>$h_n^2 - 3k_n^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\frac{1}{1}$</td>
<td>$-2$</td>
</tr>
<tr>
<td>2</td>
<td>$\frac{2}{2}$</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>$\frac{3}{3}$</td>
<td>$-2$</td>
</tr>
<tr>
<td>4</td>
<td>$\frac{4}{4}$</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>$\frac{5}{5}$</td>
<td>$-2$</td>
</tr>
</tbody>
</table>

(d) They are alternately $\pm1$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$h_n k_{n+1} - h_{n+1} k_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1 \cdot 1 - 2 \cdot 1 = -1$</td>
</tr>
<tr>
<td>2</td>
<td>$2 \cdot 3 - 5 \cdot 1 = 1$</td>
</tr>
<tr>
<td>3</td>
<td>$5 \cdot 4 - 7 \cdot 3 = -1$</td>
</tr>
<tr>
<td>4</td>
<td>$7 \cdot 11 - 19 \cdot 4 = 1$</td>
</tr>
</tbody>
</table>

5. (a) They are alternately $\pm1$. 
7. Let \( n = \lfloor d \alpha \rfloor \) rounded to the nearest integer. Then \( \frac{n}{d} \) approximates \( \alpha \) and has denominator \( d \).

Finally note that \( \alpha - \frac{n}{d} > \alpha - \frac{d\alpha - 1/2}{d} = \frac{1}{2d} \).

9. (a) For each value given in the table, \( d \) is at least the product of the denominators. So

\[
|\sqrt{2} - \frac{h_n}{k_n}| \leq \frac{1}{k_n k_{n+1}}.
\]

(b) Again, for each value given in the table, \( d \) is at least the product of the denominators. So

\[
|\pi - \frac{h_n}{k_n}| \leq \frac{1}{k_n k_{n+1}}.
\]

(c) Since the next denominator is much larger than 7, the convergent \( \frac{22}{7} \) is much better than you would expect as an approximation. It is within \( \frac{1}{7 \cdot 106} \) of \( \pi \).
(d) $\frac{355}{113}$ is a better choice. The two fractions have comparable numerators and denominators, so you don’t have to memorize more digits or do more computations. However, because the next denominator is 33102, the approximation given by $\frac{355}{113}$ is over 200 times closer to $\pi$.

14.4

<table>
<thead>
<tr>
<th>$n$</th>
<th>$-1$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_n$</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$b_n$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>10</td>
<td>23</td>
<td>79</td>
</tr>
<tr>
<td>$k_n$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>7</td>
<td>16</td>
<td>55</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>$-1$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_n$</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$b_n$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>10</td>
<td>43</td>
<td>225</td>
</tr>
<tr>
<td>$k_n$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>7</td>
<td>10</td>
<td>157</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$n$</th>
<th>$-1$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_n$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$b_n$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>$k_n$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>7</td>
<td>9</td>
</tr>
</tbody>
</table>

7. From earlier in the chapter we know that $k_5 = 33, 102$, thus the theorem says that $|\pi - \frac{355}{113}| < \frac{1}{113 \times 33, 102} \approx 2.673 \times 10^{-7}$. Computing we have $|\pi - \frac{355}{113}| \approx 2.667 \times 10^{-7}$.

9. a) 1.0000, error:.6487 2.0000,.1487 1.6667,.0179 1.6500,.0017 1.6486,.0001 1.6487252,3.942 * 10^-6 1.6487179,3.322 * 10^-6 1.6487214,1.29 * 10^-7 1.6487212658,5 * 10^-9 1.648721275,4 * 10^-9 1.6487212706,1.28 * 10^-11 1.6487212707039,4 * 10^-13 1.6487212706968,3 * 10^-13 1.6487212707002,8 * 10^-14 1.6487212707001026,2 * 10^-15 1.648721270700013,1 * 10^-15 1.6487212707000128,0 1.6487212707000128,0

b) 5.0000, error:.5678 6.0000,.4322 5.5000,.0678 5.5714,.0037 5.5675676,.0002 5.5677966,3.225 * 10^-5 5.5677419,2.243 * 10^-5 5.5677656,1.2 * 10^-6 5.5677643,6 * 10^-8 5.5677644,5 * 10^-8 5.567764355,1 * 10^-8 5.567764363,2,7,377 * 10^-9 5.5677643628,3,96 * 10^-10 5.5677643628087,2,1 * 10^-11 5.5677643628335,3 * 10^-12 5.5677643628276,2 * 10^-12 5.5677643628302,1,306 * 10^-13 5.5677643628300151,6,2 * 10^-14 5.5677643628302665,5,3 * 10^-14 5.5677643628302132,0 5.5677643628302132,0

c) 1.0000, error:.71 2.0000,.29 1.6667,.0433 1.7143,.0043 1.7097,.0003 1.7100,2.405 * 10^-5 1.70997616,1.29 * 10^-6 1.709976798,8,5 * 10^-7 1.709975865,8 * 10^-8 1.709976400,3,6 * 10^-8 1.709975939,1 * 10^-8 1.7099759468384,1.617 * 10^-10 1.7099759466768,9 * 10^-13 1.7099759466767,4,818 * 10^-14 1.70997594667693,3 * 10^-15 1.709975946676973,2,2 * 10^-16 1.709975946676970,0 1.709975946676970,0
11. Use the equations \( h_n x + h_{n+1} y = a \) and \( k_n x + k_{n+1} y = b \) to show that \((h_{n+1}k_n - k_{n+1}h_n)y = k_n a - h_n b\). Now use the Criss-Cross Lemma (14.5.3) to finish the solution.

13. Give a proof by induction that for a fixed \( m \), and every \( n > m \), \(|r_n - r_m| < \frac{1}{k_m}\).
   
   Base Case: For \( n = m + 1 \). show that \(|r_{m+1} - r_m| = \frac{|(-1)^{m+2}|}{k_{m+1}k_m}\). Since \( k_{m+1} \geq 1 \) for all \( i \), \(|r_{m+1} - r_m| < \frac{1}{k_m}\).
   
   Now assume that \(|r_i - r_m| < \frac{1}{k_m}\) for all \( m < i < n \). Show that \(|r_n - r_m| \leq \frac{|a_n(k_mh_{n-1}+k_{n-1}h_m)|}{k_nk_m} + \frac{|k_mh_{n-2}-k_{n-2}h_m|}{k_nk_{n-1}k_m} \). Then use \( k_n > a_nk_{n-1} \) to show that \(|r_n - r_m| \leq \frac{|k_mh_{n-1}+k_{n-1}h_m|}{k_nk_{n-1}k_m} + \frac{|k_mh_{n-2}-k_{n-2}h_m|}{k_nk_{n-1}k_m} \). Now use the induction hypothesis to show that \(|r_n - r_m| < \frac{1}{k_m}\).

   Finally use the above fact to show that \( \{r_n\} \) is a cauchy sequence, and the limit exists.

15. Assume that \( \alpha \neq \beta \) are both irrational numbers, but both have the same continued fraction expansion \([a_1, a_2, ...]\). This implies that the convergents, \( r_n = [a_1, a_2, ..., a_n] \) are the same. Use exercise 14 to show \( \alpha = \beta \) which is a contradiction.
15.1

1. (a) $-23$
   (b) $97$
   (c) $49$

3. Two solutions, given by the second and fourth convergents, are $(5, 2)$ and $(49, 20)$.

5. Two solutions, given by the second and fourth convergents, are $(2, 1)$ and $(7, 4)$.

7. $(19 - 6\sqrt{10})^2 = 721 - 228\sqrt{10}$ and $(721 - 228\sqrt{10})^2 = 1039681 - 328776\sqrt{10}$. So $x = 721$, $y = 228$ and $x = 1039681$, $y = 328776$ are both solutions.

9. Note that $a^b = b$ and use lemma 15.1.8.

11. (a) $N(2 + 3\sqrt{-5}) = 2^2 + 5 \cdot 3^2 = 49$
   (b) Use the definition of norm.
   (c) Show that only $a = \pm 1$ satisfy $N(a) = 1$.
   (d) Use the definition of norm to reduce the problem to solving $x^2 + 5y^2 = 13$ where $x, y$ are integers. Then show that this equation has no solution.

13. Suppose we have integers $x$ and $y$ so that $x^2 - dy^2 = 1$. Since $d = e^2$, we may write $(x + ey)(x - ey) = 1$. Use this to show that the only solutions are $x = 1, y = 0$ or $x = 1, y = 0$.

15. (a) The first convergent $\frac{2}{1}$ gives a solution to $x^2 - 5y^2 = -1$. The second convergent $\frac{9}{4}$ gives a solution to $x^2 - 5y^2 = 1$.
   (b) The first convergent $\frac{2}{1}$ gives a solution to $x^2 - 10y^2 = -1$. The second convergent $\frac{19}{6}$ gives a solution to $x^2 - 10y^2 = 1$.
   (c) The third convergent $\frac{32}{5}$ gives a solution to $x^2 - 41y^2 = -1$. The sixth convergent $\frac{2049}{320}$ gives a solution to $x^2 - 41y^2 = 1$.
   (d) The fifth convergent $\frac{18}{5}$ gives a solution to $x^2 - 13y^2 = -1$. The tenth convergent $\frac{649}{180}$ gives a solution to $x^2 - 13y^2 = 1$.

17. (a) It seems that the $n^\text{th}$ convergent gives the first solution to $x^2 - dy^2 = -1$, and the $2n^\text{th}$ convergent gives the first solution to $x^2 - dy^2 = 1$. (b) It seems that there are no solutions to $x^2 - dy^2 = -1$, and the $n^\text{th}$ convergent gives the first solution to $x^2 - dy^2 = 1$.

19. If we look at the norm equation mod 5, we get $N(a + b\sqrt{10}) = a^2 - 10b^2 \equiv 2 \pmod{5}$, but this is the same as $a^2 \equiv 2 \pmod{5}$. Since 2 is not a quadratic residue modulo 5, there is no solution.
21. Let \(a + b\sqrt{d}, c + e\sqrt{d} \in \mathbb{Z}[\sqrt{d}]\). Then
\[
a + b\sqrt{d} + c + e\sqrt{d} = (a + c) + (b + e)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]
\]
and,
\[
(a + b\sqrt{d})(c + e\sqrt{d}) = (ac + bed) + (bc + ea)\sqrt{d} \in \mathbb{Z}[\sqrt{d}],
\]
so \(\mathbb{Z}[\sqrt{d}]\) is closed under addition and multiplication, as required.

23. Simplify \(v^2 - dw^2\).

25. (a) Use Lemma 15.1.8.
(b) \(zw = (a + b\sqrt{d})(f + g\sqrt{d}) = (af + bgd) + (ag + bf)\sqrt{d}\)
(c) Note that \(g^2 - d \cdot h^2 = N(zw)\).
(d) By symmetry, it is enough to show that \((g, h)\) is a different solution than \((a, b)\). If \((g, h) = (a, b)\), then show that \(f = 0\), a contradiction.

27. Say there were some solution \((e, f)\) which is not one of the \((x_n, y_n)\). Then it follows that \(w = e + f\sqrt{d}\) is not of the form \(z^n\) for any natural number \(n\). First show that there is some \(n \in \mathbb{N}\) such that \(z^n < w < z^{n+1}\), so that \(1 < \frac{w}{z^n} < z\). Then show that \(\frac{w}{z^n} = y = g + h\sqrt{d} \in \mathbb{Z}[d]\) is also a solution to Pell’s equation. Since \(y > 1\) it follows that at least one of \(g\) and \(h\) is positive. We consider three cases:

**Case 1:** If both are positive, then \((g, h)\) is a positive solution. Show that \(y\) is a smaller solution than \(z\).

**Case 2:** If \(g\) is positive but \(h\) is not, then consider \(\frac{1}{y}\) is greater than one, a contradiction. Thus we cannot have this case.

**Case 3:** If \(h\) is positive but \(g\) is not, then consider \(-y = (-g) + (-h)\sqrt{d}\) and show that \(\frac{1}{-y} > 1\). Thus, we cannot have this case either.

Thus, there are no valid cases, so we have a contradiction. Therefore, the assumption that such a \(w\) existed is false.

15.2

1. \(25^2 + 24^2 = 1201\) which is not a perfect square. \(25^2 - 24^2 = 49 = 7^2\). So the third number is 7.

3. (a) \(40^2 + 96^2 = 10816 = 104^2\)
   (b) \(104 - 40 = 64 = 4^3\)
   \(104 - 96 = 8 = 2^3\)

5. Show that \((kx)^2 + (ky)^2 = (kz)^2\) if \(x^2 + y^2 = z^2\).
7. (a) If \( n \) has an odd prime factor then we are done. Suppose not, show that \( n \) is a power of 2 and so it is divisible by 4.
(b) Let \((a, b, c)\) be a nonzero integer solution to the equation \( x^n + y^n = z^n \). Let \( n = dm \).
Then show that \((a^m, b^m, c^m)\) is a nonzero integer solution to the equation \( x^d + y^d = z^d \).
(c) Suppose that there is a nonzero integer solution to \( x^n + y^n = z^n \). Using part (a), take \( d|n \) be an odd prime factor or 4. Then use (b) to show that there is a nonzero integer solution to \( x^d + y^d = z^d \).

9. For \( n \) even, use the fact that if \((x, y, z)\) is a solution then \((-x, \pm y, \pm z)\) are also solutions.
For \( n \) odd, use the fact that if \( y \) is negative then \( x^n = (-y)^n + z^n \), hence \((-y, x, z)\) is a solution.

11. (a) Direct computation.
(b) Just a few possibilities: \( x = 2, y = 1 \) gives the triple 3, 4, 5.
\( x = 3, y = 2 \) gives 5, 12, 13.
\( x = 4, y = 3 \) gives 7, 24, 25.
\( x = 5, y = 3 \) gives 16, 30, 34.
\( x = 5, y = 4 \) gives 9, 40, 41.
(c) Every even number greater than 2 can be written as \( 2k \) for some \( k > 1 \). We can then assign \( x = k \) and \( y = 1 \) to get \( 2xy = 2k \) as part of our triple.
(d) Note that \((n + 1)^2 - n^2 = 2n + 1\). So take \( x = n + 1 \) and \( y = n \).

13. Note that if \( p \) is a not a prime factor of \( xyz \), then \( x^{p-1} + y^{p-1} = z^{p-1} \) gives \( 1 + 1 \equiv 1 \pmod{p} \), a contradiction.

15. Suppose by way of contradiction that \( x + y \) and \( z - x \) share a nontrivial prime factor, \( p \). Then use \( z^n = x^n + y^n \) to show that \( z \) must have \( p \) as a factor. Since \( p \) divides both \( z \) and \( z - x \), it divides \( x \). Hence, \( p \) is a factor of \( z \) and \( x \), which contradicts the assumption that they were relatively prime.

17. (a) Use \( 0 = \omega^{23} - 1 = (\omega - 1)(\omega^{22} + \omega^{21} + \ldots + \omega + 1) = 0 \) to show that \( \omega^{22} = -\omega^{21} - \omega^{20} - \ldots - 1 \) and thus is in \( \mathbb{Z}[\omega] \).
(b) Use (a) to show that \( ab = 2(\omega^5 + \omega^6 + \omega^7 + \omega^9 + \omega^{10} + 3\omega^{11} + \omega^{12} + \omega^{13} + \omega^{15} + \omega^{16} + \omega^{17}) \).
(c) This is not a unique factorization domain since the number \( ab \) may be factor as \( a \) times \( b \) or \( 2d \).
CHAPTER 2. HINTS TO PROBLEMS

15.3

1. (a) \(a = 2pq = 2 \cdot 9 \cdot 4 = 72\)  
   \(b = p^2 - q^2 = 9^2 - 4^2 = 65\)  
   \(c = p^2 + q^2 = 9^2 + 4^2 = 97\)

   (b) \(a = 2pq = 2 \cdot 12 \cdot 7 = 168\)  
   \(b = p^2 - q^2 = 12^2 - 7^2 = 95\)  
   \(c = p^2 + q^2 = 12^2 + 7^2 = 193\)

   (c) \(a = 2pq = 2 \cdot 15 \cdot 8 = 240\)  
   \(b = p^2 - q^2 = 15^2 - 8^2 = 161\)  
   \(c = p^2 + q^2 = 15^2 + 8^2 = 289\)

3. Using the same formulas as in problem 2, \(p = \sqrt{\frac{39 + 89}{2}} = \sqrt{64} = 8\), and \(q = \sqrt{\frac{89 - 39}{2}} = \sqrt{25} = 5\).

5. Using the same formulas as in problem 2, \(p = \sqrt{\frac{221 + 21}{2}} = \sqrt{121} = 11\), and \(q = \sqrt{\frac{221 - 21}{2}} = \sqrt{100} = 10\).

7. Using the relation \(a^2 + b^2 = c^2\), show that if a prime number divides two of the numbers \(a, b, c\), then it divides the third one as well.

9. (a) Use the relation \(a^2 + b^2 = c^2\).

   (b) Use problem 7.

11. Show that exactly one of them is even and then by looking at the equation \(a^2 + b^2 = c^2\) modulo 4, show that it has to be \(c\).

13. Assume that \(x, y\) is a non-trivial solution to \(x^4 - 2y^2 = 1\). Then, since \(x\) must be odd, \(\frac{x^4 + 1}{2}\) and \(\frac{x^4 - 1}{2}\) are natural numbers, and \(x^4 + y^4 = x^4 + \left(\frac{x^4 + 1}{2}\right)^2 = \left(\frac{x^4 + 1}{2}\right)^2\) which has no solutions.

15. Consider \(a^2, b^2, c^2\) and \(a^2 + b^2 = c^2\) mod 8.

17. If the radius of the circle is \(r\), the note that \(r(a + b + c) = ab\). So to show that \(r\) is an integer, prove that \(ab\) is divisible by \(a + b + c\).

18. We know that \(x\) and \(y\) cannot both be 1 in the formulas \(a = 2xy, b = x^2 - y^2,\) and \(c = x^2 + y^2\).  
   (Otherwise one of the “sides” is zero, and we have no triangle.) So that means \(a = 2xy\) must be a composite number.

19. Note that the equation of the line is \(y = \frac{b}{a}x\).

21. Show that if we send a primitive Pythagorean triple to a rational point using the map from Problem 19, and then send that back to a primitive Pythagorean triple using the map from Problem 20, we get the same triple.

23. (a) insert figure

   (b) \(y^2 = x^3 - x = x(x + 1)(x - 1)\) thus for this to have integer solutions either \(x - 1, x\) or \(x + 1\) needs to be zero, since \(\gcd(x, x + 1) = 1\) for \(x > 0\) and no three consecutive integers are all squares.
1. The first few Germain primes are 3, 5, 11, 23, and 29.

3. There are no consecutive 3rd power residues.

\[
\begin{array}{c|cccccc}
  & 1 & 2 & 3 & 4 & 5 & 6 \\
  x & 1 & 1 & 6 & 1 & 6 & 6 \\
 x^5 & 1 & 1 & 6 & 1 & 6 & 6 \\
\end{array}
\]

5. (a) Case I of FLT is true for \( n = 7 \)
(b) \( x^7 + y^7 = z^7 \) implies that at least one of \( x, y, z \) divisible by 29.

7. Note that \( |z|^n = |e||d| \) and \( |z|, |e| \) and \( |d| \) are natural numbers. Apply Lemma 15.2.2 and use the fact that \( n \) is odd to finish the proof.

9. (a) Since \( q - 1 \) and \( n \) are relatively prime, \( n \) has an inverse \( m \) modulo \( q - 1 \), that is, there exists some \( m \) such that \( mn = d(q - 1) + 1 \). Show that for any natural number \( y \) less than \( q \), \( x = y^n \) satisfies \( x^n \equiv y \pmod{q} \).
(b) Not true; try \( q = 13 \) and \( n = 8 \). The only residues are 0, 1, 3, 9.

11. This proof is precisely the same as the proof of Theorem 15.4.2, replacing 5 with \( n \), 11 with \( 2n + 1 \), and finally the factorization \( x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4) \) by

\[ x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \cdots + x^2y^{n-3} - xy^{n-2} + y^{n-1}). \]

Also, note that terms of the form \( 5a^4 \) are replaced by \( na^{n-1} \).

13. (a) Let \( n \) be a Germain prime. If none of \( x, y, \) and \( z \) are divisible by \( n \) then \( x^n + y^n \neq z^n \).
(b) This is essentially the same thing as Theorem 15.4.3.

15. If any of \( x, y, \) or \( z \) are 0, then that number is divisible by \( n \) and the theorem is proven.
Otherwise, let \( d = \gcd(x, y) \). Show that \( d \mid z \) and if \( x' = \frac{x}{d}, y' = \frac{y}{d} \) and \( z' = \frac{z}{d} \) then \( (x')^n + (y')^n = (z')^n \). Finally show that \( x', y' \) and \( z' \) are pairwise relatively prime.

17. Say that \( q \) is an auxiliary prime to \( n \), and that none of \( x, y, z \) is divisible by \( q \). Then \( x \) has a multiplicative inverse \( a \) in \( \mathbb{Z}_q \). Show that \( (ya)^n + (az)^n \equiv 0 \pmod{q} \) Note that neither \( (ya)^n \) nor \( (az)^n \) can be congruent to zero mod \( q \). Thus \( (ya)^n \) and \( (az)^n \) are consecutive \( n \)th power residues mod \( q \), contrary to hypothesis. Hence one of \( x, y, \) or \( z \) is divisible by \( q \).

15.5

1. The only possibilities are:
   A 5, 12, 13 triangle. The perimeter is 30 units. The area is 30 square units.
   A 6, 8, 10 triangle. The perimeter is 24 units. The area is 24 square units.
3. (a) add picture

b. Show that any rational point on the curve gives rise to an integer solution to \( x^4 + y^4 = z^4 \).

5. Say we had some \((x, y, z)\) such that \( x^4 + y^4 = z^4 \). By dividing by the gcd of \( x \) and \( y \) if necessary, we can assume that the three are relatively prime. Thus, \( x^2, y^2, z^2 \) is a primitive Pythagorean triplet; assuming without loss of generality that \( x^2 \) is the even number, we have \( x^2 = 2pq \), \( y^2 = p^2 - q^2 \), \( z^2 = p^2 + q^2 \) for some relatively prime \( p, q \) of which exactly one is even. Then show that the right triangle with legs of length \( p \) and \( q \) has hypotenuse \( z \) and its area is \( \frac{pq}{2} = \left( \frac{x}{2} \right)^2 \), which is a perfect square since \( x \) was even. This is a contradiction by the Right Triangle Theorem, so we could not have had a solution to \( x^4 + y^4 = z^4 \).

7. (a) Show that there is a right triangle with sides \( \frac{3}{2} \) and \( \frac{20}{3} \) and area \( \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{20}{3} = 5 \) and thus \( 5 \) is a congruent number.

(b) Assume that there is such a triangle. Then \( 5 = \frac{1}{2}bh \) for some sides \( b \) and \( h \). Show that no such \( h \) and \( b \) give a right triangle.

9. (a) Show that \( w^2 + n = \left( \frac{a+b}{2} \right)^2 \) and \( w^2 - n\left( \frac{a-b}{2} \right)^2 \).

(b) Use (a).

(c) Use (b).

(d) Thus if \( n \) is a congruent number we can find rational \( x \) and \( y \) such that \( (x, y) \) is on the elliptic curve \( y^2 = x^3 - n^2x \). We know \( x \) is non-zero since \( x = w^2 = \frac{c^2}{4} \) which is non-zero, and we know \( y \) is non-zero since \( y = wv = \frac{c}{2} \sqrt{(w^2 + n)(w^2 - n)} = \frac{c}{2} \left( \frac{a+b}{2} \cdot \frac{a-b}{2} \right) \) which is non-zero.

11. I. If not, show that we can divide by the common divisor of them to get a smaller solution.

II. Note that the area of the triangle is \( \frac{1}{2}xy = \frac{1}{2}2pq(p^2 - q^2) = pq(p + q)(p - q) \), and the area is a perfect square.

III. Use part II.

IV. Since both \( c + d \) and \( c - d \) are divisible by 2, we have that \( 4|2b^2 \), or \( 2|b^2 \). Conclude that \( 4|c + d \) or \( 4|c - d \).

V. Use part IV.

VI. Use part V and the fact \( \frac{c+d}{4} \) and \( \frac{c-d}{4} \) are relatively prime.

VII. Note that \( a^2 = p = \frac{v+q+p-q}{2} = \frac{c^2+d^2}{2} \).
VIII. Use part VII and note that $a < p < z$. 
Section A.1

1. To check if $\ast$ is a binary operation, you must show that if $x, y \in \mathbb{R}$, then $x \ast y = |x - y| \in \mathbb{R}$ as well. For commutativity, you will need to show that $x \ast y = |x - y| = |y - x| = y \ast x$. Finally, for associativity, try checking a few triplets of numbers and see what happens.

3. What happens when you multiply any two non-zero elements of $S$ with one another? What will this say about the binary operation? about the existence of a multiplicative identity?

5. To show that $S$ is a ring, verify each of the ring properties. If you have any difficulty, just think of the functions in terms of their specific values for a given $x \in \mathbb{R}$. If you can show that the property is satisfied for a single element, how can you expand that to all of $\mathbb{R}$? As for the field, what number in $\mathbb{R}$ doesn’t have a multiplicative inverse? So what kind of functions would be missing a multiplicative inverse?

7. Sometimes the best way to show something is by just applying a lot of brute force. However, note that the two tables are symmetric along the diagonal. This will make it much easier to show commutativity. Don’t forget to show each of the definitional requirements.

Section A.2

1. Use the definition of $>$ given after the properties: $a > b \Rightarrow b < a$. Using this, look at the properties given for $<$, and see what they imply in turn about $>$.

3. Notice that $x - 1 < x$ for all $x \in \mathbb{Z}$. So if we have all the negative numbers below a certain value, then there’s no end to the negativity!

5. Why can you use the Well-Ordering Principle on $\mathbb{N}$? To show uniqueness of this smallest element, use the formal definition you created in Exercise 4.

7. If $C$ does have an order, the trichotomy property will guarantee that either $i < 0$, $0 = i$, or $0 < i$. Show that in each of these cases, it will cause a contradiction with the other properties.

Section A.3

1. Since $-x \in R$, it has an additive inverse $-(-x)$. How can we use associativity and the fact that 

$$-x + -(-x) = 0$$

to show $x = -(-x)$?

3. You can use Exercise 2 to pull negatives out and use Exercise 1 to cancel two negative signs in a row.
5. Assume that \( y, z \in R \) such that \( xy = 1 = xz \). Show that \( y = z \).

7. Since \( 0 < z \), we know that \( xz < yz \). Where can you go from here?

9. Use a proof by contradiction.

11. To discover the three statements, try using 1 as your odd number and 2 as your even. For proving the statements, we know that any odd number is of the form \( 2k + 1 \) and any even number of the form \( 2k \).

13. Notice that \( x - y \) is just defined as \( x + (-y) \). Are additive inverses contained in \( Z \)?

15. Since it’s an if and only if problem, you will have to show that \( x > y \Rightarrow x - y > 0 \) and also that \( x - y > 0 \Rightarrow x > y \). In both cases you will want to manipulate the starting inequality by using the additive property of the ordering.

17. Look for some examples.

19. Use a proof by contradiction: assume that \( an < b \) for all \( n \in Z \). Now apply the Well Ordering Principle to the set \( S = \{ b - an \mid n \in Z \} \).

21. Since \( 0 \neq 1 \), we can use the trichotomy property to guarantee that either \( 1 < 0 \) or \( 0 < 1 \). Use a proof by contradiction to show that \( 1 < 0 \) is impossible (this will stem from the fact that \( 1 < 0 \Rightarrow 0 < -1 \)).

23. Let \( xy > 0 \) and suppose that exactly one of them is negative. Show that this causes a contradiction. For the other direction, it is easy to show with the multiplicative property that if \( x, y \) are positive, then \( xy > 0 \). In the case where \( x, y \) are negative, apply the result from Exercise A.3.3: \((−x) \cdot (−y) = x \cdot y\).

25. \( xy = xz \) implies that \( xy - xz = 0 \), which, by Exercise A.3.16, gives \( x(y - z) = 0 \). How can we now use Exercise A.3.24?

27. Just follow the outline given by the proof and make sure you back up every non-assumption with an axiom or a lemma.

Section A.4

1. (a) (Surprise!) Use induction. Clearly, for the base case of \( n = 1 \), we have that 1 is odd. When we use the inductive hypothesis, treat the two possible cases of even or odd separately and show that each will imply the next number in sequence is also either even or odd.

(b) Let \( z \in Z \). If \( z > 0 \), then we can use the above proof. If \( z = 0 \), we easily see that 0 is even. This leaves the only difficult case as \( z < 0 \). Using the properties of order, we know that \( 0 < -z \), so \( -z \) (by the above proof) is either even or odd. What can you show from this?
3. By the definition of “divides”, we know there exists some \( q \in \mathbb{Z} \) such that \( a = dq \). Using the Trichotomy Property, we know \( q > 0 \), \( q = 0 \), or \( q < 0 \). Show that the only possibility is \( q > 0 \). Now use Corollary A.3.8 or Lemma A.3.7.

5. Varies depending on where you look. “Obvious” steps are usually the most commonly unjustified ones, so be careful not to overlook the seemingly simple steps in proofs.

7. (a) To show: there exists no \( x \in \mathbb{Z} \) such that \( 0 < x < 1 \). Well if such an \( x \) were to exist, we would have \( x > 0 \), so \( x \in \mathbb{N} \). Thus it’s enough to show that there exists no \( n \in \mathbb{N} \) such that \( n < 1 \). Use induction. Let the statement \( P(n) \) be that “\( 1 \leq n \)”.

(b) The proof uses only Lemma A.3.7 and the ring axioms.

(c) Let \( S \) be a nonempty subset of \( \mathbb{N} \) and assume that \( S \) does not have a smallest element. Use induction on the statement \( P(n) := \) “\( S \) contains no element \( x \in \mathbb{N} \) such that \( x \leq n \)”.

Using Lemmas A.3.7 and A.3.9 you can show that (with the Principle of Induction) \( P(n) \) is true for all \( n \), and thus \( S \) is empty, which gives the desired contradiction.

9. Let \( P(n) \) be a statement about the natural number \( n \) that satisfies the following hypothesis: “For every natural number \( n \), if \( P(k) \) is true for all natural numbers \( k < n \), then \( P(n) \) is true.” Now create a new statement \( Q(n) \) as follows: “\( P(m) \) is true for all \( m \in \mathbb{N} \) such that \( m < n \)”.

We have that \( Q(1) \) is true because there exists no \( m \in \mathbb{N} \) such that \( m < 1 \), and thus \( Q(1) \) can be trivially asserted as true. Continuing with induction on the statement \( Q(n) \), we can apply Lemma A.3.9 to see that \( Q(k) \) being true implies \( P(k) \) is true as well. And thus if \( P(k) \) is true, we have \( Q(k+1) \) is true as well.