Section 1.2

Theorem 1.5 The statement of the form of the Pythagorean triple is misleading, since, to obtain a Pythagorean point $(a/c, b/c)$ from a Pythagorean triple (a, b, c), we must have $a < b$, but with $a = 2pq$ and $b = q^2 - p^2$, we have $b < a$, given that $p/q > \sqrt{2} - 1$. Also, the last clause should be "where p and q are positive integers with $q > p > (\sqrt{2} - 1)q$."

Exercise 1.19(i) The answer should be $q = 4$, $p = 3$.

Exercise 1.20 This seems very difficult to do without having discussed divisibility carefully.

Exercise 1.22 We need to assume that the point Q is in the first quadrant for (a, b, c) to be a Pythagorean triple.

Exercise 1.23 This is not true. Counter-example: $P = (\frac{3}{5}, \frac{4}{5})$, $a = 21$, $b = 28$, $c = 5$. The point $(\frac{21}{5}, \frac{28}{5})$ is a rational point on the line through P and the origin, but $(21, 28, 5)$ is not a Pythagorean triple.

Theorem 1.9 Near the end of the proof, the sentence beginning with "When we clear denominators ..." should say, "When we clear denominators, we get $a^4 + 2^4c^4 = (ab)^2$, ..."

Theorem 1.11 The phrase "if and only of" should be replaced by "if and only if." Also, the theorem would be clearer if it stated explicitly that the arithmetic sequence is of perfect *rational* squares.

Section 1.3

Corollary 1.20 In the proof of sufficiency, the second sentence begins "Now D is a common divisor, ...". It should say "Now d is a common divisor, ...". Both are true, but it is the fact that d is a common divisor that is used to conclude that $d|D$.

How to Think About It, p 34 After the computation, in the second sentence, in which the gcd, 4, is being written as a linear combination of 124 and 1028, the 0 digit is omitted from 1028.

Exercises 1.51-1.54 These exercises seem to go with Proposition 1.26, so perhaps would be better placed at the end of the first set of exercises for Section 1.3, on page 30.

Exercise 1.64(iv) It seems more natural to ask about lines of the form $ax + by = c$.

Section 1.4

Page 36 The first paragraph of the section suggests that commutative rings are objects satisfying the "nine fundamental properties," when, in fact, commutative rings satisfy only eight of the properties and fields are the objects satisfying all nine.

Exercise 1.75(i) It should perhaps be explicitly stated that a, b, and c are real numbers.

Exercise 1.75(i) The two statements joined by "that is" are not equivalent, but the first implies the second.

Section 2.1

Proposition 2.7 The proof of (i) is faulty; it shows that $a^{m+n} = a^{m+n}$, which is obviously not what is intended. The first three steps of the proof are fine, but it should finish as follows:
$a^{m-1}a^n a \;=\; a^{m-1}aa^n \;=\; a^m a^n$.

Exercise 2.4 Modify to say, "If a is positive and $a \neq 1$, give two proofs that

$$1 + a + a^2 + \ldots + a^n \;=\; \frac{a^{n+1} - 1}{a - 1}$$

by induction on $n \geq 0$ and by multiplying the left-hand expression by $(a - 1)$."

Exercise 2.12(i) Seems to be false as stated. Could modify the problem so that the second condition is, "whenever p is a prime and $p|a$, the highest power of p that divides a is even."

Section 2.2

Lemma 2.23 The formula for $\binom{n}{r}$ should say that $\binom{n}{r} = 1$ if $r = 0$ or $r = n$ (not, as is stated, if $n = 0$ or $n = r$.)

Example 2.27 In the expansion of $(a + b)^4$, the last term should be $+6(ab)^2$, not $-6(ab)^2$. Hence the last term in the expression for $a^4 + b^4$ should be $-6(ab)^2$.

Section 3.1

Exercise 3.2 Given that multiplicative inverses of complex numbers have not been defined, perhaps it is better to restrict to positive integer powers of i.

Exercise 3.3 Given that multiplicative inverses of complex numbers have not been defined, perhaps it is better to restrict to positive integer powers of ω.

Exercise 3.4(v) There is a typesetting error resulting in illegible instructions. The answer should be in terms of b and c.

Section 3.2

Proposition 3.13 This proposition has three parts, labeled (i), (ii), and (iii). The proofs of parts (i) and (ii) are labeled, but there is no label for the proof of (iii). The proof of (ii) ends with "... the shortest distance between its endpoints." And the proof of (iii) is the centered computation beginning with the line $|zw| = \sqrt{(zw)(\overline{zw})}$.

Proposition 3.14 At the end of the proof, it is stated that $\sin\theta = \frac{a}{|z|}$, but it should say that $\sin\theta = \frac{b}{|z|}$.

Corollary 3.19 The imaginary unit is missing in the definitions of z and w. We should have $z = |z|(\cos\alpha + i\sin\alpha)$ and $w = |w|(\cos\beta + i\sin\beta)$.

Exercise 3.23 The imaginary unit is missing from the formula for $z - \bar{z}$. The exercise should say, "If $z \in \mathbb{C}$ show that $z + \bar{z} = 2(\Re z)$ and $z - \bar{z} = 2(\Im z) \cdot i$."

Exercise 3.26 Integer powers of complex numbers have not been defined.

Exercise 3.39 The sentence should begin "Let $n \geq 0$ be an integer ...".

Exercise 3.42 The integer n should be positive, not merely nonnegative. Also, in part (i) of the question, there is unnecessary repitition of the definition of ζ.

Section 3.3

Example 3.31 Only the primitive 8^{th} roots of unity are listed. All the 8^{th} roots of unity are depicted in Figure 3.7.

Theorem 3.32(i) The term ζ is missing from the left-hand side of the equation. The equation should be $1 + \zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{n-1} = 0$. Also, for this to be true, we need $\zeta \neq 1$. The rest of the theorem holds for any nth root of unity ζ, including $\zeta = 1$.

Exercise 3.51 In parts (i) and (ii), the primes p_1 and p_2 should be taken to be distinct. In parts (ii) and (iii) the powers e_i should be taken to be positive. Further in part (iii), the variable n is used to represent two different numbers. It should be modified to say, "Generalize to show that, if $m = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$, then

$$\phi(m) \;=\; m \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right).$$

Section 4.1

Proposition 4.3 The last sentence of the proof should begin, "Finally, $(a - b) + (b - c) = a - c \dots$"

Exercise 4.5 This exercise is formatted incorrectly. It looks like parts (i) and (ii) should be merged.

Section 4.2

Page 151 Near the end of the description of how to find a private key, "Proposition 4.17" is cited. The correct citation is Theorem 4.17.

How to Think About It, p 152 There is a typo in the third expression in the computatation of 4^{103} modulo 13. It should read $4^{103} = 4^{12 \cdot 8 + 7} = \left(4^{12}\right)^8 4^7$. The text has 10 instead of 8.

Section 4.3

Page 154 The second sentence of the last paragraph, which reminds us how addition and multiplication are compatible with congruence, should conclude by saying, "if $a \equiv a' \bmod m$ and $b \equiv b' \bmod m$, then $a + b \equiv a' + b' \bmod m$ and $ab \equiv a'b' \bmod m$."

Exercise 4.35 This exercise appears to be incorrect. It seems to me that distributivity fails.

Theorem 4.43 In the second part of the proof (beginning with "Conversely ...") there is an unfortunate line break. We are taking $m = ab$ where $0 < a, b < m$, i.e. $0 < a < m$ and $0 < b < m$, not merely $0 < a$ and $b < m$.

Proposition 4.46 This proposition is false as stated. For example, the positive integers satisfy the three listed conditions, but they do not form a subring of the integers. The proposition could be corrected by modifying (ii) to say, "if $a, b \in S$, then $a - b \in S$." The proof is also incorrect. It is not true that, having shown that $1 \in S$ and that S is closed under addition and multiplication, all the other items in the definition of a commutative ring are inherited from R. In particular, there is nothing that guarantees that $0 \in S$ or that every element in S has an additive inverse in S.

Exercise 4.58 It is not true that $\{0, 2\} \subset \mathbb{Z}_4$ has the same multiplication table as $\mathbb{Z}_2$, since $2 \cdot 2 = 0 \in \mathbb{Z}_4$. The problem could be modified to say, "(i) Show that $\{0, 3\} \subset \mathbb{Z}_6$ has the same addition and multiplication tables as $\mathbb{Z}_2$. (ii) Is $\mathbb{Z}_2$ a subring of $\mathbb{Z}_6$?"

Section 5.1

Exercise 5.3 The exercise asks us to prove that $\mathbb{Z}_m$ is a domain if and only if $\mathbb{Z}_m$ is a field and to conclude, using Theorem 4.43, that $\mathbb{Z}_m$ is a domain if and only if m is prime. (Presumably we should take $m \geq 2$, so that Theorem 4.43 applies.) That $\mathbb{Z}_m$ is a domain if it is a field follows immediately from Corollary 5.2. To prove the converse, we can prove the contrapositive: if $\mathbb{Z}_m$ is not a field, it is a domain. It is useful to invoke Theorem 4.43, that if $\mathbb{Z}_m$ is not a field, then m is composite. From this it is easy to show that $\mathbb{Z}_m$ is not a domain. However, it is puzzling that the exercise instructs us to use Theorem 4.43 to conclude that $\mathbb{Z}_m$ is a field if and only if m is prime, since Theorem 4.43 was needed to prove that $\mathbb{Z}_m$ is a not domain when it is not a field. (Note also that the claim is true for $m \geq 1$, not just $m \geq 2$, since $\mathbb{Z}_1$ is the zero ring, which is neither a domain nor a field, but the claim is not true for $m = 0$, since $\mathbb{Z}_0$ is isomorphic to $\mathbb{Z}$.)

Section 5.2

Page 196, bottom There is a space missing after the comma in the first sentence after the "How to Think About It" box.

Exercise 5.9 The elements r and s should be in the ring R not $\mathbb{R}$.

Exercise 5.23 The field of rational functions $K(x)$ has not yet been defined. Also, perhaps instead of an equality, it should be an isomorphism.

Exercise 5.28 The formatting is misleading. Only part (i) of this exercise is a true/false question.

Section 5.3

Exercise 5.30 Perhaps it should begin, "Suppose R and S are commutative rings and $\varphi : R \to S$ is a homomorphism." Part (ii) is certainly not true without the assumption that φ is a homomorphism.

Definition of evaluation homomorphism, top of page 215 We should have $e_a(f) = f^{\#}(a)$ not $e_a(f) = f(a)$. Also, while the evaluation homomorphism is defined as a map $e_a : k[x] \to k$ for some field k and some $a \in k$, the restrictions of such maps, for example $\varphi : \mathbb{R}[x] \to \mathbb{C}$ given by $\varphi(f) = f(i)$ are also refered to as "evaluation homomorphisms" throughout the text. Perhaps it should be noted that if k is a subfield of K, then the restriction of $e_a : K[x] \to K$ to $k[x]$ is also a homomorphism.

Example 5.26(iv) The map $\varphi : \mathbb{R}[x] \to \mathbb{C}$ given by $\varphi(f) = f(i)$ is not a particular example of an evaluation homomorphism $e_a : k[x] \to k$ for some field k and some $a \in k$. Rather it is the restriction of one

such, namely $e_i : \mathbb{C}[x] \to \mathbb{C}$. Of course, this restriction is still a homomorphism, but this has not actually been proven or even mentioned.

Exercise 5.43 This exercise appears to be impossible. It asks the students to construct a homomorphism $\mathbb{Z}[i] \to \mathbb{Z}[i]$ having i in its kernel. Any homomorphism having i in its kernel would have to have all of $\mathbb{Z}[i]$ in its kernel, since any i is a unit in $\mathbb{Z}[i]$. So the only possibility is the zero map. However, the definition of homomorphism given on page 207 requires that a homomorphism preserve the identity; therefore the zero map of a nonzero ring cannot be a ring homomorphism.

Exercise 5.44 The map should be $f \mapsto f^{\#}(a)$ not $f \mapsto f(a)$. Further, it will be difficult to prove that the kernel of the map in $\mathbb{Q}[x]$ is the ideal generated by $x^2 - 2$ without the results of Chapter 6. Perhaps the intention is that the students merely conjecture that this is the kernel, reasoning by analogy with the remark at the end of Example 5.27(iv), in which case it would be helpful to clarify the statement of the exercise.

Exercise 5.45 The root of a formal polynomial has not yet been defined. It is defined in Section 6.1, page 239.

Section 6.1

Proposition 6.13 It should perhaps be explicitly stated that m and n are positive integers.

Page 243 The last sentence on this page mentions that gcds are unique in $k[x]$, incorrectly citing Corollary 6.29. The correct citation is Theorem 6.30(ii).

Proposition 6.22 In the proof, the upper bound on the degrees of common divisors could be taken to be $\min\{\deg(a), \deg(b)\}$.

Theorem 6.25 The ideal I consists of multiples of $d(x)$ in $k[x]$, not simply constant multiples of $d(x)$, with constants in k, so the theorem should end by saying $I = (d) = \{rd : r \in k[x]\}$. It would be even clearer if it was written as $I = \big(d(x)\big) = \{r(x)d(x) : r(x) \in k[x]\}$.

Theorem 6.28, Corollary 6.29, and Theorem 6.30 The statement of Theorem 6.28 is true, but the proof given shows only that *there is* a gcd of f and g that is a linear combination of f and g; it does not show that *any* gcd of f and g is a linear combination of f and g. The statements of Corollary 6.29 and Theorem 6.30 are also true, but their proofs rely critically on the fact that *any* gcd of f and g is a linear combination of f and g, which still remains to be shown.

Exercise 6.15 The proof relies on Theorem 6.31 (Euclid's Lemma), which has not yet been stated.

Exercise 6.17 Part (i) relies on the definition of relatively prime and on Corollary 6.32, both of which appear on page 248, after the statement of the exercise. Part (ii) relies on unique prime factorization in $k[x]$, which is not stated until page 252.

Exercise 6.18 This exercise pertains to the Euclidean Algorithm in $k[x]$, which has not yet been discussed.

Exercise 6.23 This exercise relies on the definition of the lcm of two polynomials, which is not given until page 253.

Exercise 6.26 This is false, as stated. One way to correct it would be to add the hypothesis that h is irreducible.

Proposition 6.41 Should the polynomials f and g be taken to be monic?

Example 6.44 The triangle symbol used to indicate the end of the example appears prematurely.

Theorem 6.50 There is an incorrect reference in the proof. The reference should be Propositon 6.49, not Proposition 6.48(iii).

Exercise 6.31(ii) The ascending union of the ideals can be denoted $\bigcup_{n\geq 1} I_n$ or $\bigcup_{n=1}^{\infty} I_n$, but not the way it is currently denoted.

Exercise 6.33 The polynomial $f(x)$ should have a highest term. As denoted, it looks like a formal power series.

Section 6.2

Proposition 6.55 Though called a proposition when stated, it is called a theorem when referenced. See, for example, the three references to "Theorem 6.55" in the paragraphs following the proof.

Page 264 At the beginning of the discussion of roots of unity, the definition for a primitive nth root of unity given in Chapter 3 is referenced and purportedly restated. The stated definition is not, however, the same as the definition given in Chapter 3 (on page 111) though it is equivalent.

Lemma 6.59 The proof of the lemma is incomplete; there is no discussion of how to prove uniqueness of the divisor d. Exercise 6.52 can be cited to complete the proof.

Figure 6.1 The cyclotomic polynomials Φ_5, Φ_7, and Φ_{11} are all missing their linear terms, as is clear from looking at Proposition 6.62.

Section 7.1

Example 7.12(i) The isomorphism from the proof of Theorem 7.11 is referred to as φ, which is misleading because in the proof of Theorem 7.11, φ is the evaluation homomorphism $\mathbb{R}[x] \to \mathbb{C}$ given by $\varphi(f) = f(i)$, and $\widetilde{\varphi}$ is the isomorphism that should be referenced in the example.

Exercise 7.18 The set-up should perhaps be "Let k be a field." There is no mention of the ideal I in parts (i) or (ii) of the exercise, so it seems unnecessary to define it.

Proposition 7.18 The proof refers to "the prime field of K", but this terminology has not been defined. It is defined in Exercise 7.26, which occurs after the proposition.

Section 7.2

Example 7.26 One of the maps in the commutative diagram is mislabeled. The vertical map from $\mathbb{Q}(z) \to \mathbb{Q}(\omega z)$ should be $\theta = \Psi' \circ \Psi^{-1}$. (The prime on the Ψ is missing.)

Example 7.28 At the end of the second paragraph, the cyclotomic polynomial Φ_7 is missing its linear term. It should be $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Exercise 7.36 The end of the hint should say, "... the polynomial p may factor in $F[x]$."

Theorem 7.38 There are three issues with this proof. (1) To show that $g'(x) = -1$ in $K[x]$, we need to show that in K, $1 + \cdots + 1$ (q times) is zero. This is not stated explicitly in Proposition 7.17, but is a consequence of Proposition 7.17(i). (2) To prove that E is a subring of K, it is necessary to show that $1 \in E$, that E is closed under *subtraction*, and that E is closed under multiplication. (See correction of Proposition 4.46.) (3) In proving that E is a subfield of K, it is inappropriate to invoke Lemma 7.37, since in that lemma we assume that we are working in a field with q elements. We show that E is closed under subtraction as follows. Take $a, b \in E$. By Proposition 7.17(ii), $(a-b)^q = (a+(-b))^q = a^q + (-b)^q$. If q is odd, then clearly $(-b)^q = -b^q$, so $(a-b)^q = a^q - b^q$, which implies $g(a-b) = 0$, i.e. $a - b \in E$. If q is even, $q = 2^n$, and $(-b)^q = b^q$, but $-1 = 1$, so $(-b)^q = b^q = -b^q$, implying $a - b \in E$. To prove that E is a subfield of K, take $a \neq 0$ be in E. Since E is a subring of K, it is a domain, and $a^q = a$ implies $a^{q-1} = 1$. Thus $a \cdot a^{q-2} = 1$ in K, i.e. $a^{-1} = a^{q-2}$ in K. Since E is closed under multiplication, this proves $a^{-1} \in E$.

Example 7.41 The third sentence should begin, "By Proposition 7.20, K consists of ...".

Exercise 7.39 Modify to say, "Let $f(x)$, $g(x) \in k[x]$ be *nonconstant* monic polynomials, where k is a field. Show that, if g is irreducible and every root of f (in an appropriate splitting field) is also a root of g, then $f = g^m$ for some integer $m \geq 1$. Hint: Use *strong* induction on $\deg(f)$." (Not $\deg(h)$.)

Exercise 7.43 Should A be taken to be a finite subset of K?

Section 8.1

Exercise 8.3 The Gaussian integer z should be taken to be nonzero.

Exercise 8.4 Again, the Gaussian integer z should be taken to be nonzero. Also, it seems like the question should be asking whether $w - qz$ and $w - zq'$ are associates. Perhaps this is equivalent to asking whether $w/z - q$ and $w/z - q'$ are associates? In any case, we are not interested in whether $w/z - q$ and $w/zz - q'$ are associates, as stated in the exercise.

Section 8.2

Lemma 8.10 The result is not true in this generality! It is true for $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$, but not for $\mathbb{Z}[\zeta_p]$ with p an arbitrary prime. See Corollary 8.49 in Section 8.4.

Example 8.12 The second step of the Euclidean algorithm should be:

$$z = (3-i)(-10+15i) + (-4-7i)$$

The text has $(3+3i)$ instead of z, but this is a mistake.

Exercise 8.8 This exercise references Example 8.12, which has an error, as discussed above.

Section 8.3

Proposition 8.38 There is an unmatched parentheses in the third sentence.

Proposition 8.42 The first sentence of the second paragraph of the proof should say, "It remains to settle the case where $\lambda \not| yz$ ...".

Section 8.4

Further Results Box, bottom of page 363 The second-to-last sentence under the first bullet point should say that q "splits" not that it "spits."

Example 8.52 The very last equation in this example should read $2r - 4t + 10s = 1$.

Exercise 8.47 Perhaps it could be modified as follows, "Referring to Example 8.52, (i) the ideal generated by the norms of *generators of* J_1 is an ideal in $\mathbb{Z}$, and hence principal. Find a generator for it. (ii) Do the same for the other ideals J_2, J_3, and J_4."

Exercise 8.48 There is a sign error. The equality should read: "$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$".

Section 9.3

Exercise 9.1 There is an extra "and" in the second sentence.

Section 9.4

Exercise 9.12(iii) The binary operation should be multiplication, not addition.

Exercise 9.14(i) The first part seems to be an unnecessary repetition of Exercise 9.12(iii).