Section 4.1

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

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 $ab\equiv a'b' \bmod m$."

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 Condition (ii) is stated incorrectly. It should say, "if $a,b\in S$, then $a-b\in S$." The proof is also missing some important steps. Please see the supplemental notes for a complete proof.

Exercise 4.54 Note that M_2 is a subset of the (non-commutative!) ring of 2-by-2 matrices with entries in $\mathbb{R}$. (See the "How to Think About It" box on page 156.) Therefore several properties are inherited from that ring. (Which ones?) In particular, note that commutativity of multiplication must be proven explicitly because it does not hold in the ring of 2-by-2 matrices with entries in $\mathbb{R}$.

Exercise 4.58 Modify (i) to say, "Show that $\{0,3\}\subset\mathbb{Z}_6$ has the same addition and multiplication tables as $\mathbb{Z}_2$." Modify (ii) to say, "Is $\mathbb{Z}_2$ a subring of $\mathbb{Z}_6$?"

Section 5.1

Exercise 5.2 Hint: Use a result proven in this section.

Exercise 5.3 You are asked to prove that $\mathbb{Z}_m$ is a domain if and only if $\mathbb{Z}_m$ is a field. One direction follows immediately from a result in this section. For the other direction, use Theorem 4.43 to prove the contrapositive.

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

Section 5.3

Definition of evaluation homomorphism, top of page 215 We should have $e_a(f) = f^{\#}(a)$ not $e_a(f) = f(a)$.

Exercise 5.45 Although we have not formally defined the root of a polynomial, it is what you think it should be, namely, if f is a polynomial in $R[x]$, then an element $a \in R$ is a root of f if $f^{\#}(a) = 0$.

Section 6.1

Proposition 6.13 To be explicit, in this proposition 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).

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 correct description is: $I = (d) = \{rd : r \in k[x]\}$. 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 is not actually proven in the text. Please see the supplemental notes on Blackboard for proofs of these three results.

Exercise 6.1 Hint: Look back at Exercise 5.14, page 202.

Exercise 6.17 Part (i) relies on the definition of relatively prime and the surrounding discussion, which occur on page 248, after the statement of the exercise.

Exercise 6.23 Just do the first part of this problem, the part about gcds, generalizing Exercise 5.49.

Exercise 6.30 Hint: Aiming for a contradiction, suppose $f(x)$ factors. Then one of its factors is linear, giving a root in $\mathbb{Q}$. Let $\frac{p}{q}$ be the root, where p, q are relatively prime integers. Then $f(\frac{p}{q}) = 0$, i.e. $(\frac{p}{q})^3 + 5(\frac{p}{q})^2 - 10(\frac{p}{q}) + 15 = 0$. Muliply both sides of this equation by q^3 to get an equation in integers. ...

Exercise 6.26 Modify to say, "Let f and g be relatively prime monic polynomials in $k[x]$, where k is a field. If $h \in k[x]$ is a monic irreducible polynomial, and $h^2|fg$, prove that $h^2|f$ or $h^2|g$."

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