Errata and Corrections to *The Arithmetic of Elliptic Curves* 2nd Edition

Joseph H. Silverman

April 2, 2015

Acknowledgements
I would like to thank following people for sending me comments and corrections: Paolo Barozza, Fabrizio Barroero, Agnes Beaudry, Abbey Bourdon, Brandon Carter, Robin Chapman, Zev Chonoles, Kestutis Cesnavicius, Henry Cohn, Maarten Derickx, Xander Faber, S.D. Fordham, Matthias Franz, Alexander Goncharov, Jakob Dawid Huewer, Alan Hertgen, Warren Johnson Jonah Leshin, Sun Chia-Liang, Dino Lorenzini, Rafael von Känel, Tony Feng, Ryan Flynn, Ayhan Gunaydin, Michael Harris, Victor Loh Bo Huai, Enrique Gonzalez Jimenez, Rafael von Kanel, Timo Keller, Chan-Ho Kim, Taekyung Kim, Daniel Krenn, Carl Lian, Bart Litjens, Dino Lorenzini, Lu Hengfei, Michelle Manes, David Masser, Victor Miller, Igor Minevich, Andrea Munaro, Yoshihiro Onishi, Mitchell Owen, Abhishek Parab, Benjamin Peterson, Linda Raabe, Miles Reid, Sietse Ringers, Kazuki Sato, Bettina Schroegmeier, Barak Shani, Dane Skabelund, Kate Stange, Jane Sullivan, Andrew Sutherland, Thom Tyrrell, Nikos Tzanakis, Paul Voutier, Benjamin Weggenmann, Alan (Ka Lun) Wong, Siman Wong, Chris Wuthrich, Leonardo Zapponi, Li Zheng.

Preface (and elsewhere)
The period in the Latin phrase "et al." comes after the "al", not after the "et".

Page xviii, Line 4
"this is turn is easily accomplished" should be "this in turn is easily accomplished".

Page 5, Figure 1.1 and following
During the final production process, all of the figures in the initial print run of the book were unfortunately reproduced using a low resolution method. The

production department at Springer–Verlag and I apologize for this error. It has been corrected in subsequent print runs.

Page 8, Last displayed equation
The exponent on Y should be 3, not 2. (The equation needs to be homogeneous.) Thus it should read

$$V : 3X^3 + 4Y^3 + 5Z^3 = 0.$$

Page 11, First displayed equation in Section I.3
The "f" should be a "ϕ". So it should read

$$\phi : V_1 \longrightarrow V_2, \qquad \phi = [f_0, \ldots, f_n],$$

Page 12, Remark I.3.2
There are two typos. In (i), the polynomial ring should be $\bar{K}[X_0, \ldots, X_m]$, not $\bar{K}[X_0, \ldots, X_n]$. In part (ii), it should say "every", not "very". So it should read:

(i) the $\phi_i(X) \in \bar{K}[X] = \bar{K}[X_0, \ldots, X_m]$ are homogeneous polynomials, not all in $I(V_1)$, having the same degree;

(ii) for every $f \in I(V_2)$,

$$f\big(\phi_0(X), \ldots, \phi_n(X)\big) \in I(V_1).$$

Page 12, Remark I.3.2, Line −1
In part (iii), it should say $\psi_i(P)$, not $\psi(P)$. So it should read

(iii) $\psi_i(P) \neq 0$ for some i.

Page 15, Exercise 1.8(c)
This exercise is not correct. For example, if V is a single point defined over $\mathbb{F}_p$, then Frobenius is an isomorphism of V as a variety. So add the requirement that V be irreducible and of positive dimension.

Page 21, Line 5
The first sentence of the proof of (b) should say $C_2 \subset \mathbb{P}^N$, not say $C_1 \subset \mathbb{P}^N$. So the first sentence should read "Let $C_2 \subset \mathbb{P}^N$, and for each i, let $g_i \in K(C_2)$ be the..."

Page 21, Line −7
In the proof of Corollary 2.4.1, the reference should be to (II.2.4b) not (II.2.5b).

Page 24, Line 6
"(a) Use [111, II.6.9] with $Y = \mathbb{P}^1$ and $D = (0)$, or see..." should be "(a) Use[111, II.6.9] with $Y = C_2$ and $D = (Q)$, or see...."

Page 24, Corollary 2.7
"A map a ..." should be "A map ..."

Page 24, Example 2.9
This example is correct when it says that "ϕ is ramified at the points $[0, 1]$ and $[1, 1]$." These are the points in $\phi^{-1}\big([0, 1]\big)$, so are the only relevant points for illustrating (II.2.6a). However, it is possibly a bit misleading to phrase it in this way, because ϕ has other ramification points. More precisely, it is also ramified at the points $[3/5, 1]$ and $[1, 0]$, which have ramification indices 2 and 5, respectively. Using all four ramification points, we can illustrate the Hurwitz genus formula (II.5.9), which for a self-map of $\mathbb{P}^1$ reads

$$2\deg(\phi) - 2 = \sum_{P\in\mathbb{P}^1} \big(e_\phi(P) - 1\big).$$

So for this example we have

$$2 \cdot 5 - 2 = (3 - 1) + (2 - 1) + (2 - 1) + (5 - 1). \quad \checkmark$$

(However, in the text we can't illustrate Hurwitz' formula in section II.2, since it's not covered until section II.5.)

Page 25, Line 12
"exericse" should be exercise

Page 25, Example 2.10
In both displayed equations, the exponent of X should be 3, not 2. Both equations should be homogeneous of degree 3. So they should read

$$C : Y^2Z = X^3 + aXZ^2 + bZ^3$$

and

$$C^{(q)} : Y^2Z = X^3 + a^qXZ^2 + b^qZ^3.$$

Page 26, Line 9
$P \in K(C)$ should be $P \in C(K)$.

Page 28, Example 3.2
"is principal To see this," missing period after "principal".

Page 37, Line 9
"Let $\omega \in \Omega_C$ be a nonzero differential..." should be "Let $\omega \in \Omega_{C_2}$ be a nonzero differential...". (Add subscript 2 on Ω.)

Page 30, Definition
In the definition of *space of* (*meromorphic*) *differential forms*, it should saythat Ω_C is a $\bar{K}(C)$-vector space, not a $\bar{K}$ vector space. So this definition should read:
Definition. The *space of* (*meromorphic*) *differential forms* on C, denoted by Ω_C, is the $\bar{K}(C)$-vector space generated by symbols of the form dx for $x \in \bar{K}(C)$, subject to the usual relations:

Page 39, Exercise 2.9(c,d)
Add the assumption that a, b, c are pairwise relatively prime. Cassel's survey does not include this condition, but Hurwitz's original paper does.

Page 40, Exercise 2.14(a)
The last coordinate in the map should be x^{g+1}, not x^{g-1}. So it should read

$$[1, x, x^2, \ldots, x^{g+1}, y] : C_0 \longrightarrow \mathbb{P}^{g+2}.$$

Page 40, Exercise 2.15(ii)
"finitely many points$P \in C$" missing space between "points" and "P".

Page 42
The definition of b_2 has a typo, it should read

$$b_2 = a_1^2 + 4a_2.$$

(Note that by weight considerations, the formula for b_2 must have weight 2, so it cannot be a polynomial that involves a_4.)

Page 43, Figure 3.1
The first elliptic curve, with equation $y^2 = x^3 - 3x + 3$, has discriminant -2160, not $+2160$.

Page 45, Proposition 1.4(a)(i)
It should be $\Delta \neq 0$, not $\Delta = 0$. So the full line should read
(i) *It is nonsingular if and only if* $\Delta \neq 0$.

Page 46, Line 11 and Page 47 Line 6
The references to (III.1.2) here and elsewhere should be to Table 3.2. There is no (III.1.2), because in the first edition, that current Table 3.2 was labeled as 1.2.

Page 46, Fifth displayed equation
The formulas for a_6 and a_4 need minus signs (although this doesn't affect the conclusion). So this disply should read

$$a_6 = -f(0,0) = 0, \qquad a_4 = -\frac{\partial f}{\partial x}(0,0) = 0, \qquad a_3 = \frac{\partial f}{\partial y}(0,0) = 0,$$

Page 48, Line −5
$\omega = dy/F_x(x,y)$ should be $\omega = -dy/F_x(x,y)$ (missing minus sign).

Page 52, Part (d) of the proof
"Let the line through P and Q also intersect E at R." should be "Let the line through P and O also intersect E at R."

Page 53, 6'th displayed equation
The leading x on the right-hand side should be c. So this should read

$$F(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3)$$

Page 54, Line −6
The middle of these three displayed equation should have $g(x)$ on the right-hand side, not $f(x)$. It should thus read

$$g(x) + h(x)y = g(x) + h(x)(-y - a_1x - a_3),$$

Page 53, 7'th displayed equation
It should be a_1, not a_a. Thus the line should read

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2.$$

Page 55, 5'th displayed equation
The x-coordinate of $[2]P_2$ should be 137/64, not 127/64. So this line should read

$$[2]P_2 = \left(\frac{137}{64}, -\frac{2651}{512}\right), \qquad P_2 + P_3 = \left(-\frac{8}{9}, -\frac{109}{27}\right).$$

Page 55, Line −3
The discriminant is negative, so it should be "$\Delta = -2^4 3^3 17$".

Page 55, Line −13
It would be better to say that f is chosen in $\bar{K}(C)^*$, rather than in $\bar{K}(C)$.

Page 56, Line 10–12
The conditions on node versus cusp are reversed. This sentence should read: "We recall from (III.1.4a) that if E is singular, then there are two possibilities for the singularity, namely a node or a cusp, determined by whether $c_4 \neq 0$ or $c_4 = 0$, respectively."

Page 57, Third displayed equation
The exponent on $(X - Y)$ should be 3, not 2. Thus it should read

$$E : XYZ - (X - Y)^3 = 0.$$

Page 68, Statement of Proposition 4.2
It might be worth reminding the reader that non-constant means non-constant on $E(\bar{K})$. If K is not algebraically closed, it is, of course, quite possible for $[m]$ to be constant, e.g., if K is a finite field and $m = \#E(K)$.

Page 69, Line 8
Should say that $\mathrm{End}(E)$ has no zero divisors, since generally an integral domain is assumed to be commutative, which $\mathrm{End}(E)$ may not be.

Page 69, Line −11
"If E is strictly larger than $\mathbb{Z}$," should be "If $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$,"

Page 72, Proof of Corollary 4.9
E should be E_1, so it should read
"It is a subgroup of E_1 from (III.4.8), and..."

Page 72, Last Line of Statement of Theorem 4.10(b)
"the automorphism that τ_T induces on $\bar{K}(E_Q)$" should be "the automorphism that τ_T induces on $\bar{K}(E_1)$". (Change E_Q to E_1.)

Page 75, Lines 15-18 (lines following the third displayed equation)
The reference should be to (II.2.6(a)), and it's only necessary that ϕ be unramified at the points in the inverse image of Q. So these lines should read:
However, we also know from (II.2.6(a)) that

$$\#\phi^{-1}(Q) \le \deg\phi = \#\Phi,$$

with equality if and only if ϕ is unramified at all points in the inverse image $\phi^{-1}(Q)$. Since the points $P+T$ are distinct as T ranges over the elements of Φ, we conclude that ϕ is unramified at all points in $\phi^{-1}(Q)$; and since Q was arbitrary, the map ϕ is unramified.

Page 75, Line 20
The reference to the Hurwitz genus formula should be (II.5.9), not (II.2.7).

Page 75, Second displayed equation
There is an extra left parenthesis after the first equals sign. The line should read

$$f\big(\phi(P+T)\big) = (\tau_T^* \circ \phi^*)f\big(P\big) = (\phi^* f)(P) = f\big(\phi(P)\big),$$

Page 75, Fifth displayed equation
There's a 2 missing in front of genus(C). It should read

$$2\,\mathrm{genus}(E) - 2 = (\deg\phi)(2\,\mathrm{genus}(C) - 2).$$

Page 76, Second displayed equation
Both denominators have an extra right parenthesis. This line should read

$$\frac{dx(P+Q)}{2y(P+Q)+a_1x(P+Q)+a_3} = \frac{dx(P)}{2y(P)+a_1x(P)+a_3}.$$

Page 77, Line 7
The final Ω_E should be $\Omega_{E'}$. So this sentence should read "The second is the usual addition in the vector space of differentials $\Omega_{E'}$."

Page 77, Line −10
Reference [41] is quite long. Possibly include the more detailed reference [41, page 213, Corollary 2 and footnote].

Page 77, Line −2
"we can express $\omega(x_3, y_3)$ in terms of $\omega(x_1, y_2)$ and $\omega(x_2, y_2)$" should be "we can express $\omega(x_3, y_3)$ in terms of $\omega(x_1, y_1)$ and $\omega(x_2, y_2)$"

Page 80, Line −6
The first E_1 in this displayed formula should be E_2. So the formula should read

$$\phi^* : \mathrm{Pic}^0(E_2) \longrightarrow \mathrm{Pic}^0(E_1).$$

Page 81, First line of Theorem 6.1
"Let $E_1 \to E_2$ be a nonconstant isogeny of degree m." should be "Let $\phi : E_1 \to E_2$ be a nonconstant isogeny of degree m."

Page 81, Sentence before "Case 1"
Since (II.2.12) only applies to characteristic p, should note that Case 1 is all that's needed for characteristic 0. So maybe replace the sentence "Hence using..." with the following:

If K has characteristic 0, then ϕ is separable, while if K has positive characteristic, then (II.2.12) allows us to write ϕ as the composition of a separable isogeny and a Frobenius morphism. It thus suffices to prove the existence of $\hat{\phi}$ when ϕ is either separable or equal to the Frobenius morphism.

Page 82, Line 9
The reference to (III.4.2c) should be to (II.4.2c).

Page 84, Line 1
The terms "$+\mathrm{div}\big(\psi(x_1, y_1)\big)$" should be "$-\mathrm{div}\big(\psi(x_1, y_1)\big)$". So the entire line should read

$$D = \mathrm{div}\big((\phi+\psi)(x_1, y_1)\big) - \mathrm{div}\big(\phi(x_1, y_1)\big) - \mathrm{div}\big(\psi(x_1, y_1)\big) + (O) \in \mathrm{Div}_{K(x_1,y_1)}(E_2).$$

Page 87, Line −13
"easiesr"

Page 88, Proposition 7.1(b)
The proposition says "As a $\mathbb{Z}_\ell$-module", but then in (b) the prime is p, not ℓ. However, it is an accepted convention that if K has positive characteristic, then that characteristic is p and that ℓ is a prime that is different from the characteristic. So it is best not to change p to ℓ in (b). Instead, maybe easier to just remove the phrase "As a $\mathbb{Z}_\ell$-module", although that phrase was included to stress that the Galois action on the Tate module is not reflected in this isomorphism.

Page 89, Proof of Theorem III.7.4
The idea of extending the degree mapping from M to $M \otimes \mathbb{R}$ may seem mysterious. Or, to quote Frank Thorne's posting on MathOverlow, "When I first saw it, this proof felt like absolute voodoo to me." Here is an edited version of my explanation on MathOverflow for why it is maybe not such an unnatural proof:

How do you prove that the ring of integers in a number field is finitely generated? You embed them in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. How do you prove that the units in a number field are finitely generated? You embed them in a hyperplane in $\mathbb{R}^{r_1+r_2}$. Then you show that your group sits as lattice (a discrete subgroup), and hence it is finitely generated. Further, by looking at the co-volume of the resulting lattice, one obtains important arithmetic invariants, namely the discriminant and the regulator. So the idea of embedding a group into a real or complex vector space and using volume estimates to prove discreteness is a well-established technique. And if one simply has a group and a positive definite quadratic form, as is the case for $\mathrm{End}(E)$ and degree, or for $E(\mathbb{Q})$ and the canonical height, then it is very natural to tensor with $\mathbb{R}$ and extend the quadratic form to put a Euclidean structure on the resulting vector space. (I should mention that I first saw this proof that $\mathrm{End}(E)$ is finitely generated in Mumford's *Abelian Varieties*, but I don't know the origins of the idea.)

Page 92, Theorem III.7.9(a)
The statement doesn't need to specify that $\ell \neq \mathrm{char}(K)$, since K is a number field, so this is automatically true. So it should read:
(a) $\rho_\ell(G_{\bar{K}/K})$ is of finite index in $\mathrm{Aut}\big(T_\ell(E)\big)$ for all primes ℓ.

Page 92, Remark 7.10
The notation $\mathrm{Gal}_{\bar{K}/K}$ should be replaced with $G_{\bar{K}/K}$. This appears twice.

Page 93, Second and third paragraphs of Section III.8
The book says that "Every free module comes equipped with a natural nondegenerate alternating multilinear map, the determinant." In fact, a "nondegenerate alternating multilinear map" is only well-defined up to a choice of basis. Also, there's a typo, since the domain of the determinant map is $E[m] \times E[m]$, not just $E[m]$. So these two paragraphs should read as follows:

As an abstract group, the group of m-torsion points $E[m]$ has the form (III.6.4b)

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Thus $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank two. We can define a nondegenerate alternating multilinear map on $E[m]$ by fixing a basis $\{T_1, T_2\}$ and setting

$$\det : E[m] \times E[m] \longrightarrow \mathbb{Z}/m\mathbb{Z}, \qquad \det(aT_1 + bT_2, cT_1 + dT_2) = ad - bc.$$

However, there are two drawbacks to this approach. First, the value of the determinant depends on the choice of basis. But this is not so bad, since selecting a new basis simply multplies all of the values by an element of $(\mathbb{Z}/m\mathbb{Z})^*$. Second, and more serious, is that this determinant pairing on $E[m]$ is not Galois invariant, i.e., if $P, Q \in E[m]$ and $\sigma \in G_{\bar{K}/K}$, then the values of $\det(P^\sigma, Q^\sigma)$ and $\det(P, Q)^\sigma$ need not be the same.

We can simultaneously achieve basis independence and Galois invariance by using instead a modified pairing taking values in the group of m^{th} roots of unity. In order to define this pairing, we will make frequent use of (III.3.5), which says that a divisor $\sum n_i(P_i)$ is the divisor of a function if and only if both $\sum n_i = 0$ and $\sum [n_i]P_i = O$.

Page 93, Line −11
Saying "let $S \in E[m]$ be another m-torsion point, where we allow $S = T$" could be confusing if the word "another" is interpreted as "different from the other one". In English, this is ambiguous. So maybe replace with:

Now let $S \in E[m]$ also be an m-torsion point, where we allow $S = T$.

Page 93, Line −5
In the displayed formula, the variable should be X, not S. Thus it should read

$$E \longrightarrow \mathbb{P}^1, \qquad X \longmapsto g(X + S)/g(X)$$

Page 93, Third displayed equation
It might be clearer if the divisors being summed were put in parentheses. Thus

$$\operatorname{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} \big((T' + R) - (R)\big).$$

Page 93
Robin Chapman suggests that the definition of the Weil pairing and the proof of its properties might be clearer if the function f were not used. Thus g can be defined as in the text, and then for any $S \in E[m]$, one easily sees that $g(X)$ and $g(X + S)$ have the same divisor, so $g(X + S)/g(X)$ is a constant, which we will call $e_m(S, G)$. Replacing X by $X + [i]S$ for $i = 0, 1, \ldots, m - 1$, we find that

$$e_m(S,T)^m = \prod_{i=0}^{m-1} \frac{g\big(X+[i+1]S\big)}{g\big(X+[i]S\big)} = \frac{g\big(X+[m]S\big)}{g(X)} = 1,$$

which proves that $e_m(S,T)$ is an m^{th}-root of unity. Various parts of the proof of Theorem 8.1 would need to be modified to remove the use of the function f. In most cases, one can just deal with the divisor $m(T)-m(O)$ or $(T)-(O)$.

Page 95, Fourth displayed equation
It might be clearer if the divisors being summed were put in parentheses. Thus

$$\operatorname{div}\left(\prod_{i=0}^{m-1} f\circ\tau_{[i]T}\right) = m\sum_{i=0}^{m-1}\Big(\big([1-i]T\big)-\big([-i]T\big)\Big) = 0.$$

Page 99, Line −11
In the fourth line of the long displayed equation in the middle of the page, the roles of b and c have been reversed. So it should read

$$\begin{aligned} e(v_1,v_2)^{\deg\phi} &= \cdots \\ &= e(av_1+bv_2, cv_1+dv_2) \\ &= \cdots \\ &= e(v_1,v_2)^{\det\phi_\ell}. \end{aligned}$$

Page 104, Chapter III exercises
Victor Miller suggests adding the following exercise, which also appears in *Advanced Topics in the Arithmetic of Elliptic Curves*, Exercise 2.24, page 183.

Let E_1/K and E_2/K be elliptic curves given by Weierstrass equations of the form $y^2=x^3+ax^2+bx+c$, and let $\phi : E_1 \to E_2$ be a nonconstant separable isogeny defined over K. Prove that there is a rational function $f(x)\in K(x)$ and a nonzero constant $c\in K^*$ such that

$$\phi(x) = \big(f(x), cyf'(x)\big),$$

where $f'(x)$ is the formal derivative of $f(x)$ with respect to x.

Pages 105, Exercise 3.7, Line −4
Rather than saying "Verify that ψ_{2m} is a polynomial", it would probably be better to say "Verify that ψ_m is a polynomial", although this is obvious (by induction) for odd m, since the formula for ψ_{2m+1} is a polynomial in earlier ψ_n's. It is only for even m that the formula for ψ_m involves potentially dividing by ψ_2.

Pages 105-106, Exercise 3.7
The last formula on page 105 should have a minus sign, and the $2y$ should be $2(2y+a_1x+a_3)$. Thus

$$2(2y + a_1x + a_3)\omega_m = \psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2.$$

There is a similar problem with y in part (a) on the top of page 106. Thus some of the y's should be $2y + a_1x + a_3$. The corrected exercise is as follows: (a) Prove that if m is odd, then ψ_m, ϕ_m, and $(2y + a_1x + a_3)^{-1}\omega_m$ are polynomials in

$$\mathbb{Z}\big[a_1, \ldots, a_6, x, (2y + a_1x + a_3)^2\big],$$

and similarly for $(2(2y + a_1x + a_3))^{-1}\psi_m$, ϕ_m, and ω_m if m is even. So replacing $(2y + a_1x + a_3)^2$ by $4x^3 + b_2x^2 + 2b_4x + b_6$, we may treat each of these quantities as a polynomial in $\mathbb{Z}[a_1, \ldots, a_6, x]$.

Page 105, Exercise 3.7
The definitions of ϕ_m and ω_m for small m need the values of ψ_m for $m = 0$ and $m = -1$. So either ψ_m needs to be defined for these values, or else the values of ϕ_m and ω_m should be listed for $m = 1$ and $m = 2$.

Page 105, Exercise 3.7(b)
David Masser has suggested an extension of this exercise to compute the coefficients of the second highest terms of $\psi_m^2(x)$ and $\phi_m(x)$. For Weierstrass equations in the short form $y^2 = x^3 + Ax + B$, Masser computes the answer as

$$\psi_m^2(x) = m^2x^{m^2-1} + \frac{m^2(m^2-1)(m^2+6)A}{30}x^{m^2-3} + \cdots,$$
$$\phi_m(x) = x^{m^2} - \frac{m^2(m^2-1)A}{6}x^{m^2-2} + \cdots.$$

Page 107, Exercise 3.10(a)
The displayed equation should map E to $\mathbb{P}^3$, not $\mathbb{P}^2$, and f should be ϕ. So the displayed equation should read

$$\phi : E \longrightarrow \mathbb{P}^3, \qquad \phi = [1, x, y, x^2],$$

Page 109, Exercise 3.16(c)
This exercise is off by an inverse. So it should ask the reader to prove that $\tilde{e}_m = e_m^{-1}$, or equivalently, to prove that $\tilde{e}_m(P, Q) = e_m(Q, P)$, since e_m is alternating.

Page 110, Exercise 3.25(d)
In the formula for $j(E)$, the exponent of $\alpha^3 - 24$ should be 3, not 2. Thus

$$j(E) = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}.$$

Page 110, Exercise 3.26
(a) It is necessary to assume that m is prime. Thom Tyrrell found a counterexample with $m = 15$ over the field $\mathbb{F}_{17^8}$.

(b) It is necessary to assume that $m \ge 3$. For $m = 2$, the point $(0, 0)$ provides a counterexample, since it is fixed by $[i]$. Further, for this part we should assume that $T \in E(K)$, which ensures that $E(K)[m]$ is nonzero.

The last line refers to a map ϕ. It should refer to $[i]$. So the last line should read "The map $[i]$ is an example of a *distortion map*."

Here is how the corrected exercise reads:

3.26. Let E be the elliptic curve $y^2 = x^3 + x$ having complex multiplication by $\mathbb{Z}[i]$, let $m \ge 2$ be an integer, and let $T \in E[m]$ be a point of exact order m. In each of the following situations, prove that $\{T, [i]T\}$ is a basis for $E[m]$, and thus that $e_m\big(T, [i]T\big)$ is a primitive m^{th} root of unity.

(a) m is prime and $m \equiv 3 \pmod 4$.

(b) $m \ge 3$ is prime, K is a field with $i \notin K$, and $T \in E(K)$.

The map $[i]$ is an example of a *distortion map*.

Page 113, Exercise 3.34(a)

There is a subscript W_{n+1} that should be W_{n+2}. Thus the formula should read

$$W_{2n}W_2W_1^2 = W_n(W_{n+2}W_{n-1}^2 - W_{n-2}W_{n+1}^2).$$

This follows immediately from the general formula by substituting $(m, n) \to (n + 2, n - 1)$.

Page 113, Exercise 3.35(b,c)

The Fibonacci sequence is not an elliptic divisibility sequence. However, the sequence $1, 3, 8, 21, 55, 144, 377, 987, \ldots$ consisting of every other term in the Fibonacci sequence, starting with the second term, is an elliptic divisibility sequence. A similar caveat applies to the Lucas sequences described in (c).

Page 116, Line 6

In the fourth line of this displayed equation, there's a missing exponent 3. Thus the first four lines of the display should read as follows (where I've boldfaced the added exponent):

$$\begin{aligned} w &= z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3 \\ &= z^3 + (a_1z + a_2z^2)\big[z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3\big] \\ &\qquad + (a_3 + a_4z)\big[z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3\big]^2 \\ &\qquad + a_6\big[z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3\big]^{\mathbf{3}} \end{aligned}$$

Page 117, Statement of Lemma 1.2

We need $\alpha \in R^*$, not merely that $\alpha \in R$. This is automatic from the assumptions if $\bigcap_{n\ge1} I^n = (0)$, or if I is a maximal ideal, but for simplicity it is cleaner to add the assumption $\alpha \in R^*$ to the statement of the lemma.

Page 119, Line −7
Line −7 should read "the connecting line has equation $w = \lambda z + \nu$." (In the text it says $w = \lambda z - \nu$.)

Page 119, Line −2
The numerator of this displayed equation has an $a_2 y$ that should be $a_2 \nu$. There are also some sign errors due to using $w = \lambda z - \nu$ instead of $w = \lambda z + \nu$. The line should read

$$= -z_1 - z_2 - \frac{a_1\lambda + a_3\lambda^2 + a_2\nu + 2a_4\lambda\nu + 3a_6\lambda^2\nu}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3}$$

Page 120, Third displayed formula
The second line of the formula for $F(z_1, z_2)$ should say $z_1 + z_2$, not $z_1 + z + 2$. Further, the sign error in z_3 noted on page 119 propogates down to cause sign errors in the formula for the formal group law. Thus the full display should read

$$\begin{aligned} F(z_1, z_2) &= i\big(z_3(z_1, z_2)\big) \\ &= z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) \\ &\quad + \big(-2a_3 z_1^3 z_2 + (a_1 a_2 - 3a_3) z_1^2 z_2^2 - 2a_3 z_1 z_2^3\big) + \cdots \\ &\qquad\qquad \in \mathbb{Z}[a_1, \ldots, a_6][\![z_1, z_2]\!]. \end{aligned}$$

Page 122, Second displayed equation
The definition of $f(T)$ should have aT, not at. It should thus read

$$f(T) = aT + (\text{higher-order terms}).$$

Page 122, Line −4
$f(G(t)) = T$ should be $f(G(T)) = T$.

Page 122, Proof of Proposition IV.2.3
Lemma IV.2.4 shows that there exists a power series that is the inverse of $[m]$, but technically one should say a bit more about why the inverse is a homomorphism of the formal group $\mathcal{F}$. This follows from the usual proof for groups. Thus let $f : \mathcal{F} \to \mathcal{F}$ be a homomorphism and let g satisfy $f(g(T)) = g(f(T)) = T$. The assumption that f is a homomorphism says that

$$F\big(f(S), f(T)\big) = f\big(F(S, T)\big).$$

This is a formal identity of power series, so we can set $S = g(U)$ and $T = g(V)$ to obtain

$$F(U, V) = f\big(F\big(g(U), g(V)\big)\big).$$

Now applying g to both sides yields the desired

$$g\big(F(U,V)\big) = F\big(g(U), g(V)\big).$$

Page 124, Line 4
$\tilde{E}(\mathcal{M})$ should be $\hat{E}(\mathcal{M})$ (hat, not tilde). So this line should read:

"In this way, the study of $E(K)$ is reduced to the study of the formal group $\hat{E}(\mathcal{M})$ and the study of an elliptic curve..."

Page 125, First displayed equation
dt should be dT, so this line should read

$$\omega(T) = P(T)\,dT \in R[\![T]\!]\,dT$$

Page 126, Last line of the proof of Corollary VI.4.3
"Comparing coefficients of T on each side gives $a = f'(0)$" should be "Comparing the constant terms on each side of $\omega_{\mathcal{G}} \circ f = a\omega_{\mathcal{F}}$ gives $a = f'(0)$."

Page 126, Statement of Corollary 4.4
"There there are ..." should be "There are...".

Page 128, Second displayed equation
$\log \mathcal{F}(T)$ should be $\log_{\mathcal{F}}(T)$, so this equation should read

$$\log_{\mathcal{F}} F(T,S) = \log_{\mathcal{F}}(T) + C(S)$$

Page 128, Third displayed equation
$F(X,0) = 0$ should be $F(X,0) = X$, so this equation should read

$$F\big(X, F(Y,Z)\big) = F\big(F(X,Y), Z\big), \qquad F(X,0) = X, \qquad F(0,Y) = Y.$$

Page 130, Example 6.1.1
The second line says "If $p \geq 2$", but it should read "If $p \geq 3$".

Page 130, Third displayed equation
The third displayed equation is not centered. It should be aligned with the fourth displayed equation, and thus should look like

$$v(px) \geq v(x^p).$$

Hence

$$v(p) \geq (p-1)v(x).$$

Page 133, Line −1
There is a superfluous end-of-proof marker on this line.

Page 134, Second displayed equation
In the middle term, the exponent $\mathrm{ht}(g)$ should be $p^{\mathrm{ht}(g)}$. So it should read

$$(g \circ f)(T) = g_1\big(f_1(T^{p^{\mathrm{ht}(f)}})^{p^{\mathrm{ht}(g)}}\big) = g_1\big(\tilde{f}_1(T^{p^{\mathrm{ht}(f)+\mathrm{ht}(g)}})\big),$$

Page 135, First line of Exercise 4.3(b)
$[a] : \mathcal{F} \to \mathcal{F}$ should be $[\alpha] : \mathcal{F} \to \mathcal{F}$

Page 135, Exercise 4.6
This exercise is not correct. The problem in adapting the proof of Theorem IV.6.1 is that the formal group has the form

$$[p](T) = pf_1(T) + \pi f_2(T^p) + f_3(T^{p^h}),$$

where π is a uniformizer, so all three terms have to be taken into account. So for example, if $x \in \mathcal{F}(\mathcal{M})$ has exact order p, then one finds that

$$v(x) \le \max\left\{\frac{v(p)}{p^h-1}, \frac{v(p)-1}{p-1}\right\}.$$

There are similar formulas for points of higher p-power order. In general, Serre has noted that the optimal upper bound depends on the the Newton polygon of the series $[p](T)$.

Page 136, New Exercise
Let $\mathcal{F}$ and $\mathcal{G}$ be formal groups over a ring R, and let $\mathrm{Hom}_R(\mathcal{F},\mathcal{G})$ denote the set of formal-group homomorphisms from $\mathcal{F}$ to $\mathcal{G}$.
(a) Define a binary operation $\star$ on $\mathrm{Hom}_R(\mathcal{F},\mathcal{G})$ as follows: for $f_1, f_2, \in \mathrm{Hom}_R(\mathcal{F},\mathcal{G})$, set

$$(f_1 \star f_2)(T) = G(f_1(T), f_2(T)).$$

Prove that $f_1 \star f_2$ is in $\mathrm{Hom}_R(\mathcal{F},\mathcal{G})$, and that $\star$ makes $\mathrm{Hom}_R(\mathcal{F},\mathcal{G})$ into a group.
(b) Let $\mathrm{End}_R(\mathcal{F}) = \mathrm{Hom}_R(\mathcal{F},\mathcal{F})$. Prove that $\mathrm{End}_R(\mathcal{F})$ is a ring, where the $\star$ operation from (a) is "addition" and composition of power series is "multiplication."

Page 136, New Exercise
Prove the following generalization of Lemma IV.2.4. Let R be a ring, let x be an indeterminate, and let $f(T) \in R[x][\![T]\!]$ be a power series with coefficients in the polynomial ring $R[x]$. Suppose further that f has the form

$$f(T) = xT + (\text{higher order terms}).$$

Prove that there is a unique power series $g(T) \in R[x, x^{-1}][\![T]\!]$ such that $f(g(T)) = T$. More precisely, prove that $g(T)$ has the form

$$g(T) = \sum_{n=1}^{\infty} \frac{b_n}{x^{2n-1}} T^n \quad \text{with } b_n \in R[x].$$

Page 137, Line 3
"We start by a proving a theorem of Hasse" should be "We start by proving a theorem of Hasse"

Page 139, Paragraph after Corollary 1.4
The text says that the sum consists of q terms, each of which is ± 1. That's not quite true, since up to $\deg(f)$ of them could be 0, since by definition if $f(x) = 0$, then $\chi\big(f(x)\big) = 0$. This slighly changes the intuition, since the square of a sum of between $q - \deg(f)$ and q random ± 1's will have average value between $q - \deg(f)$ and q. But the conclusion is still the same; one expects that the character sum, on average, will be $O(\sqrt{q})$.

Page 141, Fifth displayed equation
The roots satisfy $|\alpha_{ij}| = q^{i/2}$, not $|\alpha_{ij}| = q^{1/2}$, so this line should read

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T) \quad \text{with} \quad |\alpha_{ij}| = q^{i/2}.$$

Page 141, Line −11
"Then, in 1973, Deligne [60] proved the Riemann hypothesis." The reference [60] is incorrect. The correct reference, which does not appear in the bibliography, is

- P. Deligne, La conjecture de Weil. I, *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307.

Page 145, Line −4
The final deg should be $\deg_s$ (separable degree), so it should read

$$\#E[p^r] = \deg_s\big(\hat{\phi}_r\big) = \deg_s\big(\hat{\phi}\big)^r,$$

Page 147, Line 14
"we have $\psi\big(E[p^r]\big)$ for all..." should be "we have $\psi\big(E[p^r]\big) = 0$ for all..."

Page 147, Line 14
This should read "Since $[p^r] = \hat{\phi}_r \circ \phi_r \ldots$" instead of "Since $[p^r] = \phi_r \circ \hat{\phi}_r \ldots$". (It is true that $[p^r] = \phi_r \circ \hat{\phi}_r$ as a map on $\hat{E}$, but for the subsequent argument, we're looking at $[p^r]$ on E, not on $\hat{E}$.

Page 150, Seventh displayed equation
The exponent $p^2 - 1$ should be $p^r - 1$. It should thus read

$$f(x)^{(p^{r+1}-1)/2} = f(x)^{(p^r-1)/2}\big(f(x)^{(p-1)/2}\big)^{p^r}$$

Page 150, Line −5
(b) should be (c).

Page 151, Fifth displayed equation
The coefficient of $\epsilon_p(0)$ on the right-hand side should be $\frac{2}{3}$, not $\frac{1}{2}$. It should thus read

$$\frac{1}{6}\left(\frac{p-1}{2} - 2\epsilon_p(0) - 3\epsilon_p(1728)\right) + \epsilon_p(0) + \epsilon_p(1728) \\ = \frac{p-1}{12} + \frac{2}{3}\epsilon_p(0) + \frac{1}{2}\epsilon_p(1728).$$

Page 152, Line −9
It should refer to Exercise 5.10, not Exercise 5.1.

Page 152, Line −7
It should say that "there are exactly 27 odd primes $p < 31500$ for which E is supersingular." (Note the addition of the word "odd". It turns out that 2 is also supersingular, since $a_2 = -2 \equiv 0 \pmod 2$.)

Page 152, Last sentence
The book says that "For simplicity we state everything over $\mathbb{Q}$, but suitable versions apply over any number field." This is somewhat misleading. Theorem 4.7 is true, mutatis mutandis, over number fields. The same holds for Conjectures 4.8 and Theorem 4.9 over number fields that have at least one real embedding. But for totally imaginary fields, the form of Conjecture 4.8 is somewhat different, and Theorem 4.9 is not known in general. So for (many) totally imaginary fields, Theorem 4.9 is still a conjecture.

Page 153, Exercise 5.2
There is a sign error in the exponent of q. The displayed function should read

$$q^{-\epsilon s/2} Z(V/\mathbb{F}_q; q^{-s}).$$

Page 158, Section VI.1
The text mentions that α and β generate the first homology group, but the notation $H_1(E, \mathbb{C})$ is not used. Then there is no mention of homology until Proposition 5.2, where the notation $H_1(E, \mathbb{C})$ is used without explanation. It might be helpful to explicitly say in Section 1 that $H_1(E, \mathbb{C})$ is the first homology, and also put an entry of $H_1(E, \mathbb{C})$ into the list of notation.

Page 158, First displayed equation
The Y should be lower case. So the displayed equation should read

$$y^2 = x(x-1)(x-\lambda).$$

Page 165, Last displayed equation
The denominator of the final upper bound should be $|\omega|^3$, not $|\omega|^2$. Note that we need an exponent strictly larger than 2 in order to apply (a). Here is a more complete derivation:

$$\begin{aligned}
\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| &= \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| \\
&\leq \frac{|z|\big(2|\omega| + |z|\big)}{|\omega|^2\big(|\omega| - |z|\big)^2} \\
&= \frac{|z|}{|\omega|^3} \cdot \frac{2|\omega| + |z|}{|\omega| - |z|} \cdot \frac{|\omega|}{|\omega| - |z|} \\
&= \frac{|z|}{|\omega|^3} \cdot \frac{2 + \frac{|z|}{|\omega|}}{1 - \frac{|z|}{|\omega|}} \cdot \frac{1}{1 - \frac{|z|}{|\omega|}} \\
&= \frac{|z|}{|\omega|^3} \cdot \left(2 + \frac{3}{\frac{|\omega|}{|z|} - 1}\right) \cdot \frac{1}{1 - \frac{|z|}{|\omega|}} \\
&\leq \frac{10|z|}{|\omega|^3},
\end{aligned}$$

where the last line is immediate from the assumption that $\frac{|z|}{|\omega|} < \frac{1}{2}$.

Page 166, First displayed equation
The exponent on $z - \omega$ should be 3, not 2. Thus this formula should read

$$\wp'(z) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}.$$

Page 166, Last two displayed equations
In both of these equations, it should be $(-1)^i$, not $(-1)^{i-1}$. Thus they should read

$$f^{(i)}(z) = (-1)^i f^{(i)}(-z).$$

and

$$f^{(i)}(w) = f^{(i)}(-w) = (-1)^i f^{(i)}(w).$$

Page 168, Third displayed equation
In the sum, the two minus signs should be plus signs. It should thus read

$$\log\sigma(z) = \log z + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left\{\log\left(1 - \frac{z}{\omega}\right) + \frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2\right\},$$

Page 170, First three displayed equations
The exponent of x in the first and third displayed equations should be 3, not 2. So these displayed equations should read

$$f(x) = 4x^3 - g_2x - g_3$$

and

$$E : y^2 = 4x^3 - g_2x - g_3.$$

And the exponent of g_3 in the second displayed equation should be 2, not 3, so it should read

$$\Delta(\Lambda) = g_2^3 - 27g_3^2.$$

Page 171, First displayed equation
It should be dx/y, not dx/dy, so it should read

$$\phi^*\left(\frac{dx}{y}\right) = \frac{d\wp(z)}{\wp'(z)} = dz$$

Page 171, Third displayed equation
Two of the plus signs should be minus signs, so it should read

$$\operatorname{div}(F) = \big(\phi(z_1 + z_2)\big) - \big(\phi(z_1)\big) - \big(\phi(z_2)\big) + \big(\phi(0)\big).$$

Page 173, Theorem 5.1
$4A^3 - 27B^2$ should be $A^3 - 27B^2$.

Page 174, Line 15
There's a missing subscript 1 on Λ. It should say:
"We observe that $H_1(\mathbb{C}/\Lambda_1, \mathbb{Z})$ is naturally…".

Page 175, Second paragraph
Possibly it would be worth noting that since we're given an inclusion $K \subset \mathbb{C}$, we can use this inclusion to fix a specific choice of algebraic closure of K, namely

$$\bar{K} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } K\}.$$

Alternatively, there's really no need to talk about $\bar{K}$ at all. It's enough to note, for example, that the points in $E[m]$ have coordinates that are algebraic over K, that $K \subset \mathbb{C}$ by assumption, and that $\mathbb{C}$ is algebraically closed, hence $E[m] = E(\mathbb{C})[m]$.

Page 176, Line 6–8
There is an inconsistant usage of ω_2/ω_1 versus ω_1/ω_2. Further, the lattice should be multiplied by $1/\omega_1$ (or $1/\omega_2$), not by the ratio of the periods. So these lines should read:

(ii) *The field* $\mathbb{Q}(\omega_2/\omega_1)$ *is an imaginary quadratic extension of* $\mathbb{Q}$*, and* $\mathrm{End}(E)$ *is isomorphic to an order in* $\mathbb{Q}(\omega_2/\omega_1)$*.*
PROOF. Let $\tau = \omega_2/\omega_1$. Multiplying Λ by $1/\omega_1$ shows that Λ is homothetic to $\mathbb{Z} + \mathbb{Z}\tau$,...

Page 176, Fourth displayed equation
The coefficient fo τ should be $+(a-d)$, not $-(a-d)$, so this line should read

$$b\tau^2 + (a-d)\tau - c = 0.$$

Page 178, Exercises for Chatper VI
New exercise suggested by David Masser: Show that the eight numbers

$$\zeta(\omega/3) - \frac{1}{3}\eta(\omega) \quad \text{with } \omega \in \Lambda \smallsetminus 3\Lambda$$

are the roots of the polynomial

$$3888T^8 - 216g_2\Delta T^4 - 144g_3T^2 - g_2^2.$$

Compute the corresponding polynomial for

$$\zeta(\omega/4) - \frac{1}{4}\eta(\omega) \quad \text{with } \omega \in \Lambda \smallsetminus 4\Lambda$$

(These numbers are associated with the points of order 3 and 4 on the non-trivial extension of an elliptic curve by the additive group. See Paula Cohen's paper for the fact that the heights of such points are not bounded.)

Page 182, Exercise 6.14
The recursion for b_n should read $b_{n+1} = \sqrt{a_n b_n}$, not $b_n = \sqrt{a_n b_n}$.

Page 183, Exercise 6.14(f)
The $M\big(\sqrt{2},1\big)$ should be in the denominator. So the displayed formula should read

$$\int_0^1 \frac{dz}{\sqrt{1-z^4}} = \frac{\pi}{2M\big(\sqrt{2},1\big)}.$$

Page 188, Proposition VII.2.1
For an alternative proof that the reduction map $E_0(K) \to \tilde{E}_{ns}(k)$ is a homomorphism, see Appendix A §5 of *Rational Points on Elliptic Curves*, J.H. Silverman and J. Tate, Springer, 1992.

Page 190, Last line of proof of lemma
It should read $(\partial\tilde{f}/\partial y)(\tilde{P}) \neq 0$ instead of $(\partial\tilde{f})(\partial y)(\tilde{P}) \neq 0$. So the full line should read:
lemma when $\tilde{P} \neq \tilde{O}$ and $(\partial\tilde{f}/\partial y)(\tilde{P}) \neq 0$. The other cases are proven similarly.

Page 191, Line 7
$R[\![x]\!]$ should be $R[\![z]\!]$, so this line should read: "let $w(z) \in R[\![z]\!]$ be the power series…".

Page 191, Line −15
$\tilde{E}$ should be $\hat{E}$, so this line should read: "Further, in deriving the power series giving the group law on $\hat{E}$, we simply…".

Page 193, Example 3.3.3, Third displayed equation
The fourth point in $E(\mathbb{F}_5)$ should be $(3,0)$, not $(2,0)$. So it should read

$$\tilde{E}(\mathbb{F}_5) = \big\{O, (0,0), (2,0), (3,0)\big\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Page 197, Line 6
This line should read "the curve E_2 has multiplicative reduction…". (The text says E_3.)

Page 198, Line 14
This line should read "giving a minimal Weierstrass equation for E over K'.) (The text says "over K", but the field should be K'.)

Page 200, Line −10
"We know from (VIII.2.2)" should be "We know from (VII.2.2)"

Page 200, Line −8
The inclusions on the displayed equation are backwards. Further, the third entry should be $\mathcal{M}^3$, not $\mathcal{M}^2$. So this line should read

$$\hat{E}(\mathcal{M}) \supset \hat{E}(\mathcal{M}^2) \supset \hat{E}(\mathcal{M}^3).$$

Page 201, Theorem 7.1(a)
It should read "E has good reduction" or "E has good reduction at v."

Page 201, Line 2 of the proof
"implications(b) $\Rightarrow$ …", there should be a space between "implications" and "(b)".

Page 203, Exercise 7.3
The hint should be "See (VII.3.5)", not (VIII.3.5).

Page 209, Line 2
$E[L]$ should be $E(L)$ (parentheses, not brackets), so this line should read: "Suppose that $P, P' \in E(K) \cap mE(L)$ satisfy $\lambda_P = \lambda_{P'}$. Then…".

Page 210, Line 3
The (d) should be set in upright font.

Page 210, Fifth display
There is a minus sign that should be a plus sign in chain of equalities. It should read

$$\kappa(P,\sigma\tau) = Q^{\sigma\tau} - Q = (Q^{\sigma} - Q)^{\tau} + (Q^{\tau} - Q) = \kappa(P,\sigma)^{\tau} + \kappa(P,\tau).$$

Page 214, Line 20
(VIII.2.1) should be (VIII.1.2).

Page 219, Line −8
The formula in front of the $(C_1' + C_2)$ is wrong, and in fact, it goes to infinity as n goes to infinity. This line should read as follows:

$$h(P_n) \le \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2}\left(1 + \frac{2}{m^2} + \left(\frac{2}{m^2}\right)^2 + \cdots + \left(\frac{2}{m^2}\right)^{n-1}\right)(C_1' + C_2)$$

Page 221, Fifth displayed equation
The second P should be P_0¡ so this line should read

$$P = (x,y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \qquad \text{and} \qquad P_0 = (x_0,y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right),$$

Page 222, Line −1
The term $13A63$ should be $13A^3$. So the full expression for g_2 is:

$$g_2(X,Z) = A^2bX^2 + A(5A^3 + 32B^2)X^2Z + 2B(13A^3 + 96B^2)XZ^2 - 3A^2(A^3 + 8B^2)Z^3.$$

Page 222–223, Sublemma VIII.4.3
Miles Reid has pointed out that there are simpler formulas that yield ΔX^6 and ΔZ^6, instead of ΔX^7 and ΔZ^7. With different notation than that in the book, here is Reid's derivation:

Let $g(x) = x^3 + ax + b$ and $g_1 = 3x^2 + a = \frac{\mathrm{d}g}{\mathrm{d}x}$. Calculate successively $g_2 = 3g - xg_1$, $g_3 = 3xg_2 - 2ag_1$ and $g_4 = 9bg_2 - 2ag_3$. If you're lucky, you should get $g_4 = 27b^2 + 4a^3 = -\Delta$. Work backwards through the calculation to deduce that

$$Ag + Bg_1 = -\Delta, \quad \text{where} \quad A = -18ax + 27b, \quad B = 6ax^2 - 9bx + 4a^2. \quad (1)$$

Now observe that in turn $B = -9xg + (3x^2 + 4a)g_1$. We can use this to get a simple derivation of $-\Delta$ as a combination of $f = g_1^2 - 8xg$:

$$-\Delta = (3x^2 + 4a)(g_1^2 - 8xg) + (-3x^3 + 5ax + 27b)g. \tag{2}$$

Verify the identity

$$\begin{aligned} -x^6\Delta = &\Big((a^3 + 3b^2)x^2 - a^2bx - 2ab^2\Big)f \\ &+\Big((3a^3 + 24b^2)x^3 + a^2bx^2 - (16ab^2 + a^4)x + 2a^3b\Big)g. \end{aligned} \tag{3}$$

(This can also be derived by the same kind of reasoning.)

The point of the question is to get $-\Delta q^6 = R(p,q)F(p,q) + S(p,q)G(p,q)$ and $-\Delta p^6 = R'(p,q)F(p,q) + S'(p,q)G(p,q)$. This kind of identity (with $6 \mapsto 7$) is used to bound the cancellation that can happen in $x(2P) = F(p,q)/G(p,q)$. Textbooks give a bigger formula for $-\Delta q^7$, with a much nastier derivation (e.g., [Knapp], p. 96).

Page 226, Proposition 5.4(c)
In the displayed equation, the exponent on H_K should be the degree $[L:K]$, not $[K:\mathbb{Q}]$, nor its reciprocal $1/[K:\mathbb{Q}]$. So it should read

$$H_L(P) = H_K(P)^{[L:K]}.$$

Page 227, Line −11
$\bar{\mathbb{Q}}^N$ should be $\bar{\mathbb{Q}}^{N+1}$, so this line should read: "having no common zero in $\bar{\mathbb{Q}}^{N+1}$ other than $X_0 = \cdots = X_N = 0$."

Page 229, Line −1
$|P|^{d-e}$ should be $|P|_v^{d-e}$ (missing subscript v), so this line should read: "multiplying by $|P|_v^{d-e}$ gives…".

Page 230, Line 1
The subscript on C should be 4, not v, so this equation should read:

$$|P|_v^d \le C_4^{\epsilon(v)} |G|_v \big|F(P)\big|_v,$$

Page 233, Line −2
"has a most" should be "has at most", so the full phrase should read "Since each polynomial $f_x(T)$ has at most d roots in K…"

Page 233, Fifth displayed equation
The first upper bound should be C^d, but then some mention should be made in the following line that we are replacing C^d by C. Here is the replacement text:

Thus if $H(P) \le C$ and $\big[\mathbb{Q}(P):\mathbb{Q}\big] \le d$, then

$$\max_{0\le i\le N} H_{\mathbb{Q}(P)}(x_i) \le C^d \qquad \text{and} \qquad \max_{0\le i\le N} \big[\mathbb{Q}(x_i):\mathbb{Q}\big] \le d.$$

It thus suffices to prove that the set

$$\big\{x \in \bar{\mathbb{Q}} : H(x) \le C \text{ and } \big[\mathbb{Q}(x) : \mathbb{Q}\big] \le d\big\}$$

is finite. In other words, we have reduced to the case that $N = 1$. (Since C and d are fixed, for notational convenience we've replaced C^d by C.)

Page 234, Line 2
D should be d, so this line should read: "in terms of C and d".

Page 237, Line −4
Lemma (VIII.6.2) should be lemma (VIII.6.3), so this should read: "we prove in the next lemma (VIII.6.3) that. . . ".

Page 239, Remark 6.6
"interprest" should be "interpret".

Page 251, Line −7
The reference [143, Chapter XIV, §§3,7] should be [143, Chapter XV, §§3,7].

Page 256, middle of the page
The upper bounds on f_2 and f_3 are incorrect. This sentence should read "For $p = 2$ or 3, if E has additive reduction, then $f_p(E)$ may be greater than 2, but in any case it always satisfies $f_3(E) \le 5$ and $f_2(E) \le 8$."

Page 259, Proof of Proposition 11.5(a)
"Szpiro's conjecture" should be "ABC conjecture, so this sentence should read:

"Let A, B, C be as in the statement of the ABC conjecture."

Page 259, Proof of Proposition 11.5(b)
The book says to take $C = \Delta$, but we really need to take $C = 1728\Delta$. That's okay, because the assumption that $\gcd(c_4, c_6) = 1$ and the equation $1728\Delta = c_4^3 - c_6^2$ imply that $\gcd(1728\Delta, c_4^3, c_6^2) = 1$, so it's okay to take $C = 1728\Delta$ when applying the ABC conjecture. This means that every appearance of Δ on the top half of page 260 must be replaced by 1728Δ.

Page 262, Exercise 8.7(a)
In the displayed equation, it should be $\mathbb{P}^N(\bar{\mathbb{Q}})$, not $\mathbb{P}^N(\mathbb{Q})$. So it should read

$$\big\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : H(P) \le C \text{ and } \big[\mathbb{Q}(P) : \mathbb{Q}\big] \le d\big\}.$$

Page 264, Exercise 8.14(a)
The integral idea $\mathfrak{a}$ should be in the *inverse* of the ideal class $\bar{\mathfrak{a}}_{E/K}$, i.e., $\mathfrak{a} \in \bar{\mathfrak{a}}_{E/K}^{-1}$.

Page 266, Exercise 8.19
The displayed equation defining $L_E(s)$ should have p^{-s}, not p^{-2}. So the definition should read

$$L_E(s) = \prod_{p|\Delta(E)} (1 - t_p p^{-s})^{-1} \prod_{p\nmid\Delta(E)} (1 - t_p p^{-s} + p^{1-2s})^{-1}.$$

Page 270, Line −5
The reference should be [108, Theorem 194], not [108, Theorem 195].

Page 271, Line 1
Should first point out that the proposition is trivial if $\alpha \in \mathbb{C} \smallsetminus \mathbb{R}$. We can simply take $C = \mathrm{Im}(\alpha)$, since for any $r \in \mathbb{R}$ we have $|r - \alpha| \geq \mathrm{Im}(\alpha)$. So it suffices to prove the proposition for $\alpha \in \mathbb{R}$.

Page 271, Line 6
Given the choice of C_1, this inequality is only valid for $|t - \alpha| \leq 1$. The other values are dealt with in the choice of C, but this should probably be explained more carefully.

Page 274, Second displayed equation
In the first line, the denominator of the left-hand side should be $d_v(P, Q)$, not $d_v(P, t_Q)$. In the second line, the factor of $1/e$ inside the limit should be not be there. So this displayed equation should read

$$\begin{aligned}\lim_{\substack{P\in C(K_v)\\ P\xrightarrow{v}Q}} \frac{\log\bigl|F(P)\bigr|_v}{\log d_v(P,Q)} &= \lim_{\substack{P\in C(K_v)\\ P\xrightarrow{v}Q}} \frac{\log\bigl|F(P)\bigr|_v}{\log\bigl|t_Q(P)\bigr|_v^{1/e}} \\ &= f + \lim_{\substack{P\in C(K_v)\\ P\xrightarrow{v}Q}} \frac{\log\bigl|\phi(P)\bigr|_v}{\log\bigl|t_Q(P)\bigr|_v} \\ &= f.\end{aligned}$$

Page 275, First displayed equation
Both $e_\phi(P)$'s should be $e_\phi(Q)$'s. So it should read'

$$\mathrm{ord}_Q\, t_{\phi(Q)} \circ \phi = e_\phi(Q)\, \mathrm{ord}_{\phi(Q)}\, t_{\phi(Q)} = e_\phi(Q) e_2,$$

Page 275, Line −4
There should be a log in the denominator of the fraction. So this displayed should read

$$\liminf_{\substack{P\in C(K)\\ P\xrightarrow{v}Q}} \frac{\log\bigl|f(P) - f(Q)\bigr|_v}{\log d_v(P,Q)} = e.$$

Page 276, Theorem 3.1
The theorem refers to "a nonconstant even function $f \in E(K)$." This should read "a nonconstant even function $f \in K(E)$."

Page 277, Line 2
This should be $d_v(P_i, O) \to 0$, not $d_v(P_i, O) \to \infty$.

Page 279, Second displayed equation
The distances should have logs, so this equation should read

$$\log \min\bigl\{\bigl|x(P)\bigr|_v, 1\bigr\} = \log d_v(P, Q_1) + \log d_v(P, Q_2) + O(1) \quad \text{for all } P \in E(K_v),$$

Page 279, Line 7
A reader asked why is is necessary to use (IX.3.1) in order to prove that the limit

$$\lim_{i\to\infty} \frac{\min\bigl\{\log|a_i/b_i|, 0\bigr\}}{\max\bigl\{\log|a_i|, \log|b_i|\bigr\}}$$

is 0, since the numerator is bounded. The point here is that although the numerator is obviously bounded above, it is not bounded below. Indeed, if a subsequence of the a_i/b_i approaches 0, then the numerator goes to $-\infty$, so it is not bounded below.

Page 279, Third displayed equation
In the second line, the distances should have logs. So this full display should read

$$\begin{aligned}
\lim_{i\to\infty} \frac{\min\bigl\{\log|a_i/b_i|, 0\bigr\}}{\max\bigl\{\log|a_i|, \log|b_i|\bigr\}} &= \lim_{i\to\infty} \frac{\log \min\bigl\{\bigl|x(P_i)\bigr|, 1\bigr\}}{h_x(P_i)} \\
&= \lim_{i\to\infty} \frac{\log d_v(P_i, Q_1) + \log d_v(P_i, Q_2) + O(1)}{h_x(P_i)} \\
&= 0.
\end{aligned}$$

Page 280, Line 8
(VIII.8.4) and (VIII.8.6) should be (VIII.11.4) and (VIII.11.6).

Page 280, Third displayed equation
On the left-hand side, there's a missing v subscript that has caused a parenthesis subscript. The line should read

$$\lim_{i\to\infty} \frac{\log d_v(P_i, Q)}{h_f(P_i)} = L = \liminf_{\substack{P\in E(K)\\ h_f(P)\to\infty}} \frac{\log d_v(P, Q)}{h_f(P)}.$$

Page 280, Line −6
P_i should be P_i', so this line should read: "where $P_i', R \in E(K)$ and where R does not depend on i."

Page 280, End of Line 5
Q should be Q', so it should read: "we can find a point $Q' \in E(\bar{K})$ satisfying…".

Page 283, Fourth displayed equation
Missing v subscript on first absolute value, so should read:

$$\left|\frac{X}{Y} - \gamma\right|_v \le \frac{C_1}{|Y|_v^m}.$$

Page 284, First and second displayed equations
The formulas for the point and the curve are not correct. Also, since the curve E uses x and y as its coordinate functions, it would be better to use X and Y for the curve containing the S-integral points. So this material should read:

The relation $\Delta = -16(4A^3 + 27B^2)$ implies that for each i, the point

$$\left(-\frac{12A_i}{D_i^4}, \frac{108B_i}{D_i^6}\right)$$

is an S-integral point on the elliptic curve

$$Y^2 = X^3 - 27C.$$

Page 300, Line 1
The curve is not supersingular, it is anomalous.

Page 300, Line −7
"such at the one" should be "such as the one"

Page 302, Line 9
$\mathbb{Q}(\alpha)$ should be $K(\alpha)$.

Page 307, Exercise 9.16, Second displayed equation
All of the distance functions should have logs. So this line should read

$$\log\min\bigl\{\bigl|f(P)\bigr|_v, 1\bigr\} = n_1 \log d_v(P, Q_1) + \cdots + n_r \log d_v(P, Q_r) + O(1) \quad \text{for all } P \in C(K_v),$$

Page 313, Line 4
$L\bigl([m]^{-1}E(K)\bigr)$ should be $K\bigl([m]^{-1}E(K)\bigr)$.

Page 317, Line 4
The third point in $E(\mathbb{Q})$ should be $(10/9, 80/27)$, not $(10/9, -80/27)$.

Page 319, Line 19
"The proves that" should be "This proves that"

Page 320, Line 11
"we consider the subfield field..." should be "we consider the subfield...".

Page 325, First line of second displayed equation
The minus signs in front of $(p-q)$ and $(q-p)$ should be plus signs. Thus this should read

$$\begin{aligned}\theta(q)-\theta(p) &= \Big(\big(\theta(q)+(p-q)\big)-\theta(p)\Big)+(q-p)\\ &= \Big(\theta\big(q+(p-q)\big)-\theta(p)\Big)+(q-p)\\ &= q-p.\end{aligned}$$

Page 325, Second to last display (Line −6)
Two of the minus signs should be plus signs. It should read:

$$p_0^{\sigma\tau}-p_0=(p_0^{\sigma\tau}-p_0^{\tau})+(p_0^{\tau}-p_0)=(p_0^{\sigma}-p_0)^{\tau}+(p_0^{\tau}-p_0).$$

Page 326, Second displayed equation
The first minus sign should be a plus sign. It should read:

$$\theta : C \longrightarrow C', \qquad \theta(p)=p_0'+(p-p_0)+P_0.$$

Page 326, Line 18
"cohomology group" should be "cohomology set"

Page 333, Line 19
$I_v \in G_v$ should be $I_v \subset G_v$.

Page 333, Line −8
In this displayed formula, G_v should be I_v, so it should read:

$$\xi_\sigma = \{P^\sigma - P\} = 0 \qquad \text{for all } \sigma \in I_v.$$

Page 335, Line 7
The exponent should be 3, not 2, because the rank is 1 and all of the 2-torsion is rational. So the line should read

$$S^{(2)}(E/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^3 \qquad \text{and} \qquad Ш(E/\mathbb{Q})[2] = 0.$$

Page 337, Proposition X.4.9, First displayed equation
The formula for E' should use an upper case X, and it's missing a 4. So this line should read

$$E : y^2 = x^3 + ax^2 + bx \qquad \text{and} \qquad E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X,$$

Page 345, Line 7
The discriminant of E should be $\Delta(E) = -64D^3$, not $-4D^3$.

Page 360, Exercise 10.19(d)
The conditions for $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ are reversed. Thus if $D = d^3 \neq 1$ is a cube, then

$$E(\mathbb{Q})_{\text{tors}} = \big\{\mathcal{O}, (-d, 0)\big\} \cong \mathbb{Z}/2\mathbb{Z},$$

and if $D = d^2 \neq 0$ is a square, then

$$E(\mathbb{Q})_{\text{tors}} = \big\{\mathcal{O}, (0, d), (0, -d)\big\} \cong \mathbb{Z}/3\mathbb{Z}.$$

Finally, if $D = -432$, then

$$E(\mathbb{Q})_{\text{tors}} = \big\{\mathcal{O}, (12, 36), (12, -36)\big\} \cong \mathbb{Z}/3\mathbb{Z}.$$

Page 356, Line 2
"automorphism" is misspelled.

Page 372, Second paragraph
If q is a prime power, but not prime, then should explain what is meant by the Legendre symbol. If is defined as follows: $\left(\frac{c}{q}\right) = 1$ if c is a non-zero square in $\mathbb{F}_q$, $\left(\frac{c}{q}\right) = -1$ if c is not a square in $\mathbb{F}_q$, and $\left(\frac{c}{q}\right) = 0$ if $c = 0$.

Page 372, Third displayed formula
There is a minus sign missing, the formula should read

$$a_q = -\sum_{x \in \mathbb{F}_q} \left(\frac{f(x)}{q}\right).$$

Page 372, Line −8
"In particular, if $P \in E(\mathbb{F}_q)[\ell]$" should be "In particular, if $P \in E(\bar{\mathbb{F}}_q)[\ell]$"

Page 373, Line 10
"This division polynomial has degree $\frac{1}{2}(\ell^2 - 1)$" should specify that $\ell \nmid q$. It might also be helpful to remind the reader tha under the assumption that $\ell \nmid q$, the group $E(\bar{\mathbb{F}}_q)[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ (Corollary III.6.4).

Page 373–374, Step (4) of Schoof's algorithm
The computation of $(x^{q^2}, y^{q^2}) + [q](x, y)$ requires doing divisions in the ring R_ℓ. This is not necessarily straightforward. Schoof [223] devotes 2+ pages to the issue. Here is a shorter, although possibly slower, solution shown to me by Matthias Franz.

To ease notation, let $(A_1, B_1) = (x^{q^2}, y^{q^2})$ and $(A_2, B_2) = [q](x, y)$, and let $E[\ell]^* = E[\ell] \smallsetminus \{O\}$. If $A_1 \neq A_2$, this means that $A_1(P) \neq A_2(P)$ for some $P \in E[\ell]^*$, but this does not guarantee that $A_2 - a_1$ is invertible in R_ℓ, because one might have $A_1(Q) = A_2(Q)$ for some other $Q \in E[\ell]^*$.

First, an element $A \in R_\ell$ is zero if and only if $A(P) = 0$ for all $P \in E[\ell]^*$, because $\bar{\mathbb{F}}_q \otimes_{\mathbb{F}_q} R_\ell$ is the coordinate ring fo the affine variety $E[\ell]^*$. (We assume that $\ell \nmid q$.) Second, the identity

$$[n]\tau(P) = t^2(P) + [q]P \qquad (*)$$

holds for some $P \in E[\ell]^*$ if and only if it holds for all points in $E[\ell]^*$, because these points have prime order. Now let $A = A_2 - A_1$ and invert A formally, i.e., wrok in the localization of R_ℓ at A, and compute the right-hand side of $(*)$ with the usual formulas. In order to compare both sides, multiply by all denominators and also by A to obtain two identities in R_ℓ. For $P \in E[\ell]^*$ with $A(P) \neq 0$, these two identities hold at P if and only if $(*)$ holds at P. If $A(P) = 0$, then they hold at P anyway. Since by assumptoin there is at leat one P such that $A(P) \neq 0$ and testing $(*)$ at one point suffices, we see that it is enough to compare the two identities in R_ℓ. If $A_1 = A_2$, one proceeds similarly by looking at B_1 and B_2. (Actually, if $B_1(P) = -B_2(P)$ for one $P \in E[\ell]^*$, then it holds for all.)

Page 386, Line −1
The cross references are wrong. This sentence should read: "The fastest known algorithms that solve the ECDLP on all elliptic curves are collision algorithms such as XI.5.2 and XI.5.4."

Page 391, Example XI.7.1
The statement and proof are incorrect for general N. One must make the additional assumption that N is prime. The error is in the statement that

$$a^2 + b^2 \equiv 0 \pmod{N} \qquad \Longrightarrow \qquad a \equiv b \equiv 0 \pmod{N},$$

which is true for prime values of $N \equiv 3 \pmod 4$, but not in general.

Page 394, Definition of $h_{P,Q}$
This value of $h_{P,Q}$ does not have the correct divisor if $P = O$ or $Q = O$. So we need to add an extra case that if $P = O$ or $Q = O$, then set $h_{P,Q} = 1$. Thus the full description now reads:

$$h_{P,Q} = \begin{cases} \dfrac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2 - a_1\lambda + a_2} & \text{if } \lambda \neq \infty, \\ x - x_P & \text{if } \lambda = \infty, \\ 1 & \text{if } P = O \text{ or } Q = O. \end{cases}$$

Page 401, Next to last paragraph
This argument is not quite right, since we can't conclude that S has exact order N^2/k. The following is a corrected argument:

We now consider the value of $\tau(T,T)$. Let k denote the order of $\tau(T,T)$ in $\mathbb{F}_q^*/(\mathbb{F}_q^*)^N$. Bilinearity of the Tate–Lichtenbaum pairing implies that

$$\tau([k]T,T) = \tau(T,T)^k = 1,$$

so the nondegeneracy that we already proved implies that $[k]T \in NE(\mathbb{F}_q)$. So we can write $[k]T = [N]S$ for some $S \in E(\mathbb{F}_q)$. The point T has order N, so $[N^2]S = [kN]T = O$, which shows that $S \in E(\mathbb{F}_q)[N^2]$. But by assumption, the only $\mathbb{F}_q$-rational points in $E[N^2]$ are the multiples of T, all of which have order dividing N. Hence $[N]S = O$, which shows that $[k]T = O$. The point T has exact order N, so $N \mid k$. But k is the order of an element of $\mathbb{F}_q^*/(\mathbb{F}_q^*)^N$, so $k \mid N$. This proves that $k = N$, and hence $\tau(T,T)$ is an element of exact order N in $\mathbb{F}_q^*/(\mathbb{F}_q^*)^N$. It follows immediately that $\tau(T,T)^{(q-1)/N}$ is a primitive N^{th} root of unity.

Page 409, Line −1
The discriminant is a_3^4, not a_4^3. So it should read

$$y^2 + a_3 y = x^3 + a_4 x + a_6, \qquad \Delta = a_3^4, \qquad j = 0.$$

Page 410, Second displayed equation
The numerator of j should be a_2^6, not a_2^2, so this line should read

$$\Delta = a_2^2 a_4^2 - a_2^3 a_6 - a_4^3, \qquad j = a_2^6/\Delta.$$

Page 411, Fifth displayed equation
The formula for u^4 is the reciprocal of the correct value. This line should read

$$u^4 = a_4/a_4' \qquad \text{and} \qquad r^3 + a_4 r + a_6 - u^6 a_6'.$$

Page 412, Line −10
The formula for the j-invariant is missing a power of 3. It currently reads $j = \frac{\alpha^3(\alpha-24)^3}{\alpha^3-27}$, but it should read

$$j = \frac{\alpha^3(\alpha^3-24)^3}{\alpha^3-27}.$$

Page 412, Proof of Proposition 1.3
Dino Lorenzini suggests the following more enlightening proof: Since the characteristic of K is not 3, the curve has a point of exact order 3. Translating that point to $(0,0)$, the origin becomes an inflexion point, so the equation for E has the form $y^2 + a_1 xy + a_3 y = x^3$. Now we're done after possibly taking a curve root of a_3.

Page 412, Corollary 1.4
Should really specify that there is more to being a local field than simply having a discrete valuation. For finite extensions K'/K, we want the integral closure of $\mathcal{O}_K$ in K' to be a local ring.

Page 413, Lines 6 and 7
Two occurrences of $\operatorname{char} K$ should be $\operatorname{char} k$. So these two sentences should read:

From the proofs of (VII.5.4c) and (VII.5.5), we are left to deal with the case that $\operatorname{char} k = 2$. In particular, we may assume that $\operatorname{char} k \neq 3$.

Page 418, first displayed equation
The first minus sign should be an equal sign. So it should read

$$\xi_{\tau\sigma} = \xi_\tau^\sigma + \xi_\sigma = \xi_\sigma.$$

Page 421, Line −13
Switch the domain and range of ξ, so it should read: "We again define a *continuous* 1*-cocycle from* $G_{\bar{K}/K}$ *to* M to be a map $\xi : G_{\bar{K}/K} \to M$ that satisfies the cocycle condition"

Page 426, Line 10
The reference should be (VI.5.1.1), not (VI.5.11).

Page 436, Line 8
There's a factor of q missing in the product for Δ. This line should read

$$\Delta = (2\pi)^{12} q \prod_{n=1}^{\infty} (1-q^n)^{24} = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) q^n.$$

Page 436, Fourth displayed equation, second line
The exponent of p should be 11, not 12. So this line should read

$$\tau(p^{r+1}) = \tau(p^r)\tau(p) - p^{11}\tau(p^{r-1}) \qquad \text{for } p \text{ prime and } r \geq 1.$$

Page 437, fourth displayed equation
The quotient should be by $\mathrm{SL}_2(\mathbb{Z})$, not $\mathrm{SL}_2(\mathbb{C})$. So this display should read

$$j : \mathbb{H}^* / \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}).$$

Page 440, Third paragraph
In the paragraph starting "Finally, we consider the moduli problem…", it should be $\gamma \in \Gamma(N)$, not $\gamma \in \Gamma(n)$..

Page 440, Line −9
It should be $\mathrm{SL}_2(\mathbb{Z})$, not $\mathrm{SL}_2(\mathbb{C})$. So it should read: "we note that although the Riemann surface $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ classifies elliptic curves…".

Page 443, Line 14
The proof of the full moduluarity conjecture should list Diamond, not Harris, so it should read: "culminating in a proof of the full modularity conjecture by Breuil, Conrad, Diamond, and Taylor [28] in 2001."

Page 448, Last line of table
The reason that some of the entries in the last line of the table are listed as $\tilde{j}$, rather than j. The tilde indicates that we are considering the values of j in the residue field k.

Page 454, first displayed equation
The term $x63$ should be x^3, so the full line should read

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Page 454, Third displayed equation
It might be clearer if there were parantheses to indicate that both terms are included in the limit. Thus it should read:

$$\lim_{P\to O}\left(\lambda_v(P) + \frac{1}{2}v\big(x(P)\big)\right)$$

Page 456, first displayed equation
The prime should be on the E, not on the T_ℓ. So it should read

$$\mathrm{Hom}_K(E, E') \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_K\big(T_\ell(E), T_\ell(E')\big)$$

Page 459, first paragraph
It has been suggested that the attribution for Theorem 21.2, the Sato–Tate conjecture for non-integral j-invariant curves, is misleading. The situation is somewhat complicated, because several mathematicians in various combinations worked on parts of the proof, with the final step appearing in a paper of Taylor. However, Taylor himself calls the theorem a joint effort, so the attribution should say that Theorem 21.2 is due jointly to Clozel, Harris, Shepherd-Barron, and Taylor. As justification for this attribution, we point to the following abstract used by Taylor for a talk at Columbia in 2006:

The Sato-Tate Conjecture
by Richard Taylor

Abstract: In the first part of the talk I will explain the Sato–Tate conjecture and the Tate–Serre approach via symmetric power L-functions. I will also

sketch the structure of the recent proof (by Laurent Clozel, Michael Harris, Nick Shepherd-Barron and myself) of the conjecture for elliptic curves over $\mathbb{Q}$ with somewhere multiplicative reduction.

In the second part of the talk I will explain a recent improvement to the Wiles/Taylor–Wiles method for proving modularity. This bypasses the level raising arguments of Wiles' Fermat Last theorem paper and hence bypasses Ihara's lemma. These were the last obstacles to generalising Wiles/Taylor–Wiles modularity results to higher rank unitary groups and hence to proving the Sato-Tate conjecture.

Page 462, Solution to Exercise 3.16(c)
The last line of this proof should be replaced by:

$$\begin{aligned} &= e_m(Q,P) && \text{definition of } e_m, \\ &= e_m(P,Q)^{-1} && \text{since } e_m \text{ is alternating.} \end{aligned}$$

It is also worth noting that in the literature, some sources use e_m and some sources use $\tilde{e}_m$ as the definition of the Weil pairing.

Page 494, index entry for division polynomial
The reference should be page 113, not page 114.

Page 494, index entry for Elkies
There should also be a reference to page 153 (Theorems V.4.7 and V.4.9 are due to Elkies).

Page 494, index entry for Shafarevich–Tate group
"is finite (?),, 453" has an extra comma.