Errata, Corrections, and Addenda to *The Arithmetic of Elliptic Curves* 2nd Edition, 2nd Printing (2015)

Joseph H. Silverman

October 13, 2022

IMPORTANT NOTE
This document omits errata that were corrected in the second printing.

Acknowledgements
I would like to thank following people for sending me comments and corrections: Vishal Arul, Paolo Barozza, Fabrizio Barroero, Agnes Beaudry, Ondrej Binovsky, Abbey Bourdon, Stijn Cambie, Brandon Carter, Kestutis Cesnavicius, Robin Chapman, Zev Chonoles, Kestutis Cesnavicius, Henry Cohn, Kevin D.T. Dao, Spencer Dembner, Tom Deneckere, Maarten Derickx, Riley Ellis, Xander Faber, Zhou Fang, Tony Feng, Ryan Flynn, S.D. Fordham, Matthias Franz, Toby Gee, Alexander Goncharov, Roberto Gualdi, Ayhan Gunaydin, Michael Harris, Lu Hengfei, Alan Hertgen, Florian Herzig, Campbell Hewett, Wei Ho, Victor Loh Bo Huai, Jakob Dawid Huewer, Enrique Gonzalez Jimenez, Warren Johnson Borys Kadets, Kassem Kalachi, Rafael von Känel, Arav Karighattam, Enis Kaya, Timo Keller, Chan-Ho Kim, Seoyoung Kim, Taekyung Kim, Daniel Krenn, Daniel Lauer, Jungin Lee, Jonah Leshin, Carl Lian, Sun Chia-Liang, Bart Litjens, Dino Lorenzini, Victor Lu, Michelle Manes, David Masser, Simon-Philipp Merz, Victor Miller, Igor Minevich, Grant S. Molnar, Yogesh More, Andrea Munaro, Krishnan Narayanan, Charles Nash, Eiki Norizuki, Yoshihiro Onishi, Mitchell Owen, Lorenz Panny, Abhishek Parab, Soohyun Park, Derek Perrin Benjamin Peterson, Bjorn Poonen, Linda Raabe, Miles Reid, Joost Renes, Sietse Ringers, Oded Rotem, Jeremy Rouse, Kazuki Sato, Bettina Schroegmeier, Jean-Pierre Serre, Barak Shani, Dane Skabelund, Soeren Sprehe, Katherine Stange, Reuben Stern, Jane Sullivan, Andrew Sutherland, Nicholas Triantafillou, Thom Tyrrell, Nikos Tzanakis, Doug Ulmer, Paul Voutier, Benjamin Weggenmann, Attila Wiebe, Alan (Ka Lun) Wong, Siman Wong, Chris Wuthrich, Kejian Xu, Ziquan Yang, Jeremias Yehdegho, Leonardo Zapponi, Francesco Zerman, Li Zheng.

Page 2, Top of page
The action of $G_{\bar{K}/K}$ is a left action, so it might be better to write it as ${}^{\sigma}P$. However, there are also issues with writing superscripts on the left. In any case, it might be worth noting that with our notation, we have $P^{\sigma\tau} = (P^{\tau})^{\sigma}$, and that the reader who finds this unpleasant may rewrite the group action as σP or ${}^{\sigma}P$, which better reflects the left-ness of the action.

Pages 5 and 17
The definition of M_P on page 5 is not in agreement with the definition of M_P on page 17. The former is an ideal in $\bar{K}[V]$, while the latter is an ideal in $\bar{K}[C]_P$, so in the latter case we've localized the ring. But this is a common abuse of notation, as long as it is clear from context which ring M_P is sitting in.

Page 9, Line 3
Replace $0 \leq i \leq n$ with $1 \leq i \leq n+1$.

Page 9, 5th Displayed Equation
There are not enough Y variables. It should read

$$I(V \cap \mathbb{A}^n) = \big\{ f(Y_0, \ldots, Y_{i-1}, 1, Y_i, \ldots, Y_n) : f(X_0, \ldots, X_n) \in I(V) \big\}.$$

In other words, the subscript on the Y after the 1 should be i, not $i+1$. The same correction needs to be made four lines later, where

$$f(Y_1, \ldots, Y_{i-1}, 1, Y_{i+1}, \ldots, Y_n) \text{ should be } f(Y_1, \ldots, Y_{i-1}, 1, Y_i, \ldots, Y_n).$$

Page 11, Line 4 of Remark 2.9
"at all point P where" should be "at all points P where"

Page 11, Line -4
We should allow λ to be in $\bar{K}(V_1)^*$. Thus it should read: "If, in addition, there is some $\lambda \in \bar{K}(V_1)^*$ such that $\lambda f_0, \ldots, \lambda f_n \in K(V_1)$, then ϕ is said to be *defined over* K."

Page 15, Exercise 1.7(c)
The assumptoin that V is irreducible is irrelevant to this problem (and in any case, the definition of variety includes irreduciblity), but the assumption that $\dim(V) > 0$ is required.

Further, the problem asks to prove that ϕ is not an isomorphism. The term "isomorphism" has not been defined, although on page 13 two varieties are said to be "isomorphic" if there are morphisms $V \to W$ and $W \to V$ whose compositions are the identity. So it should be clear that the maps are then called *isomorphisms*.

Page 16, Exercise 1.11(b)
Smoothness has only been defined for varieties, so possibly some note should

be included as to definition for more general algebraic sets. Also, we need to assume that $n \ge 2$.

Page 16, Exercise 1.12(b)
The hint leads to a valid proof, but it's easier to simply normalize P so that one of its coordinates equals 1. This forces $\lambda_\sigma = 1$ for all σ, and hence every coordinate of P is in K.

Page 18, Line 4
It might look nicer to put braces around the ∞, thus

$$\mathrm{ord}_P : \bar{K}(C) \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

Page 21, Statement of Theorem 2.4(c)
The text refers to a field of finite index, which is not standard terminology. Maybe clearer to say: "Let $K \subset \mathbb{K} \subset K(C_1)$ be a tower of fields with $K(C_1)/\mathbb{K}$ a finite extension."

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

Page 27, Line 1
$\mathbb{K}$ should be the pull-back of the function field, so it should read: Comparing degrees, we conclude that $\mathbb{K} = \phi^*\big(K(C_1^{(q)})\big)$.

Page 27+, Section II.3 and following
It has been noted that the book uses a somewhat antiquated convention for the definitions of $\mathrm{Div}(C)$ and $\mathrm{Pic}(C)$. It has become more or less standard in the modern arithmetic geometry literature that if a curve C (or more generally a variety) is defined over K, then $\mathrm{Div}(C)$ denotes the divisor group of C as

a variety (scheme) over K, and $\mathrm{Div}(C_{\bar{K}})$ denotes the divisor group of C as a curve after base change to $\bar{K}$, where $C_{\bar{K}}$ is the standard abbreviation for the fiber product $C \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\bar{K})$. Thus $\mathrm{Div}(C_{\bar{K}})$ is the free abelian group on the set $C(\bar{K})$, and $\mathrm{Div}(C)$ is

$$\mathrm{Div}(C) = \{D \in \mathrm{Div}(C_{\bar{K}}) : D^\sigma = D \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

It might be worth noting this, or possibly changing the notation throughout the book. However, since $\mathrm{Div}(C)$ seems ambiguous, it might be better to write $\mathrm{Div}(C_K)$ and $\mathrm{Div}(C_{\bar{K}})$ in order to explicitly indicate the base field.

Page 28, Example 3.3
It has been suggested that it might be helpful to include more detail on how $\mathrm{div}(x - e_i)$ and $\mathrm{div}(y)$ are computed. For example, note that y is a local coordinate at P_i, and that $x - e_2$ and $x - e_3$ are units in the local ring at P_1, which shows that $x - e_1 = uy^2$ for a unit u in the local ring at P_1. From this and $\mathrm{ord}_{P_1}(y) = 1$, we conclude that $\mathrm{ord}_{P_1}(x - e_1) = 2$. Alternatively, there could be an exercise to fill in these details.

Page 30–37, Sections II.4 and II.5
Throughout these sections it should be specified that "curve" means "smooth curve".

Page 30, Line preceding the Definition
Missing period at the end of the sentence ending "each element has a nonzero derivative".

Page 31, Line 1 of Proposition 4.3
"unformizer" should be "uniformizer"

Page 32, Definition of the divisor of ω
The definition should specify that the differential form ω is not zero.

Page 36, Line -8
"has finite index in K" should be "has finite index in G"

Page 39–40, Exercise 2.13
Add the assumption that the curve C is smooth.

Page 46 and following
All references to (III.1.2) should instead refer to Table 3.1.

Page 47, Line -7
The formula for Δ should have a square in the numerator, not a cube:

$$\Delta = \frac{j_0^2}{(j_0 - 1728)^3}$$

Page 47, Line −8
"A simple calculations" should be ""A simple calculation"

Page 55, Line −3
The discriminant is listed as $\Delta = 2^4 3^3 17$. It should be negative and the exponent of 17 should be 2. Thus it should be

$$\Delta = -2^4 3^3 17^2.$$

Page 57, 5th displayed equation
The exponent on $(X - Y)$ should be 3, not 2, so it should read

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

Page 60, Paragraph 2
An alternative proof that $E \to C$ has degree one is to use (II.2.6) applied to the fiber over the smooth point $[0, 1, 0]$.

Page 66, Section III.4, Definition of Isogeny
It has been pointed out that the standard definition of isogeny (more generally for abelian varieties) is that an isogeny is a surjective homomorphism with finite kernel. So for elliptic curves, the zero-map should not be called an isogeny; and if one wants to include the zero homomorphism, then one should refer to homomorphisms. The downside to this is that the set of isogenies is no longer a group. For elliptic curves it seems reasonable to include the zero-map and refer to non-zero isogenies as appropriate; but a note to the reader indicating that this is not the standard terminology for abelian varieties might be appropriate.

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 10, in the Definition
Replace "the set of points of E of order m" with "the set of points of E of order dividing m".

Page 75+, Section III.5
To avoid confusion regarding "the invariant differential" versus "an invariant differential," it might help to note that when dealing with an abstract elliptic curve, the differential ω depends on the choice of a Weierstrass equation for E, and that Table 3.1 then tells us that ω is unique up to multiplication by a scalar.

Page 79, Corollary 5.5
Possibly should point out that we are using the abbreviated notation $m + n\phi$ instead of the lengthier $[m] + [n] \circ \phi$.

Page 80, Proof Corollary III.5.6 (a)
Should also note that $a_{[1]} = 1$, which is generally required for a homomorphism of commutative rings.

Page 80, Proofs of Corollary III.5.6(b)
The ring $\mathrm{End}(E)$ also contains the constant isogeny. Claim (b) should be fixed accordingly.

Page 80, Last line of proof of III.5.6(c)
It should say that $\mathrm{End}(E)$ injects into K, not into K^*.

Page 81, Theorem 6.1(a)
Might be worth noting that if ϕ is defined over K, then $\hat{\phi}$ is also defined over K. This follows from the uniqueness of $\hat{\phi}$, since for any $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we have $[m] = [m]^\sigma = (\hat{\phi} \circ \phi)^\sigma = \hat{\phi}^\sigma \circ \phi$. Thus by uniqueness, we have $\hat{\phi}^\sigma = \hat{\phi}$. (Or this could be a new exercise.)

Page 84, first displayed equation
In this equation, we are looking at points on the elliptic curves defined over the field $K(x_1, y_1)$, so for example $\phi(x_1, y_1)$ is a point in $E_2\big(K(x_1, y_1)\big)$. Thus this displayed equation should not have any "div" operators. It should read

$$D = \big((\phi + \psi)(x_1, y_1)\big) - \big(\phi(x_1, y_1)\big) - \big(\psi(x_1, y_1)\big) + (O) \in \mathrm{Div}_{K(x_1,x_2)}(E_2).$$

Page 84, Line 10
Remove "div" from the sentence that starts "Then examining D". Thus this sentence should read:

Then examining D, specifically the term $-\big(\phi(x_1, y_1)\big)$, we see that f has a pole at P_1,...

Page 85, Definition of quadratic form
It might be worth pointing out that the bilinearity combined with $d(\alpha) = d(-\alpha)$ implies, via an easy induction argument, that $d(n\alpha) = n^2 d(\alpha)$ for all $n \in \mathbb{Z}$. This might be a good exercise.

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 it in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. How do you prove that the unit group in a number field are finitely generated? You embed it 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.)

It might be helpful to explain what it means to "extend the degree mapping to the finite-dimensional real vector space $M \otimes \mathbb{R}$" at the top of page 90. Or make an exercise.

Exercise. Let M be a finitely generated free $\mathbb{Z}$-module, and let $d : M \to \mathbb{R}$ be a quadratic form on M. Prove that there is a unique quadratic form

$$D : M \otimes \mathbb{R} \to \mathbb{R} \quad \text{satisfying} \quad D(m \otimes 1) = d(m) \quad \text{for all } m \in M.$$

Page 89, Line -5
Missing period for the sentence ending "is injective".

Page 90, bottom of page
Here we factor $\psi = [\ell^n] \circ \lambda$, while (III.4.11) says that $\psi = \lambda \circ [\ell^n]$. It might be worth mentioning that these are equal, since more generally, the multiplication-by-m maps commute with isogenies.

Page 91, Proof of Corollary 7.5
This proof is not correct. In particular, the assertion that if M is a torsion free $\mathbb{Z}$-module, then

$$\mathrm{rank}_{\mathbb{Z}} M = \mathrm{rank}_{\mathbb{Z}_\ell} M \otimes \mathbb{Z}_\ell$$

is false. For example, let p be a prime different from ℓ and let $M = \mathbb{Z}[1/p]$. Then M is clearly torsion free, but it is not finitely generated as a $\mathbb{Z}$-module. On the other hand, $M \otimes \mathbb{Z}_\ell = \mathbb{Z}_\ell[1/p] = \mathbb{Z}_\ell$ has rank 1 as a $\mathbb{Z}_\ell$-module.

Here is an alternative proof. Using the fact that $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module and the injectivity from Theorem III.7.4, tensoring with $\mathbb{Q}_\ell$ we find that

$$\Big(\mathrm{Hom}_{\mathbb{Z}}(E_1, E_2) \otimes \mathbb{Q}\Big) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \hookrightarrow \mathrm{Hom}_{\mathbb{Q}}\big(T_\ell(E_1) \otimes \mathbb{Q}, T_\ell(E_2) \otimes \mathbb{Q}\big) \cong M_2(\mathbb{Q}_\ell).$$

Hence $\mathrm{Hom}_{\mathbb{Z}}(E_1, E_2) \otimes \mathbb{Q}$ is a finite dimensional $\mathbb{Q}$-vector space, and indeed, has dimension at most 4. Hence we can pick a finite set of elements of

$\mathrm{Hom}(E_1,E_2)$ that generates $\mathrm{Hom}(E_1,E_2)\otimes\mathbb{Q}$ as a $\mathbb{Q}$-vector space, and then it follows from assertion (*) in the proof of Theorem 7.4 that $\mathrm{Hom}(E_1,E_2)$ is a finitely generated $\mathbb{Z}$-module.

Page 93, Line 10
"We can simultaneously achieve basis independent and Galois invariance" should be "We can simultaneously achieve basis independence and Galois invariance", i.e., change "independent" to "independence".

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

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

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, Proof of Proposition III.8.1 (b)
The 5th and 6th displayed equations are

$$\prod_{i=0}^{m-1} f\circ\tau_{[i]T} \tag{$*$}$$

and

$$\prod_{i=0}^{m-1} g\circ\tau_{[i]T'}. \tag{$**$}$$

We proved that $(*)$ is constant, and then we say that if we choose $T'\in E$ satisfying $[m]T'=T$, then the m'th power of $(**)$ equals $(*)$, and hence $(**)$ is also constant. However, although it is true that $(**)$ is constant, it is not true that the m'th power of $(**)$ is exactly equal to $(*)$. What we get is

$$\begin{aligned}\prod_{i=0}^{m-1} g\circ\tau_{[i]T'}(X)^m&=\prod_{i=0}^{m-1} g\bigl(X+[i]T'\bigr)^m\\&=\prod_{i=0}^{m-1} f\bigl([m]X+[mi]T'\bigr)\quad\text{since } g^m=f\circ[m],\\&=\prod_{i=0}^{m-1} f\bigl([m]X+[i]T\bigr)\quad\text{since } [m]T'=T.\end{aligned}$$

So if we let F equal the product $(*)$ and let G equal the product $(**)$, then

$$G^m = F \circ [m].$$

From this and the fact that F is constant, we can deduce that G is also constant.

Page 97, Proof of Proposition III.8.2
There is an extra parenthesis, and only part b is needed. Thus "((III.6.1ab)" should be "(III.6.1b)".

Page 98, Remark 8.5
The Weil pairing associated to an isogeny is subtler than indicated here. For example, if the kernel of $\phi : E_1 \to E_2$ is cyclic of order m, then $\deg(\phi) = m$ and there is a Weil pairing as indicated in this remark. On the other hand, if $E_1 = E_2$ and $\phi = [m]$, then $\deg(\phi) = m^2$, but the Weil pairing lands in $\boldsymbol{\mu}_m$, not in $\boldsymbol{\mu}_{m^2}$. So the remark is correct, but in general if we take $m = \deg(\phi)$, then the image of the Weil pairing might be a subgroup of $\boldsymbol{\mu}_m$.

Page 99, Proposition 8.6
One might introduce $\mathrm{tr}(\phi) = \phi + \hat{\phi}$, which is an integer from results in Section III.6. More precisely, it is an element of $\mathbb{Z}$ considered as a subring of $\mathrm{End}(E)$. Then we can write $\mathrm{tr}(\phi) = \mathrm{tr}(\phi_\ell)$.

Page 101, Last paragraph
An alternative (faster) way to show that $1, \alpha, \beta, \alpha\beta$ are linearly independent is to consider $\mathcal{K}$ as a vector space over $\mathbb{Q}(\alpha)$.

Page 104, Third displayed equation
The range should be $\mathrm{Aut}(E)$, not E. So it should read

$$[\ \ ] : \boldsymbol{\mu}_n \longrightarrow \mathrm{Aut}(E), \qquad [\zeta](x,y) = (\zeta^2 x, \zeta^3 y),$$

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.
Exercise. 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 non-constant 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.

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 105–106, Exercise 3.7(a)
"and similarly for $(2(2y + a_1x + a_3))^{-1}\psi_m$, ϕ_m, and ω_m if m is even." This should be "and similarly for $(2y + a_1x + a_3)^{-1}\psi_m$, ϕ_m, and ω_m if m is even."

Page 105–106, 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

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

Page 107, Exercie 3.10(d)
"$H \cap \phi(E) = \{P\}$" should be "$H \cap \phi(E) = \big\{\phi(P)\big\}$".

Page 107, Exercie 3.11(c)
"$H \cap \phi(E) = \{P\}$" should be "$H \cap \phi(E) = \big\{\phi(P)\big\}$".

Page 108, Exercise 3.13(e)
"Prove further that C is unique..." should be "Prove further that C' is unique ...".

Page 108, Exercise 3.13(d)
Need to specify that the characteristic of K is either 0, or else that it does not divide $\#\Phi$.

Page 108, Exercise 3.14
Need to add the assumption that the characteristic of K is not equal to ℓ. Indeed, if K has characteristic ℓ and E_1 (or E_2) is supersingular, than $T_\ell(E_1) = 0$.

Page 108, Exercise 3.16
This exercise is correct as stated, but one might want a more accurate version that would also reflects how we defined the pairing e_m on $E[m]$. So if we write $\ker(\phi) \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with $m_1 \mid m$, then the Weil pairing surjects onto $\boldsymbol{\mu}_m$.

Page 110, Exercise 3.23
It has been pointed out that it is easier to first do parts (c) and (d), since one can then find an $\alpha \in \bar{K}$ such that the Deuring model is nonsingular and has

the same j-invariant as the given E. This is true, and it provides a good lesson as to why one might not want to do problems in abc order. On the other hand, an alternative way to do (a) is to notice that (b) says that $(0,0)$ is a 3-torsion point. So one can take any given Weierstrass equation for E and move one of the 3-torsion points to $(0,0)$ and use elementary change-of-variable operations to put the Weierstrass equation into the desired form.

Page 110, Exercise 3.23(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 111, Exercise 3.30
Instead of saying "consisting of all elements of order D", it might be clearer to say "consisting of all elements of order dividing D". On the other hand, it seems reasonably clear from context what is meant.

Page 113, Exercise 3.34
Since the sequence starts with W_1 and the recurrence involves W_{n-1}, the recurrence is only defined for $m > n \ge 2$. So it should read

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 \qquad \text{for all } m > n \ge 2.$$

Page 115, Chapter IV
It might be helpful to give some motivation for defining and studying the formal group of an elliptic curve. Here is an version of an answer that I posted on MathOverflow `http://mathoverflow.net/questions/52241`.

Why should be study formal groups? The formal group of an elliptic curve E is a tool used to analyze E in a neighborhood of its identity element O. This is done by expanding the addition law as a power series in terms of the parameter $z = -x/y$, which is a uniformizer at O. Once we do this, it is natural to do the construction more generally, so we look at power series that formally define a group law. Then we find, for example, that if $\hat{G}$ is a formal group over a ring R of characteristic prime to m, it is always that case that the multiplication-by-m is invertible. In particular, if R is a complete DVR with maximal ideal M and residue characteristic p, then $\hat{G}(M)$ has no prime-to-p torsion.

This is important for the study of elliptic curves because there is an exact sequence in which the formal group is the kernel of the reduction mod M map. So for example, if E has good reduction modulo M, then there is an exact sequence

$$0 \to \hat{E}(M) \to E(K) \to E(R/M) \to 0.$$

We can use this sequence to deduce ramification information about the fields generated by torsion points, and this in turn is a crucial ingredient in the proof of the (weak) Mordell-Weil theorem in Chapter VIII.

So this explains why one studies formal groups and formal group laws. In general for any algebraic group G over a (complete local) field K with ring of integers R, maximal ideal M, and residue field k, the group $G(K)$ is complicated. So we can analyze $G(K)$ by breaking it up into the smaller group $G(k)$ and the formal group $\hat{G}(M)$. And as we shall see, formal groups are much easier to understand than algebraic groups.

Page 115, Start of Chapter IV
Instead of saying "Let E be an elliptic curve," it would be better to say "Let E/K be an elliptic curve," so that the field is specified.

Page 115, Last displayed equation
The polynomial $f(z,w)$ is supposed to be *defined* to be

$$f(z,w) = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3,$$

but this equation doesn't make this clear. Should say something like:

Thus if we start with a Weierstrass equation for E,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and if we change variables, clear denominators, and do a bit of algebra, we obtain an equation for E in the (z,w)-plane of the form

$$w = f(z,w) = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3.$$

Page 116, Lines 1–2
This might be clearer if rephrased as follows:

The goal now is to express w as a power series in z. We can do this by appealing to a general result such as Hensel's lemma, or more concretely (but less rigorously) by saying that we will recursively substitute the expression for w into itself. Thus

Page 119, Definition of λ
The coefficient A_0 is not actually defined in Proposition IV.1.1a. It's clear from that proposition that it should be $A_0 = 1$, but maybe should mention it here.

Page 121, Last line of Remark 2.1
"In this section we prove this last assertion when R has no torsion elements." Actually, this isn't proven until a later section. Should give an exact reference: "We will prove this last assertion when R has no torsion elements; see Application IV.5.3."

Page 121, Part (d)
It should be $i(0) = 0$, not $i(T) = 0$. Thus:

(d) There is a unique power series $i(T) \in R[\![T]\!]$ satisfying $i(0) = 0$ and $F\big(T, i(T)\big) = 0$ (inverse).

Page 122, Middle of the page
It says: "Then $g_n(T)$ must have the form

$$g_n(T) = g_{n-1}(T) + \lambda T^n$$

for some $\lambda \in R$." How do we know that g_n has degree (at most) n, which is implied by the "must have the form" assertion. Since we're just trying to find a sequence of polynomials that works, we can instead say:

We look for a $g_n(T)$ of the form

$$g_n(T) = g_{n-1}(T) + \lambda T^n$$

with $\lambda \in R$ so that

$$f\big(g_n(T)\big) \equiv T \pmod{T^{n+1}}.$$

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 123, middle of page
It might be worth mentioning that $\mathcal{M}^n$ is the nth power of the ideal $\mathcal{M}$, and not n-tuples of elements of $\mathcal{M}$.

Page 123, Example IV.3.1.2
Rather than saying that "$\hat{\mathbb{G}}_m(\mathcal{M})$ is the group of 1-units," it would be better to say that "$\hat{\mathbb{G}}_m(\mathcal{M})$ is isomorphic to the group of 1-units." In particular, the underlying set $\hat{\mathbb{G}}_m(\mathcal{M}) = \mathcal{M}$ is not the same as the set $1 + \mathcal{M}$.

Page 123, Example IV.3.1.3
In the displayed equation, it should be $z \mapsto P_z$, not $z \to P_z$. Thus it should read

$$\mathcal{M} \longrightarrow E(K), \qquad z \longmapsto P_z = \big(x(z), y(z)\big).$$

Page 124, Last paragraph
There is actually no need to assume that R is Noetherian, since the completeness alone implies that $\cap_{n\ge 1}\mathcal{M}^n = 0$

Page 125, Definition of invariant differential
Could explain in more detail that in the expression $\omega \circ F(T,S)$, we are viewing T as the variable quantity and S as a constant, so $T \mapsto F(T,S)$ should be viewed as the "translation-by-S map." Then using the chain rule

$$\omega\circ F(T,S) = \omega\big(F(T,S)\big) = P\big(F(T,S)\big)dF(T,S) = P\big(F(T,S)\big)\cdot\frac{\partial F}{\partial T}(T,S)\cdot dT.$$

There isn't any $(\partial F/\partial S)(T,S)\,dS$, because S is "constant," so $dS = 0$.

Page 125, Line 2 of the Proof of Proposition IV.4.2
The displayed equation should end with a period, not a comma.

Page 126, Corollary IV.4.4
Add a comma between "group" and "and", and start the second sentence with "Then". So it should read
Corollary 4.4. Let $\mathcal{F}/R$ be a formal group, and let $p \in \mathbb{Z}$ be a prime. Then there are power series $f(T), g(T) \in R[\![T]\!]$ with $f(0) = g(0) = 0$ such that

Page 126, middle of page
Although it should be clear from context and the chain rule, one could explicitly define $\omega \circ f$ via

$$\omega \circ f(T) = P\big(f(T)\big)\,df(T) = P\big(f(T)\big)\,f'(T)\,dT.$$

Page 127, Line 3 of Section IV.5
Should replace "characteristic 0" with torsion freeness, but don't want to define it here. So the first paragraph of Section IV.5 should read:

Integrating an invariant differential might, one hopes, yield a homomorphism to the additive group. Unfortunately, integration tends to introduce denominators, but at least in nice rings of characteristic 0, everything works fairly well.

Page 128, Last line
The displayed equation should end with a comma, not a period.

Page 129, Theorem 6.1
Mention that equality can hold, and refer to a new exercise to show that equality holds for the formal multiplicative group $\hat{\mathbb{G}}_m$, the ring $R = \mathbb{Z}_p[\zeta_{p^n}]$, and $x = 1 + \zeta_{p^n}$.

Page 130, Second line of Example IV.6.1.1
"If $p \geq 2$" should be "If $p \geq 3$".

(
Page 131, Lemma 6.3(a) It's not true in general that $f(x)$ converges in R, but it is true that $f(x)$ converges in the fraction field of R. The point is that a finite number of terms $a_n x^n/n$ could have negative valuation. To ensure convergence in R, we need for all $n \geq 1$ that

$$v(x^n/n) \geq 0, \quad \text{i.e., we need} \quad v(x) \geq v(n)/n.$$

The right-hand side is maximized for $n = p$, so the lemma should say something like the following:

If $x \in R$ satisfies $v(x) > 0$, then $f(x)$ converges in the field of fractions of R, and if $v(x) \geq v(p)/p$, then $f(x)$ is in R.

Page 133, Proposition 7.2(b)
Need to assume that $f(T)$ is not the zero homomorphism.

Page 134, Theorem 7.4 and Corollary 7.5
It might be worth reminding the reader that our fields are always assumed to be perfect (as specified on page 1).

Page 134, Proof of Corollary 7.5
Really should check that the invariant differential ω on E corresponds to invariant differential $\omega(T)$ on the formal group $\hat{E}$. This can be done using the explicit equations, but it's a bit messy. Alternatively, for the proof one can use Corollary IV.4.3 to note that if $\omega \circ f \neq 0$ for any differential, invariant or not, then $f'(0) \neq 0$.

Page 135, Exercise 4.4
The reference for the Weierstraass preparation theorem in Lang's *Algebra* (3rd edition) is not correct, and also quite out of date. It could be replaced by some other reference, or the reference could simply be omitted.

Page 135, Exercise 4.6
Note that this exercise may be false if one omits the assumption that $v(p) = 1$. 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. For example, if $x \in \mathcal{F}(\mathcal{M})$ has exact order p, then one finds that

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

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 $[p](T)$.

The following elliptic curve example has been provided by Bjorn Poonen: Let $R = \mathbb{Z}_2[i]$ and $K = \mathbb{Q}_2(i)$ with $i^2 = -1$, and take the uniformizer

$$\pi = 1 + i.$$

Note that $\pi^2 = 2i$, so $v(2) = 2v(\pi) = 2$. Consider the elliptic curve

$$E : y^2 + \pi xy + y = x^3.$$

It has good supersingular reduction,

$$\tilde{E} : y^2 + y = x^3 \quad \text{over the field } R/\pi R = \mathbb{F}_2.$$

The reduction modulo π of the formal group law $\mathcal{F}_E(X,Y) \in R[\![X,Y]\!]$ is a formal group law $\tilde{\mathcal{F}}_{\tilde{E}}(X,Y) \in \mathbb{F}_2[\![X,Y]\!]$ of height $h = 2$. (This follows from Theorem IV.7.4, or one can simply compute the first few terms of $\mathcal{F}_E(X,Y)$.) The 2-torsion point

$$(x_0, y_0) = \left(\frac{i}{2}, -\frac{\pi}{4}\right) = \left(-\frac{1}{\pi^2}, \frac{1}{\pi^3}\right) \in E(K)[2]$$

is in the kernel of the reduction map $E(K) \to \tilde{E}(\mathbb{F}_2)$, so it corresponds to

$$-\frac{x_0}{y_0} = \pi \in \mathcal{F}_E(\mathcal{M}) = \hat{E}(\pi R).$$

Hence $\pi \in \hat{E}(\pi R)$ is an element of exact order 2^{1+n} with $n = 0$. On the other hand, using $p = 2$ and $h = 2$ and $n = 0$ in the formula in Exercise 4.6, we have

$$v(\pi) = 1 \quad \text{and} \quad \frac{v(2)}{2^{2\cdot 0}(2^2 - 1)} = \frac{2}{3},$$

so the inequality in Exercise 4.6 is false.

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 139, first displayed equation
K should be $\mathbb{F}_q$, so it should read

$$f(x) = ax^3 + bx^2 + cx + d \in \mathbb{F}_q[x]$$

Page 140, Example 2.1
The second and third equations have $\mathbb{P}^n$ instead of $\mathbb{P}^N$. They should read

$$\log Z(\mathbb{P}^N/\mathbb{F}_q; T) = \sum_{n=1}^{\infty} \left(\sum_{i=0}^{N} q^{ni} \right) \frac{T^n}{n} = \sum_{i=0}^{N} -\log(1 - q^i T).$$

and

$$Z(\mathbb{P}^N/\mathbb{F}_q; T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^N T)}.$$

Page 146, last paragraph
In this proof, it is asserted that if E' is isogenous to E, then $\mathrm{End}(E')$ is a subring of $\mathcal{K} = \mathrm{End}(E) \otimes \mathbb{Q}$. This is true, but should either be proved or added as an exercise. Possibly in Chapter III include a discussion of why an isogeny $\phi : E \to E'$ of degree $d \geq 1$ induces a map $\phi : \mathrm{End}(E') \to \mathcal{K}$ via

$$\phi(\alpha) = \hat{\phi} \circ \alpha \circ \phi \otimes d^{-1}.$$

(The intuition is that $\phi^* : \mathrm{End}(E') \hookrightarrow \mathrm{End}(E)$ via $\phi^*\alpha = \phi^{-1}\alpha \circ \phi$, but of course, the map ϕ^{-1} won't exist if $d \geq 1$. However, we may view ϕ^{-1} as $\phi^{-1} = 1/\phi = \hat{\phi}/\phi\hat{\phi} = \hat{\phi}/d$, and we are allowed to divide by d after we tensor with $\mathbb{Q}$.)

Page 146, Line −10 and Page 147, Lines 4–5
The text talks about ℓ being *prime* in the ring $\mathrm{End}(E_m)$, but standard terminology would be to say that it is *irreducible*.

Page 147, Lines 4–5
Additional explanation: We know that the kernel of λ is cyclic of order ℓ^n. In particular, the map λ has degree ℓ^n, as does its dual$\hat{\lambda}$. Hence

$$\lambda \circ \hat{\lambda} = [\deg \lambda] = [\ell^n] = [\ell]^n.$$

We also know that ℓ is irreducible in the ring $\mathrm{End}(E_m)$, so this tells us that in this ring, the element λ is a unit times a power of $[\ell]$. Comparing degrees then shows that the power of $[\ell]$ is $n/2$, so $\lambda = u \circ [\ell^{n/2}]$, since units in $\mathrm{End}(E_m)$ are isomorphisms of E_m, hence have degree 1.

Page 148, Section V.4, First sentence
The text says that "up to isomorphism there are only finitely many elliptic curves of Hasse invariant 0." Should specify that this means for curves defined over a field of characteristic p, where we fix the prime p.

Page 153, Theorem 4.9
The stated result is true without the assumption that E not have complex multiplication, although of course if E does have CM, then far stronger results are known and were proven long before Elkies' result.

Page 153, Exercise 3.5
Rather than asking that $\ell\mathcal{R}_i$ bbe a prime ideal in $\mathcal{R}_i$, it would be more appropriate for the desired application to ask that ℓ be an irreducible element of $\mathcal{R}_i$.

Page 154, Exercise 5.10(e)
This exercise is still true if we take p^i to be the largest power of p such that $p^{2i-1} \mid q$. And this stronger version is needed in order to use 5.10(e) to solve 5.10(f). An alternative way to fix the problem is to replace (e) with:

(e) Prove that

$$p \mid \mathrm{tr}(\phi) \quad \Longleftrightarrow \quad q \mid \mathrm{tr}(\phi)^2.$$

Page 155, Exercise 5.16(b)
This is incorrect because the formula in (a) does not uniquely determine g and h. So (b) should be changed to:

(b) Prove that one can choose g and h in (a) so that they are polynomials in $\mathbb{F}_{p^2}[X, Y]$.

Page 155, Exercise 5.16(c,d)
If $\mathrm{Aut}(E)$ is larger than $\{\pm 1\}$, then these statements may not be correct. So both parts should include the assumption that $j(E) \notin \{0, 1728\}$. Example: $E : y^2 = x^3 + sx$ with $s \in \mathbb{F}_{49}$ a generator for $\mathbb{F}_{49}^2$. Then one can check that $[p]$ is the p^2-Frobenius map followed by the automorphism $(x, y) \to (-x, -iy)$. Further, need to deal with the fact that f and g are not unique. So it should read:

(c) Assume that $p \geq 3$ and that $j(E) \notin \{0, 1738\}$, and take a Weierstrass equation for E with $a_1 = a_3 = 0$. Prove that in (a) we may take $g(X) = X$ and $h(Y) = \pm Y$.
(d) Assume that $p \geq 5$, that E is defined over $\mathbb{F}_p$, and that $j(E) \notin \{0, 1728\}$. Prove that in (a) we may take $h = -Y$. Let $\phi : E \to E$ be the p^{th}-power Frobenius map on E. Prove that $\phi^2 = [-p]$ and that $\hat{\phi} = -\phi$.

First Paragraphs of Page 157 and Page 159
There is a significant duplication in this material concerning why elliptic curves have their unfortunate name. However, since people often don't read the introduction to a chapter, it's probably best to leave the duplicated material.

Page 158, Paragraph 1 of Section VI.1
In Chapter I the projective space $\mathbb{P}^1(\mathbb{C})$ is defined to be the set of homogeneous pairs, but in this chapter we are instead viewing $\mathbb{P}^1(\mathbb{C})$ as

$$\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$$

with the identification

$$\mathbb{C} \cup \{\infty\} \longrightarrow \mathbb{P}^1(\mathbb{C}), \quad \alpha \longmapsto \begin{cases} [\alpha, 1] & \text{if } \alpha \in \mathbb{C}, \\ [1, 0] & \text{if } \alpha = \infty. \end{cases}$$

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, Line −5
"the three integral" should be "the three integrals"

Page 170, Proof of surjectivity in Proposition VI.3.6(b)
Should also note that $O = [0, 1, 0] \in E$ is in the image of ϕ. This follows from the calculation

$$\phi(z) = \big[\wp(z), \wp'(z)m1\big] = \left[\frac{\wp(z)}{\wp'(z)},\, 1\,\frac{1}{\wp'(z)}\right] \xrightarrow{z \to 0} [0, 1, 0],$$

where we have used the fact that $\wp(z)$ has a pole of order 2 at $z = 0$ and that $\wp'(z)$ has a pole of order 3 at $z = 0$.

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 177, End of third paragraph
"conclusions are purely algebraic" is missing a final period.

Page 178, Exercise 6.3(d)
Should specify that $R \geq 1$, since if there is an $\omega_0 \in \Lambda$ with $|\omega_0| < 1$, then for all $R \leq |\omega_0|$ the set contains ω_0, so we have

$$\lim_{R\to 0} \#\big\{\omega \in \Lambda : R \leq |\omega| < R+1\big\} \geq 1 \quad \text{and} \quad \lim_{R\to 0} cR = 0.$$

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 nontrivial 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 176, Theorem 5.5
Could mention, or make an exercise, that this theorem works both ways. Thus given the lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, the endomorphism ring of $E = \mathbb{C}/\Lambda$ satisfies $\mathrm{End}(E) \neq \mathbb{Z}$ if and only if $\mathbb{Q}(\omega_1/\omega_2)$ is an imaginary quadratic extension of $\mathbb{Q}$.

Page 180, Exercise 6.10(c)
This is wrong if $\alpha \in \mathbb{Z}$, since then $\mathbb{Q}(\alpha) = \mathbb{Q}$ and

$$\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \mathrm{N}_{\mathbb{Q}/\mathbb{Q}}(\alpha) = |\alpha|,$$

but $\deg \phi = |\alpha|^2$. It can be fixed by letting $K = \mathrm{End}(E_1) \otimes \mathbb{Q}$ and taking the K norm. Thus:
(c) Assume that $\Lambda_1 = \Lambda_2$. Let $K = \mathrm{End}(E_1) \otimes \mathbb{Q}$. Prove that $\deg \phi = \mathrm{N}_{K/\mathbb{Q}}(\alpha)$. Deduce that $\hat{\phi}$ corresponds to the analytic map induced by $z \mapsto \bar{\alpha} z$, where $\bar{\alpha}$ is the complex conjugate of α.

Page 180, Exercise 6.11(a)
Rather than saying that "E has an equation of the form...", it would be clearer and more accurate to say that "E is birational to the affine curve...".

Page 182, Exercise 6.14(c)
The equation for $I(a_1, b_1)$ should have a_1^{-1}, not a_1^{-2}. Thus it should read

$$I(a,b) = a^{-1} K\left(\frac{2\sqrt{k}}{1+k}\right) \qquad \text{and} \qquad I(a_1,b_1) = a_1^{-1} K(k)$$

for $k = (a-b)/(a+b)$.

Page 185, Line 7
Might be worth pointing out that our definition of local field is that it be complete with respect to a discrete valuation. Some books define local field to additionally be locally compact, so for example with this definition, $\mathbb{Q}_p$ is a local field, but $\mathbb{C}_p$ is not.

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. (Need to add this book to the bibliography.)

Page 189, Lines 3, 19, and 20
$E_{\mathrm{ns}}(k)$ should be $\tilde{E}_{\mathrm{ns}}(k)$

Page 190, Line −4
"$P_3 \in E_{\mathrm{ns}}(k)$" should be (note missing two tildes) "$\tilde{P}_3 \in \tilde{E}_{\mathrm{ns}}(k)$". (Could also point out that this is equivalent to $P_3 \in E_0(K)$.)

Page 190, Line −3
"$\tilde{E}_{\mathrm{ns}} = \tilde{E}$" should be "$\tilde{E}_{\mathrm{ns}}(k) = \tilde{E}(k)$".

Page 191, Line 2
"$E(k)$" should be "$\tilde{E}(k)$".

Page 193, middle paragraph
"For an exposition of Cassel's original proof," should be "For an exposition of Cassels' original proof," or "For an exposition of Cassels's original proof,"

Page 193, Last sentence before Theorem VII.3.4
The first reference should be to Cassels' article [41], not [36]. So this should read:

For an exposition of Cassels' original proof, which involves a careful analysis of division polynomials, see [41, Theorem 17.2] or [135, Theorem III.1.5].

Page 194, Application VII.3.5
The following statement is implicit in the discussion, but for the subsequent applications, it would be helpful to state it explicitly:

We note that if E has good reduction at p, and if $P = (x, y) \in E(\mathbb{Q})_{\text{tors}}$ is in the kernel of the reduction map $E(\mathbb{Q})_{\text{tors}} \to \tilde{E}(\mathbb{F}_p)$, then p divides the denominators of x and y. But we have just proven that if P has order at least 3, then x and y are in $\mathbb{Z}$. It follows that for all primes p of good reduction, the kernel of the reduction-mod-p map is contained in $E[2]$. Since we also know from (VII.3.1) that the kernel of the reduction-mod-p map has p-power order, we see that the kernel is trivial when $p \geq 3$. This proves:

$$(p \geq 3 \text{ and } E \text{ good reduction at } p) \implies (E(\mathbb{Q})_{\text{tors}} \hookrightarrow \tilde{E}(\mathbb{F}_p) \text{ is injective}).$$

Page 197, Proof of Proposition VII.5.4 (a)
We have assumed that $\text{char}(k) \geq 5$, but could point out that the proof also works when $\text{char}(k) = 0$.

Page 198, Proof of Proposition VII.5.4 (c)
Should give a new name to the finite extension of K, or relabel: "We assume ..., and we replace K with a finite extension such that E/K has a Weierstras equation

Page 199, Proof of Theorem VII.7.1 (Néron-Ogg-Shafarevich)
In the proof, we denote by K^{nr} the completion of the maximal unramified extension of K. The extension K^{nr}/K is not algebraic, so it is not unramified according to the standard definition. Hence the application of (VII.5.4a) at the end of the proof is not valid.

One possible solution is that the argument for the first claim of the semistable reduction theorem (Proposition VII.5.4(a), with the re- striction to the given characteristics) only makes use of the fact that the field K' has the same value group of K. This is more general than the requirement that K'/K is an unramified extension, and it works also for K^{nr}/K.

Page 201, Displayed equation (ii) in the middle of the page
It would be clearer with additional parentheses, thus:
(ii) $m > \#\Big(E(K^{\text{nr}})/E_0(K^{\text{nr}})\Big)$.

Page 204, Exercise 7.13
This exercise is almost, but not quite, correct. There is a problem if $[p]P'$

or $[p]Q'$ is in $E_2(\mathbb{Q}_p)$. If p is large, this is very unlikely to happen, but it is possible. So the problem should be modified so that (c) and (d) are conditional on $[p]P', [p]Q' \notin E_2(\mathbb{Q}_p)$. Further, could add a part (e) to show that this is necessary by asking the reader to perform this process for $E : y^2 = x^3 + 3x + 2$ over the field $\mathbb{F}_5$ aand the points $P = (1, 1)$ and $Q = (2, 4)$ in $E(\mathbb{F}_5)$. One can check that $Q = 3P$, but lifting to $P' = (1, 1 + 3 \cdot 5 + 4 \cdot 5^3 + 2 \cdot 5^4 + \cdots)$ and $Q' = (2, 4)$ and using the formal logarithm, one obtains $m = 1$ instead of $m = 3$.

Page 212, Line 5
"The L/K is unramified..." should be "Then L/K is unramified..."

Page 214, Line 3
"Then the ideal aR_S is the m^{th} power of an ideal in R_S..." might be clearer if one specifies that it's a fractional ideal (although that's pretty clear from context).

Page 216, Definition before Proposition VIII.2.1
Here v is a place of K, not of $\bar{K}$, and in order to talk about the inertia group of v, one must pick an extension of the valuation v to $\bar{K}$, and the inertia group one gets depends on this extension. In this case, it doesn't matter much because a relatively straightforward calculation shows that if w_1 and w_2 are extensions of v to $\bar{K}$, then $\xi|_{I_{w_1}}$ is a coboundary if and only if $\xi|_{I_{w_2}}$ is a coboundary. See also Exericse 8.5.

Page 219, Values of C_1' and C_s
There's an implicit assumption that C_1' and C_2 are non-negative. In fact, taking $P = \mathcal{O}$ in Theorem 3.1 and using the fact that $h(\mathcal{O}) = 0$, one gets $0 \le h(Q) \le C_1$ in (b) and $0 \ge -C_2$ in (c), so the non-negativity is automatic.

Page 219, Fourth displayed equation
The $4/m^8$ should be $4/m^6$. Thus it should read

$$h(P_n) \le \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(C_1' + C_2)$$

Page 221, Line 3
This lemma should be labeled **Lemma 4.2**, not **Lemma 4.1**.

Page 222, Line −1
There are a number of typos in the expression for g_2, including sign errors, exponent errors, and a b that should be a B. It should read

$$\begin{aligned} g_2(X, Z) = &-A^2BX^3 - A(5A^3 + 32B^2)X^2Z \\ &- 2B(13A^3 + 96B^2)XZ^2 + 3A^2(A^3 + 8B^2)Z^3. \end{aligned}$$

Page 225, Example VIII.5.1
The bound should be $(2C+1)^{N+1}$, not $(2C+1)^N$.

Page 226, Third line of the proof of Proposition VIII.5.4
There's a missing subscript v on the right-hand side on the absolute value of λ. It should read

$$\prod_{v\in M_K} \max\bigl\{|\lambda x_0|_v,\dots,|\lambda x_N|_v\bigr\}^{n_v} = \prod_{v\in M_K} |\lambda|_v^{n_v} \max\bigl\{|x_0|_v,\dots,|x_N|_v\bigr\}^{n_v}$$

Page 232, 2nd Displayed Equation
Missing "max" before the last set. It should read

$$\max_{0\le i\le d}\bigl\{|a_i|_v\bigr\} = \max_{0\le i\le d}\bigl\{|b_i-\alpha_k b_{i-1}|_v\bigr\} \ge \epsilon(v)^{-1} \max_{0\le i\le d-1}\bigl\{|b_i|_v\bigr\} \max\bigl\{|\alpha_k|_v,1\bigr\}.$$

Page 238, 3rd displayed equation
The middle steps of this derivation are not correctly stated. It should read:

$$h_f = h\circ f = h\circ r\circ x = \bigl((\deg r)h + O(1)\bigr)\circ x = (\deg r)h_x + O(1).$$

Page 242, Remark 7.8
It seems that this should be Remark 7.7, since it directly follows Remark 7.6. However, the numbering of the first edition was retained to avoid erronious cross-references between editions, and the original Remark 7.7 in the first edition was omitted in the second edition. So this ostensible misnumbering is intentional.

Page 253, Theorem VIII.9.10
The reference should be [260], not [255].

Page 253, Sentence after Conjecture VIII.9.9
It should read "the constant C", i.e., the constant should be capitalized.

Page 261, Exercise 8.1
Could mention that $\operatorname{rank}_{\mathbb{Z}/m\mathbb{Z}}$ means the minimal number of generators as a $\mathbb{Z}/m\mathbb{Z}$-module, although this seems reasonably clear from the context.

Page 262, Exercise 8.5
As in the Definition before Proposition VIII.2.1 on page 216, there is an issue with extending the valuation to $\bar{K}$. We need to you pick a single inertia subgroup I_{w_1}, where w_1 is an extension of v to $\bar{K}$, and then we can arrange for c to be zero on I_{w_1}; but note that this doesn't imply that it's zero on I_{w_2} if w_2 is a different extension of v than w_1.

Page 275, 1st displayed equation and following line
All three instances of P should be Q. Thus it should read:

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

so the functions $(t_{\phi(Q)} \circ \phi)^{e_1}$ and $t_Q^{e_\phi(Q)e_2}$ vanish to the same order at Q.

Page 275, third displayed equation
There's a missing exponent of $1/e_1e_2$ on $\big|f(P)\big|_v$. This doesn't affect the value of the limit, but the corrected calculation is as follows:

$$\begin{aligned}
\frac{\log d_v\big(\phi(P),\phi(Q)\big)}{\log d_v(P,Q)} &= \frac{\log\big|t_{\phi(Q)}\big(\phi(P)\big)\big|_v^{1/e_2}}{\log\big|t_Q(P)\big|_v^{1/e_1}} \\
&= \frac{e_\phi(Q)\log\big|t_Q(P)\big|_v^{1/e_1} + \log\big|f(P)\big|_v^{1/e_1e_2}}{\log\big|t_Q(P)\big|_v^{1/e_1}} \\
&\longrightarrow e_\phi(Q) \qquad \text{as } P \underset{v}{\to} Q.
\end{aligned}$$

□

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

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

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 293, Line -7
"all primes of K lying over 2 and 3" should be "all primes of K lying over 2 or 3"

Page 295, Line 4
Two copies of Φ should be ϕ_ℓ.

Page 297, 4th Displayed Equation
The power of three should be outside of the parentheses. So it should read

$$x^3 = y^2 + 2 = (\zeta\bar{\zeta})^3 \ \text{ or } \ 2(\zeta\bar{\zeta})^3 \ \text{ or } \ 4(\zeta\bar{\zeta}^3).$$

Page 298, Conjecture IX.7.4
Since D is an arbitrary non-zero integer, the upper bound needs to take the absolute value, so it should read:

$$|x| \le C_\epsilon |D|^{2+\epsilon}.$$

Page 302, Exercise 9.2(b)
"a sequence of real numbers" should be "a sequence of integers". Further the listed assumption on $e(n)$ is too weak to apply Liouville's estimate. So change the problem to the following:
(b) Let $\epsilon > 0$, let $A, B, C \ge 1$ and $b \ge 2$ be integers, and let $\big(e(n)\big)_{n=1,2,\dots}$ be a sequence of integers with the property that

$$AC^{n^{1+\epsilon}} \le e(n) \le BC^{n^{1+\epsilon}} \qquad \text{for all } n = 1, 2, \dots.$$

Prove that the number $\sum_{n\ge1} b^{-e(n)}$ is transcendental.

Page 303, Exercise 9.3, 1st displayed equation
The pair should be in $\mathbb{Z}^2$, not in $\mathbb{Z}$, so it should read:

$$N(m) = \#\big\{(x,y) \in \mathbb{Z}^2 : y^2 = x^3 + m\big\}.$$

Page 304, Exercise 9.5(c)
This exercise is not correct as stated, since multiplying $f(T)$ be a scalar may change the required value of C_f, but does not change $H_K\big([a_0, \dots, a_n]\big)$. One solution would be to express C_f in terms of n and $H_K(a_0), \dots, H_K(a_n)$. Another solution is as follows:
(c) Assume further that $f(T)$ is monic, i.e., assume that $a_0 = 1$. Find an explicit expression for the constant C_f appearing in (b), where your value for C_f should depend only on n and $H_K\big([a_0, \dots, a_n]\big)$.

Page 305, Exercise 9.10
$y^2 - 2v^2 = -1$ should be $u^2 - 2v^2 = -1$. Also, it has been noted that this approach leads to the better value $C = 216\sqrt{2} + \epsilon$.

Page 311, Theorem X.1.1(a)
The theorem asserts that

$$e_m\big(\delta_E(P), T\big) = \delta_K\big(b(P,T)\big).$$

However, the value of e_m is in $\boldsymbol{\mu}_m$, and $\delta_E(P)$ is a function, while the value of δ_K is in $\mathrm{Hom}(G_{\bar K/K}, \boldsymbol{\mu}_m)$. So the meaning of this equation is unclear. What it really mean is that both sides define the same function from $G_{\bar K/K}$ to $\boldsymbol{\mu}_m$. So it would be more accurate to say that

$$e_m\big(\delta_E(P)(\sigma), T\big) = \delta_K\big(b(P,T)\big)(\sigma) \quad \text{for all } \sigma \in G_{\bar K/K}.$$

Page 312, Proof of Theorem X.1.1(a)
It might be a good idea to expand the explanation. Thus replace the proof of (a) with the following:

Hilbert's Theorem 90 (B.2.5c) implies that δ_K is an isomorphism. We define b to be the following composition of maps

$$\begin{aligned} E(K)/mE(K)\times E[m] &\xrightarrow{(P,T)\mapsto\left(\delta_E(P),T\right)} \operatorname{Hom}\left(G_{\bar K/K},E[m]\right)\times E[m] \\ &\xrightarrow{(\phi,T)\mapsto\left[\sigma\mapsto e_m\left(\phi(\sigma),T\right)\right]} \operatorname{Hom}(G_{\bar K/K},\boldsymbol{\mu}_m) \\ &\xrightarrow{\delta_K^{-1}} K^*/(K^*)^m. \end{aligned}$$

Then bilinearity of b follows from bilinearity of the Kummer pairing (VIII.1.2b) and bilinearity of the Weil e_m-pairing (III.8.1a).

Page 313, Proof of Theorem X.1.1(c)
Here is a more detailed explanation of the first part of the argument:

Let $\beta = b(P,T)^{1/m}$, and let $L = K\big([m]^{-1}E(K)\big)$. Then for all $\sigma \in \operatorname{Gal}_{\bar K/L}$ and all $Q \in [m]^{-1}(P)$, we have

$$\begin{aligned} \beta^\sigma/\beta = \delta_K\big(b(P,T)\big)(\sigma) &= e_m\big(\delta_E(P)(\sigma),T\big) \\ &= e_m(Q^\sigma - Q,T) = e_m(Q-Q,T) = 1. \end{aligned}$$

Thus $\beta^\sigma = \beta$ for all $\sigma \in G_{\bar K/L}$, so $\beta \in L$, and hence $K(\beta) \subseteq L$.

Page 313, Last Displayed Formula
The left-hand side of the equation should be $(x-e)\circ[2]$.

Page 317, Line 4
It has been suggested that the third point in $E(\mathbb{Q})$ should be $(10/9, 80/27)$, not $(10/9, -80/27)$. In fact, either one is possible, depending on which point (z_1,z_2,z_3) one finds in the homogeneous space. In general, the homogeneous space for (b_1,b_2) is

$$b_1z_1^2 - b_2z_2^2 = e_2 - e_1, \qquad b_1z_1^2 - b_1b_2z_3^2 = e_3 - e_1,$$

and the point in $E(\mathbb{Q})$ corresponding to a solution is $(b_1z_1^2 - e_1, b_1b_2z_1z_2z_3)$. Thus any solution (with $z_1z_2z_2 \neq 0$) gives 8 solutions $(\pm z_1, \pm z_2, \pm z_3)$, which give two points on $E(\mathbb{Q})$, namely a point and its negation.

For the specific curve $y^2 = x(x-2)(x-10)$ in this section, the homogeneous space associated to $(b_1,b_2) = (10,-2)$ is

$$10z_1^2 + 2z_2^2 = 2, \qquad 10z_1^2 + 20z_3^2 = 10.$$

After some work, one finds the solution

$$(z_1,z_2,z_3) = \left(\frac{1}{2},\frac{2}{3},\frac{2}{3}\right),$$

which gives the point $\left(\frac{10}{9},-\frac{80}{27}\right) \in E(\mathbb{Q})$, as in the text. If one instead takes the solution $\left(\frac{1}{2},\frac{2}{3},-\frac{2}{3}\right)$, then one gets the point $\left(\frac{10}{9},\frac{80}{27}\right) \in E(\mathbb{Q})$.

Proof of Theorem X.2.2, Page 319–320
Should to explain why the cocycles are continuous cocycles. Thus by definition ξ is the cocycle

$$\xi_\sigma = \phi^\sigma \phi^{-1}.$$

The map $\phi : C' \to C$ is defined over $\bar{K}$ and is given by some finite collection of polynomials. The coefficients of those polynomials generate a finite extension K' of K. It follows that $\phi^\sigma = \phi$ for all $\sigma \in G_{\bar{K}/K'}$, and hence that $\xi_\sigma = 1$ for all $\sigma \in G_{\bar{K}/K'}$. This proves that ξ is a continuous cocycle, since it is trivial on a finite index subgroup of $G_{\bar{K}/K}$.

Page 322, Section X.3, Definition of homogeneous space
When K has characteristic $p > 0$, the given definition of principal homogeneous space is incorrect, and indeed many of the subsequent propositions are false, even if K is algebraically closed. For example, the given definition allows the following. Let $C = E^{(p)}$ and let $F : E \to C$ be the p-power Frobenius map. Define an E-action on C by

$$C \times E \longrightarrow C, \quad (q, Q) \longmapsto q + F(Q).$$

This satisfies the given definition for C to be a homogenous space for E, but then Proposition X.3.2(a) fails, since in the proof of Proposition X.3.2(a) one can deduce only that the separable degree of ϕ is 1. Here is a corrected definition for the material that appears on the top of page 322:
Definition Let E/K be an elliptic curve. A (*principal*) *homogeneous space for* E/K is a smooth curve C/K together with an algebraic group action of E on C defined over K such that over $\bar{K}$, the curve C equipped with its E-action is isomorphic to E equipped with the translation action on E.

In other words, a homogeneous space for E/K consists of a pair (C, μ), where C/K is a smooth curve and

$$\mu : C \times E \longrightarrow C$$

is a morphism defined over K, and such that there exists an isomorphism

$$\iota : C \longrightarrow E$$

defined over $\bar{K}$ so that the following diagram commutes:

$$\begin{array}{ccc} C \times E & \xrightarrow{\mu} & C \\ \big\downarrow{\scriptstyle \iota \times 1} & & \big\downarrow{\scriptstyle \iota} \\ E \times E & \xrightarrow{(P,Q) \mapsto P+Q} & E. \end{array}$$

We note that this commutative diagram implies that μ has the following three properties:

(i) $\mu(p, O) = p$ for all $p \in C$.

(ii) $\mu\big(\mu(p,P),Q\big) = \mu(p,P+Q)$ for all $p \in C$ and $P,Q \in E$.

(iii) For all $p,q \in C$ there is a unique $P \in E$ satisfying $\mu(p,P) = q$.

Page 323, Line 11
"is a twist of of E/K" has an extra "of"

Page 325, Alternative proof of Lemma X.3.5
Let $P = q - p \in E$. The compatibility of θ with the action of E on the two homomgeneous spaces gives

$$\theta(p) + P = \theta(p+P) = \theta\big(p + (q-p)\big) = \theta\big(q + (p-p)\big) = \theta(q).$$

(We have used Lemma X.3.1(b), which says that $p + (q-p) = q$.) It follows that

$$P = \big(\theta(p) + P\big) - \theta(p) = \theta(q) - \theta(p).$$

Page 333, Line 15
"The arguement goes as follows" should be "The argument goes as follows"

Page 334, Proof of Lemma 10.4.3
The group of continuous homomorphisms is denoted by $\mathrm{Hom}_{\mathrm{cont}}$ in Appendix B, Remark B.2.2. So in this proof should probably use this notation for consistancy; but in any case, the text should note that we are only taking continuous homomorphisms.

Page 336, Last paragraph
It says: The isogenous curve E'/K has Weierstrass equation

$$E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X,$$

and the isogeny $\phi : E \to E'$ is given by the formula (III.4.5)

$$\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right).$$

It's unclear where E' is coming from. So it should say:

Using Proposition III.4.12 and Example III.4.5, we see that the isogenous curve E'/K has Weierstrass equation

$$E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X,$$

and the isogeny $\phi : E \to E'$ is given by the formula

$$\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right).$$

Page 337, 1st displayed equation
Two instances of $\theta \circ \phi$ should be $\phi \circ \theta$, so it should read:

$$\phi \circ \theta : C_d \longrightarrow E', \qquad \phi \circ \theta(z,w) = \left(\frac{d}{z^2}, -\frac{dw}{z^3} \right),$$

Page 338, 2nd Displayed Equation
This is the equation for E', not E, so it should read

$$E' : Y^2 = X^3 + 12X^2 - 32X,$$

Page 345, 4th displayed equation
It might be notationally more accurate to write $x\big([2]P\big)$, rather than $x(2P)$, but the meaning should be clear from context, the point being that $E(\mathbb{Q})$ is an abelian group, so it has a natural structure as a $\mathbb{Z}$-module.

Page 347, Proposition 10.6.1(b)
E should be E_D, so it should read

$$\operatorname{rank} E_D(\mathbb{Q}) \le 2\nu(2D) - 1.$$

Page 350, 4th displayed equation
The first quantity $E'(\mathbb{Q})/\phi\big(E(\mathbb{Q})[2]\big)$ should be $E'(\mathbb{Q})[\hat{\phi}]/\phi\big(E(\mathbb{Q})[2]\big)$, i.e., it is a quotient of the $\hat{\phi}$-torsion. So the full line should read

$$E'(\mathbb{Q})[\hat{\phi}]/\phi\big(E(\mathbb{Q})[2]\big) \cong \mathbb{Z}/2\mathbb{Z} \qquad \text{and} \qquad E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{1+\operatorname{rank} E(\mathbb{Q})}.$$

Page 355, Exercise 10.1(a), 2nd displayed equation
This formula is correct if it is interpreted properly, using the fact that $\delta_\phi(P)$ and $\delta_K\big(b(P,T)\big)$ are cocycles, so the formula is actually an equality of functions. For added clarity, it might be better to write

$$e_\phi\big(\delta_\phi(P)(\sigma), T\big) = \delta_K\big(b(P,T)\big)(\sigma) \quad \text{for all } \sigma \in G_{\bar{K}/K}.$$

Page 356, Exercise 10.8
It has been noted that the result is true even if v divides m. The approach suggested in the hint still works, because K^* is dense in K_v^*, and K_v^{*m} is open in K_v^*.

Page 361, New Exercise (for the end of the chapter)
10.25. Verify that the commutative diagram in the definition of homogeneous space implies that the map μ has the three properties (i), (ii), (iii) listed in the definition.

Page 361, New Exercise (for the end of the chapter)
10.26. Let K be a field of characteristic $p > 0$, let E/K be an elliptic curve, let $C = E^{(p)}$, and let $F : E \to C$ be the p-power Frobenius map. Define a map

$$\mu : C \times E \longrightarrow C, \quad (q, Q) \longmapsto q + F(Q).$$

(a) Prove that μ is an algebraic group action of E on C, i.e., prove that μ is a morphism and that it satisfies the usual group action axioms

$$\mu(q, 0) = q \quad \text{and} \quad \mu\big(\mu(q, Q_1), Q_2\big) = \mu(q, Q_1 + Q_2).$$

(b) Prove that (C, μ) satisfies the three properties (i), (ii), (iii) in the definition of homogeneous space.
(c) Prove that Proposition X.3.2(a) is not true for (C, μ). (*Hint.* In the proof, show that one can deduce only that the separable degree of ϕ is 1.)

Pages 369–370, Remarks XI.2.4.3 and XI.2.4.4
These remarks implicitly assume that the reduction map

$$E(\mathbb{Z}/N\mathbb{Z}) \to E(\mathbb{Z}/p\mathbb{Z})$$

is a homomorphism whenever addition in $E(\mathbb{Z}/N\mathbb{Z})$ is defined. This is wrong if one uses the formulas from (III.2.3) as suggested in Remark XI.2.4.3. For example, the points $(1, 1)$ and $(1, 6)$ on the curve $y^2 = x^3 + x - 1$ over $\mathbb{Z}/35\mathbb{Z}$ sum to $(2, -3)$, but they are inverse to each other modulo 7. The problem here is that when $x_1 = x_2$, one may have $y_1 + y_2 \neq 0$ in $\mathbb{Z}/N\mathbb{Z}$ and $\gcd(2y_1, N) = 1$, but $y_1 + y_2 \equiv 0 \pmod{p}$. Lenstra solves this problem by dividing by $y_1 + y_2$ instead of $2y_1$.

Page 372, Second paragraph
If q is a prime power, but not prime, then could explain what is meant by the Legendre symbol for the field $\mathbb{F}_q$ (although this is pretty standard stuff). It 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 $c = 0$. Alternatively, it is the unique non-trivial character $\mathbb{F}_q^* \to \{\pm 1\}$, extended to $\mathbb{F}_q$ by sending 0 to 0.

Page 373, Line 10
It might be helpful to remind the reader that 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 $\overline{\mathbb{F}}_q \otimes_{\mathbb{F}_q} R_\ell$ 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 389, Proposition 6.5
The algorithm needs one additional tweak. In Step (3) one wants to choose lifts P' and Q' so that $[p]P'$ or $[p]Q'$ are not in $E_2(\mathbb{Q}_p)$. If p is large, this will very likely be the case, but if not, then one can always modify E' and choose new P' and Q' so that it's true. (Computing the approximate probability and showing that the problem can always be avoided could be new exercises.)

is very unlikely to happen, but it is possible. So the problem should be modified so that (c) and (d) are conditional on $[p]P', [p]Q' \notin E_2(\mathbb{Q}_p)$. Further, could add a part (e) to show that this is necessary by asking the reader to perform this process for $E : y^2 = x^3 + 3x + 2$ over the field $\mathbb{F}_5$ aand the points $P = (1, 1)$ and $Q = (2, 4)$ in $E(\mathbb{F}_5)$. One can check that $Q = 3P$, but lifting to $P' = (1, 1 + 3 \cdot 5 + 4 \cdot 5^3 + 2 \cdot 5^4 + \cdots)$ and $Q' = (2, 4)$ and using the formal logarithm, one obtains $m = 1$ instead of $m = 3$.

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 inflection point, so the equation for E has the form $y^2 + a_1xy + a_3y = x^3$. Now we're done after possibly taking a cube 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 415-416, Definitions
The words that are italicized in the definitions of the 0th cohomology group and the 1st cohomology group are not consistant.

Page 416–417, Statement of Proposition B.1.2
Probably not worth emphasizing the phrases "exact sequence of G-modules" and "connecting homomorphism", since switching from italic to roman font is confusing.

Page 419, Definition at the top of the page
The group $G_{\bar{K}/K}$ has subgroups of finite index that are not open for the profinite topology on $G_{\bar{K}/K}$. So in the line that starts "Equivalently", we should replace "subgroups of finite index in $G_{\bar{K}/K}$" with "open subgroups of $G_{\bar{K}/K}$. Thus this sentence should read:
Equivalently, for each $m \in M$, the set $\xi^{-1}(m)$ is a union of open subgroups of $G_{\bar{K}/K}$.

Page 421, Line -10
"1st *cohomology group*" should be "1st *cohomology set*," since when M is non-abelian, $H^1(G_{\bar{K}/K}, M)$ is a marked set, but it does not have a group structure.

Appendix B.2, page 418
There are contradictory explanations of the topology on $G_{\bar{K}/K}$. This is due to the fact that if we endow $G_{\bar{K}/K}$ with the standard Krull topology, whose basis of open normal subgroups are the kernels of the projections on the Galois groups of finite extensions of K, then in general there may be some normal subgroups of finite index that are not open. So the correct definition of the standard Krull topology on $G_{\bar{K}/K}$ is that is has a basis of open sets around the identity consisting of the subgroups of $G_{\bar{K}/K}$ that are the kernels of the maps $G_{\bar{K}/K} \to G_{L/K}$ as L ranges over all finite extensions of K in $\bar{K}$.

Page 440, 2nd Displayed Equation
The text says that the Weil pairing is given by

$$e_N\left(\frac{1}{N}, \frac{\tau}{N}\right) = e^{2\pi i/N}.$$

It has been suggested that it should be

$$e_N\left(\frac{\tau}{N}, \frac{1}{N}\right) = e^{2\pi i/N}.$$

Cf. Exercise 1.15 in *Advanced Topics in the Arithmetic of Elliptic Curves*.

Page 443, Line 14
The reference [28] is due to Breuil, Conrad, Diamond, and Taylor.

Page 444, Line before 4th displayed equation
The text says that the coordinates are in the power series ring $\mathbb{Z}[\![q,u]\!]$, but since n runs over $\mathbb{Z}$, the quantity u may appear in the denominator. What is true is that the coordinates are in the power series ring $\mathbb{Z}[\![q,u,u^{-1}]\!]$

Page 444, Equation for $y(u,q)$
The exponent should be $q^{2n}u^2$, not q^nu^2. So it should read

$$y = y(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^{2n}u^2}{(1-q^nu)^3} + \sum_{n\ge 1} \frac{q^n}{(1-q^n)^2}.$$

Page 448, Table 15.1
The table should note that k is assumed to be algebraically closed, since otherwise the group of components could be smaller than indicated. Although Theorem C.15.2 does indicate that "Some of the components of the special fiber may only be defined over a finite extension of k."

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, is because the tilde indicates that we are considering the values of j in the residue field k.

Page 450, Line before Proposition 16.2
"following resul:" should be "following result:"

Page 456, 3rd Displayed Equation
E should be the specialization E_t, so it should read:

$$E_t : y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t).$$

Page 458, Line -7
The text says: "If E has complex multiplication, then it is not hard to prove that the θ_v values are uniformly distributed in the interval $[0,\pi]$." This is only true for E/K if all of $\mathrm{End}(E)$ is defined over K, i.e., if the complex multiplication is defined over K. If the CM is not defined over K, then the θ_v values for the non-split primes are 0, so half the θ_v values are 0, and the other half are uniformly distributed.

Page 459, first paragraph
Since the publication of the second edition, the full Sato–Tate conjecture has been proven for all $E/\mathbb{Q}$, and more generally for all non-CM elliptic curves E defined over a totally real field K. Assigning credit for the proof is not so easy. Here is what Richard Taylor told me:

> Sato-Tate is known for any (non-CM) elliptic curve over a totally real field. I think technically the reference is corollary 8.9 of [A].

This is not an ideal reference however, because it does not reflect where the real credit lies. The Sato–Tate conjecture does not require the main innovation of this paper. It was always clear that the full Sato–Tate conjecture would follow from the method of the original papers on the non-integral j-invariant case [B], [C] and [D], together with the advances in either [E] or [F], as well as [G]. (The latter was around for a long time as preprint before being published — hence the later publication date.) However these authors never put everything together and stated the full Sato–Tate conjecture, although they could have done so without much difficulty. As it was a special case of what we were doing in [A], we stated it there, but we don't really deserve the credit. Rather the credit for the improvement from the case of non-integral j-invariant belongs to a complicated combination of Shin, Harris, Chenevier and the various authors of the articles in the book [F].

References for the Proof of the Sato–Tate Conjecture

- [A] T. Barnet-Lamb, D. Geraghty, M. Harris and R. Taylor: "A family of Calabi-Yau varieties and potential automorphy II" *P.R.I.M.S.* **47** (2011), 29–98.
- [B] R. Taylor, "Automorphy for some l-adic lifts of automorphic mod l representations. II" *Pub. Math. IHES* **108** (2008), 183–239.
- [C] M. Harris, N. Shepherd-Barron and R. Taylor, "A family of Calabi-Yau varieties and potential automorphy" *Annals of Math.* **171** (2010), 779–813.
- [D] L. Clozel, M. Harris and R. Taylor, "Automorphy for some l-adic lifts of automorphic mod l representations" *Pub. Math. IHES* **108** (2008), 1–181.
- [E] Sug-Woo Shin, "Galois representations arising from some compact Shimura varieties" *Ann. of Math.* **173** (2011), no.3, 1645–1741.
- [F] *On the Stabilization of the Trace Formula*, Clozel, Harris, Labesse and Ngo, editors, International Press 2011
- [G] G. Chenevier and M. Harris, "Construction of automorphic Galois representations II" *Cambridge Math. Journal* **1** (2013), 53–73.

Page 476, Bibliography item [73]

Part of the title of the book appears after the publisher information. It should read:

[73] D. Eisenbud. *Commutative algebra: with a View Toward Algebraic Geometry,* volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

Page 487, Deligne reference

Deligne's paper on the Weil conjectures was omitted from the 2nd edition due to a citation error. In order to leave the citation numbering unaltered in the 2nd printing, I have added Deligne's paper to the end of the references.

Page 509, index entry for Shafarevich–Tate group
The entry "is finite (?)" appears twice with different page numbers.