

**ERRATA AND CORRECTIONS TO
ADVANCED TOPICS IN THE ARITHMETIC OF ELLIPTIC
CURVES**

JOSEPH H. SILVERMAN

Acknowledgments

The author would like to thank the following people for their assistance in compiling this errata sheet: Andrew Baker, Brian Conrad, Paulo D’Ambros, Henri Darmon, Cosmin Davidescu, Sam Derbyshire, Darrin Doud, Guy Diaz, Virgile Ducet, Lisa Fastenberg, Steven Finch, Benji Fisher, Daniel Goldstein, Alexandru Ghitza, Grigor Grigorov, John Im, Boris Iskra, Steve Harding, Qin Hourong, Carlos Ivorra, Sharon Kineke, Joan-C. Lario, Yihsiang Liow, Robert Miller, Patrick Morton, Niko Naumann, Ken Ono, Martin Orr, Bjorn Poonen, Michael Reid, Ottavio Rizzo, David Rohrlich, Jacques Rousseau-Egele, Chad Schoen, Samir Siksek, Kate Stange, Kate Thompson, Doug Ulmer, Shuzhou Wang, Horst Zimmer.

Page ix: Second Paragraph

Tate’s unpublished manuscript (Tate [9]) has now appeared.

Page xi: Table of Contents

Section I.5 starts on page 39, not on page 38

Page 6, Line 1

“and and” should be “and an”.

Page 7 and following

Possibly use \mathfrak{H} instead of \mathbf{H} for the upper half-plane, since that is more standard notation.

Page 10, Remark 1.4

Change

$$ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^3 \quad \text{to} \quad (ST)^3 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^3.$$

Page 10, Remark 1.3, Displayed equation

There should be a + before the $(d - a)$, so this equation should read

$$c\tau^2 + (d - a)\tau - b = 0 \quad \text{for all } \tau \in \mathbf{H}.$$

Page 11: Figure 1.2

- (1) There is too much white space above this figure.
- (2) The fundamental domain should be labeled using a script \mathcal{F} instead of a Times Roman F.

Page 15: Figure 1.3

- (1) The caption is missing. It should read
The geometry of $\Gamma(1)\backslash\mathbf{H}$
- (2) The typeface for the words “Figure 1.3” is too large.
- (3) The fundamental domain should be labeled using a script \mathcal{F} instead of a Times Roman F.

Page 18: Lines 11,12

The four occurrences of V_1 should all be U_1 . Thus the displayed equation and the following line should read

$$\kappa = \kappa(U_1) = \sup_{\substack{\tau \in U_1 \\ \gamma \in \Gamma(1)}} \operatorname{Im}(\gamma\tau) = \sup_{\substack{\tau \in U_1 \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)}} \frac{\operatorname{Im}(\tau)}{|c\tau + d|^2}$$

is finite. (Note that if $\tau = s + it \in U_1$, then s and t are bounded, so

Page 19, Line –13

“disjoint neighborhoods of τ_1, τ_2 ” should be “disjoint neighborhoods of x_1, x_2 .”

Page 28, Line 7

“function f of weight k ” should be “function f of weight $2k$ ”.

Page 28: Line –1

In the diagram, the left vertical arrow should be labeled g_x instead of g .

Page 31: Theorem 3.10(a)

Might be better to write $M_{2k} \cong M_{2k}^0 \oplus \mathbb{C}G_{2k}$ instead of $M_{2k} \cong M_{2k}^0 + \mathbb{C}G_{2k}$, although it is an internal direct sum.

Page 31: Theorem 3.10(c)

Change $\left\lceil \frac{k}{6} \right\rceil$ to $[k/6]$ (twice).

Page 32: Third displayed equation

The first equation should end $= \rho^2 G_4(\rho)$. (The subscript 4 is missing.)

Page 32: Line 13

All four occurrences of “ i ” in this displayed equation should be changed to “ ρ ”, since G_4 vanishes at ρ , not at i . Further, there is a missing negation sign before the $2^4 3^3 5^2 7^2$. It should thus read

$$\Delta(\rho) = (60G_4(\rho))^3 - 27(140G_6(\rho))^2 = -2^4 3^3 5^2 7^2 G_6(\rho)^3 \neq 0.$$

Page 38, Second displayed equation

In the denominator of the formula for $j(E)$, it should be $g_4(\tau_E)^3$, not $g(\tau_E)^3$.

Page 42: Figure 1.5

The origin should be 0, not 0^2

Page 45: Line 2

“ σ has a simple pole at $\pm\frac{1}{2}\omega$.” should be “ σ has a simple zero at $\pm\frac{1}{2}\omega$.”

Page 46: Second displayed equation

Sign error, the exponent should be $z - \frac{1}{2}b$. Thus the RHS of the equation should read $\pm e^{\eta(b)(z - \frac{1}{2}b)}$.

Page 53, Line 7

This line says “From (5.2b), $\zeta(\frac{1}{2}; \tau) = \eta(1)$,” but (5.2b) (with $\omega = 1$) actually says that $\zeta(\frac{1}{2}; \tau) = \frac{1}{2}\eta(1)$. This would change the formula for $\zeta(z; \tau)$ and $\eta(1)$ in the statement of Theorem 6.3, as well as carrying over to change the formula for $\sigma(z; \tau)$ in Theorem 6.4. (Everyplace that $\eta(1)$ appears, it would be replaced by $\frac{1}{2}\eta(1)$.) However, other sources (e.g., [Lang 3]) give the formula for $\sigma(z; \tau)$ as it is stated in Theorem 6.4.

Page 55: Lemma 7.1.1 Displayed Equation

There should be a factor of $1/(2k - 1)!$ in the righthand side of the displayed equation. It should thus read

$$\sum_{n \in \mathbb{Z}} \frac{1}{(\tau + n)^{2k}} = \frac{(2\pi i)^{2k}}{(2k - 1)!} \sum_{r=1}^{\infty} r^{2k-1} e^{2\pi i r \tau}.$$

Page 55: Last displayed equation

Both equation need a negation sign after the equals sign. Futher, the notation for the higher-order derivatives should be fixed (twice) to be

$$\frac{d^{2k}}{d\tau^{2k}}.$$

Thus these displayed equation should read

$$\begin{aligned} \sum_{n \in \mathbb{Z}} \frac{1}{(\tau + n)^{2k}} &= \sum_{n \in \mathbb{Z}} \frac{-1}{(2k - 1)!} \frac{d^{2k}}{d\tau^{2k}} \log(\tau + n) \\ &= \frac{-1}{(2k - 1)!} \frac{d^{2k}}{d\tau^{2k}} \log \prod_{n \in \mathbb{Z}} (\tau + n). \end{aligned}$$

Page 56, Third displayed equation

Both sums should be $n = 1$ to ∞ , and there is a sign error on the second line. Thus it should read

$$\begin{aligned} \frac{d}{d\tau} \log(\sin \pi\tau) &= \frac{1}{\tau} + \sum_{n=1}^{\infty} \frac{-2\tau}{n^2 - \tau^2} \\ &= \frac{1}{\tau} + \sum_{n=1}^{\infty} \left(\frac{1}{n + \tau} + \frac{-1}{n - \tau} \right) \end{aligned}$$

Page 56, Fourth displayed equation

Both lines on the right of the equals sign need a negation sign. Thus this formula should read

$$\begin{aligned} \frac{d^{2k}}{d\tau^{2k}} \log(\sin \pi\tau) &= -(2k - 1)! \left\{ \frac{1}{\tau^{2k}} + \sum_{n=1}^{\infty} \left(\frac{1}{(n + \tau)^{2k}} + \frac{1}{(n - \tau)^{2k}} \right) \right\} \\ &= -(2k - 1)! \sum_{n \in \mathbb{Z}} \frac{1}{(n + \tau)^{2k}}. \end{aligned}$$

Page 56, Line -3

The $+$ before the sum should be a $-$. Thus this line should read

$$= -\log(-2i) - \pi i\tau - \sum_{r=1}^{\infty} \frac{1}{r} e^{2\pi i r\tau}.$$

Page 56, Line -1

There is a sign error on the right-hand side. It should read

$$\frac{d^{2k}}{d\tau^{2k}} \log(\sin \pi\tau) = - \sum_{r=1}^{\infty} (2\pi i)^{2k} r^{2k-1} e^{2\pi i r\tau}.$$

Page 59: Displayed equation in middle of page

The formula for E_6 should use σ_5 , not σ_4 . Thus

$$E_6(\tau) = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n.$$

Page 60, Proof of Part (b)

It might be worth mentioning that the reciprocal of a power series with constant term 1 and integer coefficients is a power series with integer coefficients. (Could make this an exercise: Let R be a ring and let $f(X) \in R[[X]]$ be a power series. Prove that $(1 + Xf(X))^{-1} \in R[[X]]$.)

Page 60: Line -6 (and elsewhere)

“Apostel” should be “Apostol”, here and elsewhere (including page 62, line 10; page 67, lines 9 and 14; page 484, lines -14, -2, -1).

Page 61: Conjecture 7.6

Could also describe the conjecture of Atkin and Serre that for every $\epsilon > 0$,

$$\tau(n) \gg_{\epsilon} \sigma_0(n)n^{(9/2)-\epsilon}.$$

See Serre, J.-P., Divisibilité de certaines fonction arithmétiques, *L'Ens. Math.* **22** (1976), 227–260, especially equation 4.11.

Page 64: Lines 3–12 (second paragraph plus one line)

Replace this material, which reads “Now it’s time to ...to compute” with the following material:

In order to compute the values of the derivatives in this expression, we take the transformation formula (5.4c) for $\sigma(z, \tau)$ and differentiate it with respect to z . This gives

$$\sigma'(z + \omega, \tau) = \psi(\omega)\eta(\omega)e^{\eta(\omega)(z + \frac{1}{2}\omega)}\sigma(z) + \psi(\omega)e^{\eta(\omega)(z + \frac{1}{2}\omega)}\sigma'(z) \quad \text{for all } \omega \in \mathbb{Z}\tau + \mathbb{Z}.$$

Now put $z = 0$ and use the fact that $\sigma(0) = 0$ and $\sigma'(0) = 1$ to get $\sigma'(\omega) = \psi(\omega)e^{\omega\eta(\omega)/2}$. Taking $\omega = 1$, $\omega = \tau$, and $\omega = \tau + 1$ in succession yields

$$\sigma'(1) = -e^{\eta(1)/2}, \quad \sigma'(\tau) = -e^{\tau\eta(\tau)/2}, \quad \text{and} \quad \sigma'(\tau + 1) = -e^{(\tau+1)\eta(\tau+1)/2}.$$

Next we use Legendre’s relation (5.2d), which in our situation reads $\tau\eta(1) - \eta(\tau) = 2\pi i$, to eliminate $\eta(\tau)$. After some algebra we obtain

$$\sigma'(1) = -e^{\frac{1}{2}\eta}, \quad \sigma'(\tau) = -e^{\frac{1}{2}\eta\tau^2}q^{-\frac{1}{2}}, \quad \text{and} \quad \sigma'(\tau + 1) = -e^{\frac{1}{2}\eta(\tau+1)^2},$$

where to ease notation we write $\eta = \eta(1)$.

The next step is to use the product expansion (6.4) for σ to compute σ at the half periods. Thus

Page 64: Line –8 and –6

There are missing fourth powers in these lines. Thus on line –8,

$$\sigma\left(\frac{\tau}{2}, \tau\right)^4 = \cdots q^{-1}(1 - q^{\frac{1}{2}})\cdots \quad \text{should be} \quad \sigma\left(\frac{\tau}{2}, \tau\right)^4 = \cdots q^{-1}(1 - q^{\frac{1}{2}})^4 \cdots$$

and on line –6,

$$\sigma\left(\frac{\tau + 1}{2}, \tau\right)^4 = \cdots q^{-1}(1 + q^{\frac{1}{2}})\cdots \quad \text{should be} \quad \sigma\left(\frac{\tau + 1}{2}, \tau\right)^4 = \cdots q^{-1}(1 + q^{\frac{1}{2}})^4 \cdots$$

Page 71, Lines 12 and 13

On line 12 it says “fix an oriented basis $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ for Λ ,” while on line 13 it says “fix an oriented basis ω'_1, ω'_2 for Λ' .” Thus using two different notations for a “basis”. The second is more standard. (Both notations are used elsewhere, for example Lemma 1.2, Lemma 9.3, and Proposition 9.4.)

Page 73, First displayed equation (line 4)

The second matrix should be $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, so the entire line should read

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b + td \\ 0 & d \end{pmatrix}.$$

Page 73: Third displayed equation (line 12)

The $ad/a'd'$ should be flipped, so the full line should read

$$a = a'p, \quad d = d's, \quad ps \frac{a'd'}{ad} = 1, \quad a, d, a', d' > 0.$$

Page 77: Line –6

$T_{12}\Delta$ should be $T_{12}(n)\Delta$.

Page 81: Line 16

Change “distinct divisors of n ” to “positive divisors of n ”

Page 81: Remark 11.2.1

Need to specify that the cusp form is a normalized eigenform. So replace the phrase

“The Fourier coefficients of a cusp form of weight $2k$ actually satisfy the stronger estimate”

with the phrase

“Let $f(\tau) = \sum c(n)q^n$ be a normalized cusp form of weight $2k$ which is a simultaneous eigenfunction for all Hecke operators $T_{2k}(n)$. Then the Fourier coefficients of f actually satisfy the stronger estimate”

Need to specify that the cusp form is normalized (i.e., has leading coefficient $c(1) = 1$).

Page 81: Remark 11.2.2

There’s a missing period after “See exercise 1.24”

Page 82, Third displayed equation (line 7)

The sum inside the limit should be

$$\sum_{n \geq 1} c(n)e^{2\pi in\tau}.$$

(There’s a missing “ n ” in the exponent.)

Page 82, Line 9

“It follows that f is bounded on \mathcal{F} ” should be “It follows that ϕ is bounded on \mathcal{F} ”.

Page 84: Line –8

“fuctional” should be “functional”

Page 88, Exercise 1.13

It has been suggested that both sums should be over $(m, n) \neq (0, 0)$, rather than over (m, n) with $m \neq 0$.

Page 92, Exercise 1.25(a)

The reference to (7.2.1) should be to (7.3.1).

Page 93: Exercise 1.27

Replace the first line with

“Let $f(\tau)$ be a cusp form of weight $2k$ with k an even integer.”
(If k is odd, then $L(f, k) = 0$ from the functional equation.)

Page 93: Exercise 1.28

The first displayed equation should be

$$\chi : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \mathbb{C}^*$$

and after the next phrase “be a primitive Dirichlet character”, add the words “and extend χ to \mathbb{Z} by setting $\chi(p) = 0$.”

Page 93: Line –1

The functional equation should read

$$R(f, \chi, s) = (-1)^k \chi(-1) R(f, \bar{\chi}, 2k - s).$$

(The $\chi(-1)$ is missing.)

Page 94, Line 4

The definition of $f(\tau)$ should be

$$f(\tau) = \sum_{n \geq 1} a_n e^{2\pi i n \tau / \lambda}.$$

(There is a missing “ n ” in the exponent.)

Page 108: Line 7

$[\mathbb{Q}(\alpha) : \mathbb{Q}]$ should be $[\mathbb{Q}(\beta) : \mathbb{Q}]$.

Page 110: Lines 3 and 8

Replace the script oh (\mathcal{O}) with an italic oh (\mathcal{O}).

Page 112: Last displayed equation

The Galois group action is a left action, despite the fact that it’s written using superscript notation. So this displayed equation should read

$$(\sigma\tau) * E = E^{\sigma\tau} = (E^\tau)^\sigma = (F(\tau) * E)^\sigma = F(\sigma) * (F(\tau) * E) = (F(\sigma)F(\tau)) * E.$$

Further, the line on the top of page 113

“(Note that ... abelian group.)”

should be replaced with the remark that

“(Note that $\text{Gal}(\bar{K}/K)$ acts on the left.)”

Page 113: Line –5

The matrix A should be $n \times m$, not $m \times n$.

Page 114: Line –1

The cokernel should be $\Lambda^m / {}^t A \Lambda^n$. (The m and n are reversed.)

Page 115: Line 10

The cokernel should be $\Lambda^m / {}^t A \Lambda^n$. (The m and n are reversed.)

Page 116: Lines –11 to –4

Delete these lines “Thus $\sigma_{\mathfrak{p}} \in \text{Gal}(L/K)$ is uniquely . . . has positive \mathfrak{P} -adic valuation” and replace them with:

Thus $\sigma_{\mathfrak{p}} \in \text{Gal}(L/K)$ is uniquely determined by the condition

$$\sigma_{\mathfrak{p}}(x) \equiv x^{N_{\mathbb{Q}}^K \mathfrak{p}} \pmod{\mathfrak{P}} \quad \text{for all } x \in R_L.$$

Page 118: Theorem 3.2(b)

The kernel of the Artin map is actually the intersection of $(N_K^L I_L)P(\mathfrak{c}_{L/K})$ with $I(\mathfrak{c}_{L/K})$.

Page 120: Theorem 3.5

The characterization of the reciprocity map $s \mapsto [s, K]$ is not correct. For a finite abelian extension L/K , define a subgroup of A_K^* by

$$V_{L/K} = \{s \in A_K^* : \text{for all } \mathfrak{p} \mid \mathfrak{c}_{L/K} \text{ we have } s_{\mathfrak{p}} \in R_{\mathfrak{p}} \text{ and } s_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{c}_{L/K} R_{\mathfrak{p}}}\}.$$

Then the reciprocity map is characterized by the following two properties:

- (a) $[\alpha, K] = 1$ for all $\alpha \in K^*$, i.e., the reciprocity map is trivial on principal ideles.
- (b) For all finite abelian extensions L/K , we have

$$[s, K]|_L = ((s), L/K) \quad \text{for all } s \in V_{L/K}.$$

(More precisely, this is true if K has no real embeddings, which is the case we need. In general, if there are real places v of K that ramify in L , the definition of the set $V_{L/K}$ should include the additional condition that $s_v > 0$.)

Page 121: Line –6

Add the sentence:

“Note that the kernel of F is actually a finite quotient of $\text{Gal}(\bar{K}/K)$, since any E will be defined over some finite extension L/K , and then $F(\sigma) = 1$ for $\sigma \in \text{Gal}(\bar{K}/L)$.” at the beginning of the line. (This is just before the sentence “Since $\mathcal{C}\mathcal{L}(R_K)$ is an abelian group. . .”.)

Page 121: Line –4

The book refers to a “Frobenius element,” but really $\sigma_{\mathfrak{p}} \in \text{Gal}(K^{\text{ab}}/K)$ is only well-defined up to an element of the inertia group, since K^{ab}/K is ramified at \mathfrak{p} . This doesn’t affect the proofs because Proposition 4.2 gives a set of primes to omit which will include the ramified primes. But this should be explained more carefully.

Page 124,125: Reduction of maps

The book talks about the “natural reduction map” on isogenies, but reduction is never really carefully defined. The proof just assumes that there is a reduction map with various properties (group homomorphism, compatible with composition and evaluating/reduction of points, pullback of differential, action of Galois on points over unramified extensions and action of Galois on points of reduction, compatibility with the Weil pairing and formation of dual isogenies).

There are two ways to do all of this carefully. The first is to say that (almost) all of these properties are immediate consequences of the fact that an elliptic curve with good reduction is already a Néron model. Then add a short section in Chapter IV proving the necessary properties of reduction, and in Chapter II add a brief comment detailing the difficulties and referring the reader to Chapter IV.

The second approach is to do explicit computations on the minimal Weierstrass equation. In some sense, this means proving some of the Néron properties for E , but much of it can be done completely explicitly. For example, one can explicitly construct the functions used in the definition of the Weil pairing and show that they reduce properly. Similarly, suppose that E and E' have good reduction and that $\phi : E \rightarrow E'$ is an isogeny over K . Write ϕ out explicitly using homogeneous polynomials with coefficients in R . Then it should be possible to show directly that the reduction of ϕ gives at least a rational map on the special fiber. (Scheme theoretically, this reflects the fact that ϕ is a rational map $E/R \rightarrow E'/R$, and E and E' are regular, so ϕ is defined off of a set of codimension 2. In particular, it gives a well-defined rational map $\tilde{\phi}$ on the special fibers, and then $\tilde{\phi}$ is a morphism since the fibers are non-singular curves.)

Page 135: Proof of Theorem 5.6

I have made the implicit assumption that L/K is abelian. This is certainly not clear. There are two alternatives.

(1) Give a direct proof that L/K is abelian. It's clear, for example, that the field $K(j(E), E[\mathfrak{c}])$ is abelian over $K(j(E))$, since the Galois group injects into $\text{Aut}(E[\mathfrak{c}]) \cong (R/\mathfrak{c})^*$. Give a similar proof for L/K .

(2) In section II.3, state and give a reference for the fact that an arbitrary field extension is determined by a density 1 subset of the split primes. Then in the proof of theorem 5.6, let $L' = K(j(E), E[\mathfrak{c}])$. Choose a prime \mathfrak{P} in L lying over \mathfrak{p} and a prime \mathfrak{P}' in L' lying over \mathfrak{P} . Then the Artin symbol notation will involve these primes.

Page 149: Lines 17 and 20

Remove line 17, which reads

$$= \text{the maximal abelian quotient of } I_v.$$

(Be sure to put a period at the end line 16.)

On line 20, replace

“ I_v acts through its maximal abelian quotient I_v^{ab} ”

with just

“ I_v acts through the quotient I_v^{ab} .”

Page 160: Line 1

The automorphism σ should act trivially on K . Thus σ should be in $\text{Aut}(\mathbb{C}/K)$, not in $\text{Aut}(\mathbb{C}) = \text{Aut}(\mathbb{C}/\mathbb{Q})$.

Page 168: Line -9

(Definition of W_m) The condition on $s_{\mathfrak{p}}$ should be $s_{\mathfrak{p}} \equiv 1 \pmod{mR_{\mathfrak{p}}}$, not $\pmod{m\mathfrak{p}}$.

Page 168: Line -6

Delete the words “and has finite index”.

Page 169: Line 5

This condition should read “ $(N_L^K x)_{\mathfrak{p}} \in (1 + mR_{\mathfrak{p}}) \cap R_{\mathfrak{p}}^*$ for all \mathfrak{p} ” instead of “ $\in 1 + m\mathfrak{p}$.”

Page 169: Line -14

Delete the words “and has finite index”.

Page 173: Theorem 10.3

Replace the last sentence

“Then $L(s, \psi)$ has an analytic $\dots N = N(\psi)$.”

with the following:

“Then $L(s, \psi)$ has an analytic continuation to the entire complex plane. Further, there is a functional equation relating the values of $L(s, \psi)$ and $L(N - s, \bar{\psi})$ for some real number $N = N(\psi)$.”

Page 174: Proposition 10.4

In line 5, the Grössencharacter takes its values in \mathbb{C} . Replace $\psi_{E/L} : \mathbf{A}_L^* \rightarrow K^*$ with $\psi_{E/L} : \mathbf{A}_L^* \rightarrow \mathbb{C}^*$.

Page 175: Proposition 10.5(a)

The Grössencharacter takes its values in \mathbb{C} . Replace $\psi_{E/L} : \mathbf{A}_L^* \rightarrow K^*$ with $\psi_{E/L} : \mathbf{A}_L^* \rightarrow \mathbb{C}^*$.

Page 176: Proposition 10.5(b)

The Grössencharacter takes its values in \mathbb{C} . Replace $\psi_{E/L'} : \mathbf{A}_{L'}^* \rightarrow K^*$ with $\psi_{E/L'} : \mathbf{A}_{L'}^* \rightarrow \mathbb{C}^*$.

Page 176: Corollary 10.5.1(ii)

In the functional equation for the case that $K \not\subset L$, the exponent of the norm of the different should be $s/2$, not s .

Page 180: Exercise 2.15

The field should be $K = \mathbb{Q}(\sqrt{-2})$, not $K = \mathbb{Q}(\sqrt{2})$.

Page 181: Exercise 2.18(f)

There's a missing $\log(n)$. Thus the problem should be to prove that

$$\lim_{n \rightarrow \infty} \frac{\log |\Phi_n|}{(\deg \Phi_n)(\log n)} = 6.$$

Page 183: Exercise 2.24(b)

The formula in part (b) of this exercise is completely incorrect. The simplest example is an isogeny of degree 2 as described in Example III.4.5 on page 74 of [AEC]. For that map,

$$\phi(x, y) = (R(x), cyR'(x)) \quad \text{with } R(x) = x + a + b/x \text{ and } c = -1.$$

The discriminants are $16b^2(a^2 - 4b)$ and $256b(a^2 - 4b)^2$.

Change this exercise as follows:

(b) Show that there is a commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{z \mapsto c^{-1}z} & \mathbb{C}/\Lambda' \\ \downarrow & & \downarrow \\ E(\mathbb{C}) & \xrightarrow{\phi} & E'(\mathbb{C}) \end{array}$$

where the vertical maps are complex analytic isomorphisms and c is the number from part (a).

(c) If the map ϕ is an isomorphism, prove that the constant c in (a) satisfies

$$c^{12} = \frac{\Delta_{E'}}{\Delta_E}.$$

Page 183: Exercise 2.25

Given the correspondence between twists and cocycles in [AEC], it looks like the relation should be

$$\psi_{E \times / L} = \chi^{-1} \psi_{E/L}.$$

Page 183: Exercise 2.27

The definition of the zeta function should not have a minus sign. Thus

$$Z(\tilde{E}/\mathbb{F}_{\mathfrak{P}}) = \exp\left(\sum_{n=1}^{\infty} \#\tilde{E}(\mathbb{F}_{\mathfrak{P},n}) \frac{T^n}{n}\right).$$

Page 184: Exercise 2.30

New part (a). Prove that \mathfrak{P} is unramified in L' .

Relabel parts (a),(b),(c) to be parts (b),(c),(d).

Part (d) (old part (c)) is not quite correct. Replace it with the following:

(d) Let \tilde{E} be the reduction of E modulo \mathfrak{P} , and let p be the residue characteristic of \mathfrak{P} . Prove that

$$\tilde{E} \text{ is } \begin{cases} \text{ordinary} & \text{if } \mathfrak{P} \text{ splits in } L' \text{ and } p \text{ splits in } K, \\ \text{supersingular} & \text{if } \mathfrak{P} \text{ is inert in } L' \text{ and } p \text{ does not split in } K \end{cases}$$

Page 186: Exercise 2.35(c)

The second displayed equation should have double brackets for the R_p . Thus it should read $R_p \llbracket \text{Gal}(L_p/L') \rrbracket$ instead of $R_p [\text{Gal}(L_p/L')]$.

Page 186: Exercise 2.36(d)

In the last sentence, there should be double brackets for the \mathbb{Z}_p . Thus $\mathbb{Z}_p \llbracket \Gamma \rrbracket$ instead of $\mathbb{Z}_p[\Gamma]$.

Page 195: Line 5

There is a period missing after “is a finite subgroup of K^*/K^{*m} ”

Page 216: Line –5

Replace $(x_1 - x_2)^2$ with $\pi_t((x_1 - x_2)^2)$.

Page 227: Line 12

There is extra space between the word “infinite” and the period at the end of the sentence.

Page 228: Last two displayed equations

The points in $\phi^*((x, y), t)$ are in $\Gamma \times C$, so it makes no sense to write them as $((x'_i, y'_i), t)$. Instead just write them as (γ_i, t) . There are three displayed equations (with one line in between) that need to be changed. Thus the material at the bottom of page 228 should read:

$$\begin{aligned} \psi : \quad \mathcal{E}^0 &\longrightarrow E_0 \times C, \\ ((x, y), t) &\longmapsto \left(\sum_{i=1}^m \phi(\gamma_i, t_0), t \right) \end{aligned}$$

where the points γ_i are determined by the formula

$$\phi^*((x, y), t) = \sum_{i=1}^m (\gamma_i, t).$$

The displayed equation in the middle of page 229 should read:

$$\psi((x, y), t_0) = \left(\sum_{(\gamma, t_0) \in \phi^*((x, y), t_0)} \phi(\gamma, t_0), t_0 \right) = (m(x, y), t_0).$$

Page 229: The five lines after the displayed equation

This argument is incorrect. We can't vary t_0 , since that would have the effect of changing to a different map ψ . Replace these five lines with the following: Thus $\psi : \mathcal{E}_{t_0} \rightarrow E_0 \times \{t_0\}$ is just the multiplication-by- m map on E_0 . In particular, since the multiplication-by- m map is surjective, we see that $\psi(\mathcal{E}^0)$ contains $E_0 \times \{t_0\}$. This implies that the rational map $\mathcal{E} \rightarrow E_0 \times C$ is dominant, since otherwise the irreducibility of $\psi(\mathcal{E}^0)$ would imply that $\psi(\mathcal{E}^0) = E_0 \times \{t_0\}$, contradicting the fact that $\psi(\mathcal{E}^0)$ maps onto C (i.e., $\psi(\mathcal{E}^0)$ must contain at least one point on each fiber of $\Gamma \times C \rightarrow C$).

Page 236: Definition of fibered surface

The definition of fibered surface needs to be modified. For example, we could take $S = \mathbb{P}^1 \times \mathbb{P}^1$, $C = \mathbb{P}^1$, and $\pi(x, y) = x^2$. Then (most) fibers are disconnected, which we don't want to allow. One way to fix it would be to require that $\pi^*K(C)$ be algebraically closed in $K(S)$.

Page 239: Line 9

“Proposition 8.1 tells us” should be “Lemma 8.1 tells us”.

Page 242: Figure 3.3

There is an extraneous “3” above the “t”.

Page 244: Line 17

“it is possible eliminate one” should be “it is possible to eliminate one” (missing “to”).

Page 255: Lines –9 and –8

The divisor in the displayed equation is the divisor of the pullback of the function u_Γ , not $\phi^*\Gamma$. The displayed equation and the following line should read as follows:

$$\phi^*\Gamma = \sum_{\Delta \subset \phi^{-1}(\Gamma)} \text{ord}_\Delta(u_\Gamma \circ \phi)\Delta,$$

where the sum is over all irreducible divisors Δ contained in $\phi^{-1}(\Gamma)$ and we are writing . . .

Page 257: Definition of very ample

The definition of *very ample* currently says that $D = \phi^*H$. This should be changed to say that $D \sim \phi^*H$, i.e., D is linearly equivalent to ϕ^*H .

Page 258: Proof of Lemma 10.4

Delete the second sentence, which reads “In other words, $D = \phi^*H$ and $D = \psi^*H'$ for appropriately chosen hyperplanes in \mathbb{P}^r and \mathbb{P}^s respectively.” This statement is incorrect, but its deletion will not affect the validity of the remainder of the proof. Note that it is true that there is a divisor class associated to any morphism $\phi : V \rightarrow \mathbb{P}^r$, but it is not true that every divisor in that divisor class has the form ϕ^*H for some hyperplane H . This will only be true if ϕ corresponds to a complete linear system.

Page 259: Line –12

“Nullstellentsatz” should be “Nullstellensatz”.

Page 259: Line –7

$A(T_0, \dots, T_r)$ should be $A_j(T_0, \dots, T_r)$ (missing subscript).

Page 271: Theorem III.11.4

This should read

$$\sigma_t : E(K) \rightarrow \mathcal{E}_t(\bar{k}) \text{ is injective for all } t \in C(\bar{k}) \text{ satisfying } h_\delta(t) \geq c.$$

(The inequality on the $h_\delta(t) \geq c$ is reversed.)

Page 277: Line –13

Need to say that n is the degree of f . So this line should read:

ring of S -integers of K , and let $f(x) \in R[x]$ be a monic polynomial of degree n with

Page 277: Last displayed formula

It should be $y^{2(n-1)}$ instead of y^4 . So the formula should read

$$h(y^{2(n-1)}/\Delta) \leq 4n(n-1) \max\{2g-2 + \#S, 0\}.$$

Page 277: Line –5

It should be $y^{2(n-1)}$ instead of y^4 . So the line should read

Remark 12.3.1. The bound in (12.3) is stated for $y^{2(n-1)}/\Delta$ because this

Page 280: Exercise 3.10

Need to specify for this exercise that k is algebraically closed. Otherwise the condition in (i) that “ c_6 is a sixth power in $k(C)$ ” needs to be replaced with “ c_6 is the product of a sixth power in $k(C)$ times an element of k ”, and similarly for the other parts.

Page 281: Exercise 3.15(a)

There is a missing period at the end of this part of the exercise.

Page 284: Exercise 3.26(b)

This exercise is correct, but not interesting, since $P \mapsto \text{class } \Phi_{P,Q}$ is in fact a one-coboundary from $E(K)$ to $\text{Pic}(\mathcal{E})$. What the problem should ask is to prove that this map is a one-cocycle from $E(K)$ to the subgroup of $\text{Pic}(\mathcal{E})$ generated by fibral divisors.

Page 285: Exercise 3.32

The reference to Hartshorne should be [1, exercise V.1.7], not [1, exercise 1.7]. Also, it is a “generalization of (10.2)”, not a generalization of (10.3).

Page 285: Exercise 3.33

This exercise is not correct. A good first step is to prove that

$$\lim_{n \rightarrow \infty} \frac{1}{n^2} h_\beta([n]P) = (\deg \beta) \hat{h}(P) \quad \text{for all } \beta.$$

Then (a) needs to be modified as follows:

(a) If the divisor β is symmetric, that is, if $[-1]^*\beta = \beta$, prove that there is a constant C_β such that

$$\lim_{n \rightarrow \infty} \frac{1}{n^2} h_\beta([n]P) = \hat{h}_\beta(P) - C_\beta.$$

(More precisely, show that $C_\beta = \sum b_i \hat{h}(P_i)$.)

Also, the formula in (b) is off by a factor of 2, it should read

$$\lim_{n \rightarrow \infty} \frac{1}{n} h_\beta([n]P) = 2\hat{h}_\beta(P).$$

Finally, the inequality in (c) needs an $O(1)$ on the right-hand side. This can be absorbed in the constant c by replacing the stated inequality with

$$|\hat{h}_\beta(P)| \leq c\sqrt{\hat{h}(P) + 1} \quad \text{for all } P \in E(\bar{k}).$$

Page 285: Exercise 3.34

The formula needs an $O(1)$ on the right-hand side. This can be absorbed into the big-Oh term by replacing the stated equality with

$$\langle P_t, Q_t \rangle_t = \langle P, Q \rangle \hat{h}_C(t) + O\left(\sqrt{\hat{h}_C(t) + 1}\right).$$

Page 286: Exercise 3.35(e)

The example in this part of the exercise is not correct. It is easy to check that

$$\text{ord}_t \mathcal{D}_{E/K} = n_t = \begin{cases} 0 & \text{if } \text{ord}_t(u) \text{ is even,} \\ 6 & \text{if } \text{ord}_t(u) \text{ is odd.} \end{cases}$$

However, for the two points at infinity on C , call them $\pm\infty$, we have $\text{ord}_{\pm\infty}(u) = -1$. So for the given example we have $\mathcal{D}_{E/K} = 6(\infty) + 6(-\infty)$.

If we change the equation of C to $v^2 = u^3 - 7u^2 + 6u$, then C has only one point ∞ at infinity, and that point satisfies $\text{ord}_\infty(u) = 2$, so with the new curve C we do have $\mathcal{D}_{E/K} = 0$. However, if we change C in this way, then part (f) of the exercise is no longer correct.

Page 288: Exercise 3.38

Might be worth saying explicitly that the characteristic is different from 2, although in this chapter, there is a blanket assumption that we are working in characteristic zero.

Page 288: Exercise 3.40(b)

Actually, $E(K)_0$ cannot contain a point of exact order 6, so only $m = 2$ and $m = 3$ are possible.

Page 290: Line –9

Change “covention” to “convention”

Page 292: Line 3

Change $\mu(O_G) = O_H$ to $\phi(O_G) = O_H$.

Page 301: Lines 7,8

There is a bad line break at $(\mathcal{E} \times_C \mathcal{E})(k)$.

Page 309: Line –7

The final $(\phi \times 1)$ in this displayed equation should be $(\phi \times \pi_T)$. Thus the entire line should read

$$\phi * (\sigma_0 \circ \pi_T) = p_1 \circ (1 \times \pi_T) \circ (\phi \times 1) \circ \delta_T = p_1 \circ (\phi \times \pi_T) \circ \delta_T = \phi.$$

Page 310: Line –7

“a group group scheme”

Page 313: Line 4

“is generated x, y, y , and 2” should be “is generated by x, y , and 2”

Page 315: Line –10

We cannot necessarily write $\mathfrak{p} = tR$, since R is just a Dedekind domain. Instead, say that we choose an element $t \in R$ satisfying $\text{ord}_{\mathfrak{p}}(t) = 1$.

Page 318: Line 1

“is an R -isomorphism” should be “is an R -morphism”.

Page 331: Proposition 6.1

The text says “choose an ideal \mathfrak{p}^s of K^s .” Of course, what is meant is that one should choose an ideal \mathfrak{p}^s of R^s ,” but it’s a fairly standard convention that this is what is meant.

Page 339: Line 21

“a uniformizer for Γ ” should be “a uniformizer for Γ ” (missing i in uniformizer)

Page 341: Theorem 7.2(ii)

“with D_1 is linearly” should be “with D_1 linearly”

Page 348: Line 5

“we must to set” should be “we must set”

Page 348: Line –5

“along entire curve” should be “along the entire curve”

Page 355: Line –5

“so after we may also assume” should be “so after further relabeling we may also assume”

Page 367: Line –11

“If $P\pi \neq 2$, then” should be “If $p \neq 2$, then”.

Page 370, First displayed equation

In the formula for \mathcal{W}' , the third term should be $a_{3,1}\pi'$, not $a_{3,1}x'$.

Page 370, Last line

The last line on page 370 states “this substitution leaves the other a_i ’s ... unchanged.” In fact a_4 is changed, but one still has $\pi \mid a_4$, which is what one needs in the next step.

Page 371, Line 10

In the equation for \mathcal{W}' , the term $a_{3,1}x'$ should be $a_{3,1}\pi'$.

Page 371, Definition of the conductor

In the definition of the wild part of the conductor, probably the prime ℓ should be chosen to satisfy $\ell \geq 3$. Alternatively, one can probably take $\ell = 4$ with an appropriate definition of dimension.

Page 383: Lines –12 and –11

“Let ℓ be a prime dividing m ” should be “Let ℓ be the largest prime dividing m ” (Otherwise if $2 \parallel m$ and we took $\ell = 2$, then it would not be true that ℓ' divides m .)

Page 388: Szpiro’s Conjecture 10.6

The displayed equation should have a constant $c(K, \epsilon)$ instead of $c(E, \epsilon)$. Thus it should read

$$N_{\mathbb{Q}}^K(\mathcal{D}_{E/K}) \leq c(K, \epsilon) N_{\mathbb{Q}}^K(\mathfrak{f}_{E/K})^{6+\epsilon}.$$

Page 397: Exercise 4.6(b)

The reference should be to “(2.9)”, not to “(2.9b)”.

Page 397: Line –2

“as in (b)” should be “as in (b)”. (The “b” should be in roman font, not italic.)

Page 398: Exercise 4.12(c)

It looks like these two schemes are isomorphic. Thus let

$$G_0 = \text{Spec } R[x, y]/(x^2 - 1)$$

with group law

$$((x_1, y_1), (x_2, y_2)) \mapsto (x_1x_2, x_1y_2 + x_2y_1),$$

and let

$$\mathbb{G}_a \times \mu_2 = \text{Spec } R[S] \times \text{Spec } R[T]/(T^2 - 1).$$

Then the maps $(S, T) \mapsto (xy, x)$ and $(x, y) \mapsto (T, ST)$ give isomorphisms of group schemes.

Page 399: Exercise 4.20

This exercise is not correct as stated. It is true if $v(a_6) > 0$. In general, the exercise should include the further assumption that $a_1^6 + 432a_6 \in R^*$. And with that assumption, it’s probably not necessary to also assume that $a_1 \in R^*$.

Page 402: Exercise 4.32

In the first line, there's too much space after the comma, before the word “compute”

Change the phrase “deleting the last row and column” to “deleting a row and column corresponding to a multiplicity-1 component”

Change the phrase “is equal to the number of” to “is equal to plus or minus the number of”

Page 404: Line –2

“finitely many elliptic curve” should be “finitely many elliptic curves”

Page 407: Exercise 4.15(c)

This exercise is not correct. It is possible to get different types of reduction when $v_K(3) = 2$. For example, take $K = \mathbb{Q}_3(\sqrt{-3})$ and $E : y^2 + \sqrt{-3}$. Then $v_K(3) = 2$ and E has Type II* reduction.

Page 415: Proposition 2.2

The text reads **PropositionWithPart 2.2**. Remove “WithPart.”

Page 418: Line –4

The displayed equation should be

$$c_4(q) = u^4(12g_2(\tau)) \quad \text{and} \quad c_6(q) = u^6(216g_3(\tau)).$$

Page 418: Line –3

Replace “ $u = 2\pi i$ ” with “ $u = (2\pi i)^{-1}$ ”. Also rather than saying that this is irrelevant, might be better to say that the exact value of u doesn't matter, but it is important that u is independent of τ .

Page 420: Line –2

The formula for the isomorphism when $q < 0$ is incorrect. The correct formula is

$$u \mapsto \frac{1}{2} \left(\frac{\log |u|}{\log |q|} + \frac{1 - \text{sign}(u)}{2} \right) \pmod{\mathbb{Z}}.$$

Page 422: Chapter V, Section 2

Add a Remark 2.5 mentioning Alling [1] and the following two articles as sources for further information about elliptic curves over \mathbb{R} :

Bochnak, J., Huisman, J., When is a complex elliptic curve the product of two real algebraic curves?, *Math. Ann.* **293** (1992) 469–474.

Huisman, J., The underlying real algebraic structure of complex elliptic curves, *Math. Ann.* **294** (1992), 19–35.

Page 423: Theorem 3.1

In the first displayed equation, it should be “ $a_4(q) = -5s_3(q)$ ”.

Page 424: Remark 3.1.2

Replace with the following:

Theorem 3.1 is actually true for any field K that is complete with respect to a non-archimedean absolute value. The only time we will use the fact K is a finite extension of \mathbb{Q}_p will be in the proof that the map ϕ in (3.1c) is surjective. (In fact, we will really only need the fact that the absolute value is discrete, so our proof actually is valid somewhat more generally, for example over the completion of \mathbb{Q}_p^{nr} .) For a proof of Theorem 3.1 in the most general setting, using p -adic analytic methods, see Roquette [1].

Page 427: Line –17

The second equation in the display has a misplaced minus sign, the minus sign should go outside of the parentheses. The formula should read

$$(x_2 - x_1)y_3 = -((y_2 - y_1) + (x_2 - x_1))x_3 - (y_1x_2 - y_2x_1).$$

Page 430: Line 9

Replace “Robert [1] and Roquette [1]” with “Robert [1], Roquette [1], and Tate [9].” (Replace the old unpublished manuscript Tate [9] by a reference to its published version.)

Page 430: Line –10

Might be a good idea to point out that the equation for E_q is minimal, since its reduction modulo \mathfrak{M} is $y^2 + xy = x^3$.

Page 434: Line –9

All we know is that q/π^N is a unit, not that it is congruent to 1. So this displayed equation should read

$$y_n^2 + x_n y_n \equiv (-q/\pi^{2n}) \not\equiv 0 \pmod{\pi}.$$

Page 435: Line 3

In the subscript on the union, make the inequality strict. Thus

$$E_q(K) = E_{q,0}(K) \cup W \cup \bigcup_{1 \leq n < \frac{1}{2} \text{ord}_v q} (U_n \cup V_n).$$

Page 438: Lemma 5.1

Replace the second sentence

“Then there is a unique $q \in \mathbb{Q}_p(\alpha)^*$ with $|q| < 1$ such that $j(E_q) = \alpha$.”

with the sentence

“Then there is a unique $q \in \bar{\mathbb{Q}}_p^*$ with $|q| < 1$ such that $j(E_q) = \alpha$. This value of q lies in $\mathbb{Q}_p(\alpha)$.”

Page 440: Line 14

(Fourth line of proof) Change “for some $u \in K^*$ ” to “for some $u \in \bar{K}^*$ ”.

Page 441: Theorem 5.3(a)

Replace this part with:

“There is a unique $q \in \bar{K}^*$ with $|q| < 1$ such that E is isomorphic over \bar{K} to the Tate curve E_q . Further, this value of q lies in K .”

The first line of the proof should also be changed.

Page 447: Line –12

“for all $\psi \in \text{Gal}_{\bar{K}/K}$ ” should be “for all $\psi \in G_{\bar{K}/K}$ ”.

Page 449: Exercise 5.4(a)

Replace

“If $b < 0$, prove that ...”

with

“If $\Delta(E) > 0$, so in particular if $b < 0$, prove that ...”.

Further, the homogeneous space C is incorrect, it should be

$$C : w^2 = 4bz^4 - (1 + az^2)^2.$$

Page 450: Exercise 5.6(b)

The last line should be

$$\gamma(E/\mathbb{R}) = \text{sign}(1 - t).$$

instead of $\text{sign}(t - 1)$. (Notice that $c_6 = -1 + 504s_5(q) \rightarrow -1$ as $t \rightarrow \infty$.)

Page 451: Exercise 5.10(a)

“If E_q and E'_q ...” should be “If E_q and $E_{q'}$...”. (The prime is on the q , not on the E .)

Page 451: Exercise 5.10(b)

Replace

“homomorphisms from $K^*/q^{\mathbb{Z}}$ to $K^*/q'^{\mathbb{Z}}$ ”

with

“homomorphisms from $\bar{K}^*/q^{\mathbb{Z}}$ to $\bar{K}^*/q'^{\mathbb{Z}}$ ”.

Page 451: Exercise 5.11

Replace “consider the quadratic extension” with “consider the field”, since could have $L = K$.

Page 452: Exercise 5.13(a)

Replace “for each prime ℓ there is” with “for each prime $\ell \neq p$ there is”.

Page 453: Exercise 5.15(b)

In the Hint, replace

“Take Tate models $E = E_q$ and $E' = E_{q'}$ ”

with

“Take Tate models E_q and $E_{q'}$ ”.

(Note may need to go to the unramified quadratic extension of \mathbb{Q}_p .)

Page 454: Introduction to Chapter VI

At the end of the introduction, add the sentence “For further information about local height functions, see for example Lang [3] and Zimmer [2].”

Page 455: Second displayed equation

The absolute value on $y - y_0$ is missing a v subscript. Thus the line should read

$$U_\epsilon = \{(x, y) \in E(K) : |x - x_0|_v < \epsilon \text{ and } |y - y_0|_v < \epsilon\}, \quad \text{all } \epsilon > 0.$$

Page 462: Second line of last displayed formula

The $+v(\Delta)$ should be $-\frac{1}{4}v(\Delta)$. So this entire line should read

$$= \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v \left\{ 4\lambda_v(P) + v((2y + a_1x + a_3)(P)) - \frac{1}{4}v(\Delta) \right\}$$

Page 463: First paragraph of Section 3

Replace this paragraph with the following: Let K be a field which is complete with respect to an archimedean absolute value $|\cdot|_v$, and let E/K be an elliptic curve. Then K is isomorphic to either \mathbb{R} or \mathbb{C} , and $|\cdot|_v$ corresponds to some power of the usual absolute value. (See [** Get Reference**].) Thus in order to compute the local height function λ over $E(K)$, it suffices to consider the case that $K = \mathbb{C}$, so in this section we will derive explicit formulas for the local height on elliptic curves over the complex numbers.

Page 465: Proposition 3.1(c)

Replace

“is real-analytic away from 0”

with

“is real-analytic and non-vanishing away from 0.”

Page 466: Line 3

Replace

“real-analytic on \mathbb{C} away from Λ ”

with

“real-analytic and non-vanishing on $\mathbb{C} \setminus \Lambda$ ”.

Page 467: Corollary 3.3

Add at the end of the statement of the Corollary:

“(Note that the quantity $(x(P) - x(Q))^6/\Delta$ is well-defined, independent of the choice of a particular Weierstrass equation for E .)”

Page 470: Remark 4.1.1

Replace

“which means that $E_0(K) = E(K)$ and $v(\Delta) = 0$, then our proof will show that the function”

with

“then we can find a Weierstrass equation for E/K with $E_0(K) = E(K)$ and $v(\Delta) = 0$. In this situation, the proof of (4.1) will show that the function”

Also replace

“under finite extension of the field K (1.1c),”

with

“under finite extension of the field K (1.1c) and is independent of the choice of Weierstrass equation (1.1b),”

Page 470: Remark 4.1.2

The displayed equation should read

$$\begin{aligned} \frac{1}{2} \max\{v(x'(P)^{-1}), 0\} + \frac{1}{12} v(\Delta') \\ = \frac{1}{2} \max\{v(u^{-2}x(P)^{-1}), 0\} + \frac{1}{12} v(u^{-12}\Delta). \end{aligned}$$

(There are two changes. The first Δ requires a prime, and the second Δ has a u^{-12} in front.)

Page 472: Line 1

Replace

“where m is the slope of the tangent line to E at P . Thus”

with

“where m is the slope of the tangent line to E at P . (Note that $m \neq \infty$ since $[2]P \neq O$.) Thus”

Page 472: Line 13

The line

$$= 0 \quad \text{since either } v(F_X(P)) = 0 \text{ or } v(F_Y(P)) = 0.$$

should be

$$= 0 \quad \text{since either } v(F_X(P)) \leq 0 \text{ or } v(F_Y(P)) \leq 0.$$

(Change two = signs to \leq signs.)

Page 472: Line -16

Replace the phrase

“If $E_0(K) = E(K)$, that is, if E has good reduction, then”

with

“If $E_0(K) = E(K)$, that is, if E has good reduction and we take a minimal Weierstrass equation for E , then”

Page 472: Line –14

Replace the phrase

“However, even if E has bad reduction,”

with

“However, even if the Weierstrass equation for E has singular reduction,”

Page 474: Line 5

Replace

“This suggests that $v(\theta(u)) - \frac{1}{2}v(u)$ would be”

with

“This suggests that $v(\theta(u)) - \frac{1}{2}v(u) - \frac{1}{12}v(\Delta)$ would be”

Page 479: Exercise 6.8

The value of $\lambda(P)$ is off by $(1/12)v(\Delta)$. Thus the conclusion should read:

$$\lambda(P) = \begin{cases} -\frac{1}{6}v(F_2(P)) + \frac{1}{12}v(\Delta) & \text{if } v(F_3(P)) \geq 3v(F_2(P)), \\ -\frac{1}{16}v(F_3(P)) + \frac{1}{12}v(\Delta) & \text{otherwise.} \end{cases}$$

Page 477: Exercise 6.4(d)

The polynomial F_m is the square of the usual division polynomial, so the quantity $x \circ [m] - x$ in the formula needs to be squared. So it should read

$$F_{m+1}F_{m-1} = (x \circ [m] - x)^2 F_m^2 \quad \text{for all } m \geq 2.$$

Page 479: Exercise 6.9(c)

The value of $\lambda(P)$ is off by $(1/12)v(\Delta)$. Thus the conclusion should read:

$$\lambda(P) = \frac{1}{2} \log|x(P)| - \frac{1}{12} \log|\Delta| + \frac{1}{8} \sum_{n=0}^{\infty} \frac{1}{4^n} \log|z([2^n]P)|.$$

Page 480: Chapter VI New Exercise

Let K be a locally compact field which is complete with respect to an absolute value $|\cdot|_v$. As described in §1, the topology on K can be used to define a topology on E .

- Prove that $E(K)$ is a compact topological space.
- Prove that the negation map $E(K) \rightarrow E(K)$, $P \mapsto -P$, is a continuous map.
- Prove that the group law

$$E(K) \times E(K) \longrightarrow E(K), \quad (P, Q) \longmapsto P + Q$$

is a continuous map.

Page 480: Chapter VI New Exercise

(Hard Exercise) The previous exercise says that $E(K)$ is a compact topological group. Recall that on such a group one can construct a translation invariant measure μ , called *Haar measure*. (See [Paul R. Halmos, *Measure Theory*, GTM 18 Springer, 1978] for basic properties of Haar measure.) Let $\lambda : E(K) \setminus \{O\} \rightarrow \mathbb{R}$ be the local height function (1.1). Prove that

$$\int_{E(K)} \lambda(P) d\mu(P) = 0.$$

(This generalizes exercise 6.5(a).)

Page 480: Chapter VI New Exercise

Continuing with notation from the previous two exercises, normalize the Haar measure on $E(K)$ by the condition $\int_E(K) d\mu = 1$. Now fix a Weierstrass equation for E/K with coordinates (x, y) and discriminant Δ . Prove that λ is given by the integral formula

$$\lambda(Q) = -\frac{1}{12} \int_{E(K)} v \left(\frac{(x(P) - x(Q))^6}{\Delta} \right) d\mu(P).$$

Exercise Reference: G.R. Everest and B. Ni Fhlathuin, The elliptic Mahler measure, *Math. Proc. Camb. Phil. Soc.* 120 (1996), 13–25.

Exercise Solution: Integrate the quasi-parallelogram law (exercise 6.3) and use the translation invariance of μ to cancel most of the terms.

Page 480: Chapter VI New Exercise

Prove the following distribution relations for local heights.

(a) There is a constant C_v such that for all $n \geq 1$ and all points $P \in E(\bar{K})$ satisfying $[n]P \neq O$, we have

$$\sum_{T \in E[n]} \hat{\lambda}_v(P + T) = \hat{\lambda}_v([n]P) + (n^2 - 1)C_v.$$

(b) There is a constant C'_v such that for all $n \geq 1$, we have

$$\sum_{T \in E[n] \setminus O} \hat{\lambda}_v(T) = (n^2 - 1)C'_v.$$

(c) Evaluate the constants in (a) and (b).

Page 483, Second Table

The curve with $D = -3$ and $f = 2$ has conductor $N_E = 2^2 3^2$, not $2^2 3^3$.

The last five curves in the second table have negative discriminants.

It might help the reader to explain the relation of the entry for $-D = -7$ to the equation appearing in Proposition 2.3.1(iii) on page 111. Thus we have

$$E_1 : y^2 + xy = x^3 - x^2 - 2x - 1 \quad \text{in table on page 483,}$$

$$E_2 : y^2 = x^3 - 35x + 98 \quad \text{in Proposition 2.3.1(iii).}$$

These curves both have CM by the ring of integers in $\mathbb{Q}(\sqrt{-7})$. Further, they are isomorphic over $\bar{\mathbb{Q}}$ since $j(E_1) = j(E_2) = -3^3 5^3$. However, they are not isomorphic over \mathbb{Q} , since for example $\Delta_{E_1} = -7^3$ and $\Delta_{E_2} = -2^{12} 7^3$. (One can check that both equations are minimal Weierstrass equations.) They also have different conductors, $N_{E_1} = 7^2$ and $N_{E_2} = 2^4 7^2$. Thus E_2 is a twist of E_1 , and they have the same endomorphism ring. The table on page 483 only lists one curve over \mathbb{Q} with CM by each ring, not all twists.

Page 484: Line 12

Change “outwiegh” to “outweigh”

Page 486: Solution to Exercise 3.24(b)

It should be $\det(I_{00}) = (-1)^{n+1}n$, not $\det(I_{00}) = n$.

Page 487: New note

Add a note for exercise:

(5.10) See Tate [9], especially pages 176–177.

Page 496: References

Replace the reference Tate [9] with the following reference:

[9] A review of non-archimedean elliptic functions. In *Elliptic Curves, Modular Forms, & Fermat's Last Theorem*, J. Coates and S.T. Yau, eds., International Press, Boston, 1995, 162–184.

Page 496: References

In Vladut, change “Jugentraum” to “Jugendtraum”

Page 497: References

Add Zimmer, H., reference [2]:

Quasifunctions on elliptic curves over local fields, *J. reine angew. Math.* **307/308** (1979), 221–246; Corrections and remarks concerning quasifunctions on elliptic curves. *J. reine angew. Math.* **343** (1983), 203–211.

Page 503: Line 13, Notation

The entry $\hat{h}\mathbb{G}_m$ should just read \mathbb{G}_m .

Joseph H. Silverman
 Mathematics Department, Box 1917
 Brown University
 Providence, RI 02912 U.S.A
 <jhs@math.brown.edu>