

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

Joseph H. Silverman

August 4, 2011

Acknowledgements

I would like to thank following people for sending me comments and corrections: Paolo Barozza, Abbey Bourdon, Robin Chapman, Zev Chonoles, Henry Cohn, Maarten Derickx, Alexander Goncharov, Jonah Leshin, Sun Chia-Liang, Dino Lorenzini, Ryan Flynn, Ayhan Gunaydin, Michael Harris, Timo Keller, Chan-Ho Kim, David Masser, Victor Miller, Igor Minevich, Andrea Munaro, Yoshihiro Onishi, Mitchell Owen, Miles Reid, Kate Stange, Jane Sullivan, Thom Tyrrell, Nikos Tzanakis, Benjamin Weggenmann, Chris Wuthrich.

Preface (and elsewhere)

The period in the Latin phrase “et al.” comes after the “al”, not after the “et”.

Page 5, Figure 1.1 and following

During the final production process, all of the figures in the initial print run of the book were unfortunately reproduced using a low resolution method. The production department at Springer–Verlag and I apologize for this error. It has been corrected in subsequent print runs.

Page 21, Line 5

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

Page 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 $\phi^{-1}([0, 1])$, 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

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

So for this example we have

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

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

Page 30, Definition

In the definition of *space of (meromorphic) differential forms*, it should say that Ω_C is a $\bar{K}(C)$ -vector space, not a \bar{K} vector space. So this definition should read:

Definition. The *space of (meromorphic) differential forms* on C , denoted by Ω_C , is the $\bar{K}(C)$ -vector space generated by symbols of the form dx for $x \in \bar{K}(C)$, subject to the usual relations:

Page 42

The definition of b_2 has a typo, it should read

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

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

Page 45, Proposition 1.4(a)(i)

It should be $\Delta \neq 0$, not $\Delta = 0$. So the full line should read

(i) *It is nonsingular if and only if $\Delta \neq 0$.*

Page 53, 7'th displayed equation

It should be a_1 , not a_a . Thus the line should read

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

Page 55, 5'th displayed equation

The x -coordinate of $[2]P_2$ should be $137/64$, not $127/64$. So this line should read

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

Page 55, Line -3

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

Page 55, Line –13

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

Page 80, Line –6

The first E_1 in this displayed formula should be E_2 . So the formula should read

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

Page 82, Line 9

The reference to (III.4.2c) should be to (II.4.2c).

Page 84, Line 1

The terms “ $+\text{div}(\psi(x_1, y_1))$ ” should be “ $-\text{div}(\psi(x_1, y_1))$ ”. So the entire line should read

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

Page 87, Line –13

“easier”

Page 93, Line –5

In the displayed formula, the variable should be X , not S . Thus it should read

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

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 $i = 0, 1, \dots, m-1$, we find that

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

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 104, Chapter III exercises

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

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

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

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

Pages 105-106, Exercise 3.7

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

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

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

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

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

Page 105, Exercise 3.7(b)

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

$$\begin{aligned} \psi_m^2(x) &= m^2x^{m^2-1} + \frac{m^2(m^2-1)(m^2+6)A}{30}x^{m^2-3} + \dots, \\ \phi_m(x) &= x^{m^2} - \frac{m^2(m^2-1)A}{6}x^{m^2-2} + \dots. \end{aligned}$$

Page 107, Exercise 3.10(a)

The displayed equation should map E to \mathbb{P}^3 , not \mathbb{P}^2 . So the displayed equation should read

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

Page 110, Exercise 3.26

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

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

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

Here is how the corrected exercise reads:

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

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

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

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

Page 113, Exercise 3.35(b,c)

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

Page 117, Statement of Lemma 1.2

We need $\alpha \in R^*$, not merely that $\alpha \in R$. This is automatic from the assumptions if $\bigcap_{n \geq 1} I^n = (0)$, or if I is a maximal ideal, but for simplicity it is cleaner to add the assumption $\alpha \in R^*$ to the statement of the lemma.

Page 119, Line -7 and -2

Line -7 should read “the connecting line has equation $w = \lambda z + \nu$.” (In the text it says $w = \lambda z - \nu$.) However, the formula for z_3 on line -2 appears to use $w = \lambda z - \nu$ (with a negative sign). So there is a sign error in the formula for z_3 .

Page 119, Line -2

The numerator of this displayed equation has a a_2y that should be a $a_2\nu$. There are also some sign errors. The line should read

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

Page 120, Third displayed formula

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

$$\begin{aligned} F(z_1, z_2) &= i(z_3(z_1, z_2)) \\ &= z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) \\ &\quad + (-2a_3z_1^3z_2 + (a_1a_2 - 3a_3)z_1^2z_2^2 - 2a_3z_1z_2^3) + \dots \\ &\in \mathbb{Z}[a_1, \dots, a_6][[z_1, z_2]]. \end{aligned}$$

Page 130, Third displayed equation

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

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

Hence

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

Page 130, Example 6.1.1

The second line says “If $p \geq 2$ ”, but it should read “If $p \geq 3$ ”.

Page 152, Last sentence

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

Page 158, First displayed equation

The Y should be lower case. So the displayed equation should read

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

Page 166, First displayed equation

The exponent on $z - \omega$ should be 3, not 2. Thus this formula should read

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

Page 166, Last two displayed equations

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

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

and

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

Page 170, First and third displayed equations

The exponent of x should be 3, not 2. So these displayed equations should read

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

and

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

Page 176, Line 6–7

Part (ii) write first $\mathbb{Q}(\omega_2/\omega_1)$, and then $\mathbb{Q}(\omega_1/\omega_2)$. This should be made consistent. Since $\tau = \omega_1/\omega_2$, use that ordering.

Page 182, Exercise 6.14

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

Page 188, Proposition VII.2.1

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

Page 190, Last line of proof of lemma

It should read $(\partial\tilde{f}/\partial y)(\tilde{P}) \neq 0$ instead of $(\partial\tilde{f})(\partial y)(\tilde{P}) \neq 0$. So the full line should read:

lemma when $\tilde{P} \neq \tilde{O}$ and $(\partial\tilde{f}/\partial y)(\tilde{P}) \neq 0$. The other cases are proven similarly.

Page 193, Example 3.3.3, Third displayed equation

The fourth point in $E(\mathbb{F}_5)$ should be $(3, 0)$, not $(2, 0)$. So it should read

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

Page 197, Line 6

This line should read “the curve E_2 has multiplicative reduction...”. (The text says E_3 .)

Page 198, Line 14

This line should read “giving a minimal Weierstrass equation for E over K' .” (The text says “over K ”, but the field should be K' .)

Page 200, Line –8

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

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

Page 200, Exercise 7.3

The hint should be “See (VII.3.5)”, not (VIII.3.5).

Page 201, Line 2 of the proof

“implications(b) \Rightarrow ...”, there should be a space between “implications” and “(b)”.

Page 210, Fifth display

There is a minus sign that should be a plus sign in chain of equalities. It should read

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

Page 219, Line -8

The formula in front of the $(C'_1 + C_2)$ is wrong, and in fact, it goes to infinity as n goes to infinity. This line should read as follows:

$$h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2} \left(1 + \frac{2}{m^2} + \left(\frac{2}{m^2}\right)^2 + \cdots + \left(\frac{2}{m^2}\right)^{n-1}\right) (C'_1 + C_2)$$

Page 222, Sublemma VIII.4.3

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

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

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

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

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

Verify the identity

$$-x^6\Delta = \left((a^3 + 3b^2)x^2 - a^2bx - 2ab^2\right)f + \left((3a^3 + 24b^2)x^3 + a^2bx^2 - (16ab^2 + a^4)x + 2a^3b\right)g. \quad (3)$$

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

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

Page 226, Proposition 5.4(c)

In the displayed equation, the exponent on H_K should be the degree $[K : \mathbb{Q}]$, not its reciprocal $1/[K : \mathbb{Q}]$. So it should read

$$H_L(P) = H_K(P)^{[K:\mathbb{Q}]}.$$

Page 233, Line -2

“has a most” should be “has at most”, so the full phrase should read “Since each polynomial $f_x(T)$ has at most d roots in $K \dots$ ”

Page 251, Line -7

The reference [143, Chapter XIV, §§3,7] should be [143, Chapter XV, §§3,7].

Page 262, Exercise 8.7(a)

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

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

Page 266, Exercise 8.19

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

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

Page 335, Line 7

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

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

Page 391, Example XI.7.1

The statement and proof are incorrect for general N . One must make the additional assumption that N is prime. The error is in the statement that

$$a^2 + b^2 \equiv 0 \pmod{N} \quad \implies \quad a \equiv b \equiv 0 \pmod{N},$$

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

Page 413, Lines 6 and 7

Two occurrences of char K should be char k . So these two sentences should read:

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

Page 454, first displayed equation

The term x^6 should be x^3 , so the full line should read

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

Page 412

The formula for the j -invariant is missing a power of 3. It currently reads

$j = \frac{\alpha^3(\alpha-24)^3}{\alpha^3-27}$, but it should read

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

Page 459, first paragraph

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

The Sato-Tate Conjecture

by Richard Taylor

Abstract: In the first part of the talk I will explain the Sato–Tate conjecture and the Tate–Serre approach via symmetric power L -functions. I will also sketch the structure of the recent proof (by Laurent Clozel, Michael Harris, Nick Shepherd-Barron and myself) of the conjecture for elliptic curves over \mathbb{Q} with somewhere multiplicative reduction.

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

Page 494, index entry for Elkies

There should also be a reference to page 153 (Theorems V.4.7 and V.4.9 are due to Elkies).

Page 494, index entry for Shafarevich–Tate group

“is finite (?),, 453” has an extra comma.