

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

Joseph H. Silverman

November 1, 2009

Acknowledgements

Thanks to the following people who have sent me comments and corrections: Paolo Barozza, Ryan Flynn, Ayhan Gunaydin, Henry Cohn, David Masser, Victor Miller, Miles Reid, Thom Tyrrell.

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 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, 7th 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 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 .

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

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

Page 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}_{178} .

(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 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 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 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 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

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

(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 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.