Errata and Corrections to *Rational Points on Elliptic Curves* 2nd Edition

Joseph H. Silverman, John Tate

June 13, 2024

Acknowledgements
We would like to thank the following people for sending us comments and corrections: Alejandra Alvarado, Serdar Altuntas, Shamil Asgarli, Letian Chen, France Dacar, Guy Drory, Mark Faucette, Held Florian, Benyamin Gholami, Gaurav Goel, Justin Groves, Jacob Van Hook, Jackson Hsu, Fan-Yun Hung Seong Eun Jung, Enis Kaya, Daniel Lauer, Seungho (James) Lee, Noèmi Zoé Nagy, Jozsef Pelikan, Alessandro De Piccoli, Ashvin Rajan, Philip Turecek, Laura Walton Mike Zieve.

Page xvi, Third displayed equation
The second point should be

$$\left(\frac{129}{10^2}, \frac{383}{10^3}\right).$$

There's an incorrect minus sign on the y-coordinate in the text.

Page 4, Line -1
"the it would" should be "then it would".

Page 10, Line 3
"intersections of multiplicity great than one" should be "intersections of multiplicity greater than one".

Page 17, Line 4 and Footnote 5
We need to move $\mathcal{O}$ to the point $[1, 0, 0]$, and we need to fix the footnote, which is incorrect. So replace the sentence "We assume that we are given a rational point $\mathcal{O}$ on C, so we begin by taking $Z = 0$ to be the tangent line to C at $\mathcal{O}$." with the following material, including replacing the footnote:

We assume that we are given a rational point $\mathcal{O}$ on C, so we begin changing coordinates to move $\mathcal{O}$ to the point $[1, 0, 0]$ and to make $Z = 0$ the tangent line to C at $\mathcal{O}$.[1]

Detailed Explanation: The following is a description of the calculations used to analyze the case that $\mathcal{O}$ is an inflection point. It is too much material to include in the text, but is included here for completeness. The assumptions that $\mathcal{O} = [1, 0, 0] \in C$ and that the tangent line at $\mathcal{O}$ is $Z = 0$, means that the homogeneous equation of C has the form

[1] If $\mathcal{O}$ is a point of inflection, i.e., if the line $Z = 0$ intersects C only at the point $\mathcal{O}$, then setting $x = Y/Z$ and $y = X/Z$ and dividing by the coefficient of y^2 gives an equation of the form $y^2 + (ax + b)y =$ cubic in x, so we may skip down to this equation and pick up the proof at that point.

$$A_2Y^3 + A_3Z^3 + A_5X^2Z + A_6XY^2 + A_7Y^2Z + A_8XZ^2 + A_9YZ^2 + A_{10}XYZ = 0$$

(The A_1X^3 term is omitted since $\mathcal{O} = [1, 0, 0] \in C$, and the A_4X^2Y term is omitted since tangent line at $\mathcal{O}$ is $Z = 0$, so $F_Y(\mathcal{O}) = 0$.) The intersection of C with $Z = 0$ is the set

$$A_2Y^3 + A_6XY^2 = 0.$$

Hence $\mathcal{O}$ is an inflection point if and only if $A_6 = 0$, in which case the equation for C is

$$A_2Y^3 + A_3Z^3 + A_5X^2Z + A_7Y^2Z + A_8XZ^2 + A_9YZ^2 + A_{10}XYZ = 0.$$

We note that $A_5 \neq 0$, since otherwise $\mathcal{O}$ is a singular point. We divide by Z^3 and set $x = Y/Z$ and $y = X/Z$ to obtain the affine equation

$$A_2x^3 + A_3 + A_5y^2 + A_7x^2 + A_8y + A_9x + A_{10}xy = 0.$$

Dividing by A_5 and moving terms around, we obtain an equation of the form

$$y^2 + (ax + b)y = \text{cubic in } x,$$

which is the equation at the bottom of page 17. The proof then proceeds as given on page 18+.

Page 18, First paragraph
It's probably better to instead replace x and y with x/λ and y/λ and then multiply the equation by λ^2, since that will result in the other coefficients being multiplied by powers of λ, instead of being divided by powers of λ. Explictly, if the displayed equation at the top of page 18 were to look like

$$y^2 = \lambda x^3 + ax^2 + bx + c,$$

then replacing x and y with x/λ and y/λ and multiplying by λ^2 yields

$$y^2 = x^3 + ax^2 + \lambda bx + \lambda^2 c.$$

Page 20, Line 2
"equation" should be "equivalent".

Page 23, Line 2
First, "$r = x/y$" should be "$r = y/x$". Second, it should be noted that each

point $(x, y) \neq (0, 0)$ corresponds to a specific rational number r, but that the point $(0, 0)$ comes from both $r = 1$ and $r = -1$.

Page 27, Second displayed equation
Since $x_1 = -1$, the equation should really use $f'(-1)$ instead of $f'(1)$, although they are equal. So the displayed equation should read

$$\lambda = \frac{f'(x_1)}{2y_1} = \frac{f'(-1)}{8} = \frac{3}{8}.$$

Page 31 Exerercise 1.14
$u^3+v^2 = u+v+1$ should be $u^3+v^3 = u+v+1$. (v should have exponent 3.)

Page 33, Exercise 1.21(a)
The numerator $f'(x)^2 - (a + 2x)f(x)$ should be $f'(x)^2 - 4(a + 2x)f(x)$. (There is a missing factor of 4.)

Page 33–34, Exercise 1.22(b)
The three partial derivatives of $\mathcal{O} = [1, 0, 0]$ on C are 0, 0, and $-c$, while the three partial derivatives of $\mathcal{O}' = [0, 1, 0]$ on W are 0, 0, and 1. So the non-singularity condition is different if $c = 0$. So we should really add the assumption that $c \neq 0$. The geometry when $c = 0$ is interesting. In that case, the curve W is the union of the line $Z = 0$ and a conic, while the curve C is singular at $\mathcal{O}$. The rational map $W \to C$ maps the entire line $Z = 0$ of W to the singular point $\mathcal{O}$ of C, and it maps the conic part of W onto C.

Page 40, Line 4–5
"although it does not look it" would be clearer if it were repaced by "although it does not look compact".

Page 42, First displayed equation
There should be an exponent of 3 on the first $\wp(u)$, so it should read

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3.$$

Page 44, Line 10
"subfield of the complex number" should be "subfield of the complex numbers" (plural).

Page 45, Line 1
"But again those solution" should be "But again those solutions" (plural).

Page 52, Line -1
In the displayed equation, the initial $\alpha\beta$ in the coefficient of t^2 should be $a\beta$ (thus "a" instead of "α"), so it should read

$$0 = (1 + a\alpha + b\alpha^2 + c\alpha^3)t^3 + (a\beta + 2b\alpha\beta + 3c\alpha^2\beta)t^2 + \cdots .$$

Page 53, Second displayed equation
The initial $\alpha\beta$ in the numerator should be $a\beta$ (thus "a" instead of "α"), so it should read

$$t_1 + t_2 + t_3 = -\frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}.$$

Page 53, Penultimate paragraph
The argument in the paragraph starting "This proves that if the t-coordinates..." is incomplete, because in order to show that a point (s, t) is in $C(p^\nu)$, one must show both that $t \in p^\nu R$ and $s \in p^{3\nu}R$. (It actually suffices to show that $s \in pR$; see the added exercise in this document.) The text only does the former. So replace that paragraph with the following material:

The definition of P_3 says that the line $s = \alpha t + \beta$ through P_1 and P_2 (tangent to C if $P_1 = P_2$) also goes through P_3, so we have

$$s_3 = \alpha t_3 + \beta.$$

We showed earlier that

$$\alpha \in p^{2\nu}R \quad \text{and} \quad \beta \in p^{3\nu}R \quad \text{and} \quad t_3 \in p^\nu R,$$

so we see that $s_3 \in p^{3\nu}R$. This proves that

$$P_1 + P_2 = -P_3 = (-t_3, -s_3) \in C(p^\nu),$$

so $C(p^\nu)$ is closed under addition. It is clearly also closed under the negation map

$$-(t, s) = (-t, -s),$$

which completes the proof that $C(p^\nu)$ is a subgroup of $C(\mathbb{Q})$.

Page 54, Middle of the page
What is actually proven in the texzt is that there is a well-defined homomorphism

$$C(p^\nu) \longrightarrow p^\nu R/p^{3\nu}R, \quad P \longmapsto t(P) = x(P)/y(P),$$

whose kernel is

$$\big\{P \in C(p^\nu) : t(P) \in p^{3\nu}\big\}.$$

It is asserted that the kernel is $C(p^{3\nu})$, but

$$C(p^{3\nu}) = \big\{P \in C(\mathbb{Q}) : t(P) \in p^{3\nu} \text{ and } s(P) \in p^{9\nu}\big\}.$$

So although the material in the book shows that $C(p^{3\nu})$ is contained in the kernel, and hence that there is a well-defined homomorphism

$$C(p^\nu)/C(p^{3\nu}) \longrightarrow p^\nu R/p^{3\nu}R, \quad P \longmapsto t(P) = x(P)/y(P);$$

more work is needed to prove the injectivity. This can be done using the new exercise for Chapter 2 in this document. It asserts that if $(t, s) \in C(\mathbb{Q})$ and $s \in pR$, then $\operatorname{ord}(s) = 3\operatorname{ord}(t)$. Hence $(t, s) \in C(p^\nu)$ and $t \in p^{3\nu}R$ for some $\nu \geq 1$ implies that $\operatorname{ord}(s) \geq 3\nu > 0$, so the exercise gives

$$\operatorname{ord}(s) = 3\operatorname{ord}(t) \geq 3 \cdot (3\nu) = 9\nu.$$

Therefore $(t, s) \in C(p^{3\nu})$.

Page 58, Exercise 2.1(b)
"Prove that A is the direct product of two cyclic groups of order m" should be "Prove that A is the direct product of two cyclic groups of order M".

Page 59, Exercise 2.3(c)
The displayed equation should omit the points u in L, since both sides have poles if $u \in L$. So it should read

$$\wp(u + \omega) = \wp(u) \quad \text{for every } u \in \mathbb{C} \smallsetminus L \text{ and every } \omega \in L.$$

Page 59, Line -1
"to test you conjecture" should be "to test your conjecture"

Page 61, Exercise 2.6(d)
"where by convention we set $\|r\| = 0$" should be "where by convention we set $\|0\| = 0$"

Page 63, New Exercise for Chapter 2
Let C be given in (t, s) coordinates as described in Section 2.4.

(a) Let $(t, s) \in C(\mathbb{Q})$, let p^ν be the highest power of p dividing the numerator of t, and let p^μ be the highest power of p dividing the numerator of s. Suppose further that $\mu \geq 1$. Prove that

$$\mu = 3\nu.$$

(b) Deduce that

$$C(p^\nu) = \big\{(t,s) \in C(\mathbb{Q}) : t \in p^\nu R \text{ and } s \in pR\big\}.$$

Page 68, Theorem 3.5
"Desecent Theorem" should be "Descent Theorem".

Page 81, Line 8
"neither $a^2 - b$ nor b is zero" should be "neither $a^2 - 4b$ nor b is zero" (missing 4 in the formula).

Page 83, Displayed equation
The description of $\overline{u}$ is missing a $\frac{1}{2}$ in front of the ω_1 and has an extra 2 in front of $\overline{\omega}_1$. Thus it should read

$$u = c_1\omega_1 + c_2\omega_2 \quad \text{is sent to} \quad \overline{u} = \frac{1}{2}c_1\omega_1 + c_2\omega_2 = c_1\overline{\omega}_1 + c_2\overline{\omega}_2.$$

Page 85, Line 1
The text forgot to compose with the map $(x,y) \mapsto (x/4, y/8)$. So there should be an extra 4 and 8 in the denominators, and the first formula should read

$$\psi(\overline{P}) = \begin{cases} \left(\dfrac{\overline{y}^2}{4\overline{x}^2}, \dfrac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2}\right), & \text{if } \overline{P} = (\overline{x},\overline{y}) \neq \overline{\mathcal{O}}, \overline{T}, \\ \mathcal{O}, & \text{if } \overline{P} = \overline{\mathcal{O}} \text{ or } \overline{P} = \overline{T}. \end{cases}$$

Page 86, Line -5
"To check, say, that $\phi(P_1) = (x_1, y_1) = (\overline{x}_1, \overline{y}_1)$" should be "To check, say, that $\phi(P_1) = \phi(x_1, y_1) = (\overline{x}_1, \overline{y}_1)$". (Missing ϕ)

Page 87, Line 2
In the numerator of the first fraction, it should be $-b(y_1 + \lambda x_1)$, not $-b(y_1 - \lambda x_1)$, so that line should read

$$= \frac{\lambda(x_1^3 + bx_1) - b(y_1 + \lambda x_1) + \nu x_1^2}{x_1^2}$$

Page 89, Line -11
"$\overline{T} \in \phi(G)$" should be "$\overline{T} \in \phi(\Gamma)$".

Page 91, Second line for first displayed equation
The numerator of the middle fraction should have a negative sign. Thus it should read

$$\frac{y_2(x_2^2-b)}{x_2^2} = \frac{-x_2 w(x_2^2 - x_1x_2)}{x_2^2} = w(x_1 - x_2).$$

Page 97, Line -13
$(G : 2\Gamma)$ should be $(\Gamma : 2\Gamma)$.

Page 105, Line after boxed formula
The curve $y^2 = x^3 + 10x$ is supposed to be $y^2 = x^3 + 20x$. The former has rank 0, while Example 3.13 says that the latter has rank 1.

Page 107, Lines 18–19
"Then one can checks that" should be "Then one can check that"

Page 108, Third displayed equation
It should be $r^3 - r$, not $r^3 - 1$, so the map should be

$$r \longmapsto (r^2 - 1, r^3 - r).$$

Page 111, Exercise 3.1
Both parts of the exercise are also true if we allow numbers whose height $H(x)$ is "less than or equal to κ", which is the more standard way to count points of bounded height; although the exercise as stated is correct.

Page 112, Line -3
"but that such such a point" should be "but that such a point".

Page 113, Exercise 3.8(c)
The condition for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is incorrect, it should be d^2, not d^4. Thus

$$\bigl\{P \in C(\mathbb{Q}) : P \text{ has finite order}\bigr\} \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } D = 4d^4 \text{ for some } d, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } D = -d^2 \text{ for some } d, \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

Page 124, Line 18
"Similarly for $y = 0$ and $z = 0$" should be "Similarly for $x = 0$ and $y = 0$".

Page 125, Line -2
"Out next task is to" should be "Our next task is to". ("Our", not "Out")

Page 128, Line -5
$b\alpha_e$ should be $b\alpha_3$.

Page 129, Line 9
$A = 2k - 2$ should be $A = 3k - 2$

Page 131, Line 2
"the group of points on the curve $x^3 + y^3 + z^2 = 0$" should be "the group of points on the curve $x^3 + y^3 + z^3 = 0$" (exponent 3 on z)

Page 132, Middle of the page
"If we ask for a formula for the number of solutions M_p, then it is only for some very special cubics that we get an answer like the one that we obtained for $x^3 + y^3 = 1$." In the first edition we noted that these "very special cubics are the ones that have what is known as complex multiplication." It might be worth putting that note back into the text, or as a footnote.

Page 135, Lines 5–6
"So we have a map from the group $C(\mathbb{Q})$ to the group $\tilde{C}(\mathbb{F}_p)$" should be "So we have a map from the group Φ to the group $\tilde{C}(\mathbb{F}_p)$"

Page 159, Line -1
$cz = d$ should be $cz - d$, so it should read

$$\Phi\left(\frac{az+b}{cz-d}\right) = (cz+d)^2\Phi(z)$$

Page 161, Line -2
$C(p) \cap \Phi = \emptyset$ should be $C(p) \cap \Phi = \{\mathcal{O}\}$.

Page 169, Line 15
"If D is a positive square-free integer" should be "If $D \geq 2$ is a square-free integer", since we don't want $D = 1$.

Page 177, Line -3 **(displayed equation)**
There's a missing y in $\left(x + \frac{1}{2}\beta\right)^2$, so it should read

$$x^2 + \beta xy + \beta^2 y^2 = \left(x + \frac{1}{2}\beta y\right)^2 + \frac{3}{4}\beta^2 y^2 \geq \frac{3}{4}\beta^2 y^2,$$

Page 192, First line of second displayed equation
The exponent on b should be $28/3$, not $38/3$, so it should read

$$\sum_{k=n}^{m+n} \left|F^{(k)}(\beta,\beta)\right| \binom{k}{t} |x-\beta|^{k-n} \le (m+1)\cdot 4(2^{38}b^{28/3})\cdot 2^{m+n}.$$

Page 202, Fourth displayed equation
First, the inequality should be reversed, so it should read

$$\left|\frac{p}{q} - \sqrt[3]{2}\right| \ge \frac{10^{-6}}{q^{2.9955}}.$$

Second, in the next line, it should say "valid for all rational numbers p/q with $q \ge 1$." (Alternatively, use $|q|^{2.9955}$ in the displayed equation.)

Page 203, Exercise 5.2
Should note that the given bound is most likely not best possible, and add the further exercise to find an improved bound.

Page 204, Exercise 5.9(a)
There's a missing C on the upper bound of the displayed equation. It should read

$$\left|\frac{p}{q} - \sqrt[d]{b}\right| \le \frac{C}{q^3}.$$

Page 205, Exercise 5.12(a)
$x(nP)$ should just be nP, so it should read

$$nP = \left(\frac{a_n}{d_n^2}, \frac{b_n}{d_n^3}\right) \quad \text{with } \gcd(a_n, d_n) = \gcd(b_n, d_n) = 1.$$

Page 209, Middle of the page
"the unit circle $|z| = 1$ in the unit plane" should be "the unit circle $|z| = 1$ in the complex plane."

Page 221, Line -7
The displayed equation listing the points in $C[4]$ is actually only the list of points of exact order 4. So change the preceding line to say that " a little algebra gives us a complete description of the points of exact order four" and remove $C[4]$ from the displayed equation, or include in the set $C[4]$ points

$$\{\mathcal{O},\ (0,0),\ (i,0),\ (-i,0)\}$$

of orders 1 and 2.

Page 230, Third displayed equation
In the formula for $2P$, the denominators should be $4y^2$ and $8y^3$ (missing factors of 4 and 8).

Page 232, Line 13
"the curve $C; y^2 = x^3 + bx$" should be "the curve $C : y^2 = x^3 + bx$" (colon instead of semicolon).

Page 247, Line -1 of text
There's a missing apostrophe on "Wiles". So it should read "Later, a number of mathematicians extended Wiles' argument,..."

Page 248, Line 14
There's a "#" missing from in front of $\tilde{E}_p(\mathbb{F}_p)$. So this displayed equation should read

$$\#\tilde{E}_p(\mathbb{F}_p) = p + 1 - \epsilon_p \quad \text{with} \quad |\epsilon_p| \le 2\sqrt{p}.$$

Page 249, line -6 of text
"consistant" should be "consistent"

Page 251, Line -1
The matrix should specify that it is in SL_2. So this displayed equation should read

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

(In fact, $\Gamma_0(N)$ is usually viewed as a subgroup of PGL_2, so we should write PSL_2.)

Page 257, Exercise 6.4(b)
If n is even, then we need to multiply ψ_n by y^{-1} (or could multiply by y to get a weaker result). So it should say that "$y^{-1}\psi_n$, ϕ_n, and ω_n are in $\mathbb{Z}[x, y^2]$."

Page 262, Exercise 6.21(c)
In the first and third displayed equations in this exercise, the second coordinate should not have a minus sign. ' Also in the third equation, there is an extra i. So the first equation should say

$$C(\mathbb{C}) \longrightarrow C(\mathbb{C}), \quad (x,y) \longmapsto (-x, iy)$$

and the third equation should say

$$\wp(iz) = -\wp(z) \quad \text{and} \quad \wp'(iz) = i\wp'(z).$$

Page 266, Line -6
"We see that these solutions approach (∞, ∞)." We should mention that we're not distinguishing between ∞ and $-\infty$, so all we really means is that $|a_i/c_i| \to \infty$ and $|b_i/c_i| \to \infty$.

Page 279, Line -13
The phrase "we substitute $X' = a$, $Y' = b$, and $Z' = c$" should be "we substitute $X' = a'$, $Y' = b'$, and $Z' = c'$."

Page 293, Line after label (1.5)
The formula

$$\phi(d) - \phi(d-n_1) - \phi(d-n_2) - \phi(d-n_1-n_2) = n_1 n_2$$

should be

$$\phi(d) - \phi(d-n_1) - \phi(d-n_2) + \phi(d-n_1-n_2) = n_1 n_2.$$

(Last sign should be plus.)

Page 294, Line -7
"Deduce that $\deg g_i \le d - n$" should be "$\deg g_i \le d - n_i$". (Missing i subscript)

Page 302, Line 3
"Each point $P \in \mathbb{P}^1(\mathbb{Q})$" should be ""Each point $P \in \mathbb{P}^2(\mathbb{Q})$", since we're working in $\mathbb{P}^2$, not $\mathbb{P}^1$.

Page 305, First displayed equation
It should be L_2, not P_2, so it should read

$$C \cap L_1 = \{P, Q, S\} \quad \text{and} \quad C \cap L_2 = \{S, \mathcal{O}, R\}.$$

Page 311, Line -4
The coefficient of $X_1^2 Y_1$ in the equation of C needs a minus sign, so it should read

$$C : -X_1^2Y_1 + 6X_1Y_1^2 + 2Y_1^3 + 5X_1^2Z_1 - 7X_1Y_1Z_1 + 12X_1Z_1^2 + 4Z_1^3 = 0.$$

Page 312, Line -6
The coefficient of Z_4^3 should be 3200, so it should read

$$C : 16129X_4Y_4^2 - 5X_4^2Z_4 + 3937X_4Y_4Z_4 + 984X_4Z_4^2 + 19050Y_4Z_4^2 + 3200Z_4^3 = 0.$$

Page 313, Footnote
The footnote describes a substitution that gives a Weierstrass equation with smaller coefficients. However, if one allows more general Weierstrass equations, one can do even better and obtain the equation

$$y^2 + xy = x^3 - 302x - 2036.$$

In fancier terminology, the equation in the footnote is not a minimal Weierstrass equation; its discriminant is too large by a factor of 2^{12}.