Errata List for *Rational Points on Elliptic Curves*
by Joseph H. Silverman and John Tate
Version 1.3— July 5, 1994

The authors would like to thank the following individuals for their assistance in compiling this errata sheet: G. Allison, P. Berman, D. Appleby, K. Bender, G. Bender, J. Blumenstein, D. Freeman, L. Goldberg, A. Guth, A. Granville, J. Kraft, J. Lipman, M. Mossinghoff, R. Pennington, R. Pries, K. Ribet, H. Rose, L. Gómez-Sánchez J.-P. Serre, M. Szydlo, J. Tobey, C.R. Videla, J. Wendel.

Material referred to as being on "attached pages" is not yet available for distribution.

Page vii: Computer Packages
Remove the offer to send a formatted disk and give the ftp site for picking up computer packages. Also include sites for pari, simath, and maple packages as described in *The Arithmetic of Elliptic Curves* Volume II.

Page 1: Footnote 2
Fermat's Last Theorem is now Wiles' Theorem (Summer 1993)! Then again, maybe not (Spring 1994)! Yes, looks okay (Summer 1995)!

Page 4–5: Footnote
Replace "$f(x,y)$" with "$f(x_1,x_2,\dots,x_n)$", since this footnote deals with polynomials in many variables. Further, this footnote is split at a very bad place between pages 4 and 5, since the part on page 4 alone is grammatically correct and gives a false statement.

Page 7: Line 1
"turns them" should be "turns it"

Page 11: Figure 1.2
The point marked $(-1,t)$ should be $(-1,0)$.

Page 13: Lines 11–12
Replace "you take two relatively prime integers m and n and let" with "you take two relatively prime integers m and n, one odd and one even, and let"

Page 15: Line 3
After "solution in integers", add ", not all zero,".

Page 17: Paragraph 1
Reiterate that this is just a plausibility argument, not a proof, because the linear conditions might not be independent.

Page 22: Line -1
After "simple form.", add the explanation "(When we speak of the "X axis" in $\mathbb{P}^2$, we mean the line $X=0$, and similarly for the Y and Z axes.)"

Page 23: Figure 1.10
The lines labeled X, Y, Z should be labeled $X = 0$, $Y = 0$, $Z = 0$. The point labeled $\mathcal{O}$ should be labeled $\mathcal{O} = [1, 0, 0]$. The point where the Z-line hits C should be labeled $[0, 1, 0]$.

Page 24: Example
Add a more typical example, worked out in detail. (See attached pages for $X^3+2Y^3+4Z^3 = 0$, $\mathcal{O} = [1, 1, 1]$.) Note that the $u^3 + v^3 = \alpha$ example is referred to on the bottom of page 149.

Page 26–27: Singular curves
Since we're working over $\mathbb{R}$, we should also include the "non-split" case. In other words, it's possible to have distinct tangent directions which are not defined over $\mathbb{R}$. A typical equation is $y^2 = x^2(x - 1)$, and the picture has an isolated point at $(0, 0)$. So we should say that there are three possible pictures for the singularity, and include a third picture. A good exercise would be to show that if $y^2 = f(x)$ is singular, then there is a change of variables (over $\mathbb{R}$) which puts the curve into one of the three standard forms.

Page 28: Section 4
Mention the fact that for distinct points P, Q, R on a Weierstrass equation, we have $P + Q + R = \mathcal{O}$ if and only if P, Q, R are colinear. More generally, include an exercise to prove that if P, Q, R are distinct points on any elliptic curve, then $P + Q + R = \mathcal{O} * \mathcal{O}$ if and only if P, Q, R are colinear.

Page 33: Line −2 of Exercise 1.8
$5 - adic$ should be 5-adic. (The "adic" should not be italicized.)

Page 34: Exercise 1.11(c)(iii)
Use "$P * (\mathcal{O} * (Q * R)) = R * (\mathcal{O} * (P * Q))$", since that matches better with $(P + Q) + R = P + (Q + R)$.

Page 36: Exercise 1.18
Use $Q_1, Q_2, \ldots, Q_7$ for the names of the points in this exercise, since this curve is considered on page 31, where the point $(2, 5)$ is called P_2.

Page 37: Chapter I Exercises
Add a new exercise to show that $xy^2 + \cdots$ is smooth if and only if $y^2 + \cdots$ is smooth. (See attached note from Tate.)

Page 39: Line −6
"of $2P$ and equal" should be "of $2P$ equal"

Page 42: Line −1
"order $\frac{1}{2}m$" should be "order m".

Page 48: Last two lines
"so $r(x)$ and $s(x)$ are integers" makes it sound like the polynomials are constant. Change to "so $r(x)$ and $s(x)$ take on integer values when evaluated at the integer x."

Page 51: Figure 2.6
The figure in the *st*-plane is really not accurate. In general there can be more than one value of s for a given value of t. See the attached sheets for a corrected version. This means that the proof is incomplete, we need to consider vertical lines (i.e., $\alpha = \infty$). Figure 2.7 should also be corrected to match the new version of Figure 2.6.

Page 52: Paragraph 3
If $P_1 \neq P_2$ and $t_1 = t_2$, it is not true that $P_1 = -P_2$. This argument needs to be rewritten.

Page 67: Line 2
"contant" should be "constant"

Page 77: 3rd Displayed Equation
"$\bar{\bar{C}} : y^2 = x^2 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$" should be "$\bar{\bar{C}} : y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$".

Page 78: 2nd Displayed Equation
"$\bar{u} = \frac{1}{2}c_1\omega_1 + c_2\omega_2 = c_1\bar{\omega}_1 + c_2\bar{\omega}_2$" should be "$\bar{u} = c_1\omega_1 + c_2\omega_2 = 2c_1\bar{\omega}_1 + c_2\bar{\omega}_2$."

Page 81: Line −8
"$(\bar{\lambda}x+\bar{\nu})^2 = f(x)$" should be "$(\bar{\lambda}x+\bar{\nu})^2 = \bar{f}(x)$", or else write it out in full as "$(\bar{\lambda}x+\bar{\nu})^2 = x^3 + \bar{a}x^2 + \bar{b}x$".

Page 87: 2nd Displayed Equation
"$\pm$(rational number)^2" should be "$\pm$(integer)^2"

Page 94–96: Examples 1 and 3
If we only check the allowable b_1's modulo squares, then we have to allow M, e, N to have some common factors. The point is that every $(x, y) \in \Gamma$ leads to a factorization $b = b_1 b_2$ and to a solution of $N^2 = b_1 M^4 + aM^2e^2 + b_2e^4$ with M, e, N pairwise relatively prime, but (x, y) need not lead to a square-free b_1. Basically, if we replace b_1 by its square-free part, then we have to allow M, e, N to have common factors dividing the square part we canceled.

Page 98: Line 15
Change "$N^2 = 68M^4 - e^4$" to "$N^2 = 17M^4 - 4e^4$". (Although it is true that both equations have non-trivial p-adic solutions for all p, the first equation doesn't actually have a solution modulo 4 if we require N and e to be relatively prime.)

Page 98: Line −2
"has rank 15" should be "has rank at least 15". (Update to give current record, which is now at least 19.)

Page 99: Line −3
The second coordinate should be $-\dfrac{\nu^3}{y_1y_2}$ instead of $\dfrac{\nu^3}{y_1y_2}$. Exercise 3.10 on Page 105 also needs to be changed.

Page 100: Top of Page and Theorem

"We observed in Chapter I that there are two possible pictures for the singularity S" is not correct, there are three possibilities. The theorem should be restated to include the third case $y^2 = x^2(x-1)$. Further, over $\mathbb{Q}$, the structure in general is more complicated. This is explained in Exercise 3.15, so possibly just mention that there exists the third case and refer the reader to exercise 15 for more details.

Page 100: 3rd Displayed Equation

"$(x,y) \longmapsto \dfrac{x}{y}$" should be "$(x,y) \longmapsto \dfrac{y}{x}$"

Page 105: Exercise 3.7(c)

The first condition in the table should be "$\dfrac{\mathbb{Z}}{4\mathbb{Z}}$, if $D = 4d^4$ for some d,".

Page 105: Exercise 3.11

"1 if $P = \mathcal{O}$" should be "0 if $P = \mathcal{O}$".

Page 107: Line −6

"an element of $\mathbb{F}_p$.)" should be "an element of $\mathbb{F}_p$)."

Page 109: Line −1 of Paragraph 3

"non-residues.)" should be "non-residues)."

Page 117: Line 6

"$\beta_1\beta_2\beta_3 = 3k - 2$" should be "$\beta_1\beta_2\beta_3 = (3k-2)p$". (The p was omitted on the RHS.)

Page 126: Line 2

"1, 000, 000" should be "$1,000,000$". (Close up space after the commas by using math mode.)

Page 132: Pollard's Algorithm, Step 4

Replace "Calculate $D = \gcd(a^k - 1, n)$" with something like "Calculate $b \equiv a^k - 1 \pmod{n}$, and then $D = \gcd(b, n)$".

Page 132: Pollard's Algorithm, Step 4

Change the last line to "If $D = n$, either go back to Step 2 and choose another a, or go back to Step 1 and take a smaller k." The reason for the change is the (unlikely) possibility that every p dividing n has the property that $p - 1$ divides k.

Page 135: Equation for λ in Center of Page

The equation given for λ is actually the formula for $x(2Q)$. Replace it with $\lambda = \dfrac{f'(x)}{2y} = \dfrac{3x^2 + 2ax + b}{2y} \pmod{n}$.

Page 136: Computation of kP at Bottom

The third line should be $1104P = (1372980126, 736595454)$, and all of the points after this are incorrect. The corrected version of this table is as follows:

$$\begin{aligned}
2^4P = 16P &= (385062894, 618628731)\\
(2^4 + 2^6)P = 80P &= (831572269, 1524749605)\\
(2^4 + 2^6 + 2^{10})P = 1104P &= (1372980126, 736595454)\\
(2^4 + 2^6 + 2^{10} + 2^{12})P = 5200P &= (1247661424, 958124008)\\
(\text{previous partial sum}) + 2^{13}P = 13392P &= (1548582473, 1559853215)\\
(\text{previous partial sum}) + 2^{14}P = 29776P &= (201510394, 7154559)\\
(\text{previous partial sum}) + 2^{15}P = 62544P &= (629067322, 264081696)\\
(\text{previous partial sum}) + 2^{17}P = 193616P &= (844665131, 537510825)\\
(\text{previous partial sum}) + 2^{19}P = 717904P &= (886345533, 342856598)\\
(\text{previous partial sum}) + 2^{20}P = 1766480P &= (370579416, 1254954111)\\
(\text{previous partial sum}) + 2^{21}P = 3863632P &= (77302130, 514483068)\\
(\text{previous partial sum}) + 2^{23}P = 12252240P &= (1225303014, 142796033)
\end{aligned}$$

Page 137: Table at Top of Page

The table heading should be "$2^iP \pmod{1715761513}$". (The modulus listed, 246082373, is the modulus used in the Pollard example earlier in the section.) The entries in the table are correct.

Page 137: Line 3

The value of "kP" is incorrect. This line should read

$$kP = 12252240(2, 1) \equiv (1225303014, 142796033) \pmod{1715761513}.$$

Page 137: Line −5 ff

The book asserts that no factor is found with $P = (2, 1)$ and $1 \le b \le 253$, but a factor is found with $b = 254$. Mossinghoff did not find a factor with $b = 254$, but did find a factor with $b = 42$. (Guth found a factor using $P = (17, 1)$, $b = 4$, $c = -4980$.) For Mossinghoff's version one gets the table

$$\begin{aligned}
2^4 P = 16P &= (1126060215, 1502149623)\\
(2^4 + 2^6)P = 80P &= (1711657470, 477996011)\\
(2^4 + 2^6 + 2^{10})P = 1104P &= (234439070, 38804882)\\
(2^4 + 2^6 + 2^{10} + 2^{12})P = 5200P &= (1158684598, 1064974943)\\
(\text{previous partial sum}) + 2^{13}P = 13392P &= (487240237, 1393430236)\\
(\text{previous partial sum}) + 2^{14}P = 29776P &= (1236999455, 390791552)\\
(\text{previous partial sum}) + 2^{15}P = 62544P &= (1695955849, 1498221355)\\
(\text{previous partial sum}) + 2^{17}P = 193616P &= (1616297325, 461346409)\\
(\text{previous partial sum}) + 2^{19}P = 717904P &= (373023881, 1510113896)\\
(\text{previous partial sum}) + 2^{20}P = 1766480P &= (1211273029, 1248862167)\\
(\text{previous partial sum}) + 2^{21}P = 3863632P &= (1115004543, 1676196055)
\end{aligned}$$

Now the material on the bottom of page 137 (starting at line −5) and the top half of page 138 can be replaced with:

we find that we are able to compute $kP \pmod n$ for all $b = 3, 4, 5, \ldots, 41$.

However, when we try $b = 42$, and $c = -91$, the addition law breaks down and we find a factor of n. What happens is the following. We have no trouble making a table of $2^i P \pmod n$ for $0 \le i \le 23$, just as above. Then we start adding up the points in the table to compute $kP \pmod n$. At the penultimate step we find

$$\begin{aligned}
(2^4 + 2^6 + 2^{10} + \cdots + 2^{20} + 2^{21})P &= 3863632P\\
&\equiv (1115004543, 1676196055) \pmod n.
\end{aligned}$$

Next, we read off from the (omitted) table

$$2^{23}P \equiv (1267572925, 848156341) \pmod n.$$

So to get kP we need to add these two points,

$$(1115004543, 1676196055) + (1267572925, 848156341) \pmod n.$$

To do this we have to take the difference of their x coordinates and find the inverse modulo n. But when we try to do this, we discover that the inverse does not exist because

$$\gcd(1115004543 - 1267572925, n) = \gcd(-152568382, 1715761513) = 26927.$$

So the attempt to compute $12252240(2,1)$ on the curve

$$y^2 = x^3 + 42x - 91 \pmod{1715761513}$$

fails, but it leads to the factorization

$$n = 1715761513 = 26927 \times 63719.$$

One easily checks that each of these factors is prime, so this gives the full factorization of n.

Page 144: Exercise 4.17(a)

The r_i remainders may be negative, so the condition on r_{i+1} needs absolute value signs: $-\frac{1}{2}|r_i| < r_{i+1} \le \frac{1}{2}|r_i|$.

Page 144: Exercise 4.21

The given parameters do not give a factor of n. Mossinghoff finds the first b is $b = 59$, and Guth finds a factor using $b = 234$ and $k = 12252240$. So replace the given elliptic curve with

$$C : y^2 = x^3 + 59x - 59.$$

On this curve we have

$$\begin{aligned} 8104P &= (3834541, 80821724) \pmod{199843247} \quad \text{and} \\ 2^{13}P = 8192P &= (116509380, 17880653) \pmod{199843247}. \end{aligned}$$

When we try to add these two points we find that

$$\gcd(3834541 - 116509380, 199843247) = \gcd(-112674839, 199843247) = 10289.$$

This leads to the factorization

$$199843247 = 10289 \cdot 19423.$$

Page 151: top

"smallest m is 3242197" should be "smallest m is 3367", since

$$3367 = -33^3 + 34^3 = -9^3 + 16^3 = -2^3 + 15^3.$$

Could also include the following cube-free example with 4 representations, and thank Abderrahmane Nitaj (Univ. Caen) for providing the example.

$$\begin{aligned} 16776487 &= 7 \cdot 13 \cdot 19 \cdot 31 \cdot 313 \\ &= -201^3 + 292^3 = -9^3 + 256^3 = 183^3 + 220^3 = 58^3 + 255^3. \end{aligned}$$

Page 151: Middle of Page
"To conclude, we want to describe a conjecture of Serge Lang ...". But the conjecture is never actually stated.

Page 156: Line -10
"proof!)" should be "proof)!"

Page 165: Line -4
"contant" should be "constant"

Page 176: Bottom Half of Page
Either the Baker lower bound should be $> 10^{-6}/q^{2.955}$ or else the bound on y should be $|y| \le 10^{1317} \cdot |c|^{2000/9}$.

Page 181: Line 13
"smallest subfield of $\mathbb{C}$ contain all of" should be "smallest subfield of $\mathbb{C}$ containing all of"

Page 203: Lines 8,9
"contains no non-empty set" should be "contains no non-empty open set"

Page 203: Line -5
"because f is a homomorphism" is not strictly true, it's only true locally. Say instead "from given property of f".

Page 204: Line 10
Replace $\frac{\mathbb{C}}{L}$ by either $\mathbb{C}/L$ or $\dfrac{\mathbb{C}}{L}$.

Page 204: Line 2 of Paragraph 2
"if L is an integer" should be "if c is an integer"

Page 214: Exercise 6.4
"$2y\psi_{2n} = \psi_n(\psi_{n+1}\psi_{n-1}^2 - \cdots$" should be "$2y\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \cdots$".
"$4y\omega_n = \psi_{n+1}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$" should be "$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$".

Page 219: Exercise 6.21(b)
"$z \longmapsto \big(4\wp(z), 4\wp'(z)\big)$" should be "$z \longmapsto \big(4\gamma^2\wp(z), 4\gamma^3\wp'(z)\big)$"

Page 225: Line 6 of Paragraph 3
"in the the projective plane", remove a "the".

Page 237: -12
There is a bad line break in the middle of $I(C_1 \cap C_2, P) = 1$.

Page 240: Lines 3–6
This "exercise" is difficult. Warn the reader that it is difficult, and refer them to exercise A.17 in the case that the 8 points are distinct.

Page 253: Line 12
"some coefficient of $\tilde{F}$ is not" should be "some coefficient of F is not"

Page 256: Exercise A.10(a) and A.10(b)
"tranformation" should be "transformation" (2 times).

Page 1–∞: Entire book

It has been strongly suggested that we write G/H for quotient groups, rather than $\dfrac{G}{H}$.

Joseph H. Silverman
Mathematics Department, Box 1917
Brown University
Providence, RI 02912 U.S.A
(401) 863-1132
⟨jhs@gauss.math.brown.edu⟩