

ERRATA AND CORRECTIONS TO RATIONAL POINTS ON ELLIPTIC CURVES

JOSEPH H. SILVERMAN AND JOHN TATE

A separate list of errata that were corrected in the second printing is included at the end of this document. You can verify that you have the second corrected printing by looking on page viii and checking that it includes acknowledgements for the second printing. (You can also check at the bottom of the copyright page, where it will say “Corrected Second Printing.”)

Acknowledgments

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, A. Berkovich, J. Blumenstein, J. Brillhart, D. Clausen, D. Freeman, L. Goldberg, F. Goldstein, A. Guth, D. Gupta, A. Granville, I. Igusic, M. Kida, P. Kahn, J. Kraft, C. Levesque, B. Levin, J. Lipman, R. Lipes, A. Mazel-Gee, M. Mossinghoff, K. Nolish, B. Pelz, R. Pennington, R. Pries, A. Rajan, K. Ribet, M. Reid, H. Rose, L. Gómez-Sánchez J.-P. Serre, M. Szydlo, J. Tobey, C.R. Videla, J. Wendel, A. Ziv.

Page vii: Computer Packages

Remove the offer to send a formatted disk. Give URLs for some computer packages, such as the free packages

Sage (<http://www.sagemath.org>),
Pari (<http://pari.math.u-bordeaux.fr/>).

Page 1: Footnote 2

Fermat’s Last Theorem is now Wiles’ Theorem.

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 17: Paragraph 1

Reiterate that this is just a plausibility argument, not a proof, because the linear conditions might not be independent.

Page 24: Example

Add a more typical example, worked out in detail. (One such example is given later in errata sheet.) 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 that 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}) that 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 34: Exercise 1.11(d)

The given isomorphism is incorrect. It should be

$$P \longmapsto \mathcal{O}' * (\mathcal{O} * P).$$

Page 36: Exercise 1.18

Use Q_1, Q_2, \dots, 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 $xy^2 + (ax + b)y = cx^2 + dx + e$ is smooth if and only if $y^2 + (ax + b)y = cx^3 + dx^2 + ex$ is smooth. (These equations appear on page 23 in Section I.3.)

More precisely, call the first equation C and the second equation W . Let \mathcal{O}, P , and Q be points on C given by

$$\mathcal{O} = [1, 0, 0], \quad P = [0, 1, 0], \quad Q = [0, ?, Z] \quad \text{with } Z \neq 0.$$

(a) Show that the corresponding points on W are

$$\mathcal{O}' = [0, 1, 0], \quad P' = [0, -b, 1], \quad Q' = [0, 0, 1].$$

(It is possible that $P = Q$.)

(b) Write down conditions on the coefficients of C for it to be nonsingular at \mathcal{O}, P , and Q , and similarly write down conditions on the coefficients of W for it to be nonsingular at \mathcal{O}', P' , and Q' .

(c) Use (b) to show that \mathcal{O}, P , and Q are nonsingular points of C if and only if \mathcal{O}', P' , and Q' are nonsingular points of W .

(d) Explain why at the other points $R = [x, y, 1] \in C$ and $R' = [x, xy, 1] \in W$ with nonzero x -coordinate, it is clear that R is a nonsingular point on C if and only if R' is a nonsingular point on W .

Page 46, Caption to Figure 2.5

The caption should read

Points of Order Dividing Five on a Complex Torus

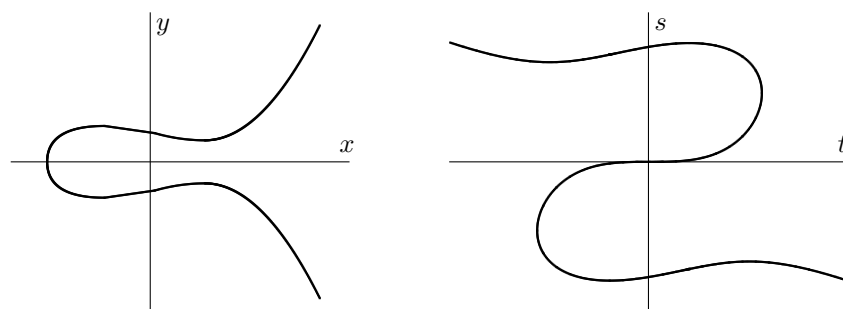
(The point \mathcal{O} is included in the figure, and it has order one, not order five.)

Page 48, Line –6

“Since x , X , and a are all integers, it follows that λ is also an integer.” Possibly point out that we know *a priori* that λ is a rational number, so λ is an integer if and only if λ^2 is an integer.

Page 51: Figure 2.6

The figure in the st -plane is not accurate. In general there are values of t that correspond to more than one value of s . Here is a corrected version of Figure 2.6.



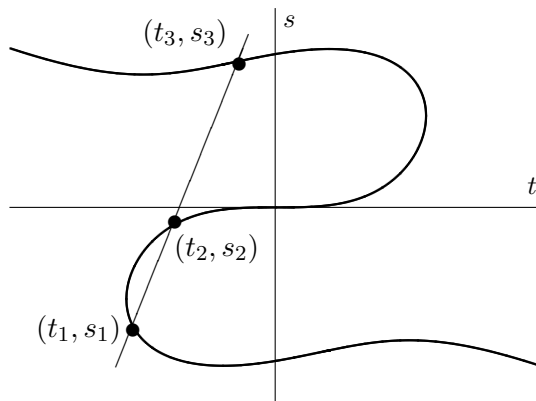
Two Views of a Cubic Curve
Figure 2.6

Page 52: Paragraph 3

If $P_1 \neq P_2$ and $t_1 = t_2$, it is not true that $P_1 = -P_2$. The argument for this case needs to be corrected.

Page 53: Figure 2.7

This figure is not an accurate depiction of the curve in the (t, s) plane. Here is a better picture:



Adding Points in the (t, s) Plane

Figure 2.7

Page 61, Exercise 2.11

This is not a mistake, but it may confuse students who know too much! The resultant of $\phi(x)$ and $f(x)$ is actually D^2 , so general theory only yields an equation of the form $Ff + \Phi\phi = D^2$. However, it is in fact possible to find F and Φ satisfying $Ff + \Phi\phi = D$, as the problem states.

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 $N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4$ 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 –2

“has rank 15” should be “has rank at least 15”. (Update to give current record, which is currently at least 28 by an example of Elkies. Refer reader to a website that contains up-to-date information.)

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 105: Exercise 3.9

Add the following sentence: “If the rank is positive, find points in $C(\mathbb{Q})$ that generate $C(\mathbb{Q})/2C(\mathbb{Q})$.”

Page 117: Lines –4 and –3

This sentence should read: “Since p divides the product on left-hand side, it divides one of the factors on the right, say $p \mid (AB_1 - A_1B)$.”

Thus left and right have been reversed.

Page 120, Lines 6–10

Replace the sentence:

In general, not much is known about the behavior of M_p as a function of p , although there is conjecture due to Taniyama and Weil which would associate to the collection of M_p 's a certain holomorphic function (called a *modular form*) which has some wonderful transformation properties.

with the sentence:

In general, the behavior of M_p as a function of p is quite complicated. There is a deep theorem of Wiles et. al. that associates to the collection of M_p 's a certain holomorphic function (called a *modular form*) that has some wonderful transformation properties. Wiles' theorem, which was originally conjectured by Shimura and Taniyama and studied by Weil, plays a key role in the proof of Fermat's last theorem.

Page 120, Lines –11

“We also recall the standard notation $\pi(X)$ for the number of primes less than X .” should be “We also recall the standard notation $\pi(X)$ for the number of primes less than or equal to X .”

Page 125, Chapter IV, Section 4

This section should be rewritten to reflect the fact that it is much easier to compute $a^{K!}$ in Pollard's algorithm and to compute $K! \cdot P$ in Lenstra's algorithm. For example, in Lenstra's algorithm, start with P and perform the loop:

```
Loop  $k = 1, 2, \dots, K$ 
  Replace  $P$  with  $kP$ 
End  $k$  Loop
```

Note that revising the algorithms also requires reworking all of the examples.

Page 125, Lines –12 and –11

“Then we will have conclusively proven that n is composite without having any idea how to factor it!” should be “Then we will have conclusively proven that n is composite without having any idea what the factors are!”

This should be changed because we do, in fact, know how to factor it, although the computation that we have done does not help in performing that factorization.

Page 125, Line –8

This is not the standard definition of *pseudo-prime*. The correct definition is that n is a *pseudoprime to the base a* if $a^{n-1} \equiv 1 \pmod{n}$. If this holds for all bases a that are relatively prime to n , then n is called a *Carmichael number*.

Thus in Exercise 4.13 on page 143, part (a) asks for a proof that 561 is a Carmichael number, while (b) asks for a proof that for any a , there are infinitely many pseudo-primes to the base a .

Page 125, Line –4

Change “the smaller factor must be less than \sqrt{n} ” to “the smaller factor must be less than or equal to \sqrt{n} ”.

Page 125, Line –2

It has been pointed out that in practice, there’s no need to check if $4|n$, since in practice, if $2|n$, then we factor out the 2 and check if 2 divides what left. It thus suffices to check if n is divisible by p for all primes up to \sqrt{n} . On the other hand, if one does not have a list of primes available, the most naive thing to do is simply check divisibility of n by all integers k up to \sqrt{n} , without worrying about winnowing out some values of k as being unnecessary.

Pages 126–127, Example 1

The method for computing powers described in the text is correct, but is not the method normally used because it requires more bookkeeping than necessary. Instead one uses the binary digits of k to square and multiply. The algorithm described in the book is a little easier to understand, but it would be worth mentioning that there is a more efficient method and give an exercise describing it.

Page 131, Computation at top of page

The value for 2^7 using in the first displayed equation is incorrect. The correct value is in the last line of the table on the bottom of page 130. The first six lines of Page 131 should read:

Using this table, we can compute

$$\begin{aligned} 2^{180} &= 2^{2^2+2^4+2^5+2^7} \\ &\equiv 16 \cdot 65536 \cdot 111566955 \cdot 214344997 \pmod{246082373} \\ &\equiv 2921261 \pmod{246082373} \end{aligned}$$

Then a short calculation using the Euclidean algorithm yields

$$\gcd(2^{180} - 1, n) = \gcd(2921260, 246082373) = 1.$$

Page 131, Displayed equations on bottom half of page

The value of 2^{2520} is incorrect (although the table of values of 2^i is correct). These two displayed equations should read:

Now we can compute

$$2^{2520} = 2^{2^3+2^4+2^6+2^7+2^8+2^{11}} \equiv 130940741 \pmod{246082373}.$$

Then the Euclidean algorithm yields

$$\gcd(2^{2520} - 1, n) = \gcd(130940740, 246082373) = 2521,$$

Page 132, Pollard’s Algorithm, Step 4

Replace “Calculate $D = \gcd(a^k - 1, n)$ ” with “Calculate $b \equiv a^k - 1 \pmod{n}$, and then $D = \gcd(b, n)$,” since we certainly don’t want to calculate the exact value of a^k .

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 prime p dividing n has the property that $p - 1$ divides k .

Page 137: Line 3

The value of “ kP ” is incorrect. This line should read

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

Page 151: Line 11

“the smallest value of m is 3242197” is not correct. It should say “the smallest value of m is 3367, which has the representations

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

And as long as we are allowing x or y to be negative, there is also an example with four representations,

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

(Abderrahmane Nitaj and Masanari Kida sent this example.)

Page 178, Problem 5.7

This exercise should specify that β is a real number that is not rational. Thus “Let $\beta \in \mathbb{R}$ be a real number with $\beta \notin \mathbb{Q}$.”

Page 217, Exercise 6.17

Parts (b) and (c) of this exercise are incorrect. Here are correct versions:

(b) Prove that for all $s \in \text{Gal}(K_n/\mathbb{Q}(i))$ there is an integer $m \in (\mathbb{Z}/n\mathbb{Z})^*$ such that

$$(s\tau s\tau^{-1})(P) = mP \quad \text{for all } P \in C[n].$$

In other words, the matrix describing the action of $s\tau s\tau^{-1}$ on $C[n]$ is the diagonal matrix $\begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}$.

(c) Prove that $\text{Gal}(K_n/\mathbb{Q})$ is abelian if and only if for every element $s \in \text{Gal}(K_n/\mathbb{Q}(i))$ there is an integer m such that

$$s^2(P) = mP \quad \text{for all } P \in C[n].$$

Page 237: Line -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 238, line -14

“than the number $(d+1)(d+1)/2$ of unknown coefficients” should be “than the number $(d+1)(d+2)/2$ of unknown coefficients”

Page 247, Lines 5 and 6

Two of the three occurrences of \mathcal{O}_P should be $(f_1, f_2)_P$. Thus these two lines should read:

so $t_1 t_2 \cdots f_i(1 - t_{i+1}\phi) = \psi \in (f_1, f_2)_P$. But $(1 - t_{i+1}\phi)(P) = 1$, so we have $(1 - t_{i+1}\phi)^{-1} \in \mathcal{O}_P$. Hence $t_1 t_2 \cdots t_r = \psi t_{i+1} \cdots t_r (1 - t_{i+1}\phi)^{-1} \in (f_1, f_2)_P$

Page 249, Line 22

“they are are invariant”

Page 257, Exercise A.14(b)

“we gave a plausibility argument” should be “we gave a plausibility argument”. (“argument” is misspelled.)

Page 1–∞: Entire book

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

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

Transformation to Weierstrass Form: An Example for Page 24

To illustrate this procedure, we will take the curve

$$C : X^3 + 2Y^3 + 4Z^3 - 7XYZ = 0 \quad \text{and the point } \mathcal{O} = [1, 1, 1]$$

and put it into Weierstrass form. Before starting, we observe that in general, the tangent line in \mathbb{P}^2 to a curve described by a homogeneous equation

$$F(X, Y, Z) = 0$$

at the point $P_0 = [X_0, Y_0, Z_0] \in \mathbb{P}^2$ is given by the homogeneous linear equation

$$\frac{\partial F}{\partial X}(P_0)X + \frac{\partial F}{\partial Y}(P_0)Y + \frac{\partial F}{\partial Z}(P_0)Z = 0.$$

Looking at Figure 1.1, we see that a good first step is to move the point \mathcal{O} to the point $[1, 0, 0]$, so we make the substitution

$$X_1 = X, \quad Y_1 = Y - X, \quad Z_1 = Z - X.$$

This transforms the equation for C into

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

The tangent line to C at $\mathcal{O} = [1, 0, 0]$ is $Y_1 - 5Z_1 = 0$, and according to Figure 1.10, we want this tangent line to be the line $Z = 0$. So we make the substitution

$$X_2 = X_1, \quad Y_2 = Y_1, \quad Z_2 = Y_1 - 5Z_1,$$

which gives the equation

$$C : 635X_2 Y_2^2 + 254Y_2^3 - 125X_2^2 Z_2 + 55X_2 Y_2 Z_2 - 12Y_2^2 Z_2 \\ + 60X_2 Z_2^2 + 12Y_2 Z_2^2 - 4Z_2^3 = 0.$$

The tangent line at $\mathcal{O} = [1, 0, 0]$ is now the line $Z_2 = 0$. To find the other intersection point of this line with C , we substitute $Z_2 = 0$ into the equation for C . This leads to $127Y_2^2(5X_2 + 2Y_2) = 0$, and thus the third intersection point is

$$\mathcal{O} * \mathcal{O} = [2, -5, 0].$$

Again looking at Figure 1.10, we move this point to $[0, 1, 0]$ by making the substitution

$$X_3 = 5X_2 + 2Y_2, \quad Y_3 = Y_2, \quad Z_3 = Z_2,$$

which gives

$$C : 127X_3 Y_3^2 - 5X_3^2 Z_3 + 31X_3 Y_3 Z_3 - 54Y_3^2 Z_3 + 12X_3 Z_3^2 - 12Y_3 Z_3^2 - 4Z_3^3 = 0.$$

The tangent line to C at the point $[0, 1, 0]$ is now easily computed; it turns out to be $127X_3 - 54Z_3 = 0$. A final look at Figure 1.10 shows that this line should be moved to $X = 0$, we we make the substitution (note that we want the line $Z = 0$ and the point $[1, 0, 0]$ to stay where they are)

$$X_4 = 127X_3 - 54Z_3, \quad Y_4 = Y_3, \quad Z_4 = Z_3.$$

This transforms C into

$$C : 16129X_4 Y_4^2 - 5X_4^2 Z_4 + 3937X_4 Y_4 Z_4 + 984X_4 Z_4^2 \\ + 19050Y_4 Z_4^2 + 32000Z_4^3 = 0.$$

Don't despair, we're almost done. We dehomogenize using $x_5 = X_4/Z_4$ and $y_5 = Y_4/Z_4$ to get

$$C : 3200 + 984x_5 - 5x_5^2 + 19050y_5 + 3937x_5y_5 + 16129x_5y_5^2 = 0.$$

Next we multiply by x_5 and let $x_6 = x_5$ and $y_6 = x_5y_5$, which gives

$$C : 3200x_6 + 984x_6^2 - 5x_6^3 + 19050y_6 + 3937x_6y_6 + 16129y_6^2 = 0.$$

To make the coefficient of x_6^3 equal to 1 and the coefficient of y_6^2 equal to 4, we set $x_7 = 20x_6$ and $y_7 = 2540y_6 = 4 \cdot 5 \cdot 127y_6$ and obtain

$$C : 256000x_7 + 3936x_7^2 - x_7^3 + 12000y_7 + 124x_7y_7 + 4y_7^2 = 0.$$

Finally, we complete the square in y_7 by setting

$$x = x_7 \quad \text{and} \quad y = 2y_7 + 31x_7 + 3000,$$

which puts C into Weierstrass form,

$$C : y^2 = x^3 - 2975x^2 - 70000x + 9000000.$$

Further, tracing through all of the substitutions, we find that the transformation taking the original equation

$$C : X^3 + 2Y^3 + 4Z^3 - 7XYZ = 0$$

to the Weierstrass equation is given by the formulas

$$x = \frac{100(33X + 40Y + 54Z)}{4X + Y - 5Z},$$

$$y = \frac{-63500(6X^2 - 7XY - 18Y^2 + 21XZ - 14YZ + 12Z^2)}{(4X + Y - 5Z)^2}.$$

(The substitution $(x, y) = (25x_0, 125y_0)$ gives an equation with smaller integer coefficients, $y_0^2 = x_0^3 - 119x_0^2 - 112x_0 + 576$.)

Errata That Were Fixed In The Second Printing

Page 4–5: Footnote (corrected in 2nd printing)

Replace “ $f(x, y)$ ” with “ $f(x_1, x_2, \dots, x_n)$ ”, since this footnote deals with polynomials in many variables.

Page 7: Line 1 (corrected in 2nd printing)

“turns them” should be “turns it”

Page 11: Figure 1.2 (corrected in 2nd printing)

The point marked $(-1, t)$ should be $(-1, 0)$.

Page 15: Line 3 (corrected in 2nd printing)

After “solution in integers”, add “, not all zero,”.

Page 22: Line –1

Rewrite this paragraph to talk about the line $X = 0$ instead of the X -axis, similarly with Y and Z .

Page 23: Figure 1.10 (corrected in 2nd printing)

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 33: Line –2 of Exercise 1.8 (corrected in 2nd printing)

$5 - \textit{adic}$ should be 5 -adic. (The “adic” should not be italicized.)

Page 39: Line –6 (corrected in 2nd printing)

“of $2P$ and equal” should be “of $2P$ equal”

Page 42: Line –1 (corrected in 2nd printing)

“order $\frac{1}{2}m$ ” should be “order m ”.

Page 48: Last two lines (corrected in 2nd printing)

“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 67: Line 2 (corrected in 2nd printing)

“contant” should be “constant”

Page 77: 3rd Displayed Equation (corrected in 2nd printing)

“ $\bar{C} : y^2 = x^2 + \bar{a}x^2 + \bar{b}x$ ” should be “ $\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$ ”. (I.e., the exponent on x should be 3, not 2.)

Page 78: 2nd Displayed Equation (corrected in 2nd printing)

“ $\bar{u} = \frac{1}{2}c_1\omega_1 + c_2\omega_2 = c_1\bar{\omega}_1 + c_2\bar{\omega}_2$ ” 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 (corrected in 2nd printing)

“ $(\bar{\lambda}x + \bar{\nu})^2 = f(x)$ ” should be “ $(\bar{\lambda}x + \bar{\nu})^2 = f(x)$ ”, 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 (corrected in 2nd printing)

“ $\pm(\text{rational number})^2$ ” should be “ $\pm(\text{integer})^2$ ”

Page 98: Line 15 (corrected in 2nd printing)

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 99: Line -3 (corrected in 2nd printing)

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

Page 100: 3rd Displayed Equation (corrected in 2nd printing)

“ $(x, y) \mapsto \frac{x}{y}$ ” should be “ $(x, y) \mapsto \frac{y}{x}$ ”

Page 105: Exercise 3.7(c) (corrected in 2nd printing)

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

Page 105: Exercise 3.11 (corrected in 2nd printing)

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

Page 107: Line -6 (corrected in 2nd printing)

“an element of \mathbb{F}_p .” should be “an element of \mathbb{F}_p .”

Page 109: Line -1 of Paragraph 3 (corrected in 2nd printing)

“non-residues.” should be “non-residues.”

Page 117: Line 6 (corrected in 2nd printing)

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

Page 126: Line 2 (corrected in 2nd printing)

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

Page 135: Equation for λ in Center of Page (corrected in 2nd printing)

The equation given for λ is actually the formula for $x(2Q)$. Replace it with $\lambda =$

$$\frac{f'(x)}{2y} = \frac{3x^2 + 2ax + b}{2y} \pmod{n}.$$

Page 136: Computation of kP at Bottom (corrected in 2nd printing)

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 (corrected in 2nd printing)

The table heading should be “ $2^iP \pmod{1715761513}$ ”. (I.e., the modulus should be 1715761513, not 246082373.) The entries in the table are correct.

Page 137: Line –5 ff (corrected in 2nd printing)

The book asserts that no factor is found with $P = (2, 1)$ and $1 \leq b \leq 253$, 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

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

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 $b = 3, 4, 5, \dots, 41$.

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 $0 \leq i \leq 23$, just as above. Then we start adding up the points in the table to compute $kP \pmod{n}$. At the penultimate step we find

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

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) (corrected in 2nd printing)

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

Page 144: Exercise 4.21 (corrected in 2nd printing)

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: Middle of Page (corrected in 2nd printing)

“To conclude, we want to describe a conjecture of Serge Lang ...”. But the conjecture is never actually stated.

Page 156: Line –10 (corrected in 2nd printing)

“proof!” should be “proof)!” Or just remove the parentheses.

Page 165: Line –4 (corrected in 2nd printing)

“contant” should be “constant”

Page 176: Line –3 (corrected in 2nd printing)

The bound on y should be $|y| \leq 10^{1317} \cdot |c|^{2000/9}$.

Page 181: Line 13 (corrected in 2nd printing)

“smallest subfield of \mathbb{C} contain all of” should be “smallest subfield of \mathbb{C} containing all of”

Page 203: Lines 8,9 (corrected in 2nd printing)

“contains no non-empty set” should be “contains no non-empty open set”

Page 203: Line –5 (corrected in 2nd printing)

“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 (corrected in 2nd printing)

Replace $\frac{\mathbb{C}}{L}$ by either \mathbb{C}/L or $\frac{\mathbb{C}}{L}$.

Page 204: Line 2 of Paragraph 2 (corrected in 2nd printing)

“if L is an integer” should be “if c is an integer”

Page 214: Exercise 6.4 (corrected in 2nd printing)

“ $2y\psi_{2n} = \psi_n(\psi_{n+1}\psi_{n-1}^2 - \dots)$ ” should be “ $2y\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \dots)$ ”.

“ $4y\omega_n = \psi_{n+1}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$ ” 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) (corrected in 2nd printing)

“ $z \mapsto (4\wp(z), 4\wp'(z))$ ” should be “ $z \mapsto (4\gamma^2\wp(z), 4\gamma^3\wp'(z))$ ”

Page 225: Line 6 of Paragraph 3 (corrected in 2nd printing)

“in the the projective plane”, remove a “the”.

Page 253: Line 12 (corrected in 2nd printing)

“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) (corrected in 2nd printing)

“tranformation” should be “transformation” (2 times).