A First Course in Modular Forms:
Corrections to the Third Printing

March 21, 2016

(*The corrections here are also corrections to the earlier printings, but the third printing's pagination has changed a bit. In case of problems locating a correction here in an earlier printing, please email* `jerry@reed.edu`.)

Chapter 1

- Pages 21–22: The wording of exercise 1.2.4 can be improved a bit because the condition $d = 0$ is impossible in $\varGamma_0(4)$.

Chapter 2

- Page 47, lines (-2)–(-1): Change "group" to "subset of $\mathrm{SL}_2(\mathbb{R})$" on line (-2), and change "group" to "subgroup" on line (-1).
- Page 55, line 2: Change "$\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$" to "$\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$".
- Page 55, line (-6): Change "proving (1)" to "proving (c)".
- Page 56, exercise 2.3.2: Change "If" to "If the nontrivial transformation".
- Page 56, exercise 2.3.5(b): Change "third" to "fourth".
- Page 61, line 14: Change "width" to "period".

Chapter 3

- Page 65, line (-2): Change "$Y \backslash h(\mathcal{E})$" to "$Y \backslash f(\mathcal{E})$".
- Page 66, line 20: Change "equal genus" to "equal genus $g \geq 1$".
- Page 69, lines 4–5 (and the relevant bibliography item): Helena Verrill's fundamental domain drawer is at
  `http://www.math.lsu.edu/ verrill/fundomain/`
  on April 8, 2008.
- Page 70, line (-14): Change "of order 4" to "with $j' \neq j$".
- Page 70, line (-6): Change "$-6, \dots, 7$" to "$-6, \dots, 6, \infty$".
- Page 70, line (-5): Change "of order 3 or 6" to "with $j' \neq j$".
- Page 70, line (-1): Change "with with" to "with".

- Page 72: The quantity denoted h in lines 4–7 should be given a different name such as $\hbar$, as it is not necessarily the h or the h' in the discussion on page 74. The sentence "Thus f has period $\hbar$." on lines 4–5 is correct, but $\hbar$ need not be the smallest period of f.
- Page 74, line (-9): Change "$q_{h'} = e^{2\pi i/h'}$" to "$q_{h'} = e^{2\pi i\tau/h'}$".
- Page 74, line (-8): Delete "$q_{h'} = e^{2\pi i\tau/h'}$ and".
- Pages 74–75: The discussion in the "Defining…" paragraph on page 74 has an error: the period is $2h$ in the third case independently of k, even though $f(\tau+h) = f(\tau)$ for k even. That is, in the first two cases we have $h' = 2\hbar = 2h$ but in the third case we have $h' = \hbar = 2h$. On page 75, remove "and k is odd" from (3.3), and change the text immediately following, from "This can be half-integral in the exceptional case, when $\pi(s)$ or s itself is called an *irregular cusp* of Γ. For example, when k is odd $1/2$ is an irregular cusp…" to "This is half-integral if $(\alpha^{-1}\Gamma\alpha)_\infty = \langle -\left[\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right]\rangle$ (when $\pi(s)$ or s itself is called an *irregular cusp* of Γ) and k is odd. For example, $1/2$ is an irregular cusp…".
- Page 81, paragaph beginning "On the other hand...": Replace the discussion leading up to (3.7) with "On the other hand, if U_j contains a cusp s_j then δ_j takes s_j to ∞ and the function $(f[\alpha]_{2n})(z)$ takes the form $g_j(q_h)$ where h is the width of s and $q_h = e^{2\pi iz/h}$; here g_j is meromorphic in q_h at 0 if the cusp is regular and g_j is meromorphic in $q_h^{1/2} = e^{\pi iz/h}$ at 0 if the cusp is irregular, but we think of g_j as a series in powers of q_h (half-integral powers in the irregular case) so that the order is the index of the leading coefficient. The relevant local differential is now".
- Page 81, line (-7): Change "$\Omega^{k/2}(\mathcal{H})$" to "$\Omega^{\otimes k/2}(\mathcal{H})$".
- Page 90: Change "$\varepsilon_{3,i}$" to "ε_3" on the first line of the three-line display.
- Page 95, line 4: Change "γ" to "γ_J".
- Page 95, line 15: Change "$\gamma =$" to $\gamma = \det m \cdot$".
- Section 3.7: A more transparent approach comes from the moduli space point of view, identifying $Y_0(N)$ and $\mathrm{S}_0(N)$ as in Theorem 1.5.1. For $N = 1$, elliptic points of $Y_0(N)$ correspond to elliptic curves $\mathbb{C}/\Lambda_\tau$ with automorphisms other than multiplication by ± 1. Since only two imaginary quadratic orders have more than two units, and they are both PID's, there are two elliptic points: one of order 2 corresponding to $\Lambda_\tau = i\mathbb{Z} \oplus \mathbb{Z}$, and one of order 3 corresponding to $\Lambda_\tau = \mu_3\mathbb{Z} \oplus \mathbb{Z}$. For $\Gamma_0(N)$, reason likewise. To find elliptic points of order 3, for example, look at the order N cyclic subgroups of the lattice $\mu_3 N\mathbb{Z} \oplus N\mathbb{Z}$, and count how many of them are invariant under multiplication by μ_3. These are precisely the subgroups generated by $m\mu_3 + 1$ where $m^2 - m + 1 \equiv 0 \pmod N$. Thus the number of elliptic points of order 3 is the number of solutions of the congruence $m^2 = m + 1 \equiv 0 \pmod N$.
- Page 103, line 9: Change "$y_0 \equiv c'c^{-1} \pmod N$" to "$y_0 \equiv c'c^{-1} \pmod{N/d}$". A procedure to list the cusps of $\Gamma_0(N)$ is as follows: For each positive divisor of N choose some nonnegative integer c such that $\gcd(c, N)$ is the

given divisor (e.g., take $c = 0$ if the divisor is N and otherwise take c to be the divisor), then for each class in $(\mathbb{Z}/\gcd(c, N/\gcd(c,N))\mathbb{Z})^*$ choose a representative a coprime to c and take a matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$. Note that $(\mathbb{Z}/\mathbb{Z})^\times$ is not empty but rather consists of one class, all of $\mathbb{Z}$. Especially, if $\gcd(c, N/\gcd(c,N)) = 1$ then the only corresponding cusp is $\left[\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right]$ (though for $c = 1$ the representative $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ is preferable to $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$), and thus a squarefree level $N = p_1 \cdots p_t$ has 2^t cusps. Similarly, for $N = 4$ there are three cusps, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right]$, and $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, and for $N = 9$ there are four cusps, $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 2 & 1 \\ 3 & 2 \end{smallmatrix}\right]$, and $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.
- Page 106, fifth line of section 3.9: Change "$X_1(N)$" to "$X(1)$".
- Page 106, after the displayed formula for $d(\Gamma_1(N))$: Change "So $-I \notin \Gamma_0(N)$ while $-I \in \mathrm{SL}_2(\mathbb{Z})$." to "So $-I \notin \Gamma_1(N)$ but $-I \in \Gamma_0(N)$."

Chapter 4

- Page 123, line 9: Change "$a_{n^{-1}}(k)$" to "$a_n(k)$".
- Page 123, exercise 4.4.1(c): Change "$\mathrm{Re}(s) > 1$" to "$\mathrm{Re}(s) > 0$".
- Page 127, line 13: Change "$e' \equiv (e + c'b_\gamma)d_\gamma \pmod u$" to "$e' \equiv (e + c'b_\gamma)d_\gamma - q \pmod u$, where $q = (d' - dd_\gamma)/v$".
- Page 131: On the second line of the first two-line display the summand should begin "$m\mu_N^{d_v m}$" rather than "$\mu_N^{d_v m}$". On the third line of the three-line display a right parenthesis is missing from "$(1 - \delta(\overline{c}_v))$" and the summand has the same error.
- Page 133: Add an Exercise 4.6.4: "Use results from Chapter 3 to show that $\mathcal{S}_2(\Gamma_0(4)) = 0$ and that $\dim(\mathcal{M}_2(\Gamma_0(4))) = 2$. This section shows that $E_2^{\mathbf{1}_1,\mathbf{1}_1,2}$ and $E_2^{\mathbf{1}_1,\mathbf{1}_1,4}$ form a basis of $\mathcal{M}_2(\Gamma_0(4))$; the function $\theta(\tau,4)$ from the beginning of Section 1.2 lies in $\mathcal{M}_2(\Gamma_0(4))$ as well. Show that $\theta(\tau,4)$ is a scalar multiple of $E_2^{\mathbf{1}_1,\mathbf{1}_1,4}$. Show that $E_2^{\mathbf{1}_1,\mathbf{1}_1,4} - 3E_2^{\mathbf{1}_1,\mathbf{1}_1,2}$ is a scalar multiple of the function

$$f(\tau) = \sum_{\substack{n \geq 1 \\ \text{odd}}} \sigma_1(n) q^n$$

(which is not a cusp form despite vanishing at infinity). Thus $\theta(\tau,4)$ and $f(\tau)$ form a basis of $\mathcal{M}_2(\Gamma_0(4))$."
- Page 136, line 11: Change "negated" to "preserved".
- Page 136, line 12: Change "$t > 0$" to "$t < 0$".
- Page 136, line 13: Change "$\int_{t=-\infty}^{0}$" to "$\int_{t=0}^{-\infty}$".
- Page 137, line 9: Change "(n)" to "(k)".
- Page 139: Right parenthesis missing from "$(1 - \delta(\overline{c}_v))$" on the second line of the second two-line display.
- Page 140, line 8: Change "$-c_v$" to "$N - c_v$" in the first superscript. Make the same change on page 142 in exercise 4.8.6.
- Page 140, line (-1): Change the first ζ-superscript to "$\overline{d + ev}$".

- Page 146, exercise 4.9.2: In part (a), change the condition defining S_m to "$|n| = m$", omit the "Note that..." sentence, and change "$l(2m+1)^{l-1}$" to "$(2m+1)^l$". In part (c), change "$l(2m+1)^{l-1}$" to "$(2m+1)^l$" and take the first sum over $n \in \mathbb{Z}^l$ such that $|n| \geq M$.
- Page 155, line 5: Change "$g(\bar{\varphi})/v$" to "$\varphi(-1)g(\bar{\varphi})/v$".
- Page 155, line 11: Change "$(-1)^k$" to "$\psi(-1)$".
- Page 155, line 19: Remove "$\varphi(-1)$".
- Page 157, line 14: The two-line display should end "$\cdots = \theta^{\overline{v}}(it, N)$".
- Page 162, exercise 4.11.5(c): The definition of $\sigma_0^{\psi,\mathbf{1}}(m)$ should sum over divisors of m.

Chapter 5

- Page 174, diagram (5.8): Change "$\mathcal{D}$" to "Div" four times.
- Page 186, line 4: Change "$\beta_j' = \det(\beta)\beta^{-1}$" to "$\beta_j' = \det(\beta_j)\beta_j^{-1}$".
- Page 192, line 8: Delete "$\pi_{d_1 d_2} =$".
- Page 202, third line of the three-line display in the middle of the page: Change "p^{1-k-2s}" to "p^{k-1-2s}".
- Page 204, second line of section 5.10: Change "n^s" to "n^{-s}".
- Page 204, line (-3): Change "idempotent" to "an involution".
- Page 205, line 4: Delete "under the Hecke algebra".
- Page 206, line 3: Change "idempotent" to "an involution".
- Section 5.11: The calculation of orthogonality is formally correct, but the absolute convergence of the double integral is not supported correctly by the text.
- Page 209, line 1: Change $f(\alpha(\tau'))$ to $(f[\alpha]_k)(\tau')$.
- Page 209, lines 2–3: Delete "if $\mathrm{Re}(k+2s) > 0$".

Chapter 6

- Page 212, lines (-4) and (-5): Change "$V_{1,2}$" to "V_1" and change "$V_{2,1}$" to "V_2".
- Page 214, line 12 (third display): Change "$f \in \mathbb{C}(X)$" to "$f \in \mathbb{C}(X)^*$".
- Page 215, line (-3): Change "homomorphic" to "homomorphism".
- Page 220, line (-5): Change "γ" to "δ".
- Page 221, line (-1): Change "$\int \gamma$" to "$\int_\gamma$".
- Page 228: In diagram (6.11), change "$[\gamma_{Y,j}]_2$" to $[\alpha^{-1}\gamma_{Y,j}]_2$" and also change the last "X" to "Y"; in the following display, change "$[\gamma_{Y,j}]_2$" to $[\alpha^{-1}\gamma_{Y,j}]_2$".
- Page 232, line (-2): Change "$R(f(x), g(x), x)$" to "$R(f(x), g(x); x)$".
- Page 233, line (-3): Change "characteristic" to "minimal".
- Page 235, paragraph starting "Again suppose": Also A and $\mathbf{k}$ are assumed to be structurally compatible as needed.
- Page 239, second display: Change "g" to "g_i" on the right side of the equality.

Chapter 7

- Page 268, line 3: Change "$\in$" to "$\subset$" twice.
- Page 273: Change "$\overline{\mathbf{k}}[x]$" to "$\overline{\mathbf{k}}(x)$" in (7.6).
- Page 275: Change Exercise 7.3.4(b) to "Show that if $\nu_P(x)$ is even and nonzero, or if $\nu_P(x) = 0$ and $\nu_P(y) \neq 0$, then $\nu_P(F(x))$ is even for any rational function F.". These are the cases used in the text.
- Page 277, line 9: Change "$(f_2 \circ [N]$" to "$(f_2 \circ [N])$".
- Page 283, lines 8–10: Replace the sentence beginning, "A complementary argument. . . " with "For each $\overline{v} \in (\mathbb{Z}/N\mathbb{Z})^2$, the function $f_0^{\pm\overline{v}}$ determines two N-torsion points of E_j unless $2v = 0$, in which case it determines one (Exercise 7.5.5(a)), and so we have found all N^2 points of $E_j[N]$ (Exercise 7.5.5(b))."
- Page 286: Replace Exercise 7.5.5. The new exercise is, "(a) Show that for each $\overline{v} \in (\mathbb{Z}/N\mathbb{Z})^2$, the function $f_0^{\pm\overline{v}}$ determines two N-torsion points of E_j unless $2v = 0$, in which case it determines one. (b) Show that consequently, regardless of whether N is odd or even, we have found all N^2 points of $E_j[N]$."
- Page 290: In the second paragraph of Section 7.7, change "three" to "two" and remove the references to $\mathbb{K}_0'$, $\mathbb{C}(j, j_N)$, and K_0'. (It takes some work to show that $\mathbb{K}_0'$ is an intermediate field as claimed, and we do not need this result.)
- Page 291, line 14: Change "indeterminants" to "indeterminates".
- Page 291, line (-6): Change "either f_0 or j_N" to "f_0".
- Page 294, line (-9): Change "K_0, K_0', and K_1" to "K_0 and K_1".

Chapter 8

- Page 316, line (-15): Change "lie in $\mathbf{k}$." to "lie in $\mathbf{k}$. For $\mathrm{char}(\mathbf{k}) = 2$, assume that every element of $\mathbf{k}$ is a square.".
- Page 326, line 1: Change the initial value "$a_1(E) = 1$" to "$a_1(E) = 2$". Furthermore, the normalized solution-counts that are denoted $a_{p^e}(E)$ on page 325 should be given a different name, as the true $a_{p^e}(E)$ are indeed defined as on page 361 by the same initial value and recurrence as the Fourier coefficients $a_{p^e}(f)$ of a newform. For now the normalized solution-counts are renamed $t_{p^e}(E)$. Note that $t_p(E) = a_p(E)$.
- Page 333, line (-15): Change "$\overline{\mathbb{Z}}$" to "$\overline{\mathbb{Z}}_{(\mathfrak{p})}$".
- Page 334, line 3: Change "kernel" to "kernel zero and".
- Page 335, line 12: Change "$[N]$" to "$[p]$" twice.
- Page 336, line 3: Change "μ^6" to "μ_6".
- Page 342, line 20 (end of first complete paragraph): Change "J_i" to "$J_{(i)}$".
- Page 346, line 5: Change "$I \mapsto IM$" to "$I \mapsto I\mathbf{k}[C]_P$".
- Page 351, lines 4–6 (clarification, not correction): The argument given is necessary. The fact that the bottom arrow of the diagram is the zero map does not immediately show that $\ker(\tilde{\psi}) = \widetilde{E'}[p]$, because the domain of $\tilde{\psi}$ is all of $\widetilde{E'}$.
- Page 353, line (-8): Change "(7.18)" to "(7.18) (page 304)".

- Page 361: The right idea is to define for any prime p the local counting zeta-function of E, encoding the normalized solution-counts $t_{p^e}(E) = p^e + 1 - |\widetilde{E}(\mathbb{F}_{p^e})|$, as

$$Z_p(X, E) = \exp\left(\sum_{e=1}^{\infty} \frac{t_{p^e}(E)}{e} X^e\right).$$

Taking logarithmic derivatives shows that in fact for $X = p^{-s}$ the local zeta-function takes the form of an Euler factor,

$$Z_p(p^{-s}, E) = (1 - a_p(E)p^{-s} + \mathbf{1}_E(p)p^{1-2s})^{-1}.$$

(The relation $a_p(E) = t_p(E)$ is explained in the correction to page 326.) The *Hasse-Weil L-function of E* is the product of these Euler factors,

$$L(s, E) = \prod_p (1 - a_p(E)p^{-s} + \mathbf{1}_E(p)p^{1-2s})^{-1}.$$

By the methods of the proof of Theorem 5.9.2, the Dirichlet series form of the L-function is

$$L(s, E) = \sum_{n=1}^{\infty} a_n(E)n^{-s}$$

where similarly to the Fourier coefficients of a newform, the $a_n(E)$ satisfy

$$\begin{aligned} a_1(E) &= 1, \\ a_p(E) &= p + 1 - |\widetilde{E}(\mathbb{F}_p)|, \\ a_{p^e}(E) &= a_p(E)a_{p^{e-1}}(E) - \mathbf{1}_E(p)pa_{p^{e-2}}(E), \quad e \geq 2, \\ a_{mn}(E) &= a_m(E)a_n(E), \quad (m, n) = 1, \end{aligned}$$

Chapter 9

- Page 367, second display: Also $d \neq 0, 1$.
- Page 368, third display: No claim is made that the powers of μ_N are independent over $\mathbb{Z}$.
- Page 368, line 16: Change "ramify in $\mathbb{Q}(\mu_N)$." to "ramify in $\mathbb{Q}(\mu_N)$ (except that 2 does not ramify if $N \equiv 2 \pmod 4$, but then $\mathbb{Q}(\mu_N) = \mathbb{Q}(\mu_{N/2})$ and $N/2$ is odd)."
- Page 375, line 5: Change "$1 + \ell^n\mathbb{Z}_\ell^*$" to "$1 + \ell^n\mathbb{Z}_\ell$".
- Page 381, line 12: Change "of C" to "of the curve C from Section 9.2".
- Page 383, middle of the page: Replace "For each n the field $\mathbb{Q}(E[\ell^n])$ is a Galois number field, giving a restriction map

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q}), \qquad \sigma \mapsto \sigma|_{\mathbb{Q}(E[\ell^n])},$$

and there is also an injection

$$\mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[\ell^n]).\text{”}$$

with “Under the isomorphic identification of E with $\mathrm{Pic}^0(E)$, multiplication by ℓ^n on E for any $n \in \mathbb{Z}^+$ becomes purely formal on $\mathrm{Pic}^0(E)$, and so it clearly commutes with the $G_{\mathbb{Q}}$-action on $\mathrm{Pic}^0(E)$. Thus the actions on E commute as well, and so the Galois action restricts to ℓ^n-torsion,

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\ell^n]).\text{”}$$

- Page 384, line (-10): Replace “Theorem 8.4.4” by “Proposition 8.4.4”.
- Page 384: The second paragraph of the proof of Theorem 9.4.1 is correct but it can be replaced by the following two paragraphs if desired.

  “The relation $a_p(E) = \sigma_{p,*} + \sigma_p^*$ as endomorphisms of $\mathrm{Pic}^0(\widetilde{E})$ (Proposition 8.3.2) and the preservation of ℓ^n-torsion under reduction combine to show that $\mathrm{Frob}_{\mathfrak{p}}$ satisfies its asserted characteristic equation. Consider the diagram

$$\begin{array}{ccc} E[\ell^n] & \xrightarrow{a_p(E)} & E[\ell^n] \\ \downarrow & & \downarrow \\ \widetilde{E}[\ell^n] & \xrightarrow{\sigma_p + p\,\sigma_p{}^{-1}} & \widetilde{E}[\ell^n]. \end{array}$$

  Identifying elliptic curves with their degree-0 Picard groups as earlier, and recalling from equations (8.14) and (8.15) that $\sigma_p = \sigma_{p,*}$ and $p\sigma_p^{-1} = \sigma_p^*$ under the identification, we see that the diagram commutes. The same diagram but instead with $\mathrm{Frob}_{\mathfrak{p}} + p\,\mathrm{Frob}_{\mathfrak{p}}^{-1}$ across the top row also commutes. Since the vertical arrows are isomorphisms, $a_p(E) = \mathrm{Frob}_{\mathfrak{p}} + p\,\mathrm{Frob}_{\mathfrak{p}}^{-1}$ on $E[\ell^n]$, and since n is arbitrary, the equality extends to $\mathrm{Ta}_\ell(E)$. Multiply the equality through by $\mathrm{Frob}_{\mathfrak{p}}$ to get $\mathrm{Frob}_{\mathfrak{p}}^2 - a_p(E)\mathrm{Frob}_{\mathfrak{p}} + p = 0$.

  The previous paragraph shows that the minimal polynomial of $\mathrm{Frob}_{\mathfrak{p}}$ divides $x^2 - a_p(E)x + p$ but not yet that this is the characteristic polynomial. (For example, the identity operator on a 2-dimensional vector space satisfies any quadratic polynomial $(x-1)(x-a)$, not only its characteristic polynomial $(x-1)^2$.) To finish establishing the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{p}}$ for $p \nmid \ell N$, we show that $\det \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}) = p$. Let let $\rho_n : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ be the nth entry of $\rho_{E,\ell}$ for $n \in \mathbb{Z}^+$. As in Lemma 7.6.1, the Weil pairing shows that the action of $\sigma \in G_{\mathbb{Q}}$ on the root of unity μ_{ℓ^n} is given by the determinant, but by definition the action is also to raise μ_{ℓ^n} to the nth entry of the cyclotomic character $\chi_\ell(\sigma)$,

$$\mu_{\ell^n}^{\sigma} = \mu_{\ell^n}^{\det \rho_n(\sigma)} = \mu_{\ell^n}^{\chi_{\ell,n}(\sigma)}.$$

  That is, $\det \rho_n(\sigma) = \chi_{\ell,n}(\sigma)$ in $(\mathbb{Z}/\ell^n\mathbb{Z})^*$ for all n, so $\det \rho_{E,\ell}(\sigma) = \chi_\ell(\sigma)$ in $\mathbb{Z}_\ell^*$. In particular (9.13) gives $\det \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}) = p$, as desired.”
- Page 385: Exercise 9.4.2 requires many changes.

The exercise applies to the $t_{p^e}(E)$ rather than to the $a_{p^e}(E)$, and so this change should be made throughout.

Change the initial value from $t_1(E) = 1$ to $t_1(E) = 2$.

At the end of the text leading up to part (a), delete "except when $p = 2$ and $2 \mid N$".

With the proof of Theorem 9.4.1 modified, change A^e to $\mathrm{Frob}_{\mathfrak{p}}^2$ throughout parts (a) and (b).

At the end of part (a), add the sentence, "Note that the equality holds for $e = 0$ as well."

In part (b), change "Show that" to "Show that for $e \geq 2$".

Change part (c) to "(c) For $p \mid N$, (8.11) says that we may take $\widetilde{E}$: $(y - m_1x)(y - m_2x) = x^3$ with $m_1 + m_2, m_1m_2 \in \mathbb{F}_p$. Show that the formula

$$t \mapsto ((t - m_1)(t - m_2), t(t - m_1)(t - m_2))$$

describes a map from $\mathbb{P}^1(\mathbb{F}_q)$ to $\widetilde{E}(\mathbb{F}_q)$. By considering the map $(x, y) \mapsto y/x$ from $\widetilde{E}(\mathbb{F}_q) - \{(0, 0)\}$ to $\mathbb{P}^1(\mathbb{F}_q)$ also, show that the displayed map injects except for possibly hitting $(0, 0)$ more than once (when m_1, m_2 are distinct and lie in $\mathbb{F}_q$) and that the map surjects except for possibly missing $(0, 0)$ (when m_1, m_2 do not lie in $\mathbb{F}_q$), and so the map bijects when $m_1 = m_2$ lies in $\mathbb{F}_q$.

The reduction $\widetilde{E}$ is multiplicative if $m_1 \neq m_2$. Show that if the reduction is split, i.e., $m_1, m_2 \in \mathbb{F}_p$, then $t_{p^e}(E) = 1$ for all $e \geq 1$. Show that if the reduction is nonsplit, i.e., $m_1, m_2 \notin \mathbb{F}_p$, then $t_{p^e}(E) = (-1)^e$ for all $e \geq 1$. Show that the recurrence is satisfied in both cases.

The reduction is additive if $m_1 = m_2$. Show that the common value m lies in $\mathbb{F}_p$ (the argument will be different for $p = 2$). Show that $t_{p^e}(E) = 0$ for all $e \geq 1$, and show that the recurrence is satisfied in this case as well."

Add a new part to the exercise: "(d) Again assume that $p \nmid N$. Show that

$$(1 - a_p(E)x + px^2)^{-1} = (1 - \lambda_1 x)^{-1}(1 - \lambda_2 x)^{-1} = \sum_{e=0}^{\infty} \left(\sum_{c+d=e} \lambda_1^c \lambda_2^d \right) x^e.$$

Explain why it follows that whereas the normalized prime-power solution-counts of the elliptic curve are $t_{p^e}(E) = \lambda_1^e + \lambda_2^e$, the corresponding prime-power Dirichlet coefficients of $L(s, E)$ are $a_{p^e}(E) = \sum_{c+d=e} \lambda_1^c \lambda_2^d$."

- Page 388, line 4: Replace "The field extension $\mathbb{Q}(\mathrm{Pic}^0(X_1(N))[\ell^n])/\mathbb{Q}$ is Galois for each $n \in \mathbb{Z}^+$" with "The Galois action commutes with the purely formal action of multiplication by ℓ^n for any $n \in \mathbb{Z}^+$".
- Page 390: The proof of Lemma 9.5.2 can be clarified as follows.

  "Multiplication by ℓ^n is surjective on $I_f \mathrm{J}_1(N)$. Indeed, it is surjective on the complex torus $\mathrm{J}_1(N)$, and the commutative Hecke algebra $\mathbb{T}_{\mathbb{Z}}$ contains both I_f and ℓ^n, so that $\ell^n I_f \mathrm{J}_1(N) = I_f \ell^n \mathrm{J}_1(N) = I_f \mathrm{J}_1(N)$.

To show the first statement of the lemma, take any $y \in A_f[\ell^n]$. Then $y = x + I_f \mathrm{J}_1(N)$ for some $x \in \mathrm{J}_1(N)$ such that $\ell^n x \in I_f \mathrm{J}_1(N)$. Thus $\ell^n x = \ell^n x'$ for some $x' \in I_f \mathrm{J}_1(N)$ by the previous paragraph. The difference $x - x'$ lies in $\mathrm{J}_1(N)[\ell^n] = \mathrm{Pic}^0(X_1(N))[\ell^n]$ and maps to y as desired.

The kernel is $\mathrm{Pic}^0(X_1(N))[\ell^n] \cap I_f \mathrm{J}_1(N) = (I_f \mathrm{J}_1(N))[\ell^n]$. We claim that the containment

$$(I_f \mathrm{Pic}^0(X_1(N)))[\ell^n] \subset (I_f \mathrm{J}_1(N))[\ell^n],$$

is in fact equality. Granting the equality, the second statement of the lemma follows quickly: the kernel is now $(I_f \mathrm{Pic}^0(X_1(N)))[\ell^n]$. That is, the kernel is $\mathrm{Pic}^0(X_1(N))[\ell^n] \cap I_f \mathrm{Pic}^0(X_1(N))$, which is stable under the Galois action: the first intersectand is stable because the Galois action on $\mathrm{Pic}^0(X_1(N))$ preserves ℓ^n-torsion, and the second is stable because the Galois and Hecke actions on $\mathrm{Pic}^0(X_1(N))$ commute.

To prove that the containment is equality, note that it is a containment of torsion of I_f-images, while if instead we were considering I_f-images of torsion then there would be nothing to show, i.e., $\mathrm{Pic}^0(X_1(N))[\ell^n] = \mathrm{J}_1(N)[\ell^n]$ and thus $I_f(\mathrm{Pic}^0(X_1(N))[\ell^n]) = I_f(\mathrm{J}_1(N)[\ell^n])$. So the argument will relate the given containment of torsion of I_f-images to an equality of I_f-images of torsion, To do so, let $\mathcal{S}_2 = \mathcal{S}_2(\Gamma_1(N))$ and $H_1 = \mathrm{H}_1(X_1(N)_\mathbb{C}, \mathbb{Z}) \subset \mathcal{S}_2^\wedge$. Thus $\mathrm{J}_1(N) = \mathcal{S}_2^\wedge / H_1$ and

$$I_f \mathrm{J}_1(N) = (I_f \mathcal{S}_2^\wedge + H_1)/H_1 \cong I_f \mathcal{S}_2^\wedge / (H_1 \cap I_f \mathcal{S}_2^\wedge).$$

Now suppose that $y \in (I_f \mathrm{J}_1(N))[\ell^n]$. Then $y = x + H_1$ where by the previous display we may take

$$x \in I_f \mathcal{S}_2^\wedge \quad \text{and} \quad \ell^n x \in H_1 \cap I_f \mathcal{S}_2^\wedge.$$

Proposition 6.2.4 shows that $H_1 \cap I_f \mathcal{S}_2^\wedge$ contains $I_f H_1$ as a subgroup of some finite index M. Consequently $H_1 \cap I_f \mathcal{S}_2^\wedge \subset I_f M^{-1} H_1$. From the previous display and the containment, $\ell^n x \in I_f M^{-1} H_1$, and so

$$x \in I_f M^{-1} \ell^{-n} H_1.$$

That is, $x = T x_0$ where $T \in I_f$ and $x_0 \in \mathcal{S}_2^\wedge$ and $M \ell^n x_0 \in H_1$, and so $y = T(x_0 + H_1)$ where $x_0 + H_1 \in \mathrm{J}_1(N)$ and $M\ell^n(x_0 + H_1) = 0$. In sum, our y from $(I_f \mathrm{J}_1(N))[\ell^n]$ lies in $I_f(\mathrm{J}_1(N)[M\ell^n])$, and we are set up to use the equality of I_f-images of torsion,

$$y \in I_f(\mathrm{J}_1(N)[M\ell^n]) = I_f(\mathrm{Pic}^0(X_1(N))[M\ell^n]) \subset I_f \mathrm{Pic}^0(X_1(N)).$$

And since $\ell^n y = 0$ in fact $y \in (I_f \mathrm{Pic}^0(X_1(N)))[\ell^n]$. Thus the opposite containment is proved, establishing the desired equality. As explained above, the proof of the lemma is complete."

- Page 391: Replace the two lines before Lemma 9.5.3 with "Since the Tate module $\mathrm{Ta}_\ell(A_f) \cong \mathbb{Z}_\ell^{2d}$ is a module over $\mathcal{O}_f$, the tensor product
$$V_\ell(A_f) = \mathrm{Ta}_\ell(A_f) \otimes \mathbb{Q} \cong \mathbb{Q}_\ell^{2d}$$
is a module over $\mathcal{O}_f \otimes \mathbb{Q} = \mathbb{K}_f$. Also, it is a module over $\mathbb{Q}_\ell$, with the two actions commuting and with the restrictions of the two actions to $\mathbb{Q}$ agreeing. Thus $V_\ell(A_f)$ is a module over $\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$."
Replace the proof of the lemma with "Since $\mathrm{Ta}_\ell(A_f)$ is the inverse limit of the torsion groups $A_f[\ell^n]$, we need to describe $A_f[\ell^n]$ in a fashion that will help establish the freeness.
As above, let $\mathcal{S}_2 = \mathcal{S}_2(\Gamma_1(N))$ and let $H_1 = \mathrm{H}_1(X_1(N)_{\mathbb{C}}, \mathbb{Z}) \subset \mathcal{S}_2^\wedge$. Consider the quotients $\overline{\mathcal{S}_2^\wedge} = \mathcal{S}_2^\wedge / I_f \mathcal{S}_2^\wedge$ and $\overline{H}_1 = (H_1 + I_f\mathcal{S}_2^\wedge)/I_f\mathcal{S}_2^\wedge$, both $\mathcal{O}_f$-modules. Compute that
$$\begin{aligned} A_f = \mathrm{J}_1(N)/I_f\mathrm{J}_1(N) &= \big(\mathcal{S}_2^\wedge/H_1\big) \,/\, \big((I_f\mathcal{S}_2^\wedge + H_1)/H_1\big) \\ &\cong \mathcal{S}_2^\wedge/(I_f\mathcal{S}_2^\wedge + H_1) \\ &\cong \big(\mathcal{S}_2^\wedge/I_f\mathcal{S}_2^\wedge\big) \,/\, \big((H_1 + I_f\mathcal{S}_2^\wedge)/I_f\mathcal{S}_2^\wedge\big) = \overline{\mathcal{S}_2^\wedge}/\overline{H}_1. \end{aligned}$$
Thus $A_f[\ell^n] \cong \ell^{-n}\overline{H}_1/\overline{H}_1$ for any $n \in \mathbb{Z}^+$. The $\mathcal{O}_f$-linear isomorphisms $\ell^{-n}\overline{H}_1/\overline{H}_1 \longrightarrow \overline{H}_1/\ell^n\overline{H}_1$ induced by multiplication by ℓ^n on $\ell^{-n}\overline{H}_1$ assemble to give an isomorphism of $\mathcal{O}_f \otimes \mathbb{Z}_\ell$-modules,
$$\mathrm{Ta}_\ell(A_f) = \varprojlim_n \{A_f[\ell^n]\} = \varprojlim_n \{\ell^{-n}\overline{H}_1/\overline{H}_1\} \cong \varprojlim_n \{\overline{H}_1/\ell^n\overline{H}_1\} \cong \overline{H}_1 \otimes \mathbb{Z}_\ell,$$
where the transition maps in the last inverse limit are the natural projection maps.
The fact that A_f is a complex torus of dimension d and the calculation a moment ago that $A_f \cong \overline{\mathcal{S}_2^\wedge}/\overline{H}_1$ combine to show that the $\mathcal{O}_f$-module $\overline{H}_1 \cong H_1/(H_1 \cap I_f\mathcal{S}_2^\wedge)$ has $\mathbb{Z}$-rank $2d$. Since $\mathbb{K}_f$ is a field, $\overline{H}_1 \otimes \mathbb{Q}$ is a free $\mathbb{K}_f$-module whose $\mathbb{Q}$-rank is $2d$ and whose $\mathbb{K}_f$-rank is therefore 2. Consequently, $\overline{H}_1 \otimes \mathbb{Q}_\ell = \overline{H}_1 \otimes \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is free of rank 2 over $\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
So finally,
$$V_\ell(A_f) = \mathrm{Ta}_\ell(A_f) \otimes \mathbb{Q} \cong \overline{H}_1 \otimes \mathbb{Z}_\ell \otimes \mathbb{Q} \cong \overline{H}_1 \otimes \mathbb{Q}_\ell$$
is an isomorphism of $\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-modules, and the proof is complete."
- Page 396, line (−11): Change "$\lambda \in \mathcal{O}_{\mathbb{K}_f}$" to "$\lambda \subset \mathcal{O}_{\mathbb{K}_f}$".
- Page 397, line 11: For the Fermat equation, it is understood that ℓ is an odd prime.

Hints and Answers to the Exercises

- Page 410, hint to Exercise 5.3.1: Replace "$M_{p^e} \cup \left[\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right] M_{p^{e-2}}$" with "$M_{p^e} \cup \bigcup_{j=0}^{p-1} \left[\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right] M_{p^{e-2}} \left[\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right]$".
- Page 414, hint to Exercise 7.7.1: Remove "$j_N = j(E_j/\langle Q_\tau\rangle)$ and since", remove "$j_N^\sigma = j(E_j/\langle Q_\tau^\sigma\rangle)$ and", and change "In both cases the" to "The".