A

Hints and Answers to the Exercises

Chapter 1

1.1.4. (b) For $|\delta| < 1$, $|\tau + \delta| \geq B = B \cdot \sup\{1, |\delta|\}$ for all $\tau \in \Omega$. For $1 \leq |\delta| \leq 3A$ and $\mathrm{Im}(\tau) > A$, $|\tau + \delta| > A \geq |\delta|/3 = \sup\{1, |\delta|\}/3$. For $1 \leq |\delta| \leq 3A$ and $B \leq \mathrm{Im}(\tau) \leq A$, the quantity $|\tau + \delta|/|\delta|$ takes a nonzero minimum m, so $|\tau + \delta| \geq m|\delta| = m \cdot \sup\{1, |\delta|\}$. For $|\delta| > 3A$, $|\tau + \delta| \geq |\delta| - A \geq 2|\delta|/3 = 2\sup\{1, |\delta|\}/3$. So any positive C less than $\inf\{B, 1/3, m\}$ works. For (c), break the sum into $2\zeta(k) + \sum_{c \neq 0, d} |c\tau + d|^{-k}$. For $c \neq 0$, $|c\tau + d| = |c||\tau + \delta|$ where $\delta = d/c$. Apply (b) and then (a). Since any compact subset of $\mathcal{H}$ sits inside a suitable Ω, holomorphy follows from a theorem of complex analysis.

1.1.5. For the first formula, take the logarithmic derivative of the product expansion $\sin \pi\tau = \pi\tau \prod_{n=1}^{\infty}(1 - \tau^2/n^2)$. The second formula follows from the definitions of sin and cos in terms of the complex exponential.

1.1.6. (d) To show $\hat{h}(0) = 0$, simply antidifferentiate. To show $\hat{h}(m) = 0$ for $m < 0$ replace τ by $-\tau$ and reason as in part (c) except now the rectangle no longer goes around the singularity at the origin.

1.2.2. (a) Let $g = \gcd(c, d)$ and note that g is relatively prime to N. If $c \neq 0$, set $s = 0$, and use the Chinese Remainder Theorem to find t congruent to 1 modulo primes $p \mid g$ and congruent to 0 modulo primes $p \nmid g$, $p \mid c$. If $c = 0$ then $d \neq 0$ (unless $N = 1$, in which case the whole problem is trivial) and a similar argument works.

1.2.3. (a) One way is by induction on e. For $e = 1$, $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|$ is the number of bases of $(\mathbb{Z}/p\mathbb{Z})^2$, and $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is the kernel of the surjective determinant map to $(\mathbb{Z}/p\mathbb{Z})^*$. For the induction, count $\ker(\mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}))$. The map surjects since $\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ does. For (b), $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_i \mathrm{SL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$ where $N = \prod_i p_i^{e_i}$, by the Chinese Remainder Theorem.

F. Diamond, J. Shurman, *A First Course in Modular Forms*,
Graduate Texts in Mathematics 228, DOI 10.1007/978-0-387-27226-9

1.2.6. (b) Since $(f[\alpha]_k)(\tau+N) = f[\alpha]_k(\tau)$ we may estimate $|f[\alpha]_k|$ as $q_N \to 0$ letting $y \to \infty$ and assuming $0 \le x < N$ where $\tau = x + iy$. So $|c\tau + d|$ grows as y and $|(f[\alpha]_k)(\tau)| = |f(\alpha(\tau))||c\tau+d|^{-k}$ is bounded by $(C_0+C/\mathrm{Im}(\alpha(\tau))^r)\cdot |c\tau + d|^{-k}$, or $(C_0 + C|c\tau + d|^{2r}/y^r)|c\tau + d|^{-k}$. We may take $r \ge 1$ and thus absorb the first term into the second. The result follows.

1.2.8. (b) For the inverse, note $E_2(\tau) = E_2(\gamma(\gamma^{-1}(\tau)))$. For (e), note that for $\gamma \in \Gamma_0(N)$, $N\gamma(\tau) = \gamma'(N\tau)$ for a certain $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$. Use the Fourier series and Proposition 1.2.4 to check the holomorphy condition.

1.2.9. See Exercise 1.1.7(b) for the relevant ζ-values.

1.2.10. (a) The sum is $-\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} q^{nm}/m$. The sum of absolute values is $\sum_m \sum_n |q|^{nm}/m = \sum_m |q|^m/(m(1-|q|^m))$, and this converges since its terms are bounded by $e^{-2\pi m \mathrm{Im}(\tau)}$ as $m \to \infty$. The convergence is uniform on compact sets because any compact subset of $\mathcal{H}$ has a point with minimal imaginary part.

1.2.11. (b) If $c \ne 0$ then write $a/c = a'/c'$ with $a', c' \in \mathbb{Z}$, $\gcd(a', c') = 1$. Now left multiplying by an $\mathrm{SL}_2(\mathbb{Z})$ matrix with top row $(c', -a')$ clears out the lower left entry. For the second part, if $f[\alpha]_k$ has period h then $f[\gamma]_k$ has period dh.

1.3.2. Show (1) $\implies$ (3) $\implies$ (2) $\implies$ (1).

1.3.3. (c) The entire exercise is set in one E, so multiplying by d takes points $P + \Lambda$ to $dP + \Lambda$, not to $dP + d\Lambda$.

1.4.1. (c) The integrals along opposing pairs of boundary edges cancel down to $1/(2\pi i)(\omega_2 \int_0^{\omega_1} f'(z)dz/f(z) - \omega_1 \int_0^{\omega_2} f'(z)dz/f(z))$. Each of these integrals is $\int d\log f(z)$ along a path with equal f-values at the endpoints, so $\log f$ changes by an integer multiple of $2\pi i$ along each path. For the second part, if $f(z) = (z-x)^{\nu_x(f)}g(z)$ where $g(x) \ne 0$ then $zf'(z)/f(z) = \nu_x(f)z/(z-x) + zg'(z)/g(z)$ has residue $\nu_x(f)x$ at x, so the Residue Theorem gives the result.

1.4.3. For Λ_{μ_3} show that $\wp(\mu_3 z) = \mu_3\wp(z)$ and $\wp(\overline{z}) = \overline{\wp(z)}$. If $\wp(z) = 0$ then also $\wp(\mu_3 z) = 0$, so $\mu_3 z \equiv \pm z \pmod{\Lambda}$ since $\wp$ is even and has only two zeros. The minus sign can not arise because it would imply $z \equiv -z \pmod{\Lambda}$ but $\wp$ is nonzero at the order 2 points. The zeros are $z = (1 + 2\mu_3)/3$ and $z = (2 + \mu_3)/3$.

1.5.1. For $\Gamma(N)$, take any point $[E, (P, Q)]$ of $\mathrm{S}(N)$. After applying an isomorphism (which preserves the Weil pairing by Exercise 1.3.3(d)) we may assume $E = \mathbb{C}/\Lambda_{\tau'}$, $P = (a\tau' + b)/N + \Lambda_{\tau'}$, $Q = (c\tau' + d)/N + \Lambda_{\tau'}$ with $a, b, c, d \in \mathbb{Z}/N\mathbb{Z}$ and $\tau' \in \mathcal{H}$. Since P and Q generate $E[N]$ and have Weil pairing $e_N(P, Q) = e^{2\pi i/N}$, $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Lift this matrix back to some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, let $\tau = \gamma(\tau')$ and $m = c\tau' + d$, so that $m\tau = a\tau' + b$, and show that $[E, (P, Q)] = [\mathbb{C}/\Lambda_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)]$.

1.5.2. The map $\mathrm{S}(N) \longrightarrow \mathrm{S}_1(N)$ takes $\psi^{-1}(\Gamma(N)\tau)$ to $\psi_1^{-1}(\Gamma_1(N)\tau)$. Compute this first for points in the form $[\mathbb{C}/\Lambda_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)]$, and then show that in general the map works out to $[E,(P,Q)] \mapsto [E,Q]$.

1.5.3. Each $b \pmod N \in \mathbb{Z}/N\mathbb{Z}$ acts on the modular curve $Y(N)$ as $b \pmod N : \Gamma(N)\tau \mapsto \Gamma(N)\gamma(\tau)$ where $\gamma = \left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma_1(N)$. The corresponding action on the moduli space $\mathrm{S}(N)$ under ψ^{-1} is therefore

$$b \pmod N : [E_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)] \\ \mapsto [E_{\gamma(\tau)}, (\gamma(\tau)/N + \Lambda_{\gamma(\tau)}, 1/N + \Lambda_{\gamma(\tau)})].$$

By the methods of the section, letting $m = j(\gamma,\tau)$ shows that the image is $[E_\tau, (m\gamma(\tau)/N + \Lambda_\tau, m/N + \Lambda_\tau)]$. Since $\gamma = \left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right]$, $m = 1$ and this is $[E_\tau, ((\tau+b)/N + \Lambda_\tau, 1/N + \Lambda_\tau)]$, showing that the map is

$$b \pmod N : [E,(P,Q)] \mapsto [E,(P+bQ,Q)].$$

Argue similarly for $d \mod N \in (\mathbb{Z}/N\mathbb{Z})^*$ acting on $\mathrm{S}_1(N)$, this time letting $\gamma = \left[\begin{smallmatrix} a & k \\ N & d \end{smallmatrix}\right] \in \Gamma_0(N)$ for suitable a, k, N.

1.5.4. Note that multiplying $\Lambda_{-1/(N\tau)}$ by τ gives the lattice $\tau\mathbb{Z} \oplus (1/N)\mathbb{Z}$. The map is $[E,C] \mapsto [E/C, E[N]/C]$.

1.5.6. (a) Recall the condition $C \cap \langle Q \rangle = \{0_E\}$. If $p \nmid N$ then the bottom row of the matrix is not always $(0,1)$.

Chapter 2

2.1.3. (a) Let $y_1 = \inf\{\mathrm{Im}(\tau) : \tau \in U_1'\}$, $Y_1 = \sup\{\mathrm{Im}(\tau) : \tau \in U_1'\}$, $y_2 = \inf\{\mathrm{Im}(\tau) : \tau \in U_2'\}$, all positive. Then for $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in U_1'$, the formula $\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}(\tau)/|c\tau + d|^2$ shows that $\mathrm{Im}(\gamma(\tau)) \le \min\{1/(c^2 y_1), Y_1/(c\mathrm{Re}(\tau) + d)^2\}$. The first of these is less than y_2 for all but finitely many values of c; for each exceptional c, the second is less than y_2 uniformly in τ for all but finitely many values of d.

2.2.5. Both π and ψ are open and continuous.

2.3.4. (b) For part (b), $\mathbb{Z}[\gamma]$ is ring isomorphic to $\mathbb{Z}[i]$. For part (a), if γ has order 3 then $-\gamma$ has order 6.

2.3.5. (a) The matrices fixing μ_3 are $\left[\begin{smallmatrix} a & b \\ -b & a-b \end{smallmatrix}\right]$, $(2a-b)^2 + 3b^2 = 4$.

2.3.7. (c) It suffices to show the result for $\Gamma_0(p)$, $p \equiv -1 \pmod{12}$. If $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ fixes a point then $a + d \in \{0, \pm 1\}$ and $ad \equiv 1 \pmod p$. If $a + d = 0$ then this means $a^2 \equiv -1 \pmod p$, impossible by the nature of $p \pmod 4$. The other two cases are similar with $p \pmod 3$.

2.3.8. The proof of Lemma 2.3.1 shows that given any $\tau \in \mathcal{H}$, some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ transforms some $\tau_0 \in \mathcal{D}$ to τ.

2.4.4. (a) $\Gamma(N) \subset \delta\Gamma\delta^{-1}$ for some $N \in \mathbb{Z}^+$. (b) Note that $\mathrm{SL}_2(\mathbb{Z}) = \delta\mathrm{SL}_2(\mathbb{Z})\delta^{-1}$.

2.4.6. See Corollary 2.3.4, recall that $\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}(\tau)/|c\tau + d|^2$ for $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, and note that if $\tau \in \{i, \mu_3\}$ then $|c\tau + d| \geq 1$ for all nonzero integer pairs (c, d).

Chapter 3

3.1.1. Let $\{\pm I\}\Gamma_2 = \bigcup_j \{\pm I\}\Gamma_1\gamma_j$. Then $f^{-1}(\Gamma_2\tau) = \{\Gamma_1\gamma_j\tau\}$ and these are distinct when τ is not an elliptic point for Γ_2.

3.1.2. Show that for $\gamma \in \Gamma_2$, the indices $[\{\pm I\}\Gamma_{2,\gamma(\tau)} : \{\pm I\}\Gamma_{1,\gamma(\tau)}]$ and $[\{\pm I\}\Gamma_{2,\tau} : \{\pm I\}\Gamma_{1,\tau}]$ are equal.

3.1.4. (b) The cusps are 0 and ∞, cf. Figure 3.1. For (c), $\gamma\alpha_j(i) = \alpha_j(i)$ if and only if $\alpha_j^{-1}\gamma\alpha_j(i) = i$, and by Corollary 2.3.4 the nontrivial transformations in $\mathrm{SL}_2(\mathbb{Z})_i$ are $\pm\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. Similarly for (d). The data to compute g in this and the next two problems are tabulated in Figure H.1.

Γ	d	ε_2	ε_3	ε_∞
$\Gamma_0(p)$	$p+1$	1 if $p = 2$ 2 if $p \equiv 1$ (4) 0 if $p \equiv 3$ (4)	1 if $p = 3$ 2 if $p \equiv 1$ (3) 0 if $p \equiv 2$ (3)	2
$\Gamma_1(2) = \Gamma_0(2)$	3	1	0	2
$\Gamma_1(3)$	4	0	1	2
$\Gamma_1(p),\ p > 3$	$\frac{p^2-1}{2}$	0	0	$p-1$
$\Gamma(2)$	6	0	0	3
$\Gamma(p),\ p > 2$	$\frac{p(p^2-1)}{2}$	0	0	$\frac{p^2-1}{2}$

Figure H.1. Data to compute the genus

3.1.5. (b) For $p > 3$ the answer is $g = 1 + (p-1)(p-11)/24$.

3.1.6. The cusp ∞ has ramification degree p under $\pi : X(p) \longrightarrow \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^*$, and since $\Gamma(p)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$ so do all the other cusps, cf. Exercise 2.4.4(c). The number of cusps follows from the degree of the map and the number of cusps of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^*$. For $p > 2$ the answer is $g = 1 + (p^2-1)(p-6)/24$.

3.2.2. Let $A = 240\sum_{n=1}^{\infty}\sigma_3(n)q^n$ and $B = -504\sum_{n=1}^{\infty}\sigma_5(n)q^n$. Cite Exercise 1.1.5 to show that $(60E_4(\tau))^3 = (64\pi^{12}/27)(1+A)^3$ and $\Delta(\tau) = (64\pi^{12}/27)((1+A)^3-(1+B)^2)$. Consequently $j(\tau) = 1728(1+A)^3/(3A+3A^2+A^3-2B-B^2)$. The numerator lies in $1728(1+q\mathbb{Z}[[q]])$, where the double brackets denote power series. In the denominator $3A^2$ and A^3 and B^2 lie in $1728q^2\mathbb{Z}[[q]]$, and since $d^3 \equiv d^5 \pmod{12}$ for all integers d, also $3A-2B$ lies in $1728q(1+q\mathbb{Z}[[q]])$.

3.2.3. We may assume $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. For weight-2 $\mathrm{SL}_2(\mathbb{Z})$-invariance use the chain rule relation $(j\circ\gamma)'(\tau) = j'(\gamma(\tau))\gamma'(\tau)$. Also remember to check meromorphy at ∞. Show that $(j')^{k/2} \in \mathcal{A}_k(\mathrm{SL}_2(\mathbb{Z}))$ for positive even k.

3.2.5. The group is the matrices $\pm\left[\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right]$ such that $\pm\alpha\left[\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right]\alpha^{-1} \in \Gamma_1(4)$.

3.5.3. For the last part show that for all $k \in \mathbb{Z}$, multiplying by the cusp form Δ defines an isomorphism $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) \longrightarrow \mathcal{S}_{k+12}(\mathrm{SL}_2(\mathbb{Z}))$.

3.5.5. Recall Exercise 3.5.4(b) with $N = 11$.

3.7.1. (a) Suppose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ has order 4 or 6 and fixes the point $\tau \in \mathcal{H}$, and suppose $\gamma^{-1} = \alpha\gamma\alpha^{-1}$ with $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Then γ^{-1} fixes $\alpha(\tau)$, so α fixes τ since α takes $\mathcal{H}$ to $\mathcal{H}$ and the other fixed point of γ^{-1} is $\bar{\tau}$. Thus $\alpha \in \langle\gamma\rangle$ and $\gamma^{-1} = \gamma$, contradiction. For (c), recall Proposition 2.3.3.

3.7.4. The bottom entry of $u \odot_\gamma l = (aI + c\gamma)\left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right]$ works out to $cc_\gamma x + (a + cd_\gamma)y$. Use information about c_γ and d_γ to show that this is 0 (mod N).

3.7.5. (b) For period 2, the ring $A = \mathbb{Z}[i]$ is a principal ideal domain and its maximal ideals are

- for each prime $p \equiv 1 \pmod 4$, two ideals $J_p = \langle a+bi\rangle$ and $\overline{J}_p = \langle a-bi\rangle$ such that $\langle p\rangle = J_p\overline{J}_p$ and the quotients A/J_p^e and $A/\overline{J}_p^e$ are isomorphic to $\mathbb{Z}/p^e\mathbb{Z}$ for all $e \in \mathbb{N}$,
- for each prime $p \equiv -1 \pmod 4$, the ideal $J_p = \langle p\rangle$ such that the quotient A/J_p^e is isomorphic to $(\mathbb{Z}/p^e\mathbb{Z})^2$ for all $e \in \mathbb{N}$,
- for $p = 2$, the ideal $J_2 = \langle 1+i\rangle$ such that $\langle 2\rangle = J_2^2$ and the quotient A/J_2^e is isomorphic to $(\mathbb{Z}/2^{e/2}\mathbb{Z})^2$ for even $e \in \mathbb{N}$ and is isomorphic to $\mathbb{Z}/2^{(e+1)/2}\mathbb{Z} \oplus \mathbb{Z}/2^{(e-1)/2}\mathbb{Z}$ for odd $e \in \mathbb{N}$.

3.7.6. (a) This is another elementary number theory problem. Use the Chinese Remainder Theorem to reduce to prime power N, and then see what happens when you try to lift solutions modulo primes p to solutions modulo powers p^e.

3.8.1. (a) The numerator and denominator linearly combine back to a and c under γ^{-1}.

3.8.2. (b) Since the summand $(N/d)\phi(d)\phi(N/d)$ is multiplicative in d, the sum is multiplicative in N, so it suffices to take $N = p^e$.

3.8.7. Since $\Gamma(4)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$, and since the cusp ∞ is regular, all cusps are regular. See Exercise 5 of Section 3.2 for the argument that $s = 1/2$ is an irregular cusp of $\Gamma_1(4)$. Checking the cusp $s = 0$ is similar.

3.9.1. Since the calculations involve only one value of N such that $-I$ belongs to the groups, only one irregular cusp, and only one nonzero value of ε_2, the formulas for even k and odd k usually agree.

Chapter 4

4.2.4. (b) Since $\overline{v}$ is a point of order N, $\gcd(\gcd(c_v, d_v), N) = 1$.

4.3.1. If χ is nontrivial then replace n by $n_0 n$ in the sum for some value n_0 such that $\chi(n_0) \neq 0$. The second relation is proved similarly since if $n \neq 1$ in $(\mathbb{Z}/N\mathbb{Z})^*$ then the proof of duality shows that $\chi(n) \neq 1$ for some character χ.

4.3.4. (a) This is a standard result from representation theory. Alternatively, for each $d \in (\mathbb{Z}/N\mathbb{Z})^*$ define the operator $\langle d \rangle$ on $\mathcal{M}_k(\Gamma_1(N))$ to be $\langle d \rangle = [\left[\begin{smallmatrix} a & b \\ c & \delta \end{smallmatrix}\right]]_k$ for any $\left[\begin{smallmatrix} a & b \\ c & \delta \end{smallmatrix}\right] \in \Gamma_0(N)$ with $\delta \equiv d \pmod{N}$. Chapter 5 will show that this operator is well defined and multiplicative. For each character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*$, define the operator

$$\pi_\chi = \frac{1}{\phi(N)} \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(d)^{-1} \langle d \rangle$$

on $\mathcal{M}_k(\Gamma_1(N))$. Show that $\pi_\chi^2 = \pi_\chi$, so π_χ is a projection; show that $\pi_\chi(\mathcal{M}_k(\Gamma_1(N))) \subset \mathcal{M}_k(N, \chi)$ and that $\pi_\chi = 1$ on $\mathcal{M}_k(N, \chi)$, so the projection is on $\mathcal{M}_k(N, \chi)$. Show that $\sum_\chi \pi_\chi = 1$ and that $\pi_\chi \circ \pi_{\chi'} = 0$ when $\chi \neq \chi'$, so the subspaces $\mathcal{M}_k(N, \chi)$ span and are linearly disjoint.

4.4.1. For (b), change variables to get a Gaussian integral. For (c), integrate by parts.

4.4.2. Compute that

$$\begin{aligned} \frac{(-2\pi i)^k}{2\Gamma(k)} &= \frac{2^{\frac{k}{2}} \pi^k (-1)^{k/2}}{(1 \cdot 3 \cdots (k-1))(1 \cdot 2 \cdots (\frac{k}{2} - 1))} \\ &= \frac{\pi^{\frac{k-1}{2}} \Gamma\left(\frac{1}{2}\right)}{(-\frac{1}{2})(-\frac{3}{2}) \cdots \frac{1-k}{2} \pi^{-\frac{k}{2}} \Gamma\left(\frac{k}{2}\right)} = \frac{\pi^{-\frac{1-k}{2}} \Gamma\left(\frac{1-k}{2}\right)}{\pi^{-\frac{k}{2}} \Gamma\left(\frac{k}{2}\right)}. \end{aligned}$$

4.4.5. For (c), Exercise 4.4.4 and the fact that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1 show that $L(\mathbf{1}_N, s) \sim \phi(N)/(N(s-1))$ as $s \to 1$. And $(1 + (-1)^{-s})/(s-1) = (e^{-\pi i s} - e^{-\pi i})/(s-1)$ is a difference quotient for the derivative of $e^{-\pi i s}$ at $s = 1$. For (d), compute that

$$\sum_{\chi\neq\mathbf{1}_N}\chi(n^{-1})L(1,\chi)=\sum_{\chi\neq\mathbf{1}_N}\chi(n^{-1})\sum_{\substack{m=1\\(m,N)=1}}^{N-1}\chi(m)\sum_{d=0}^{\infty}\frac{1}{m+dN}$$
$$=\frac{1}{N}\sum_{d}\sum_{m}\frac{1}{m/N+d}\sum_{\chi\neq\mathbf{1}_N}\chi(mn^{-1}\,(N)).$$

The inner sum is $\phi(N)-1$ if $m\equiv n \pmod N$ and -1 otherwise. The middle sum is taken over $\phi(N)$ values of m, so now

$$\sum_{\chi\neq\mathbf{1}_N}\chi(n^{-1})L(1,\chi)=\frac{1}{N}\sum_{d=0}^{\infty}\sum_{\substack{m=1\\(m,N)=1}}^{N-1}\left(\frac{1}{n/N+d}-\frac{1}{m/N+d}\right),$$

where in this calculation the equivalence class $n \pmod N$ and its representative in $\{1,\dots,N-1\}$ are identified. Replacing n by $-n$ and its representative by $N-n$ gives

$$-\sum_{\chi\neq\mathbf{1}_N}\chi((-n)^{-1})L(1,\chi)=\frac{1}{N}\sum_{d=0}^{\infty}\sum_{\substack{m=1\\(m,N)=1}}^{N-1}\left(\frac{1}{n/N-d-1}+\frac{1}{m/N+d}\right).$$

Thus the sum $\dfrac{1}{\phi(N)}\displaystyle\sum_{\chi\neq\mathbf{1}_N}(\chi(n^{-1})-\chi((-n)^{-1}))L(1,\chi)$ in $\zeta^{\overline{n}}(1)$ is

$$\frac{1}{N}\sum_{d=0}^{\infty}\left(\frac{1}{n/N+d}+\frac{1}{n/N-d-1}\right).$$

This is

$$\frac{1}{N}\sum_{d=0}^{\infty}\left(\frac{1}{n/N+d+1}+\frac{1}{n/N-d-1}+\frac{1}{n/N+d}-\frac{1}{n/N+d+1}\right)$$
$$=\frac{1}{N}\left[\sum_{d=0}^{\infty}\left(\frac{1}{n/N+d+1}+\frac{1}{n/N-d-1}\right)+\frac{1}{n/N}\right]=\frac{1}{N}\cot\left(\frac{\pi n}{N}\right).$$

4.4.6. Use the expression for Γ in the exercise and switch to polar coordinates to get

$$\Gamma(a)\Gamma(b)=4\int_{r=0}^{\infty}e^{-r^2}r^{2(a+b-1)}\,r\,dr\int_{\theta=0}^{\pi/2}\cos^{2a-1}\theta\,\sin^{2b-1}\theta\,d\theta.$$

Let $x=\cos^2\theta$.

4.5.3. (c) For each character ψ modulo d where $d\mid N$, Lemma 4.3.2 shows that half of the characters φ modulo N/d combine with ψ to meet the parity

condition unless $N/d = 1$ or $N/d = 2$. For the exceptional values $d = N$ and $d = N/2$ (if N is even), for each character φ modulo N/d, Lemma 4.3.2 shows that half of the characters ψ modulo d combine with φ to meet the parity condition unless $d = 1$ or $d = 2$. Thus $|B_{N,k}| = (1/2)\sum \phi(d)\phi(N/d)$ for $N \nmid 4$, as required by formula (4.3). For the exceptional cases, count that $|B_{N,k}|$ for even k is 1 when $N = 1$, 2 when $N = 2$, and 3 when $N = 4$, and that $|B_{N,k}|$ for odd k is 0 when $N = 1$ or $N = 2$, and 2 when $N = 4$. Again these match formula (4.3).

4.6.4. To show that $\theta(\tau, 4)$ and $E_2^{\mathbf{1}_1,\mathbf{1}_1,4}(\tau)$ are proportional, it suffices to show that in both cases the first Fourier coefficient is 8 times the zeroth. The difference $E_2^{\mathbf{1}_1,\mathbf{1}_1,4}(\tau) - 3E_2^{\mathbf{1}_1,\mathbf{1}_1,2}(\tau)$ leads to the expression $\sum_{\substack{m|n \\ 4\nmid m}} m - 3\sum_{\substack{m|n \\ 2\nmid m}} m$, and this is $-2\sigma_1(n)$ for odd n and is 0 for even n.

4.7.3. Cite the Monotone Convergence Theorem from real analysis, the fact that absolute integrability implies integrability, and the Dominated Convergence Theorem from real analysis.

4.7.5. (c) Let $z = \varepsilon e^{i\theta}$ and bound the absolute value of the integral by a quantity of the order $|\varepsilon^{s-1}|$.

4.8.2. This is very similar to Exercise 1.4.1, but integrate Z_Λ over $t + \partial P$ instead.

4.8.7. For (b) See Figure 3.4 and Theorem 3.6.1. For (c), $\mathcal{M}_1(\Gamma_1(4)) = \mathbb{C}\, E_1^{\chi,\mathbf{1},1}$ where χ is the nontrivial character of $(\mathbb{Z}/4\mathbb{Z})^*$. A basis of $\mathcal{M}_3(\Gamma_1(4))$ is $\{E_3^{\chi,\mathbf{1},1}, E_3^{\mathbf{1},\chi,1}\}$. A basis of $\mathcal{M}_4(\Gamma_1(4))$ is $\{E_4^{\mathbf{1},\mathbf{1},1}, E_4^{\mathbf{1},\mathbf{1},2}, E_4^{\mathbf{1},\mathbf{1},4}\}$. Here all three basis elements contribute to $\theta(\tau, 8)$.

4.9.1. $\hat{f}(x)$ is uniformly approximated within ε by an integral over a compact subset K of $\mathbb{R}^l$. In the integral $\hat{f}(x + \delta x) - \hat{f}(x)$, note that $e^{-2\pi i\langle y, x+\delta x\rangle} - e^{-2\pi i\langle y,x\rangle} = e^{-2\pi i\langle y,x\rangle}(e^{-2\pi i\langle y,\delta x\rangle} - 1)$, and if δx is small enough then the quantity in parentheses is uniformly small as y runs through K.

4.9.3. (b) The square of the integral is $\iint_{x,y} e^{-\pi(x^2+y^2)} dx\, dy$. Change to polar coordinates.

4.9.4. The Fourier transform is $\hat{f}(x) = \int_{y=0}^{\infty} y^{s-1} e^{2\pi i y(\tau - x)} dy$. Replace y by $z/(-2\pi i(\tau - x))$, going from 0 to ∞ along a ray in the right half plane. The resulting integral equals a gamma function integral by complex contour integration.

4.9.5. (b) $\Gamma(s)$ is the Mellin transform of e^{-t}. Use part (a).

4.10.2. Compute that

$$\int_{y\in\mathbb{R}^2} f(y\gamma r)e^{-2\pi i\langle y,x\rangle}dy = \int_{y\in\mathbb{R}^2} f(y)e^{-2\pi i\langle y\gamma^{-1}/r,x\rangle}d(y\gamma^{-1}/r)$$
$$= r^{-2}\int_{y\in\mathbb{R}^2} f(y)e^{-2\pi i\langle y,x\gamma^{-T}/r\rangle}dy.$$

4.10.3. For nonzero $\overline{x} \in G$, note that $\mu_N^{\langle x,e_jS\rangle} \neq 1$ for $j = 1$ or $j = 2$ where the e_j are the standard basis vectors, and that $\sum_v \mu_N^{\langle x,vS\rangle} = \mu_N^{\langle x,e_jS\rangle}\sum_v \mu_N^{\langle x,vS\rangle}$, so the sum is 0.

4.10.5. (a) For the first part, show that $\sum_u a(u)b(u) = \sum_v \hat{a}(-v)\hat{b}(v)$ in general. For the second part, replace b by $\hat{b}$.

4.10.6. (b) For $k < 0$, since $f_k(x) = \overline{f}_{-k}(x)$ and in general $\hat{\overline{\varphi}}(x) = \overline{\hat{\varphi}}(-x)$ (show this), it follows from $\hat{f}_{-k} = (-i)^{-k}f_{-k}$ that $\hat{f}_k = (-i)^k f_k$ as before. Similarly since $f_{-k}(xS) = (-i)^{-k}f_{-k}(x)$, also $f_k(xS) = (-i)^k f_k(x)$ as before. Note that $h_k(xt^{1/2}) = h_k(x)t^{|k|/2}$, that $|n\gamma|^{-|k|-2s} = y^{-k/2+s}/|c\tau+d|^{-k+2s}$, and that $h_k(n\gamma) = \overline{h}_{-k}(n\gamma) = y^{k/2}/(c\tau+d)^k$.

4.10.8. For (a), recall formula (4.11). For (c), show that $g(\psi)g(\bar{\psi}) = \psi(-1)u$ similarly to the calculation after (4.11) and recall that $(\psi\varphi)(-1) = (-1)^k$.

Chapter 5

5.1.2. Take integers N_1, N_2 such that $\Gamma(N_i) \subset G_i$ for $i = 1, 2$, and let $N_3 = \mathrm{lcm}(N_1, N_2)$; use the fact that each $[G_i : \Gamma(N_3)]$ is finite.

5.1.3. Suppose that β and β' represent the same orbit in $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$, i.e., $\Gamma_1\beta = \Gamma_1\beta'$. Letting $\beta = \gamma_1\alpha\gamma_2$ and $\beta' = \gamma_1'\alpha\gamma_2'$ translates this condition into $\alpha\gamma_2 \in \Gamma_1\alpha\gamma_2'$. Since f is weight-k invariant under Γ_1, it quickly follows that $f[\beta]_k = f[\beta']_k$.

5.1.4. Set $h = \mathrm{lcm}(\{h_j\})$ where each g_j has period h_j.

5.2.5. (c) If $uv = N$ then $t = 1$ and part (b) holds for all p. Suppose $p \nmid N$; if $t \mid n$ then use part (b), if $t \nmid n$ but $t \mid np$ then $p \mid t \mid N$, contradiction and hence this case can't arise, and if $t \nmid np$ then there is nothing to check. For $n = 0$ there is nothing to check unless $\psi = \mathbf{1}_1$. For (d), $a_n(E) = \sigma_1(n) - t\sigma_1(n/t)$ and $a_n(T_pE) = \sigma_1(np) - \mathbf{1}_N(p)p\sigma_1(n/p) - t(\sigma_1(np/t) - \mathbf{1}_N(p)p\sigma_1(n/(tp)))$ when $n \geq 1$. If $p \nmid N$ then use parts (b) and (c). If $p \mid N$ then the assumption is $t = p$, $N = p^f$. Verify the result for $p \nmid n$ and for $p \mid n$. Also verify the result for $n = 0$.

5.2.6. (a) For $n \geq 1$, let $n = p^e m$ with $p \nmid m$ and then compute both $a_n(T_pf_t)$ and a_n(right side) in each of the three cases. One can also check $n = 0$ or note that the difference of the two sides is constant and therefore zero.

5.2.8. (a) In the desired equality $((\tau+j)/p)\mathbb{Z}\oplus\mathbb{Z} = ((\tau+j)/p)\mathbb{Z}+\tau\mathbb{Z}\oplus\mathbb{Z}$ one containment is obvious, and for the other note that $\tau = p(\tau+j)/p-j$. The groups $(Np\tau+p)\Lambda_{\left[\begin{smallmatrix}m & n\\ N & p\end{smallmatrix}\right](p\tau)}$ and $\Lambda_{p\tau}$ are equal by Lemma 1.3.1, and multiplying through by $1/p$ gives the second desired equality of groups.

5.2.9. Recall the proof of Lemma 2.3.1 and Lemma 2.3.2.

5.3.1. Checking $n=p$ is straightforward. For $e>1$ show that $M_{p^{e-1}}M_p = M_{p^e}$ if $p\mid N$ and $M_{p^{e-1}}M_p = M_{p^e}\cup\bigcup_{j=0}^{p-1}\left[\begin{smallmatrix}p & 0\\ 0 & p\end{smallmatrix}\right]M_{p^{e-2}}\left[\begin{smallmatrix}1 & j\\ 0 & 1\end{smallmatrix}\right]$ if $p\nmid N$, and the result follows for $n=p^e$. When $\gcd(m,n)=1$, M_{mn} isn't quite M_mM_n but since $\left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]\in\Gamma_0(N)$ the difference doesn't affect the weight-k operator.

5.4.1. (a) Start by writing $x=(\tau+\overline{\tau})/2$, $y=(\tau-\overline{\tau})/2i$, and recall that in the algebra of differential forms, $d\tau\,d\tau = d\overline{\tau}\,d\overline{\tau}=0$ and $d\overline{\tau}\,d\tau = -d\tau\,d\overline{\tau}$.

5.4.3. If the unions $\mathrm{SL}_2(\mathbb{Z}) = \bigcup(\{\pm I\}\Gamma)\alpha_i$, $\{\pm I\}\Gamma = \bigcup(\{\pm I\}\Gamma')\beta_j$ are disjoint then so is $\mathrm{SL}_2(\mathbb{Z}) = \bigcup(\{\pm I\}\Gamma')\beta_j\alpha_i$.

5.4.4. Let $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \Gamma\beta_j$ so that also $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i,j}\Gamma'\alpha_i\beta_j$.

5.5.1. (c) Use Proposition 5.5.2 for the first part.

5.6.3. (a) Add a parenthesized subscript to the Hecke operators to denote level. Checking the diagram reduces to showing that for $f,g\in\mathcal{S}_k(\Gamma_1(Np^{-1}))$, (1) $T_{(Np^{-1})}f = T_{(N)}f$ and (2) $(T_{(Np^{-1})}g)[\alpha_p]_k = T_{(N)}(g[\alpha_p]_k)$.

For $T=\langle d\rangle$, show that if $\gamma\in\Gamma_0(N)$ has bottom right entry d then (1) since also $\gamma\in\Gamma_0(Np^{-1})$ it follows that $\langle d\rangle_{(Np^{-1})}$ is $\langle d\rangle_{(N)}$ restricted to level Np^{-1}; and (2) since $\alpha_p\gamma\alpha_p^{-1}\in\Gamma_0(Np^{-1})$ has bottom right entry d as well, it follows that $\langle d\rangle_{(Np^{-1})}$ is $[\alpha_p]_k\cdot\langle d\rangle_{(N)}\cdot[\alpha_p^{-1}]_k$ (composing left to right).

For $T=T_{p'}$, show that (1) $T_{p',(Np^{-1})}$ is $T_{p',(N)}$ restricted to level Np^{-1}; and (2) if $g\in\mathcal{S}_k(Np^{-1},\chi)$ for some character $\chi:(\mathbb{Z}/Np^{-1}\mathbb{Z})^*\longrightarrow\mathbb{C}^*$, then $g[\alpha_p]_k\in\mathcal{S}_k(N,\chi)$ where χ is now lifted to $(\mathbb{Z}/N\mathbb{Z})^*$. Use Proposition 5.2.2(b) to show $(T_{p',(Np^{-1})}g)[\alpha_p]_k = T_{p',(N)}(g[\alpha_p]_k)$.

(b) Going down and across takes (f,g) to $\sum_j f[\left[\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right]]_k+\sum_j g[\left[\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right]\left[\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right]]_k$ (this relies on $p\mid N$); at level Np^{-1} the first sum is $T_pf-(\langle p\rangle f)[\alpha_p]_k$ regardless of whether $p\mid Np^{-1}$; the second sum is $\sum_j g[\left[\begin{smallmatrix}p & 0\\ 0 & p\end{smallmatrix}\right]\left[\begin{smallmatrix}1 & j\\ 0 & 1\end{smallmatrix}\right]]_k$ which is $p^{k-1}g$. Going across and then down gives the same expression.

(e) Show that $w_{(N)}f = (w_{(Np^{-1})}f)[\alpha_p]_k$ and $w_{(N)}(g[\alpha_p]_k) = p^{k-2}w_{(Np^{-1})}g$, and now checking the diagram is straightforward.

5.7.2. If $\gamma_2 = \left[\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right]\in\Gamma_d$ then $\det\gamma_2 = 1$ and $\gamma_2\equiv\left[\begin{smallmatrix}1 & \beta\\ 0 & 1\end{smallmatrix}\right]\pmod N$ and $\beta = kN/d$ for some $k\in\mathbb{Z}$. Write $k=qd+b$, $0\le b<d$, and compute

$$\gamma_2\begin{bmatrix}1 & -bN/d\\ 0 & 1\end{bmatrix} = \begin{bmatrix}\alpha & \beta-\alpha bN/d\\ \gamma & \delta-\gamma bN/d\end{bmatrix}\overset{\text{call}}{=}\gamma_1.$$

Then $\det \gamma_1 = 1$, and $\beta - \alpha bN/d \equiv (1-\alpha)bN/d \pmod N \equiv 0 \pmod N$, and $\delta - \gamma bN/d \equiv 1 \pmod N$, so $\gamma_1 \equiv I \pmod N$. Thus $\gamma_1 \in \Gamma(N)$ and $\gamma_2 \in \Gamma(N)\left[\begin{smallmatrix}1 & bN/d\\ 0 & 1\end{smallmatrix}\right]$. For uniqueness, the coset $\Gamma(N)\left[\begin{smallmatrix}1 & bN/d\\ 0 & 1\end{smallmatrix}\right]$ has its upper right entry $\pmod N$ determined by $b \pmod d$.

5.7.4. If π is a projection then so is $1-\pi$. If π_1 and π_2 are commuting projections then $\ker(\pi_1\pi_2) = \ker(\pi_1) + \ker(\pi_2)$ (one containment is clear; for the other, write $x = y + z$ where $y = \pi_2(x)$ and $z = x - y$ and show $y \in \ker(\pi_1)$, $z \in \ker(\pi_2)$). If π is a projection then $x \in \mathrm{im}(\pi)$ if and only if $\pi(x) = x$ (if $x = \pi(y)$ then $\pi(x) = \pi^2(y) = \pi(y) = x$), and it follows that $\ker(1-\pi) = \mathrm{im}(\pi)$.

5.7.5. For example, the right side summand in Theorem 5.7.5 is

$$\begin{aligned}
\mathcal{S}_k(\Gamma^1(N/p)) &= \mathcal{S}_k(\Gamma(N))^{\Gamma^1(N/p)/\Gamma(N)} \\
&= \mathcal{S}_k(\Gamma(N))^{\prod_{j\neq i}\Gamma^1(p_j^{e_j})/\Gamma(p_j^{e_j})\times\Gamma^1(p_i^{e_i-1})/\Gamma(p_i^{e_i})} \\
&= \mathcal{S}_k(\Gamma(N))^{\prod_{j\neq i}H_j\times\langle H_i,K_i\rangle} \quad \text{by Lemma 5.7.6} \\
&= \mathcal{S}_k(\Gamma(N))^{\langle H,K_i\rangle}.
\end{aligned}$$

5.7.6. Setting $V = \mathcal{S}_k(\Gamma(N))$ isn't enough since the proposition requires V to be irreducible.

5.8.3. (c) Formula (5.4) with $\chi = \mathbf{1}_{11}$ describes the T_p-action on $\mathcal{S}_2(\Gamma_0(11))$, and the same formula with $\chi = \mathbf{1}_{88}$ describes the T_p-action on $\mathcal{S}_2(\Gamma_0(88))$.

5.8.4. By the methods early in the section, if $a_1(f) = 0$ then $f = 0$ and if $a_1(f) \neq 0$ then normalizing to $a_1(f) = 1$ gives $T_n f = a_n(f) f$ for all $n \in \mathbb{Z}^+$. Let $f = g + h$ with g old and h new. Applying T_n gives $a_n(f)f = T_n g + T_n h$, and since T_n preserves the decomposition of $\mathcal{S}_k(\Gamma_1(N))$ as a direct sum of old and new subspaces necessarily $T_n g = a_n(f)g$ and $T_n h = a_n(f)h$. Similarly g and h are $\langle n\rangle$-eigenforms for all $n \in \mathbb{Z}^+$. Thus g and h are eigenforms with T_n-eigenvalues $a_n(f)$. If $h = 0$ then $f = g$ is old. If $h \neq 0$ then again by the methods early in the section $a_1(h) \neq 0$ and $T_n h = (a_n(h)/a_1(h))h$, showing that $a_n(f) = a_n(h)/a_1(h)$ and thus $f = h/a_1(h)$ is new.

5.8.6. (a) The condition $p_i \nmid N/M_i$ gives $T_{p_i}(f_i(n\tau)) = (T_{p_i} f_i)(n\tau)$ by Proposition 5.6.2, and also the condition makes $T_{p_i} f_i$ at level N match $T_{p_i} f_i = a_{p_i}(f_i) f_i$ at level M_i, so that altogether $T_{p_i} f_{i,n} = a_{p_i}(f_i) f_{i,n}$. For the last statement of the proposition, the diamond operator $\langle n\rangle$ is the same at levels M and N for n coprime to N.

5.9.1. (a) See the more general argument in Section 5.4.

5.9.2. First consider the product over a finite set of primes and the sum over n divisible only by these primes.

5.9.6. (b) Consider characters ψ, ψ', φ, φ' modulo N, not necessarily primitive, such that $\psi(p) + \varphi(p)p^{k-1} = \psi'(p) + \varphi'(p)p^{k-1}$ for all $p \nmid N$. If $\psi \neq \psi'$ then $\psi(a) \neq \psi'(a)$ for some a. By the Dirichlet theorem on primes in an arithmetic progression there exist arbitrarily large primes p congruent to a modulo N, but the condition $0 < p^{k-1}|\varphi'(a) - \varphi(a)| = |\psi(a) - \psi'(a)| \leq 2$ gives a contradiction for large enough p.

5.11.2. For (a), let $T_p^* f = \tilde{a}_p f$ and compute that

$$\tilde{a}_p \langle f, f \rangle = \langle T_p^* f, f \rangle = \langle f, T_p f \rangle = \bar{a}_p \langle f, f \rangle.$$

For (b), if $b_p = a_p$ for all p then Proposition 5.8.5 shows that $E_k^{\psi,\varphi}/2 - f$ is constant, making it the zero function, but this violates the linear disjointness of $\mathcal{S}_k(\Gamma_1(N))$ and $\mathcal{E}_k(\Gamma_1(N))$. For (c), compute similarly to (a) that

$$a_p \langle E_k^{\psi,\varphi}, f \rangle = \langle E_k^{\psi,\varphi}, T_p^* f \rangle = \langle T_p E_k^{\psi,\varphi}, f \rangle = b_p \langle E_k^{\psi,\varphi}, f \rangle.$$

For (d), use Proposition 5.5.2(a) and then Exercise 5.4.3.

Chapter 6

6.1.3. If $\deg(f) = 1$ then there is no ramification.

6.1.4. By Proposition 6.1.4 $\varphi(z + \Lambda_g) = mz + \Lambda$ for some row vector $m \in \mathbb{C}^g$ such that $m\Lambda_g \subset \Lambda$, and $m \neq \mathbf{0}$ since φ surjects. Thus $\ker(\varphi)$ takes the form $V + \Lambda_g$ where $V \subset \mathbb{C}^g$ is a vector subspace of dimension $g - 1$. On the other hand $\mathrm{im}(f)$ contains $\int_{x_0}^{x}$ for all $x \in X_0(N)$. This includes $0_{\mathrm{J}_0(N)}$ so $0_E \in \mathrm{im}(\varphi \circ f)$, and $\mathrm{span}(\mathrm{im}(f)) = \mathrm{J}_0(N)$ by Abel's Theorem so $\mathrm{im}(f)$ can't be a subset of $\ker(\varphi)$. This makes $\varphi \circ f$ a nonconstant holomorphic map of compact Riemann surfaces, therefore a surjection.

6.2.2. (a) The result is clear on the subset Y' of Y defined later in the section. Since $\mathrm{norm}_h f$ extends continuously to Y as a function to $\widehat{\mathbb{C}}$ it is meromorphic.

6.3.1. (a) Regardless of whether the weight-k operator in general is defined by $(f[\alpha]_k)(\tau) = (\det \alpha)^e j(\alpha, \tau)^{-k} f(\alpha(\tau))$ with $e = k - 1$ or with $e = k/2$, the exponent is $e = 1$ for $k = 2$. The diagram says that $g(\alpha(\tau))d(\alpha(\tau)) = (g[\alpha]_2)(\tau)d\tau$ for $g \in \mathcal{S}_2(\Gamma_Y)$, and this is easy to check for any $g : \mathcal{H} \longrightarrow \mathbb{C}$.

6.4.1. By definition of r as a resultant, $r(u) = 0$ if and only if there exists some t such that $\tilde{q}(t, u) = 0$ and $q(t) = 0$, and by definition of $\tilde{q}$ as a resultant, there exists some t such that $\tilde{q}(t, u) = 0$ if and only if there exists some s such that $p(s) = 0$ and $u = s + t$. Thus $r(u) = 0$ if and only if there exist s and t such that $p(s) = 0$, $q(t) = 0$, and $u = s + t$. In particular, $r(\alpha + \beta) = 0$.

6.4.3. If $\alpha \in \overline{\mathbb{Z}} \cap \mathbb{Q}$ then $\alpha = s/t$ with $\gcd(s,t) = 1$ and $t^n p(\alpha) = 0$ for some monic polynomial p with integer coefficients. This last relation implies $t \mid s$, so $t = 1$. The other containment is clear.

6.4.4. Each algebraic number α satisfies a polynomial $x^n + (c_1/d)x^{n-1} + \cdots + (c_n/d)$ with $c_1, \ldots, c_n, d \in \mathbb{Z}$. Consider $d^n\alpha$.

6.5.2. For each $d \in (\mathbb{Z}/N\mathbb{Z})^*$ take two primes p and p' both congruent to d modulo N. Use formula (5.10) with $r = 2$ to express $\chi(d)$ in terms of $a_p(f)$, $a_{p^2}(f)$, $a_{p'}(f)$, and $a_{p'^2}(f)$.

6.5.3. For the first isomorphism, if $\varphi \in (M/JM)^\wedge$ then the map $\tilde{\varphi} : m \mapsto \varphi(m + JM)$ is an element of $M^\wedge[J]$, and if $\psi \in M^\wedge[J]$ then the map $\tilde{\psi} : m + JM \mapsto \psi(m)$ is a well defined element of $(M/JM)^\wedge$. Show that $\varphi \mapsto \tilde{\varphi}$ and $\psi \mapsto \tilde{\psi}$ invert each other and that either of them is an A-module homomorphism. The second isomorphism follows from the first since a finite-dimensional vector space is naturally isomorphic to its double dual. In particular, if $\varphi + JM^\wedge \in M^\wedge/JM^\wedge$ then the restriction $\tilde{\varphi} = \varphi|_{M[J]}$ is the corresponding element of $M[J]^\wedge$.

6.6.5. (a) Taking $\varphi \in \mathrm{J}_1(N)$ and omitting cosets from the notation, $((\Psi_{f,n} \circ T_p)\varphi)(f^\sigma) = n\varphi((T_p f^\sigma) \circ n)$ while $((a_p(f) \circ \Psi_{f,n})\varphi)(f^\sigma) = n\varphi(T_p(f^\sigma \circ n))$. These are the same by Section 5.6 since $p \nmid N$.

(b) Stack (6.19) on (6.20), show that the outer rectangle commutes, combine this with the top square commuting and isogenies surjecting to show that the bottom square commutes.

Chapter 7

7.1.4. (b) Substitute the relation $y = \lambda x + \mu$ into (7.1) to get a cubic equation $4x^3 - \lambda^2 x^2 + \cdots = 0$. Show that the roots are x_P, x_Q, and r as in (7.3). Also letting s be as in (7.3), the sum $P + Q = (r, s)$ agrees with (7.2).

7.2.3. (a) Since φ is a combination $\sum_i f_i\varphi_i$ where the f_i are polynomials, use the product rule and then the fact that $\varphi_i(P) = 0$ for all i. (c) If $D_2E(P) \neq 0$ then $(0,1) \notin T_p(\mathcal{E})$, so $T_p(\mathcal{E})$ is spanned by some (a,b) with $a \neq 0$. Thus $x - x_P + m_P^2$ can serve as the dual basis under the pairing. (d) One containment is clear. For the other, suppose $s \in m_P \cap M_P^2$. Then $s = r/t$ where $r \in m_P^2$ and $t \in \overline{\mathbf{k}}[C] - m_P$. Since m_P is maximal, $1 - tv \in m_P$ for some $v \in \overline{\mathbf{k}}[C]$. But $s = s(1 - tv) + rv$, showing that $s \in m_P^2$.

7.3.2. Renotate $\{v_P\}$ as $\{v_1, \ldots, v_N\}$ and use induction on N. The case $N = 1$ is clear since $v_1^\perp$ is a subspace of codimension 1. For the induction step suppose some a_{N-1} satisfies $a_{N-1} \cdot v_i \neq 0$ for $i = 1, \ldots, N-1$. If $a_{N-1} \cdot v_N \neq 0$ then there is nothing to show. Otherwise take some u such that $u \cdot v_N \neq 0$ and consider vectors $a_N = u - k a_{N-1}$.

7.3.4. (a) Let $F_1(x,y) = (F(x,y) - F(x,-y))/(2y)$ and $F_2(x,y) = (F(x,y) + F(x,-y))/2$. These are both invariant under $y \mapsto -y$, making them functions of x.

7.5.1. (c) First evaluate the limit termwise and then convince yourself that doing so is justified.

7.5.3. (c) For the first part, $f_0(\Gamma(N)\infty) = \frac{3N(N-1)}{2}$ while $(f_0 \circ \gamma)(\Gamma(N)\infty)$ is strictly smaller if $\gamma \notin \Gamma_0(N)$. Geometrically, as $\mathrm{Im}(\tau) \to +\infty$ so that $j \to \infty$, the universal elliptic curve is degenerating to the singular curve $y^2 = 4x^3 - 27x - 27$, whose singular point $(-3/2, 0)$ is an isolated point of the curve's real points. All N-torsion points coming from complex torus points $(c\tau + d)/N$ with $c \neq 0 \pmod N$ go to the isolated point as $\mathrm{Im}(\tau) \to +\infty$, but the N-torsion points coming from complex torus points d/N stay on the other real piece. Section 8.1 will discuss singular curves such as this one. For the second part, the formula before the display shows that j_N is γ-invariant if and only if j is γ'-invariant. Clearly γ' has rational entries and determinant 1. If $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ then j is γ'-invariant. If $\gamma' \notin \mathrm{SL}_2(\mathbb{Z})$ then it identifies points that are incongruent under $\mathrm{SL}_2(\mathbb{Z})$, because any $\tau \in \mathcal{H}$ such that $\gamma'(\tau) = \delta(\tau)$ for some $\delta \in \mathrm{SL}_2(\mathbb{Z})$ satisfies a quadratic equation over $\mathbb{Q}$. But j takes a different value at each point of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, so it is not γ'-invariant. Thus j_N is γ-invariant if and only if $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$, and it follows quickly from the display that this condition is $\gamma \in \Gamma_0(N)$.

7.5.4. First compute j for the curve $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$ obtained from the map $(\wp, \wp')$. Since the curve E_j differs from this curve by an admissible change of variable it has the same invariant.

7.7.1. Since $f_0 = x(\langle Q_\tau \rangle)$ is the sum of the finite x-coordinates of $\langle Q_\tau \rangle$, it follows that $f_0^\sigma = x(\langle Q_\tau^\sigma \rangle)$ for $\sigma \in H_{\mathbb{Q}}$. The results obtained over $\mathbb{C}$ show that the fixing subgroup is the subgroup that preserves $\langle Q_\tau \rangle$, i.e., $Q_\tau^\sigma = dQ_\tau$ for some d.

7.8.1. (b) Since $\ell(P) = 1$ and $L(P)$ contains $\mathbf{k}$, $L(P)$ is no more than $\mathbf{k}$. Thus there is no function with a simple pole at P. Any set of elements with distinct valuations at P is linearly independent, by properties of the valuation. Thus the linear relation at the end must involve at least one of X^3 and Y^2 since the other five elements are linearly independent. Take the coefficient of X^3 to be 1 and the coefficient of Y^2 to be a. Substitute aX and aY for X and Y and then divide by a^3.

7.8.2. (a) The group law is $(\sigma, P)(\sigma', P') = (\sigma\sigma', \sigma'(P) + P')$. Check that $(\sigma, P)((\sigma', P')f) = ((\sigma, P)(\sigma', P'))f$.

(b) The semidirect product acts on constant functions in $\mathbb{K}$ as H since translating the variable has no effect. Showing that $\mathbb{K} \cap \mathbf{l} = \mathbf{k}'$ in fact shows $\mathbb{K} \cap \overline{\mathbf{k}'} = \mathbf{k}'$ by the nature of the rest of the configuration.

(d) Write the restriction of i as $\mathbf{l}(E)^{H \ltimes C} \longrightarrow \mathbf{l}(E)^H$.

7.8.4. $\varphi \circ \psi \circ \varphi = \varphi \circ [\deg(\varphi)] = [\deg(\varphi)] \circ \varphi$ since φ is a homomorphism. Since φ surjects it cancels on the right, giving the result.

7.8.5. Take a point $Q \in E'$ and any point $P \in E$ such that $\varphi(P) = Q$. Then at the level of divisors, $\hat{\psi}_*((Q) - (0_{E'})) = ([\deg(\varphi)]P) - (0_E)$ while since φ is unramified,

$$\varphi^*((Q) - (0_{E'})) = \sum_{R \in \ker(\varphi)} (P + R) - \sum_{R \in \ker(\varphi)} (R).$$

These are not equal, but their difference satisfies the characterization of principal divisors in Theorem 7.3.3 since $\deg(\varphi) = |\ker(\varphi)|$, so their classes are equal in $\mathrm{Pic}^0(E)$.

7.9.2. (a) $w_N : X_0(N) \longrightarrow X_0(N)$ given by $\Gamma_0(N)\tau \mapsto \Gamma_0(N)\tau'$ is a holomorphic map of compact Riemann surfaces. By Section 7.3 it can be viewed instead as a morphism over $\mathbb{C}$ of algebraic curves over $\mathbb{C}$. Its pullback is $w_N^* : \mathbb{C}(X_0(N)) \longrightarrow \mathbb{C}(X_0(N))$, a $\mathbb{C}$-injection of function fields over $\mathbb{C}$. By Section 7.5 this is $w_N^* : \mathbb{C}(j(\tau), j_N(\tau)) \longrightarrow \mathbb{C}(j(\tau), j_N(\tau))$, taking $j(\tau)$ to $j(\tau')$ and $j_N(\tau)$ to $j_N(\tau')$. If $j(\tau')$ and $j_N(\tau')$ are in $\mathbb{Q}(j(\tau), j_N(\tau))$ then it restricts to $w_N^* : \mathbb{Q}(j(\tau), j_N(\tau)) \longrightarrow \mathbb{Q}(j(\tau), j_N(\tau))$, a $\mathbb{Q}$-injection of function fields over $\mathbb{Q}$. This is $w_N^* : \mathbb{Q}(X_0(N)_{\mathrm{alg}}) \longrightarrow \mathbb{Q}(X_0(N)_{\mathrm{alg}})$ by Section 7.7, and now Theorem 7.2.6 gives $w_N : X_0(N)_{\mathrm{alg}} \longrightarrow X_0(N)_{\mathrm{alg}}$, a morphism over $\mathbb{Q}$ of algebraic curves over $\mathbb{Q}$. For the last part, compute that $j(\tau') = j_N(\tau)$ and $j_N(\tau') = j(\tau)$.

(b) A point of $X_0(N)_{\mathrm{alg}}^{\mathrm{planar}}$ is $(j, x) \in \overline{\mathbb{Q}}^2$ such that $p_0(j, x) = 0$. The map is $[E, C] \mapsto (j(E), x(C))$ where $x(C)$ is the sum of the x-coordinates of the nonzero points of C. For the second part, recall Exercise 1.5.4.

7.9.3. (b) The full extensions have the same Abelian Galois group. The upper and lower Galois extensions on the left inject into the ones on the right, so the extension degrees must match. Now use the fact that the Galois group is cyclic.

(e) Compute

$$\begin{aligned} f_1(p\tau)^\sigma &= x(Q_{\tau',N})^\sigma = x(Q_{\tau',N}^\sigma) = x(\varphi(Q_{\tau,Np})^\sigma) = x(\varphi^\sigma(Q_{\tau,Np}^\sigma)) \\ &= x(\pm\varphi(Q_{\tau,Np})) = f_1(p\tau), \end{aligned}$$

the second-to-last step using parts (b) and (d) to show that $\varphi(Q_{\tau,Np}^\sigma) = \varphi(Q_{\tau,Np})$.

7.9.4. Consider the map $[N] : E \longrightarrow E$ and recall that the structure of $E_{\mathbb{C}}[N]$ was established in Chapter 1.

Chapter 8

8.1.1. (b) Consider the matrices

$$\begin{bmatrix} u^2 & 0 & r \\ su^2 & u^3 & t \\ 0 & 0 & 1 \end{bmatrix}.$$

For (c), the condition implies $v^3 = w^2$. Take $u = w/v$. For (e), take $r = -3/2$, $s = i3\sqrt{2}/2$, $t = 0$, and $u = i3\sqrt{2}$.

8.1.5. (a) If $\mathrm{char}(\mathbf{k}) \neq 2$ then we may take $a_1 = a_3 = 0$ and so $P = (x, 0)$ where x is a repeated root of a cubic polynomial over $\mathbf{k}$. If $\mathrm{char}(\mathbf{k}) = 2$ and $a_1 \neq 0$ then $x = a_1^{-1}a_3$ and $y = a_1^{-1}(x^2 + a_4)$. If $\mathrm{char}(\mathbf{k}) = 2$ and $a_1 = 0$ then use the fact that every element of $\mathbf{k}$ is a square.

8.2.1. For uniqueness, the $q - 1$ nonzero elements of such a subfield satisfy $x^{q-1} = 1$.

8.3.1. Recall that $1728\Delta = c_4^3 - c_6^2$.

8.3.2. (a) Since $\Delta'_p = \Delta/u_p^{12}$ and $\nu_p(\Delta'_p) \leq \nu_p(\Delta)$ it follows that $\nu_p(u_p) \geq 0$. If $\nu_p(u_p) = 0$ then we may take $u_p = 1$ and $r_p = s_p = t_p = 0$, so now assume $\nu_p(u_p) > 0$. Since $\nu_p(a_i) \geq 0$ and $\nu_p(a'_{i,p}) \geq 0$ the formula $a'_{1,p} = (a_1 + 2s_p)/u_p$ shows that $\nu_p(s_p) \geq 0$. (Note that for $p = 2$ this requires $\nu_2(u_2) > 0$.) Similarly the formula $a'_{2,p} = (a_2 - s_p a_1 + 3r_p - s_p^2)/u_p^2$ shows that $\nu_p(r_p) \geq 0$, and $a'_{3,p} = (a_3 + r_p a_1 + 2t_p)/u_p^3$ shows that $\nu_p(t_p) \geq 0$.

(c) For each $p \mid \Delta$ let $r_p = p^{e_p} m_p / n_p$. Then $\nu_p(r - r_p) = \nu_p(n_p r - p^{e_p} m_p)$ for $r \in \mathbb{Z}$. The congruence $n_p r \equiv p^{e_p} m_p \pmod{p^{6\nu_p(u)}}$ has a solution $r \pmod{p^{6\nu_p(u)}}$, and thus $\nu_p(r - r_p) \geq 6\nu_p(u)$. The Chinese Remainder Theorem gives an integer r simultaneously satisfying the condition for all primes $p \mid \Delta$.

8.3.3. (b) If the a_i and the a'_i are integral then so are the b_i and the b'_i. The relation $b'_2 - b_2 = 12r$ shows that $\nu_p(r) \geq 0$ for all primes p except possibly 2 and 3. If $\nu_3(r) < 0$ then the relation $\nu_3(b'_6 - b_6) \geq 0$ is impossible, and similarly for 2 and $b'_8 - b_8$.

(c) The relation $\pm a'_1 - a_1 = 2s$ shows that $\nu_p(s) \geq 0$ for all primes p except possibly 2, and the relations $\nu_2(s) < 0$ and $a'_2 - a_2 = -sa_1 + 3r - s^2$ are incompatible. Similarly for t, using the relations between $\pm a'_3$ and a_3, and a'_6 and a_6.

8.3.5. Show that $a_p(E) \equiv 0 \pmod{p}$ if and only if $|\widetilde{E}(\mathbb{F}_{p^e})| \not\equiv 0 \pmod{p}$ for all $e \geq 1$. By Theorem 8.1.2 this holds if and only if $\widetilde{E}(\mathbb{F}_{p^e}) \cap \widetilde{E}[p] = \{0_E\}$ for all $e \geq 1$, and this in turn holds if and only if $\widetilde{E}[p] = \{0\}$.

8.3.6. (a) The discriminant is $-2^4 3^3$ and $c_4 = 0$. Recall Proposition 8.1.3.

(b) If $x^3 = 1$ and $x \neq 1$ then $x^2 + x + 1 = 0$, impossible in $\mathbb{F}_p$ when $p \equiv 2 \pmod 3$ by Quadratic Reciprocity. So as x runs through $\mathbb{F}_p$ so does $x^3 - 1$, giving one point (x, y) on the curve for each $y \in \mathbb{F}_p$. Remember 0_E as well.

(c) For the first displayed equality, remember 0_E. For the last part, remember that f is cubic.

(e) The reduction is ordinary for $p \equiv 1 \pmod 4$, supersingular for $p \equiv 3 \pmod 4$.

8.4.1. (b) For the first part, $\beta = \tilde{\alpha}$ for some $\alpha \in \overline{\mathbb{Z}}$, this α satisfies some monic polynomial $f \in \mathbb{Z}[x]$, and so β satisfies the monic polynomial $g = \tilde{f} \in (\mathbb{Z}/p\mathbb{Z})[x]$ obtained by reducing the coefficients of f modulo p,

$$g(\beta) = \tilde{f}(\tilde{\alpha}) = \widetilde{f(\alpha)} = \widetilde{0_{\overline{\mathbb{Z}}}} = 0_{\overline{\mathbb{Z}}/\mathfrak{p}}.$$

For the second part, since $f(x) = \prod(x - \alpha_i)$ in $\overline{\mathbb{Z}}[x]$ it follows that $g(x) = \prod(x - \tilde{\alpha}_i)$ in $(\overline{\mathbb{Z}}/\mathfrak{p})[x]$.

8.4.3. Since we don't have a valuation on $\overline{\mathbb{Q}}$, one method is to work in the number field $\mathbb{K}$ generated by the Weierstrass coefficients and the change of variable parameters, arguing as in the proof of Lemma 8.4.1 that this field has a valuation and then continuing as in Exercise 8.3.3(b,c). Another method is to use the lemma itself as follows. The conditions $u \in \overline{\mathbb{Z}}^*_{(\mathfrak{p})}$ and $u^2 b'_2 - b_2 = 12r$ show that $r \in \overline{\mathbb{Z}}_{(\mathfrak{p})}$ unless $\mathfrak{p}$ lies over 2 or 3. If $r \notin \overline{\mathbb{Z}}_{(\mathfrak{p})}$ then $1/r \in \mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$ by the lemma and the union $\overline{\mathbb{Z}}_{(\mathfrak{p})} = \overline{\mathbb{Z}}^*_{(\mathfrak{p})} \cup \mathfrak{p}\overline{\mathbb{Z}}_{(\mathfrak{p})}$. If $\mathfrak{p}$ lies over 3 then the relation

$$u^6 b'_6 - b_6 = (2b_4/r^2 + b_2/r + 4)r^3$$

gives a contradiction since the left side lies in $\overline{\mathbb{Z}}_{(\mathfrak{p})}$ and the first factor on the right side lies in $\overline{\mathbb{Z}}^*_{(\mathfrak{p})}$, but $r^3 \notin \overline{\mathbb{Z}}_{(\mathfrak{p})}$. If $\mathfrak{p}$ lies over 2 then use the relation

$$u^8 b'_8 - b_8 = (3b_6/r^3 + 3b_4/r^2 + b_2/r + 3)r^4.$$

So $r \in \overline{\mathbb{Z}}_{(\mathfrak{p})}$. Argue similarly for s and t.

8.4.4. (c) Recall Exercise 8.3.6(e).

8.5.1. $I = \langle \{p\varphi_i\}, p(p\phi - 1), \{(p\phi - 1)\psi_j\} \rangle$.

8.5.2. (c) Part (b) applies with $i = 0$.

8.5.4. $I_{(0)} = \langle x_1 + px_2^2 \rangle$ works.

8.5.6. (c) If $yz \in J$ and $y \notin J$ then $z \in \mathrm{Ann}_S(xy)$, so $\langle J, z \rangle \subset \mathrm{Ann}_S(xy)$, contradicting maximality unless $z \in J$.

8.5.7. (a) Let C be the curve and C_i the nonempty affine piece. Then $P \in C - C_i$ if and only if $(x_i/x_j)(P) = 0$ for some $j \neq i$, but each x_i/x_j (where x_j is not identically 0 on C) has a finite set of zeros.

(b) This is immediate from (a) since the projective curve is infinite.

8.6.1. Taking $[E_j, Q]$ across and then down gives $(j, x(Q))$ and then $(\tilde{j}, \widetilde{x(Q)})$. Taking it down and then across gives $[\widetilde{E}_j, \widetilde{Q}]$ and then $(j(\widetilde{E}_j), x(\widetilde{Q}))$. These are the same.

8.7.1. Let $E' = E/C$ and $Q' = Q + C$. Let $\varphi : E \longrightarrow E'$ be the quotient isogeny, so that $Q' = \varphi(Q)$. Properties of degree and the calculation $\ker(\tilde{\varphi}) \subset \ker([p]_{\widetilde{E}}) = \widetilde{E}[p] = \{0\}$ combine to show that $\tilde{\varphi} = i \circ \sigma_p$ where $i : \widetilde{E}^{\sigma_p} \longrightarrow \widetilde{E'}$ is an isomorphism taking $\widetilde{Q}^{\sigma_p}$ to $\widetilde{Q'}$. The first equality follows. The second is shown similarly using the dual isogeny ψ, citing Proposition 8.4.4(b), and applying σ_p^{-1} to the coefficients of the resulting isomorphism i in this case.

8.7.2. (a) For the first diagram, going across and then down takes $[\widetilde{E}_j, Q]$ to $[\widetilde{E}_j^{\sigma_p}, Q^{\sigma_p}]$ and then to $(j(\widetilde{E}_j^{\sigma_p}), x(Q^{\sigma_p}))$, while going down and then across takes it to $(j, x(Q))$ and then to $(j^{\sigma_p}, x(Q)^{\sigma_p})$. For the second diagram, going across and then down takes $[\widetilde{E}_j, Q]$ to $p[\widetilde{E}_j^{\sigma_p^{-1}}, Q^{\sigma_p^{-1}}]$ and then to $p(j(\widetilde{E}_j^{\sigma_p^{-1}}), x(Q^{\sigma_p^{-1}}))$, while going down and then across takes it to $(j, x(Q))$ and then to $p(j^{\sigma_p^{-1}}, x(Q)^{\sigma_p^{-1}})$, cf. (8.15). In both cases the results are the same.

(b) There is a birational equivalence h from $\widetilde{X}_1(N)^{\text{planar}}$ to $\widetilde{X}_1(N)$ as described in Theorem 8.6.1. Consider the diagram

$$\begin{array}{ccc} \mathrm{Div}^0(\widetilde{X}_1(N)^{\text{planar}}) & \xrightarrow{\sigma_{p,*}} & \mathrm{Div}^0(\widetilde{X}_1(N)^{\text{planar}}) \\ \Big\downarrow{\scriptstyle h_*} & & \Big\downarrow{\scriptstyle h_*} \\ \mathrm{Div}^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_{p,*}} & \mathrm{Div}^0(\widetilde{X}_1(N)) \end{array}$$

and recall formula (8.17). The map across the bottom row descends to Picard groups. The other diagram is similar by formula (8.19).

(c) Set up a cube diagram as in the section, but with $\langle d \rangle$ and $\langle d \rangle_*$ across the top rows and with the reductions $\widetilde{\langle d \rangle}$ and $\widetilde{\langle d \rangle}_*$ across the bottom rows. Thus the bottom square is diagram (8.39). Explain why all the other squares of the cube commute and why the map from the top front left to the bottom front left surjects. Complete the argument.

(d) Combine the second diagram from part (b) with diagram (8.39) to get a commutative diagram

$$\begin{array}{ccccc} \mathrm{Div}^0(\widetilde{S}_1(N)') & \xrightarrow{p\sigma_p^{-1}} & \mathrm{Div}^0(\widetilde{S}_1(N)') & \xrightarrow{\widetilde{\langle d \rangle}} & \mathrm{Div}^0(\widetilde{S}_1(N)') \\ \Big\downarrow & & \Big\downarrow & & \Big\downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_p^*} & \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\widetilde{\langle d \rangle}_*} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array}$$

Along with the first diagram from part (b) this gives (8.34).

8.8.1. (a) $\mathrm{Pic}^0(X_0(N)_{\mathbb{C}})$ is generated by the image of $X_0(N)_{\mathbb{C}}$, and the third stage of $\beta_{\mathbb{C}}$ is an isomorphism.

Chapter 9

9.1.1. The extension $\mathbb{Q}(d^{1/3})/\mathbb{Q}$ is not Galois but the extensions $\mathbb{F}/\mathbb{Q}(d^{1/3})$, $\mathbb{F}/\mathbb{Q}(\mu_3)$, and $\mathbb{Q}(\mu_3)/\mathbb{Q}$ are. Recall from Exercise 8.3.6(b) that if $p \equiv 2 \pmod 3$ then every a is a cube modulo p.

9.2.1. (b) A basis of the product topology is the subsets $S = \prod_n S_n$ where $S_n = \mathbb{Z}/\ell^n\mathbb{Z}$ for all but finitely many n. Each C_n is the subgroup of compatible elements, naturally isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z}$.

9.2.2. Any nonidentity $m \in \mathrm{GL}_d(\mathbb{C})$ that is close enough to I takes the form $m = \exp(a)$ where $a \in \mathrm{M}_d(\mathbb{C})$ is nonzero, and $m^n = \exp(na)$ for all $n \in \mathbb{Z}$.

9.2.3. (a) Since λ lies over ℓ it follows that $\lambda^{ne_\lambda} \cap \mathbb{Z} = \ell^{n'}\mathbb{Z}$ for some n'. The condition $\ell^m \in \lambda^{ne_\lambda}$ is $\prod_\lambda \lambda^{me_\lambda} \subset \lambda^{ne_\lambda}$, and the unique factorization of ideals in $\mathcal{O}_{\mathbb{K}}$ shows that this holds if and only if $m \geq n$. Thus $n' = n$. So the map $\mathbb{Z} \longrightarrow \mathcal{O}_{\mathbb{K}}/\lambda^{ne_\lambda}$ has kernel $\ell^n\mathbb{Z}$, making $\mathbb{Z}/\ell^n\mathbb{Z} \longrightarrow \mathcal{O}_{\mathbb{K}}/\lambda^{ne_\lambda}$ an injection for all n and λ. This gives an injection $\mathbb{Z}_\ell \longrightarrow \mathcal{O}_{\mathbb{K},\lambda}$ for all λ.

(b) The injection surjects if $|\mathcal{O}_{\mathbb{K}}/\lambda^{ne_\lambda}| = \ell^n$ for all n, i.e., $|\mathcal{O}_{\mathbb{K}}/\lambda|^{e_\lambda} = \ell$, i.e., $e_\lambda f_\lambda = 1$.

9.3.1. Let U be any open normal subgroup. Then $U(\mathbb{F}) \subset U$ for some Galois number field $\mathbb{F}$, giving a surjection $\mathrm{Gal}(\mathbb{F}/\mathbb{Q}) = G_{\mathbb{Q}}/U(\mathbb{F}) \longrightarrow G_{\mathbb{Q}}/U$. This shows that $G_{\mathbb{Q}}/U = \mathrm{Gal}(\mathbb{F}'/\mathbb{Q})$ for some $\mathbb{F}' \subset \mathbb{F}$, and so $U = U(\mathbb{F}')$.

9.3.2. Consider any neighborhood $U = U_\sigma(\mathbb{F})$ in $G_{\mathbb{Q}}$. We want to find some $\mathrm{Frob}_{\mathfrak{p}} \in U$. This holds if $\mathrm{Frob}_{\mathfrak{p}}|_{\mathbb{F}} = \sigma|_{\mathbb{F}}$. But $\sigma|_{\mathbb{F}}$ takes the form $\mathrm{Frob}_{\mathfrak{p}_{\mathbb{F}}}$ for some maximal ideal of $\mathcal{O}_{\mathbb{F}}$ by Theorem 9.1.2. Lift $\mathfrak{p}_{\mathbb{F}}$ to a maximal ideal $\mathfrak{p}$ of $\overline{\mathbb{Z}}$.

9.3.4. Take a neighborhood V of I in $\mathrm{GL}_d(\mathbb{C})$ containing no nontrivial subgroup, cf. Exercise 9.2.2. Let $U = \rho^{-1}(V)$. As a neighborhood of 1 in $G_{\mathbb{Q}}$, U contains $U(\mathbb{F})$ for some Galois number field $\mathbb{F}$. So ρ is defined on $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$.

9.3.5. Let $M = \mathrm{lcm}(N, N')$, so $\rho|_{\mathbb{Q}(\mu_M)}$ can be viewed via the isomorphism (9.1) as a character χ of $(\mathbb{Z}/M\mathbb{Z})^*$ that factors through $(\mathbb{Z}/N\mathbb{Z})^*$ and $(\mathbb{Z}/N'\mathbb{Z})^*$. Since $\chi(n \mod M)$ is trivial if $n \equiv 1 \pmod N$ and if $n \equiv 1 \pmod{N'}$ it follows that χ is defined modulo $\gcd(N, N')$.

9.3.7. (a) $\mathbb{L}^d$ is a d-dimensional topological vector space over $\mathbb{L}$. The groups $\mathrm{GL}_d(\mathbb{L})$ and $\mathrm{Aut}(\mathbb{L}^d)$ are naturally identified. Since ρ is continuous so is its composition with vector-by-matrix multiplication,

$$\mathbb{L}^d \times G_{\mathbb{Q}} \longrightarrow \mathbb{L}^d, \qquad (v, \sigma) \mapsto v\rho(\sigma).$$

Thus ρ makes $\mathbb{L}^d$ a $G_{\mathbb{Q}}$-module satisfying the continuity condition of Definition 9.3.4. On the other hand, any choice of ordered basis of V identifies $\mathrm{Aut}(V)$ with $\mathrm{GL}_d(\mathbb{L})$, and then the map $G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(V)$ gives a map $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_d(\mathbb{L})$. Specifically, the matrix entries are $\rho(\sigma)_{ij} = x_j(e_i\sigma)$ where the ordered basis is $(e_1, \ldots, e_d)$ and $x_i : V \longrightarrow \mathbb{L}$ is $\sum_\iota a_\iota e_\iota \mapsto a_i$. Each ρ_{ij} is a continuous function, making ρ a Galois representation as in Definition 9.3.2.

(b) Equivalent representations ρ and ρ' as in Definition 9.3.2 determine $G_{\mathbb{Q}}$-linear isomorphic $G_{\mathbb{Q}}$-module structures of $\mathbb{L}^d$, and if V and V' are equivalent as in Definition 9.3.4 then any choice of ordered bases B and B' determines equivalent representations as in Definition 9.3.2. Also, going from ρ to $\mathbb{L}^d$ and then choosing a basis B gives a representation ρ' equivalent to ρ, while on the other hand starting with V and then choosing a basis to define ρ gives $\mathbb{L}^d$ a $G_{\mathbb{Q}}$-module structure equivalent to V.

9.4.3. The isogeny $E \longrightarrow E'$ induces a map $V_\ell(E) \longrightarrow V_\ell(E')$. The map is an isomorphism since the dual isogeny induces a similar map in the other direction and the composite is multiplication by the degree of the isogeny, an automorphism because $\mathbb{Q}_\ell$ has characteristic 0.

9.4.4. (c) Since ℓ-torsion contains an ℓ-cyclic subgroup of points with rational coordinates, $\overline{\rho}_{E,\ell} \sim \left[\begin{smallmatrix} 1 & 0 \\ 0 & \overline{\chi_\ell} \end{smallmatrix}\right]$ where $\overline{\chi_\ell} : G_{\mathbb{Q}} \longrightarrow \mathbb{F}_2$ is the mod 2 reduction of the cyclotomic character. Alternatively, the ℓ-cyclic subgroup of points with rational coordinates implies that $\ell \mid |\widetilde{E}(\mathbb{F}_\ell)|$, i.e., $a_p(E) \equiv p + 1 \pmod{\ell}$.

9.5.1. This follows from Lemma 9.5.2.

9.5.2. (a) Each $\mathbb{K}_{f,\lambda}$ acts on $V_\lambda(f)$ via i^{-1}. The dimension is 2 because $V_\lambda(f) = e_\lambda V_\ell(A_f) \cong e_\lambda(\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^2 \cong \mathbb{K}_{f,\lambda}^2$. Apply each e_λ to any linear dependence $\sum_{\lambda'} e_{\lambda'} v_{\lambda'} = 0$ to show that the sum $\sum_\lambda V_\lambda(f)$ is direct. The relation $v = \sum_\lambda e_\lambda v$ for any $v \in V_\ell(A_f)$ shows that the sum spans $V_\ell(A_f)$. The $G_{\mathbb{Q}}$-action restricts to $V_\lambda(f)$ because it commutes with e_λ.

(b) The first part is explained at the end of Section 9.2. For the second part, $\rho_{A_f,\ell}$ is continuous, making $V_\ell(A_f) \times G_{\mathbb{Q}} \longrightarrow V_\ell(A_f)$ continuous, and $V_\lambda(f)$ is a $\mathbb{Q}_\ell$-vector subspace of $V_\ell(A_f)$.

9.6.1. (a) Since *conj* has order 2 the only possible eigenvalues are ± 1. Recall that $\det \rho(\mathrm{conj}) = -1$.

(b) Irreducibility immediately gives σ with $b \neq 0$ and σ' with $c \neq 0$. If neither σ nor σ' works then $\sigma\sigma'$ does. For the last part, conjugate by a matrix of the form $\left[\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right]$.

9.6.4. (a) To verify that the map is an embedding check the orders of the elements by using characteristic polynomials to compute eigenvalues. This also shows that the two elements of $\mathrm{GL}_2(\mathbb{F}_3)$ generate a subgroup H of order divisible by 24. Since A_4 is the only order 12 subgroup of S_4, $\mathrm{SL}_2(\mathbb{F}_3)$ is

the only order 24 subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$, but the second generator of H has determinant -1.

(b) The first statement follows from the end of part (a). Working modulo λ, compute for $p \nmid 3M_f N_E$ that

$$a_p(f) \equiv \operatorname{tr} \overline{\rho}_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}}) = \operatorname{tr} \overline{\rho}_{E,3}(\mathrm{Frob}_{\mathfrak{p}}) \equiv a_p(E).$$

Since $\psi = \det \rho_{f,\lambda}$ is a lift of $\det \overline{\rho}_{E,3} = \chi_3 \pmod 3$ from $\mathbb{F}_3^*$ to $\mathcal{O}_{\mathbb{K}}^*$ it suffices to consider the latter character, $\det \overline{\rho}_{E,3} = \chi_3 \pmod 3$. This surjects, making ψ quadratic, and since as a Galois representation it is defined on $\mathrm{Gal}(\mathbb{Q}(\mu_3)/\mathbb{Q})$, as a Dirichlet character ψ has conductor 3.

(c) Use results in Chapter 4 to evaluate the leading coefficient of the Eisenstein series.

(d) Since $\psi(p) \equiv p \pmod \lambda$ the operators T_p on $\mathcal{S}_1(M_f, \psi)$ and T_p on $\mathcal{S}_2(\Gamma_0(M_f))$ are congruent modulo λ. This observation and part (c) show that $T_p g \equiv T_p f = a_p(f) f \pmod \lambda$. On the one hand the right side is congruent modulo λ to $a_p(E)g$ for all but finitely many p by parts (b) and (c), giving the first statement. On the other hand the right is also congruent modulo λ to $a_p(g)g = a_1(T_p g)g$ for all p by part (c). The second statement follows.

(e) For all but finitely many primes $\phi(T_p) \equiv a_p(E) \pmod \lambda$, and so $T_p - a_p(E) \in \ker \phi = m$, implying $\phi'(T_p) - a_p(E) \in \phi'(m) \subset \lambda'$.

(h) The argument in Exercise 9.6.1 applies over any field whose characteristic is not 2. Let $\mathbb{L}$ be a finite Galois extension of $\mathbb{Q}$ containing $\mathbb{K}_{g''}$ and $\mathbb{K}_{g'}$. Use Strong Multiplicity One to show that if $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ then $(g'')^\sigma$ is the newform associated to $(g')^\sigma$; in particular if σ fixes $\mathbb{K}_{g'}$ then it fixes $\mathbb{K}_{g''}$.

List of Symbols

$\left(\frac{a}{2}\right)$ (Kronecker symbol), 373
A_f (Abelian variety associated to f), 245
A'_f (Abelian variety associated to f and $\Gamma_0(N)$), 250
$\mathcal{A}(\Gamma)$ (automorphic forms of all weights with respect to Γ), 73
$\mathcal{A}_k(\Gamma)$ (automorphic forms of weight k with respect to Γ), 72
$A_{N,1}$ (set of triples to parametrize a basis of $\mathcal{E}_1(\Gamma_1(N))$), 141
$A_{N,2}$ (set of triples to parametrize a basis of $\mathcal{E}_2(\Gamma_1(N))$), 133
$a_n(E)$ (nth Dirichlet series coefficient of the L-function of E), 366
$a_n(f)$ (nth Fourier coefficient of f), 4
$A_{N,k}$ (set of triples to parametrize a basis of $\mathcal{E}_k(N,\chi)$), 129
$a_p(E)$ (modified solution count of E modulo p), 329
$t_{p^e}(E)$ (modified solution count of E modulo p^e), 330
$a_{p^e}(E)$ (p^eth Dirichlet series coefficient of the L-function of E), 366

b_2, b_4, b_6, b_8 (Weierstrass coefficients), 314
B_k (Bernoulli number), 9
$\mathcal{B}_k(N)$ (basis of $\mathcal{S}_k(\Gamma_1(N))$), 198
$B_{k,\psi}$ (kth Bernoulli number of ψ), 135
$B_k(X)$ (kth Bernoulli polynomial), 134
β_j, β_∞ (matrices contributing to T_p), 170

C (algebraic curve), 261
c_4, c_6 (Weierstrass coefficients), 314
C_{hom} (projective algebraic curve), 262
$\mathbb{C}(j, E_j[N])$ (field generated over $\mathbb{C}(j)$ by N-torsion coordinates of the universal elliptic curve), 287
C_k (constant in many Eisenstein series), 114
$\mathbb{C}(X)$ (field of meromorphic functions on X), 83
$\mathbb{C}(X(\Gamma))$ (field of meromorphic functions on $X(\Gamma)$), 72
χ_ℓ (ℓ-adic cyclotomic character), 386
χ^σ (Galois conjugate of a Dirichlet character), 239
$\bar{\chi}$ (complex conjugate of a Dirichlet character), 116

$\mathcal{D}$ (fundamental domain), 52
$\langle d \rangle$ (diamond Hecke operator, $d \nmid N$), 168
$\text{Div}^0(C)$ (degree-0 divisor group of C), 274
$\text{Div}(C)$ (divisor group of C), 273
$\text{Div}^\ell(C)$ (principal divisors of C), 274
$d\mu(\tau)$ (hyperbolic measure on $\mathcal{H}$), 182
d_N (degree of the projection $X(N) \longrightarrow X(1)$), 101
$D_{\mathfrak{p}}$ (absolute decomposition group), 384
$D_{\mathfrak{p}}$ (decomposition group), 375
$\text{Div}_{\mathbb{Q}}(X(\Gamma))$ (free $\mathbb{Q}$-module on the points of a modular curve), 86
$\text{Div}(X)$ (divisor group of a Riemann surface), 83

F. Diamond, J. Shurman, *A First Course in Modular Forms*,
Graduate Texts in Mathematics 228, DOI 10.1007/978-0-387-27226-9

$H_{\mathbb{Q}}$ ($\mathrm{Gal}(\mathbb{Q}(j, E_j[N])/\mathbb{Q}(j))$), 291
h_s (width of a cusp), 59
h_τ (period of an elliptic point), 49
$\mathcal{H}^*$ (extended upper half plane), 57
h^* (induced reverse map of Picard groups), 275
h^* (pullback of a nonconstant morphism of algebraic curves), 269
h_* (induced forward map of Picard groups), 275
$H_1 \backslash G / H_2$ (double cosets), 103

I (ideal of polynomials), 261
I_f (kernel of eigenvalue homomorphism), 238
$I_{\mathfrak{p}}$ (absolute inertia group), 384
$I_{\mathfrak{p}}$ (inertia group), 375
I_{hom} (homogeneous ideal), 262

j (invariant of a Weierstrass equation), 314
$\mathrm{J}_0(N)$ (Jacobian of $X_0(N)$), 219
$\mathrm{J}_1(N)$ (Jacobian of $X_1(N)$), 230
$j(\gamma, \tau)$ (factor of automorphy), 14
j_N (modular function of level N), 283
$j(\tau)$ (modular function, modular invariant), 7
$\mathrm{Jac}(X)$ (Jacobian of X), 218
$\mathrm{Jac}(X(\Gamma))$ (Jacobian of a modular curve), 231

$\mathbf{k}(C)$ (field of functions of C defined over $\mathbf{k}$), 267
$\mathbb{K}_f$ (number field of a modular form), 238
$\mathbb{K}_\lambda$ (λ-adic numbers), 382
$\mathbf{k}_{\mathrm{prime}}$ (prime subfield of $\mathbf{k}$), 316
$\overline{\mathbf{k}}$ (algebraic closure of $\mathbf{k}$), 254
$\overline{\mathbf{k}}(C)$ (function field of C), 261
$\overline{\mathbf{k}}[C]$ (coordinate ring of C), 261
$\overline{\mathbf{k}}[C]_P$ (local ring of C at P), 263

$\mathbb{L}$ (finite extension field of $\mathbb{Q}_\ell$), 386
$\mathcal{L}^1(\mathbb{R}^l)$ (measurable absolutely integrable functions on $\mathbb{R}^l$), 143
$L(D)$ (linear space of a divisor on a Riemann surface), 84
$L(s, \chi)$ (Dirichlet L-function), 121
$L(s, E)$ (Hasse–Weil L-function of E), 366
$L(s, f)$ (L-function of a modular form), 201
Λ (lattice in $\mathbb{C}$), 25
Λ_f (lattice associated to f), 246
λ_f (eigenvalue homomorphism), 238
Λ_g (lattice in $\mathbb{C}^g$), 84
$\Lambda_N(s)$ (normalized Mellin transform of a cusp form), 209
Λ_τ (lattice spanned by τ and 1), 26

$\mathcal{M}(\Gamma)$ (modular forms of all weights with respect to Γ), 17
$\mathcal{M}_k(\Gamma)$ (modular forms of weight k with respect to Γ), 17
$\mathcal{M}_k(N, \chi)$ (χ-eigenspace of $\mathcal{M}_k(\Gamma_1(N))$), 119
$\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ (modular forms of weight k), 4
M_P (maximal ideal of the local ring), 264
m_P (maximal ideal of the coordinate ring), 263
$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ (modular forms of all weights), 4
μ (Möbius function), 113
$\boldsymbol{\mu}_N$ (Nth roots of unity), 279
μ_n (nth root of unity $e^{2\pi i/n}$), 7

$[N]$ (multiply-by-N isogeny), 27
$\langle n \rangle$ (diamond Hecke operator, n any positive integer), 179
N_E (algebraic conductor of E), 328
ν_p (p-adic valuation), 326
$\nu_{\pi(s)}(f)$ (order of a function on a modular curve at a cusp), 75
$\nu_{\pi(\tau)}(f)$ (order of a function on a modular curve at a noncusp), 74
$\nu_\tau(f)$ (order of vanishing of a function), 71

$\mathcal{O}(f)$ (a function on the order of f), 33
$\mathcal{O}_{\mathbb{K}}$ (number ring of $\mathbb{K}$), 236
$\mathcal{O}_{\mathbb{K},\lambda}$ (λ-adic integers), 382
$\omega(f)$ (meromorphic differential of an automorphic form), 80
$\Omega^1_{\mathrm{hol}}(X(\Gamma))$ (holomorphic differentials of degree 1 on a modular curve), 82
$\Omega^1_{\mathrm{hol}}(X)^\wedge$ (dual space of $\Omega^1_{\mathrm{hol}}(X)$), 217

Index

F. Diamond, J. Shurman, *A First Course in Modular Forms*,
Graduate Texts in Mathematics 228, DOI 10.1007/978-0-387-27226-9

References

[AL70] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Mathematische Annalen*, 185:134–160, 1970.

[BBB00] Lennert Berggren, Jonathan Borwein, and Peter Borwein. *Pi: A Source Book*. Springer-Verlag, second edition, 2000.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of ellipic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[BDSBT01] K. Buzzard, M. Dickinson, N. Shepherd-Barron, and R. Taylor. On icosahedral Artin representations. *Duke Math. J.*, 109(2):283–318, 2001.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, 1990.

[Bum97] Daniel Bump. *Automorphic Forms and Representations*. Studies in Advanced Mathematics **55**. Cambridge University Press, 1997.

[Car86] H. Carayol. Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. E. N. S.*, 19:409–468, 1986.

[Car99] D. Carlton. On a result of Atkin and Lehner. http://math.stanford.edu/∼carlton/math/, 1999.

[Car01] D. Carlton. Moduli for pairs of elliptic curves with isomorphic N-torsion. *Manuscripta Mathematica*, 105(2):201–234, 2001.

[Cox84] D. Cox. The arithmetic-geometric mean of Gauss. *L'Enseignement Mathématique*, 30:275–330, 1984.

[Cox97] David Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Wiley, second edition, 1997.

[Cre97] J. E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, second edition, 1997.

[CS86] Gary Cornell and Joseph H. Silverman, editors. *Arithmetic Geometry*. Springer-Verlag, 1986.

[CS05] D. Cox and J. Shurman. Geometry and number theory on clovers. *Amer. Math. Monthly*, 112, October 2005.

[CSS97] Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors. *Modular Forms and Fermat's Last Theorem*. Springer-Verlag, 1997.

[DDT94] H. Darmon, F. Diamond, and R. Taylor. Fermat's last theorem. *Current developments in mathematics, 1995*, pages 1–154, 1994.

F. Diamond, J. Shurman, *A First Course in Modular Forms*,
Graduate Texts in Mathematics 228, DOI 10.1007/978-0-387-27226-9

[Del71] P. Deligne. Forms modulaires et représentations ℓ-adiques. In *Lecture Notes in Math.*, volume 179, pages 139–172. Springer-Verlag, 1971.

[Die04] L. Dieulefait. Existence of families of Galois representations and new cases of the Fontaine–Mazur conjecture. *J. Reine Angew. Math.*, 577:147–151, 2004.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular Functions of One Variable, II*, volume 349 of *Lecture Notes in Math.*, pages 143–316. Springer-Verlag, 1973.

[DS74] P. Deligne and J.-P. Serre. Forms modulaires de poids 1. *Ann. Sci. Ec. Norm. Sup.*, 7:507–530, 1974.

[FH91] William Fulton and Joe Harris. *Representation Theory: A First Course.* Graduate Texts in Mathematics **129**. Springer-Verlag, 1991.

[FK80] Hershel M. Farkas and Irwin Kra. *Riemann Surfaces.* Graduate Texts in Mathematics **71**. Springer-Verlag, 1980.

[FM93] J.-M. Fontaine and B. Mazur. Geometric Galois representations. *Elliptic Curves, Modular Forms and Fermat's Last Theorem*, 17:41–78, 1993.

[Ful69] William Fulton. *Algebraic Curves.* Benjamin, 1969.

[God66] R. Godement. The decomposition of $L^2(G/\Gamma)$ for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. *Proc. Symp. Pure Math IX*, pages 211–224, 1966.

[Gun62] R. P. Gunning. *Lectures on Modular Forms.* Annals of Mathematics studies. Princeton University Press, 1962.

[Hec26] E. Hecke. Zur Theorie der elliptischen Modulfunktionen. *Math. Annalen*, 97:210–242, 1926.

[Hec27] E. Hecke. Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie un Arithmetik. *Abh. Math. Sem. Hamburg*, 5:199–224, 1927.

[Hid86] H. Hida. Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms. *Inv. Math.*, 85:545–613, 1986.

[Hid93] Haruzo Hida. *Elementary theory of L-functions and Eisenstein series.* London Math. Soc. Student Texts **26**. Cambridge University Press, second edition, 1993.

[Hus04] Dale Husemöller. *Elliptic Curves.* Graduate Texts in Mathematics **111**. Springer-Verlag, second edition, 2004.

[Igu59] J. Igusa. Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.*, 81:561–577, 1959.

[IR92] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory.* Graduate Texts in Mathematics **84**. Springer-Verlag, second edition, 1992.

[JS87] Gareth A. Jones and David Singerman. *Complex Functions, an Algebraic and Geometric Viewpoint.* Cambridge University Press, 1987.

[Kha06] C. Khare. Serre's modularity conjecture: the level one case. *Duke Math. J.*, 134(3):557–589, 2006.

[Kis09a] M. Kisin. The Fontaine–Mazur conjecture for GL_2. *J. Amer. Math. Soc.*, 22(3):641–690, 2009.

[Kis09b] M. Kisin. Modularity of 2-adic Barsotti-Tate representations. *Invent. Math.*, 178(3):587–634, 2009.

[Kis09c] M. Kisin. Moduli of finite flat group schemes, and modularity. *Ann. of Math. (2)*, 170(3):1085–1180, 2009.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves.* Annals of Math. Studies **108**. Princeton University Press, 1985.

[Kna93] Anthony W. Knapp. *Elliptic Curves*. Princeton Math. Notes **40**. Princeton University Press, 1993.

[Kob93] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Mathematics **97**. Springer-Verlag, second edition, 1993.

[KW09a] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[KW09b] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[Lan73] Serge Lang. *Elliptic Functions*. Advanced book program. Addison-Wesley, 1973.

[Lan76] Serge Lang. *Introduction to Modular Forms*. Grundl. Math. Wiss. **222**. Springer-Verlag, 1976.

[Lan80] R. P. Langlands. *Base change for* GL(2), volume 96 of *Annals of Math. Studies*. Princeton Univ. Press, 1980.

[Mar] G. Martin. Dimensions of spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$. http://arXiv.org/abs/math/0306128.

[Mar89] Daniel Marcus. *Algebraic Number Theory*. Springer-Verlag, 1989.

[Maz91] B. Mazur. Number theory as gadfly. *Amer. Math. Monthly*, 7:593–610, 1991.

[Mil] J. S. Milne. Modular functions and modular forms. http://www.jmilne.org/math.

[Miy89] Toshitsune Miyake. *Modular Forms*. Springer-Verlag, 1989.

[Mun00] James R. Munkres. *Topology*. Prentice-Hall, second edition, 2000.

[Mur95] V. Kumar Murty, editor. *Seminar on Fermat's Last Theorem*, volume 17 of *CMF Conf. Proc.* Amer. Math.Soc., 1995.

[Ogg69] Andrew Ogg. *Modular Forms and Dirichlet Series*. Benjamin, 1969.

[Ram02] R. Ramakrishna. Deforming Galois representations and the conjectures of Serre and Fontaine–Mazur. *Ann. of Math. (2)*, 156(1):115–154, 2002.

[Ran39] R. Rankin. Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions, i and ii. *Proc. Cambridge Phil. Soc.*, 35:351–356, 1939.

[Rib90] K. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.*, 100:431–476, 1990.

[Ros81] M. Rosen. Abel's theorem on the lemniscate. *Amer. Math. Monthly*, 88:387–395, 1981.

[Rud74] Walter Rudin. *Real and Complex Analysis*. McGraw-Hill, second edition, 1974.

[Sam72] Pierre Samuel. *Algebraic Theory of Numbers*. Kershaw, 1972.

[Sch74] Bruno Schoeneberg. *Elliptic Modular Functions*. Springer-Verlag, 1974.

[Sel40] A. Selberg. Bemerkungen über eine Dirichletsche Reihe, die mit der Theorie der Modulformen nahe verbunden ist. *Arch. Math. Naturvid.*, 43:47–50, 1940.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics **7**. Springer-Verlag, 1973.

[Ser87] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54:179–230, 1987.

[Shi71] G. Shimura. On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. *Nagoya Math. J.*, 43:199–208, 1971.

[Shi73] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Iwanami Shoten and Princeton University Press, 1973.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics **106**. Springer-Verlag, 1986.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics **151**. Springer-Verlag, 1994.

[ST92] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics **7**. Springer-Verlag, 1992.

[Swi74] H. P. F. Swinnerton-Dyer. *Analytic Theory of Abelian Varieties*. Cambridge, 1974.

[Tat02] J. Tate. The millennium prize problems. A lecture by John Tate. Springer VideoMATH, 2002.

[Tay03] R. Taylor. On icosahedral Artin representations, II. *Amer. J. Math.*, 125(3):549–566, 2003.

[Tun81] J. Tunnell. Artin's conjecture for representations of the octahedral type. *Bull. Amer. Math. Soc.*, 5:173–175, 1981.

[TW95] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.*, 141(3):553–572, 1995.

[Ver] H. A. Verrill. Fundamental domains. http://www.math.lsu.edu/∼verrill/.

[Was03] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and Its Applications. Chapman and Hall/CRC, 2003.

[Wei67] A. Weil. Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Annalen*, 168:149–156, 1967.

[Wil95] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.*, 141(3):443–551, 1995.

(continued from page ii)

64 EDWARDS. Fourier Series. Vol. I. 2nd ed.
65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
66 WATERHOUSE. Introduction to Affine Group Schemes.
67 SERRE. Local Fields.
68 WEIDMANN. Linear Operators in Hilbert Spaces.
69 LANG. Cyclotomic Fields II.
70 MASSEY. Singular Homology Theory.
71 FARKAS/KRA. Riemann Surfaces. 2nd ed.
72 STILLWELL. Classical Topology and Combinatorial Group Theory. 2nd ed.
73 HUNGERFORD. Algebra.
74 DAVENPORT. Multiplicative Number Theory. 3rd ed.
75 HOCHSCHILD. Basic Theory of Algebraic Groups and Lie Algebras.
76 IITAKA. Algebraic Geometry.
77 HECKE. Lectures on the Theory of Algebraic Numbers.
78 BURRIS/SANKAPPANAVAR. A Course in Universal Algebra.
79 WALTERS. An Introduction to Ergodic Theory.
80 ROBINSON. A Course in the Theory of Groups. 2nd ed.
81 FORSTER. Lectures on Riemann Surfaces.
82 BOTT/TU. Differential Forms in Algebraic Topology.
83 WASHINGTON. Introduction to Cyclotomic Fields. 2nd ed.
84 IRELAND/ROSEN. A Classical Introduction to Modern Number Theory. 2nd ed.
85 EDWARDS. Fourier Series. Vol. II. 2nd ed.
86 VAN LINT. Introduction to Coding Theory. 2nd ed.
87 BROWN. Cohomology of Groups.
88 PIERCE. Associative Algebras.
89 LANG. Introduction to Algebraic and Abelian Functions. 2nd ed.
90 BRØNDSTED. An Introduction to Convex Polytopes.
91 BEARDON. On the Geometry of Discrete Groups.
92 DIESTEL. Sequences and Series in Banach Spaces.
93 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part I. 2nd ed.
94 WARNER. Foundations of Differentiable Manifolds and Lie Groups.
95 SHIRYAEV. Probability. 2nd ed.
96 CONWAY. A Course in Functional Analysis. 2nd ed.
97 KOBLITZ. Introduction to Elliptic Curves and Modular Forms. 2nd ed.
98 BRÖCKER/TOM DIECK. Representations of Compact Lie Groups.
99 GROVE/BENSON. Finite Reflection Groups. 2nd ed.
100 BERG/CHRISTENSEN/RESSEL. Harmonic Analysis on Semigroups: Theory of Positive Definite and Related Functions.
101 EDWARDS. Galois Theory.
102 VARADARAJAN. Lie Groups, Lie Algebras and Their Representations.
103 LANG. Complex Analysis. 3rd ed.
104 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part II.
105 LANG. $SL_2(\mathbf{R})$.
106 SILVERMAN. The Arithmetic of Elliptic Curves.
107 OLVER. Applications of Lie Groups to Differential Equations. 2nd ed.
108 RANGE. Holomorphic Functions and Integral Representations in Several Complex Variables.
109 LEHTO. Univalent Functions and Teichmüller Spaces.
110 LANG. Algebraic Number Theory.
111 HUSEMÖLLER. Elliptic Curves. 2nd ed.
112 LANG. Elliptic Functions.
113 KARATZAS/SHREVE. Brownian Motion and Stochastic Calculus. 2nd ed.
114 KOBLITZ. A Course in Number Theory and Cryptography. 2nd ed.
115 BERGER/GOSTIAUX. Differential Geometry: Manifolds, Curves, and Surfaces.
116 KELLEY/SRINIVASAN. Measure and Integral. Vol. I.
117 J.-P. SERRE. Algebraic Groups and Class Fields.
118 PEDERSEN. Analysis Now.
119 ROTMAN. An Introduction to Algebraic Topology.
120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.
121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
122 REMMERT. Theory of Complex Functions. *Readings in Mathematics*
123 EBBINGHAUS/HERMES et al. Numbers. *Readings in Mathematics*

124 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part III
125 BERENSTEIN/GAY. Complex Variables: An Introduction.
126 BOREL. Linear Algebraic Groups. 2nd ed.
127 MASSEY. A Basic Course in Algebraic Topology.
128 RAUCH. Partial Differential Equations.
129 FULTON/HARRIS. Representation Theory: A First Course.
Readings in Mathematics
130 DODSON/POSTON. Tensor Geometry.
131 LAM. A First Course in Noncommutative Rings. 2nd ed.
132 BEARDON. Iteration of Rational Functions.
133 HARRIS. Algebraic Geometry: A First Course.
134 ROMAN. Coding and Information Theory.
135 ROMAN. Advanced Linear Algebra.
136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
137 AXLER/BOURDON/RAMEY. Harmonic Function Theory. 2nd ed.
138 COHEN. A Course in Computational Algebraic Number Theory.
139 BREDON. Topology and Geometry.
140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
142 LANG. Real and Functional Analysis. 3rd ed.
143 DOOB. Measure Theory.
144 DENNIS/FARB. Noncommutative Algebra.
145 VICK. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
146 BRIDGES. Computability: A Mathematical Sketchbook.
147 ROSENBERG. Algebraic *K*-Theory and Its Applications.
148 ROTMAN. An Introduction to the Theory of Groups. 4th ed.
149 RATCLIFFE. Foundations of Hyperbolic Manifolds.
150 EISENBUD. Commutative Algebra with a View Toward Algebraic Geometry.
151 SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves.
152 ZIEGLER. Lectures on Polytopes.
153 FULTON. Algebraic Topology: A First Course.
154 BROWN/PEARCY. An Introduction to Analysis.
155 KASSEL. Quantum Groups.
156 KECHRIS. Classical Descriptive Set Theory.
157 MALLIAVIN. Integration and Probability.
158 ROMAN. Field Theory.
159 CONWAY. Functions of One Complex Variable II.
160 LANG. Differential and Riemannian Manifolds.
161 BORWEIN/ERDÉLYI. Polynomials and Polynomial Inequalities.
162 ALPERIN/BELL. Groups and Representations.
163 DIXON/MORTIMER. Permutation Groups.
164 NATHANSON. Additive Number Theory: The Classical Bases.
165 NATHANSON. Additive Number Theory: Inverse Problems and the Geometry of Sumsets.
166 SHARPE. Differential Geometry: Cartan's Generalization of Klein's Erlangen Program.
167 MORANDI. Field and Galois Theory.
168 EWALD. Combinatorial Convexity and Algebraic Geometry.
169 BHATIA. Matrix Analysis.
170 BREDON. Sheaf Theory. 2nd ed.
171 PETERSEN. Riemannian Geometry.
172 REMMERT. Classical Topics in Complex Function Theory.
173 DIESTEL. Graph Theory. 2nd ed.
174 BRIDGES. Foundations of Real and Abstract Analysis.
175 LICKORISH. An Introduction to Knot Theory.
176 LEE. Riemannian Manifolds.
177 NEWMAN. Analytic Number Theory.
178 CLARKE/LEDYAEV/STERN/WOLENSKI. Nonsmooth Analysis and Control Theory.
179 DOUGLAS. Banach Algebra Techniques in Operator Theory. 2nd ed.
180 SRIVASTAVA. A Course on Borel Sets.
181 KRESS. Numerical Analysis.
182 WALTER. Ordinary Differential Equations.

183 MEGGINSON. An Introduction to Banach Space Theory.
184 BOLLOBAS. Modern Graph Theory.
185 COX/LITTLE/O'SHEA. Using Algebraic Geometry. 2nd ed.
186 RAMAKRISHNAN/VALENZA. Fourier Analysis on Number Fields.
187 HARRIS/MORRISON. Moduli of Curves.
188 GOLDBLATT. Lectures on the Hyperreals: An Introduction to Nonstandard Analysis.
189 LAM. Lectures on Modules and Rings.
190 ESMONDE/MURTY. Problems in Algebraic Number Theory. 2nd ed.
191 LANG. Fundamentals of Differential Geometry.
192 HIRSCH/LACOMBE. Elements of Functional Analysis.
193 COHEN. Advanced Topics in Computational Number Theory.
194 ENGEL/NAGEL. One-Parameter Semigroups for Linear Evolution Equations.
195 NATHANSON. Elementary Methods in Number Theory.
196 OSBORNE. Basic Homological Algebra.
197 EISENBUD/HARRIS. The Geometry of Schemes.
198 ROBERT. A Course in *p*-adic Analysis.
199 HEDENMALM/KORENBLUM/ZHU. Theory of Bergman Spaces.
200 BAO/CHERN/SHEN. An Introduction to Riemann–Finsler Geometry.
201 HINDRY/SILVERMAN. Diophantine Geometry: An Introduction.
202 LEE. Introduction to Topological Manifolds.
203 SAGAN. The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions.
204 ESCOFIER. Galois Theory.
205 FÉLIX/HALPERIN/THOMAS. Rational Homotopy Theory. 2nd ed.
206 MURTY. Problems in Analytic Number Theory.
Readings in Mathematics
207 GODSIL/ROYLE. Algebraic Graph Theory.
208 CHENEY. Analysis for Applied Mathematics.
209 ARVESON. A Short Course on Spectral Theory.
210 ROSEN. Number Theory in Function Fields.
211 LANG. Algebra. Revised 3rd ed.
212 MATOUŠEK. Lectures on Discrete Geometry.
213 FRITZSCHE/GRAUERT. From Holomorphic Functions to Complex Manifolds.
214 JOST. Partial Differential Equations.
215 GOLDSCHMIDT. Algebraic Functions and Projective Curves.
216 D. SERRE. Matrices: Theory and Applications.
217 MARKER. Model Theory: An Introduction.
218 LEE. Introduction to Smooth Manifolds.
219 MACLACHLAN/REID. The Arithmetic of Hyperbolic 3-Manifolds.
220 NESTRUEV. Smooth Manifolds and Observables.
221 GRÜNBAUM. Convex Polytopes. 2nd ed.
222 HALL. Lie Groups, Lie Algebras, and Representations: An Elementary Introduction.
223 VRETBLAD. Fourier Analysis and Its Applications.
224 WALSCHAP. Metric Structures in Differential Geometry.
225 BUMP: Lie Groups
226 ZHU. Spaces of Holomorphic Functions in the Unit Ball.
227 MILLER/STURMFELS. Combinatorial Commutative Algebra.
228 DIAMOND/SHURMAN. A First Course in Modular Forms.
229 EISENBUD. The Geometry of Syzygies.
230 STROOCK. An Introduction to Markov Processes.