CHANGES FOR A REVISED EDITION OF "ELLIPTIC CURVES, MODULAR FORMS, AND THEIR L-FUNCTIONS"

Dear Readers,

Here is a list of known typos, errors and omissions, with the text as it appeared in the first edition, followed by the corrected text (as it will/should appear in a revised edition). Some typos have been found since the revised edition came out, so those are here listed too (but the page numbers refer to the first printing).

(1) **Page xiv.** Added my gratitude to Fernando Gouvêa who went out of his way to read and give me great suggestions on the entire book. Also added thanks to Enis Kaya who found a bunch of the typos listed in this document.

- (**Old text**) Last, but not least, I would like to express my gratitude to Keith Conrad, David Pollack and William Stein, whose abundant comments and suggestions have improved this manuscript much more than it would be safe to admit.
- (**New text**) Last, but not least, I would like to express my gratitude to Keith Conrad, Fernando Gouvêa, Enis Kaya, David Pollack and William Stein, whose abundant comments and suggestions have improved this manuscript much more than it would be safe to admit.

(2) **Page 4.** The text claimed that Fermat showed that 1 is not a congruent number *in order to* prove Fermat's last theorem for $n = 4$. In fact, it seems Fermat proved that 1 is not a congruent number for its own sake.

- (**Old text**) The proof of such a claim had to wait until Pierre de Fermat (1601-1665) settled that the number 1 (and every square number) is not a congruent number (a result that he showed in order to prove the case $n = 4$ of Fermat's last theorem).
- (**New text**) The proof of such a claim had to wait until Pierre de Fermat (1601-1665) settled that the number 1, and every square, are not congruent numbers (interestingly, his proof can be applied to prove the case $n = 4$ of Fermat's last theorem; see Example 1.1.5).

(3) **Page 5.** In the statement of Theorem 1.15 the word *cardinality* gives the impression that the sets may be infinite, when of course they are finite. So we replaced the word cardinalities by numbers:

- (**Old text**) If n is an odd square-free positive integer and n is the area of a right triangle with rational sides, then the following cardinalities are equal:

- (**New text**) If n is an odd square-free positive integer and n is the area of a right triangle with rational sides, then the following numbers are equal:

(4) **Page 6.** We changed the word *marvellous* for its more common spelling, *marvelous.*

- (**Old text**) ... he had found a marvellous proof, but the margin was too small to contain it.

- (**New text**) ... he had found a marvelous proof, but the margin was too small to contain it.

(5) **Page 14.** This error in the revised edition was found by John Gilling and I would like to thank him for pointing this out to me:

- (**Old text**) For any $n > 0$, the symbol $\left(\frac{-n}{\cdot}\right)$ induces a Dirichlet character χ_n defined by $\chi_n(a) = \left(\frac{-n}{a}\right)$, and we can define...

- (**Corrected text**) For any square-free $n > 0$, the Kronecker symbol induces a Dirichlet character χ_n defined by $\chi_n(a) = \left(\frac{-n}{a}\right)$ if $-n \equiv 1 \bmod 4$, and by $\chi_n(a) = \left(\frac{-4n}{a}\right)$ if $-n \equiv 2$ or $3 \bmod 4$, and we can define...

The reason is that x_n needs to be a *primitive* Dirichlet character.

(6) **Page 16.** In Hint (a) of Exercise 1.4.8, the expression $\frac{1}{1+x} = \sum_{k=0}^{\infty} x^k$ should read $\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k$ instead.

(7) **Page 18.** In addition to Yuri Matiyasevich, Hilary Putnam and Julia Robinson, another mathematician, **Martin Davis**, should have been mentioned as one of the contributors to the solution of Hilbert's 10th problem.

- (**Old text**) Surprisingly, in 1970, Matiyasevich, Putnam and Robinson discovered that there is no such general algorithm that decides whether equation ...

- (**New text**) Surprisingly, in 1970, Davis, Matiyasevich, Putnam, and Robinson discovered that there is no such general algorithm that decides whether equation ...

(8) **Page 20.** We added the following picture of surfaces of genus 0, 1, 2, and 3, to illustrate the last paragraph of Section 2.1, located at the end of Section 2.1, and before Section 2.2 (the images were made by users Oleg Alexandrov and "Geek3" for the Wikipedia page on genus of a surface):

(9) **Page 22.** We have added detail to Example 2.2.3. As it was written, the change of variables ψ was unnecessarily mysterious:

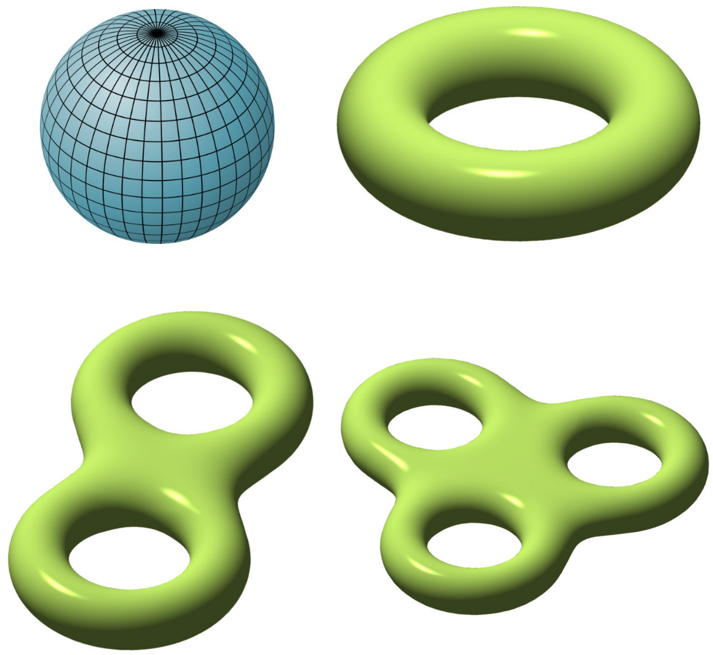

FIGURE 1. A surface of genus 0 (a sphere), and surfaces of genus 1, 2, and 3 (with 1, 2, and 3 holes, respectively).

- (**Old text**) **Example 2.2.3.** Let $d \in \mathbb{Z}$, $d \neq 0$ and let E be the elliptic curve given by the cubic equation
$$X^3 + Y^3 = dZ^3$$
with $\mathcal{O} = [1, -1, 0]$. The reader should verify that E is a smooth curve. We wish to find a Weierstrass equation for E and, indeed, one can find a change of variables $\psi : E \to \hat{E}$ given by
$$\psi([X, Y, Z]) = [12dZ,\ 36d(X - Y),\ X + Y] = [x, y, z]$$
such that $zy^2 = x^3 - 432d^2z^3$. The map ψ is invertible; the inverse map $\psi^{-1} : \hat{E} \to E$ is
$$\psi^{-1}([x, y, z]) = \left[\frac{36dz + y}{72d}, \frac{36dz - y}{72d}, \frac{x}{12d}\right].$$
In affine coordinates, the change of variables is going from $X^3 + Y^3 = d$ to the curve $y^2 = x^3 - 432d^2$:
$$\begin{aligned} \psi(X, Y) &= \left(\frac{12d}{X + Y}, \frac{36d(X - Y)}{X + Y}\right), \\ \psi^{-1}(x, y) &= \left(\frac{36d + y}{6x}, \frac{36d - y}{6x}\right). \end{aligned}$$
$\square$

- (**New text**) **Example 2.2.3.** Let $d \in \mathbb{Z}$, $d \neq 0$ and let E be the elliptic curve given by the cubic equation

$$X^3 + Y^3 = dZ^3$$

with $\mathcal{O} = [1, -1, 0]$. The reader should verify that E is a smooth curve. We wish to find a Weierstrass equation for E. Note that if we change $X = U + V$, $Y = -V$, $Z = W$, then we obtain a new equation

$$U^3 + 3U^2V + 3UV^2 = dW^3. \tag{1}$$

Since this equation is quadratic in V, and cubic in W, with no other cubic monomials that involve W, the variable W will end up playing the role of x, and the variable V will play the role of y in our Weierstrass model. Next, we change variables to obtain a coefficient of 1 in front of V^2 and W^3. If we multiply Eq. (1) through by d^2, we obtain

$$d^2U^3 + 3d^2U^2V + 3d^2UV^2 = d^3W^3, \tag{2}$$

and now we change variables $x = 3dW$, $y = 9dV$, and $z = U$. Then, Eq. (2) becomes

$$d^2z + \frac{dyz}{3} + \frac{y^2z}{27} = \frac{x^3}{27}, \tag{3}$$

or, equivalently, $y^2z + 9dyz = x^3 - 27d^2z$, which is a Weierstrass equation. Thus, $[x, y, z] = [3dW, 9dV, U] = [3dZ, -9dY, X + Y]$ and we have found a change of variables $\psi : E \to \widehat{E}$ given by

$$\psi([X, Y, Z]) = [3dZ, -9dY, X + Y]$$

such that the image lands on the curve in Weierstrass equation $\widehat{E} : y^2z + 9dyz = x^3 - 27d^2z$. The map ψ is invertible; the inverse map $\psi^{-1} : \widehat{E} \to E$ is

$$\psi^{-1}([x, y, z]) = \left[\frac{9dz + y}{9d}, -\frac{y}{9d}, \frac{x}{3d}\right].$$

In affine coordinates, the change of variables is going from $X^3 + Y^3 = d$ to the curve $y^2 + 9dy = x^3 - 27d^2$ via the maps:

$$\begin{aligned} \psi(X, Y) &= \left(\frac{3d}{X + Y}, -\frac{9dY}{X + Y}\right), \\ \psi^{-1}(x, y) &= \left(\frac{9d + y}{3x}, -\frac{y}{3x}\right). \end{aligned}$$

We leave it as an exercise for the reader to verify that the model can be further simplified to the form $y^2 = x^3 - 432d^2$. $\square$

(10) **Page 28.** Although Poincaré's name was Jules Henri, we know him as Henri Poincaré.

- (**Old text**) The next step in the study of the structure of $E(\mathbb{Q})$ was conjectured by Jules Poincaré in 1908...

- (**New text**) The next step in the study of the structure of $E(\mathbb{Q})$ was conjectured by Henri Poincaré in 1908 ...

(11) **Page 37.** The Definition 2.6.5 needs a picture to go with it. We include this new figure (which in the text should be Figure 6 in Chapter 2!). See Figure 6 below.

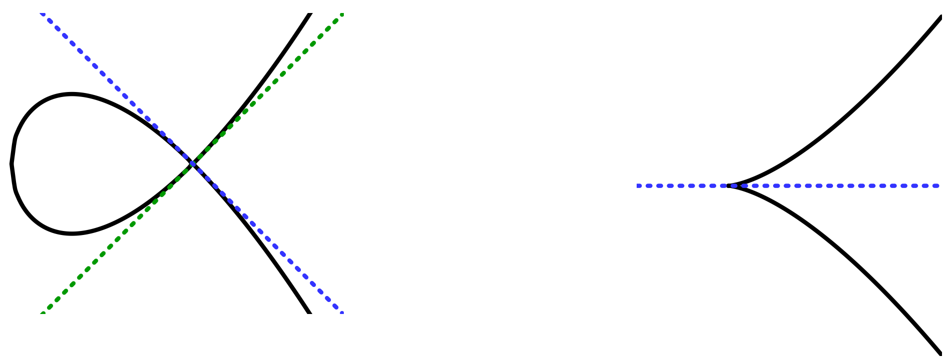

FIGURE 6. A node (left) with two tangent lines, and a cusp (right) with only one tangent line.

(12) **Page 47.** In Example 2.7.5. I claimed that the reduction at $p = 2$ is multiplicative, but in reality the reduction is additive. The bound on the rank then says that $R_{E_1} \leq 1$ which is insufficient to prove that there are only finitely many points. One has to resort to a 2-descent to conclude that the rank is 0. My thanks to Ron Burns for pointing this out to me.

(13) **Page 63.** In case (11) of Example 2.10.4, a $(-2, 2)$ should be $(2, 1)$.
- (**Old text**) The other pairs correspond to $(-2, 2) \cdot \gamma$, with $\gamma = (-1, 34)$, $(-34, 2)$ or $(34, 17)$.
- (**New text**) The other pairs correspond to $(2, 1) \cdot \gamma$, with $\gamma = (-1, 34)$, $(-34, 2)$ or $(34, 17)$.

(14) **Page 72.** In the statement of Exercise 2.12.4, the projective equation for E should be $E : zy^2 = x^3 - 4xz^2$ (instead of $zy^2 = x^3 + z^3$). I'd like to thank Ben Clare for pointing this out.

- (**Old text**) Next, we work in projective coordinates. Let $C : W^2V^2 = U^4 + W^4$ and $E : zy^2 = x^3 + z^3$.
- (**New text**) Next, we work in projective coordinates. Let $C : W^2V^2 = U^4 + W^4$ and $E : zy^2 = x^3 - 4xz^2$.

(15) **Page 73.** In the statement of Exercise 2.12.18, the condition on e_1, e_2, e_3 should be $e_1 - e_2 = n^2$ and $e_1 - e_3 = m^2$ (instead of $e_2 - e_3 = m^2$).

- (**Old text**) Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in \mathbb{Q}$, distinct, and such that $e_1 + e_2 + e_3 = 0$. Additionally, suppose that $e_1 - e_2 = n^2$ and $e_2 - e_3 = m^2$ are squares.

- (**New text**) Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in \mathbb{Q}$, distinct, and such that $e_1 + e_2 + e_3 = 0$. Additionally, suppose that $e_1 - e_2 = n^2$ and $e_1 - e_3 = m^2$ are squares.

(16) **Page 78.** In Example 3.1.3, an occurrence of $\mathbb{Z}(\sqrt{2})$ should be $\mathbb{Z}[\sqrt{2}]$ instead.

(17) **Page 82.** In Definition 3.2.1, it is more appropriate to write $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ rather than $f(z) : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$.

(18) **Page 85.** In Example 3.3.3, the displayed equation $Mz = M(1+i) = \ldots$ should read instead $M'z = M'(1+i) = \ldots$. Similarly, the equation $z'' = Mz$ should be $z'' = M''z$.

(19) **Page 86.** The fundamental region that appears in **Figure 3** on p. 86 is not the correct region, and needs to be replaced by the Figure 3 that appears here.

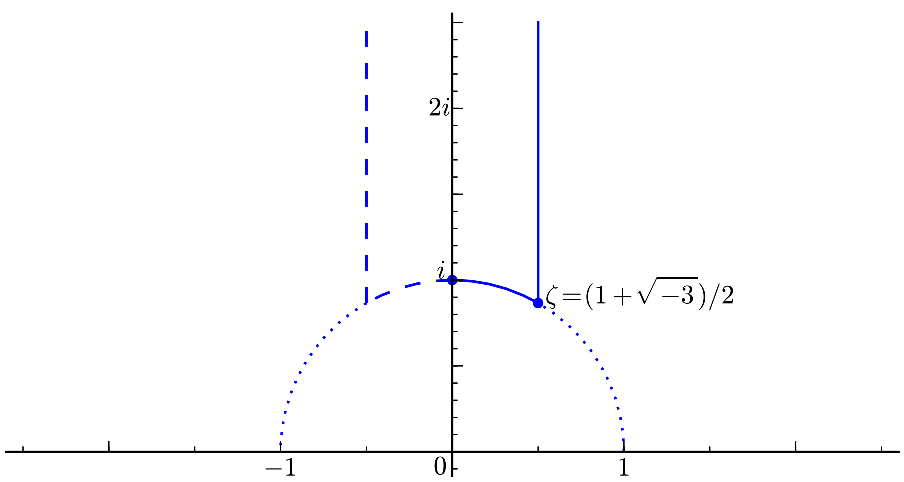

Figure 3. The fundamental domain $\mathcal{F}(1)$ for the quotient $\mathbb{H}/\Gamma(1)$.

(20) **Page 86.** In Definition 3.3.4, the elements of $\mathcal{F}(1)$ should be picked from $\mathbb{H}$ instead of all of $\mathbb{C}$, otherwise it would contain elements in the lower half plane.

(21) **Page 91.** In Example 3.6.1, the number p should be prime.

(22) **Page 95.** Exercise 3.7.4 refers to part (a) of Theorem 3.2.4. We have changed that to "the first part of Theorem 3.2.4".

(23) **Page 101.** The expression "analytic everywhere" should be changed by "holomorphic everywhere".

- (**Old text**) f is a *modular form of weight* k for $\mathrm{SL}(2,\mathbb{Z})$ if f is a modular function of weight k and it is *analytic everywhere on* $\mathbb{H}$ *and at the cusp* ∞ of $X(1)$.

- (**New text**) f is a *modular form of weight* k for $\mathrm{SL}(2,\mathbb{Z})$ if f is a modular function of weight k and it is *holomorphic everywhere on* $\mathbb{H}$ *and at the cusp* ∞ of $X(1)$.

(24) **Page 101.** In Proposition 4.1.5, "a function of $\tau \in \mathbb{H}$" should be "a function of $z \in \mathbb{H}$" instead.

(25) **Page 104.** In Example 4.1.13, "both $f_1(z)$ and $f_2(Z)$" should be "both $f_1(z)$ and $f_2(z)$".

(26) **Page 107.** The text states that "$X(\Gamma)$ only has a finite number of cusps" without proof. We have reworded this:

> Notice also that $X(\Gamma)$ only has a finite number of cusps (the number of cusps is at most the number of cosets of the form $\Gamma \cdot \alpha$ in $\mathrm{SL}(2,\mathbb{Z})$, which is finite since the index $[\mathrm{SL}(2,\mathbb{Z}) : \Gamma]$ is finite), say...

(27) **Page 108.** The definition 4.2.6 of *old form* and $M_k^{\mathrm{old}}(\Gamma(N))$ is not complete. In Remark 4.2.5 (see also Exercise 4.5.9), we learned of two ways that one form can be "old", but only one way is listed in Definition 4.2.6. The definition should be, instead, this one:

Definition 4.2.6. *Let N, $k \geq 1$ be integers. A modular form $f(z)$ of weight k for $\Gamma(N)$ is said to be an* **old form** *if one of the following holds:*
(a) *there is a divisor $M \geq 1$ of N such that $f(z)$ is a modular form in the space $M_k(\Gamma(M))$, or*
(b) *there is a divisor $d \geq 1$ of N and a modular form $g(z) \in M_k(\Gamma(N/d))$ such that $f(z) = g(dz)$, or*
(c) *$f(z)$ is a $\mathbb{C}$-linear combination of modular forms as in* (a) *or* (b).
The $\mathbb{C}$-linear subspace of all old forms of $M_k(\Gamma(N))$ is denoted by $M_k^{old}(\Gamma(N))$. We also define

$$S_k^{old}(\Gamma(N)) := M_k^{old}(\Gamma(N)) \cap S_k(\Gamma(N)).$$

For instance, if $N = pq$, where p, q are distinct primes, then $M_k^{\mathrm{old}}(\Gamma(N))$ is the $\mathbb{C}$-linear space of all modular forms

$$f(z) + g(pz) + h(qz) + k(pqz)$$

where $f \in M_k(\Gamma(1)) + M_k(\Gamma(p)) + M_k(\Gamma(q))$, $g \in M_k(\Gamma(q))$, $h \in M_k(\Gamma(p))$ and $k \in M_k(\Gamma(1))$.

(28) **Page 109.** The text of Remark 4.2.9 is incorrect. It should say that the spaces of modular forms $M_k(\Gamma_1(N))$ and $M_k(\Gamma_0(N))$ have a basis formed by Eisenstein series **and** cusp forms, and not just Eisenstein series.

- (**Old text**)

  Remark 4.2.9. *The Eisenstein series are very useful because most of the spaces we are discussing in this book have a basis formed by Eisenstein series, and we* *can calculate their q-expansions. For precise statements see* [?], *Chapter 7, or* [?], *Chapter 5 (in particular, see Section 5.3).*

Remark 4.2.10. *Let $k \geq 1$ and let Γ be a congruence subgroup. Then $M_k(\Gamma)$ is a finite-dimensional $\mathbb{C}$-vector space. The formulas for the dimension of the spaces of modular forms $M_k(\Gamma)$ and $S_k(\Gamma)$ can be found by calculating the genus and the number of cusps of the modular curve $X(\Gamma)$. Since we will not use these formulas here, we simply refer the reader to* [?], *Theorem 3.5.1 and Figure 3.3 (page 108).*

Example 4.2.11. Let $N = 11$ and let the weight be 2. The space $M_2(\Gamma_0(11))$ is a 2-dimensional $\mathbb{C}$-vector space with basis elements $\{f, g\}$ given by the q-expansions

$$\begin{aligned} f(q) &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + O(q^{11}) \\ g(q) &= 1 + \frac{12}{5}q + \frac{36}{5}q^2 + \frac{48}{5}q^3 + \frac{84}{5}q^4 + \frac{72}{5}q^5 + \frac{144}{5}q^6 + O(q^7), \end{aligned}$$

where $q = e^{2\pi i z}$. Thus, we deduce that $S_2(\Gamma_0(11))$ is 1-dimensional, generated by $f(q)$.

Example 4.2.12. Let $N = 37$ and let the weight be 2. The space $M_2(\Gamma_0(37))$ is a 3-dimensional $\mathbb{C}$-vector space with basis elements $\{f, g, h\}$ given by the q-expansions:

$$\begin{aligned} f(q) &= q + q^3 - 2q^4 - q^7 - 2q^9 + 3q^{11} - 2q^{12} - 4q^{13} + O(q^{16}) \\ g(q) &= q^2 + 2q^3 - 2q^4 + q^5 - 3q^6 - 4q^9 - 2q^{10} + 4q^{11} + O(q^{12}) \\ h(q) &= 1 + \frac{2}{3}q + 2q^2 + \frac{8}{3}q^3 + \frac{14}{3}q^4 + 4q^5 + 8q^6 + \frac{16}{3}q^7 + O(q^8), \end{aligned}$$

where, once again, $q = e^{2\pi i z}$. Thus, we deduce that $S_2(\Gamma_0(37))$ is 2-dimensional, generated by $f(q)$ and $g(q)$.

- (**New text**)

Remark 4.2.9. *The Eisenstein series are very useful because the spaces of modular forms $M_k(\Gamma_1(N))$ and $M_k(\Gamma_0(N))$ have a basis formed by Eisenstein series and cusp forms, and we can easily calculate the q-expansions of the Eisenstein series. For precise statements see* [?], *Chapter 7, or* [?], *Chapter 5.*

Remark 4.2.10. *Let $k \geq 1$ and let Γ be a congruence subgroup. Then $M_k(\Gamma)$ is a finite-dimensional $\mathbb{C}$-vector space. The formulas for the dimension of the spaces of modular forms $M_k(\Gamma)$ and $S_k(\Gamma)$ can be found by calculating the genus and the number of cusps of the modular curve $X(\Gamma)$. Since we will not use these formulas here, we simply refer the reader to* [?], *Theorem 3.5.1 and Figure 3.3 (page 108).*

Example 4.2.11. Let $N = 11$ and let the weight be 2. The space $M_2(\Gamma_0(11))$ is a 2-dimensional $\mathbb{C}$-vector space with basis elements $\{f, g\}$ given by the q-expansions

$$\begin{aligned} f(q) &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + O(q^{11}) \\ g(q) &= 1 + \frac{12}{5}q + \frac{36}{5}q^2 + \frac{48}{5}q^3 + \frac{84}{5}q^4 + \frac{72}{5}q^5 + \frac{144}{5}q^6 + O(q^7), \end{aligned}$$

where $q = e^{2\pi iz}$. Here f is a cusp form and g is an Eisenstein series. Thus, we deduce that $S_2(\Gamma_0(11))$ is 1-dimensional, generated by $f(q)$, and $M_2(\Gamma_0(11))$ is generated by a cusp form and an Eisenstein series (as mentioned in Remark 4.2.9).

Example 4.2.12. Let $N = 37$ and let the weight be 2. The space $M_2(\Gamma_0(37))$ is a 3-dimensional $\mathbb{C}$-vector space with basis elements $\{f, g, h\}$ given by the q-expansions:

$$\begin{aligned} f(q) &= q + q^3 - 2q^4 - q^7 - 2q^9 + 3q^{11} - 2q^{12} - 4q^{13} + O(q^{16}) \\ g(q) &= q^2 + 2q^3 - 2q^4 + q^5 - 3q^6 - 4q^9 - 2q^{10} + 4q^{11} + O(q^{12}) \\ h(q) &= 1 + \frac{2}{3}q + 2q^2 + \frac{8}{3}q^3 + \frac{14}{3}q^4 + 4q^5 + 8q^6 + \frac{16}{3}q^7 + O(q^8), \end{aligned}$$

where, once again, $q = e^{2\pi iz}$. Here f and g are cusp forms, while h is an Eisenstein series. Thus, we deduce that $S_2(\Gamma_0(37))$ is 2-dimensional, generated by $f(q)$ and $g(q)$.

(29) **Pages 112-113.** In the discussion of diamond operators we allowed $\delta \in \mathbb{Z}$ but those δ with $\gcd(\delta, N) > 1$ are not used elsewhere (and, in fact, would bring about unnecessary complications), so we restrict the definition to $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$ from the beginning instead. So we replace every instance of $\delta \in \mathbb{Z}$ by $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$.

- (**Old text**)

  Let $\delta \in \mathbb{Z}$ and $N, k \geq 1$. The diamond operator $\langle \delta \rangle$ is a linear map from $M_k(\Gamma_1(N))$ to itself, defined as follows.

  Definition 4.4.3. *Let $\delta \in \mathbb{Z}$ be fixed. Let $M = (a, b; c, d)$ be a matrix in $\Gamma_0(N)$ such that $d \equiv \delta \bmod N$. The diamond operator $\langle \delta \rangle$ is a linear map $\langle \delta \rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ defined by*

  $$(\langle \delta \rangle f)(z) = (cz + d)^{-k} f(Mz) = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right).$$

  Exercise **??** shows that the definition of $\langle \delta \rangle$ does not depend on the choice of a matrix M. Thus, $\langle \delta \rangle$ is determined by the value of $\delta \bmod N$, so there are N distinct diamond operators, one for each value $0, 1, \ldots, N - 1$. Notice that $\langle 1 \rangle f = f$ is the identity operator, because we can pick $M = \mathrm{Id}$ in the definition of the diamond operator. Moreover, the following proposition shows that the diamond operators with $(\delta, N) = 1$ form a group under multiplication.

  Proposition 4.4.4. *Let $N, k \geq 1$ be fixed and let $\delta, \delta' \in \mathbb{Z}$ with $(\delta\delta', N) = 1$. Then $\langle \delta' \rangle(\langle \delta \rangle f) = \langle \delta \rangle(\langle \delta' \rangle f) = \langle \delta' \delta \rangle f$. In particular, $\langle \delta \rangle^{\varphi(N)} = \langle 1 \rangle = \mathrm{Id}$ and the eigenvalues of $\langle \delta \rangle$ must be roots of unity of order dividing $\varphi(N)$, where φ is the Euler phi function.*

  The proof of this proposition is left to the reader: Exercise **??**.
  Let $\mu_{\varphi(N)}$ be the set of all roots of unity of order dividing $\varphi(N)$. Then, for each $\delta \in \mathbb{Z}$ and every $\zeta \in \mu_{\varphi(N)}$, there is an eigenspace of $M_k(\Gamma_1(N))$ formed by eigenvectors with eigenvalue ζ. More concretely, let $\delta \in \mathbb{Z}$ be fixed. Then, for each $\zeta \in \mu_{\varphi(N)}$, the set

  $$M_k(\Gamma_1(N), \langle \delta \rangle, \zeta) = \{f(z) \in M_k(\Gamma_1(N)) : (\langle \delta \rangle f)(z) = \zeta \cdot f(z)\}$$

is a linear subspace of $M_k(\Gamma_1(N))$, which is the eigenspace for $\langle\delta\rangle$ formed by all eigenvectors with eigenvalue ζ. Furthermore, for each $\delta \in \mathbb{Z}$, the space of modular forms $M_k(\Gamma_1(N))$ can be decomposed as a direct sum of eigenspaces:

$$M_k(\Gamma_1(N)) = \bigoplus_{\zeta \in \mu_{\varphi(N)}} M_k(\Gamma_1(N), \langle\delta\rangle, \zeta).$$

- (**New text**)

Let $N, k \geq 1$ and $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$. The diamond operator $\langle\delta\rangle$ is a linear map from $M_k(\Gamma_1(N))$ to itself, defined as follows.

Definition 4.4.3. *Let $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$ be fixed. Let $M = (a, b; c, d)$ be a matrix in $\Gamma_0(N)$ such that $d \equiv \delta \bmod N$. The diamond operator $\langle\delta\rangle$ is a linear map $\langle\delta\rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ defined by*

$$(\langle\delta\rangle f)(z) = (cz+d)^{-k} f(Mz) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

Exercise **??** shows that the definition of $\langle\delta\rangle$ does not depend on the choice of a matrix M. Thus, $\langle\delta\rangle$ is determined by the value of $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$, so there are $\varphi(N)$ distinct diamond operators, one for each value in $(\mathbb{Z}/N\mathbb{Z})^\times$. Notice that $\langle 1\rangle f = f$ is the identity operator, because we can pick $M = \mathrm{Id}$ in the definition of the diamond operator. Moreover, the following proposition shows that the diamond operators form a group under multiplication.

Proposition 4.4.4. *Let $N, k \geq 1$ be fixed and let $\delta, \delta' \in (\mathbb{Z}/N\mathbb{Z})^\times$. Then, $\langle\delta'\rangle(\langle\delta\rangle f) = \langle\delta\rangle(\langle\delta'\rangle f) = \langle\delta'\delta\rangle f$. In particular, $\langle\delta\rangle^{\varphi(N)} = \langle 1\rangle = \mathrm{Id}$ and the eigenvalues of $\langle\delta\rangle$ must be roots of unity of order dividing $\varphi(N)$, where φ is the Euler phi function.*

The proof of this proposition is left to the reader: Exercise **??**.
Let $\mu_{\varphi(N)}$ be the set of all roots of unity of order dividing $\varphi(N)$. Then, for each $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$ and every $\zeta \in \mu_{\varphi(N)}$, there is an eigenspace of $M_k(\Gamma_1(N))$ formed by eigenvectors with eigenvalue ζ. More concretely, let $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$ be fixed. Then, for each $\zeta \in \mu_{\varphi(N)}$, the set

$$M_k(\Gamma_1(N), \langle\delta\rangle, \zeta) = \{f(z) \in M_k(\Gamma_1(N)) : (\langle\delta\rangle f)(z) = \zeta \cdot f(z)\}$$

is a linear subspace of $M_k(\Gamma_1(N))$, which is the eigenspace for $\langle\delta\rangle$ formed by all eigenvectors with eigenvalue ζ. Furthermore, for each $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$, the space of modular forms $M_k(\Gamma_1(N))$ can be decomposed as a direct sum of eigenspaces:

$$M_k(\Gamma_1(N)) = \bigoplus_{\zeta \in \mu_{\varphi(N)}} M_k(\Gamma_1(N), \langle\delta\rangle, \zeta).$$

(30) **Pages 114-115.** The text was a bit vague about the domain and codomain of the operators U_m and V_m, so we added a few words to clarify. In addition, the definition of T_p when χ_0 is trivial, needed fixing when $p|N$.

- (**Old text**)

Before we define the Hecke operators T_n, we need to define the auxiliary operators U_m and V_m.

Definition 4.4.6. *Let $m \geq 1$ and let $f \in M_k(\Gamma_1(N))$. We define operators V_m and U_m by*

$$(V_m(f))(z) = f(mz) \quad \textit{and} \quad (U_m(f))(z) = \frac{1}{m}\sum_{j=0}^{m-1} f\left(\frac{z+j}{m}\right).$$

If f is given by a q-expansion $f(z) = \sum_{n\geq 0} a_n q^n$, then

$$V_m(f) = \sum_{n\geq 0} a_n q^{mn} \quad \textit{and} \quad U_m(f) = \sum_{n\equiv 0 \bmod m} a_n q^{n/m}.$$

Recall that in Prop. **??** we defined spaces $M_k(N,\chi)$ by

$$M_k(N,\chi) = \{f \in M_k(\Gamma_1(N)) : \langle\delta\rangle f = \chi(\delta) f \text{ for all } \delta \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Definition 4.4.7. *Let $f(z) \in M_k(N,\chi)$ and suppose $f(z)$ is given by a q-expansion $f(z) = \sum_{n\geq 0} a_n q^n$. Let $p \geq 2$ be a prime. We define an operator T_p by*

$$T_p(f) = U_p(f) + \chi(p)p^{k-1}V_p(f),$$

where $\chi(p) = 0$ if $N \equiv 0 \bmod p$. Equivalently,

$$T_p(f(z)) = \sum_{n\geq 0} b_n q^n, \quad \textit{such that} \quad b_n = a_{pn} + \chi(p)p^{k-1}a_{n/p}$$

and $a_{n/p} = 0$ if $n \not\equiv 0 \bmod p$. In particular, if χ_0 is trivial and $f \in M_k(N,\chi_0) = M_k(\Gamma_0(N))$, then

$$T_p(f) = U_p(f) + p^{k-1}V_p(f).$$

Next, we define Hecke operators T_n for all $n \geq 1$.

Definition 4.4.8. *Let $f \in M_k(N,\chi)$. We define Hecke operators T_n for all $n \geq 1$ as follows:*

- *If $n = p \geq 2$ is a prime, then $T_p(f) = U_p(f) + \chi(p)p^{k-1}V_p(f)$ as before;*
- *If $n = p^r$ and $p|N$, then $T_{p^r} = (T_p)^r$, i.e., T_p composed r times with itself;*
- *If $n = p^r$ and $p \nmid N$, then T_{p^r} can be calculated using the following recurrence relation:*

$$T_p \cdot T_{p^r} = T_{p^{r+1}} + p^{k-1}\langle p\rangle T_{p^{r-1}}.$$

- *If $(n,m) = 1$, then $T_{nm}(f) = (T_n \cdot T_m)(f) = (T_m \cdot T_n)(f) = T_m(T_n(f))$.*

Remark 4.4.9. *There are several equivalent ways to define Hecke operators. T_n can be defined as above, or as a function on lattices, or as a double coset operator. See* [?], [?] *or* [?] *for alternative definitions.*

- (**New text**)

Before we define the Hecke operators T_n, we need to define the auxiliary operators U_m and V_m. We remark here that while U_m and V_m are just given as operators on functions given by power series, i.e., $\mathbb{C}[[q]] \to \mathbb{C}[[q]]$, the Hecke operators are defined so that they preserve the space of modular forms $M_k(N,\chi)$.

Definition 4.4.6. *Let $m \geq 1$ and let $f \in M_k(\Gamma_1(N))$. We define operators V_m and $U_m : \mathbb{C}[[q]] \to \mathbb{C}[[q]]$ by*

$$(V_m(f))(z) = f(mz) \quad \text{and} \quad (U_m(f))(z) = \frac{1}{m}\sum_{j=0}^{m-1} f\left(\frac{z+j}{m}\right).$$

If f is given by a q-expansion $f(z) = \sum_{n\geq 0} a_n q^n$, then

$$V_m(f) = \sum_{n\geq 0} a_n q^{mn} \quad \text{and} \quad U_m(f) = \sum_{n\equiv 0 \bmod m} a_n q^{n/m}.$$

Recall that in Prop. **??** we defined spaces $M_k(N,\chi)$ by

$$M_k(N,\chi) = \{f \in M_k(\Gamma_1(N)) : \langle\delta\rangle f = \chi(\delta) f \text{ for all } \delta \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Definition 4.4.7. *Let $f(z) \in M_k(N,\chi)$ and suppose $f(z)$ is given by a q-expansion $f(z) = \sum_{n\geq 0} a_n q^n$. Let $p \geq 2$ be a prime. We define an operator $T_p : M_k(N,\chi) \to M_k(N,\chi)$ by*

$$T_p(f) = U_p(f) + \chi(p)p^{k-1}V_p(f),$$

where $\chi(p) = 0$ if $N \equiv 0 \bmod p$. Equivalently,

$$T_p(f(z)) = \sum_{n\geq 0} b_n q^n, \quad \text{such that} \quad b_n = a_{pn} + \chi(p)p^{k-1}a_{n/p}$$

and $a_{n/p} = 0$ if $n \not\equiv 0 \bmod p$. In particular, if χ_0 is trivial and $f \in M_k(N,\chi_0) = M_k(\Gamma_0(N))$, then

$$T_p(f) = \begin{cases} U_p(f) + p^{k-1}V_p(f) & , \text{ if } p \nmid N, \\ U_p(f) & , \text{ if } p \mid N. \end{cases}$$

Next, we define Hecke operators $T_n : M_k(N,\chi) \to M_k(N,\chi)$ for all $n \geq 1$.

Definition 4.4.8. *Let $f \in M_k(N,\chi)$. We define Hecke operators T_n for all $n \geq 1$ as follows:*

- *If $n = p \geq 2$ is a prime, then $T_p(f) = U_p(f) + \chi(p)p^{k-1}V_p(f)$ as before;*
- *If $n = p^r$ and $p|N$, then $T_{p^r} = (T_p)^r$, i.e., T_p composed r times with itself;*
- *If $n = p^r$ and $p \not| N$, then T_{p^r} can be calculated using the following recurrence relation:*

$$T_p \cdot T_{p^r} = T_{p^{r+1}} + p^{k-1}\langle p\rangle T_{p^{r-1}}.$$

- *If $(n,m) = 1$, then $T_{nm}(f) = (T_n \cdot T_m)(f) = (T_m \cdot T_n)(f) = T_m(T_n(f))$.*

Remark 4.4.9. *There are several equivalent ways to define Hecke operators. T_n can be defined as above, or as a function on lattices, or as a double coset operator. See [?], [?] or [?] for alternative definitions. The reader can also find in these references a proof of the fact that the Hecke operators indeed preserve the space $M_k(N,\chi)$, a fact that we will not show here.*

- **Page 116.** The wording in Example 4.4.10 makes it sound as if $E_{2k}(z)$ was an eigenform at any level, but the point here is that $E_{2k}(z)$ is an eigenform at level 1. Also, $a_0 = -B_{2k}/4k$.

    – (**Old text**)

Example 4.4.12. Let $k \geq 2$ and let

$$E_{2k}(z) = \frac{1}{2\zeta(2k)} G_{2k}(z) = 1 - \frac{4k}{B_{2k}} \sum_{n \geq 1} \sigma_{2k-1}(n) q^n$$

be the (normalized) Eisenstein series of weight $2k$ for $\mathrm{SL}(2, \mathbb{Z})$, as in Proposition **??**. We can write

$$\widehat{E}_{2k}(z) = -\frac{B_{2k}}{4k} E_{2k}(z) = -\frac{B_{2k}}{4k} + \sum_{n \geq 1} \sigma_{2k-1}(n) q^n.$$

Therefore, $a_1 = 1$ and $a_n = \sigma_{2k-1}(n) = \sum_{0<d|n} d^{2k-1}$. Since $\widehat{E}_{2k}$ is a modular form for $\mathrm{SL}(2, \mathbb{Z})$, it may also be considered as a form for $\Gamma_0(N)$ for any $N \geq 1$. Hence, $\widehat{E}_{2k} \in M_{2k}(N, \chi_0) = M_{2k}(\Gamma_0(N))$, where χ_0 is the trivial character of $(\mathbb{Z}/N\mathbb{Z})^\times$, and so

$$a_n = \sum_{0<d|n} \chi_0(d) d^{2k-1}$$

since $\chi_0(d) = 1$. Also notice that $a_0 = B_{2k}/4k \neq 0$, so $\widehat{E}_{2k}$ is not a cusp form. Hence, Hecke's theorem **??** suggests that E_{2k} may be an eigenform; that is, it suggests that E_{2k} is an eigenvector for all T_n, with $n \geq 1$, with eigenvalue a_n. In other words, $T_n(E_{2k}) = \sigma_{2k-1}(n) E_{2k}$ for all $n \geq 1$. This equality is left as an exercise for the reader (see Exercise **??**). $\square$

– (**New text**)

Example 4.4.12. Let $k \geq 2$ and let

$$E_{2k}(z) = \frac{1}{2\zeta(2k)} G_{2k}(z) = 1 - \frac{4k}{B_{2k}} \sum_{n \geq 1} \sigma_{2k-1}(n) q^n$$

be the (normalized) Eisenstein series of weight $2k$ for $\mathrm{SL}(2, \mathbb{Z})$, as in Proposition **??**. We can write

$$\widehat{E}_{2k}(z) = -\frac{B_{2k}}{4k} E_{2k}(z) = -\frac{B_{2k}}{4k} + \sum_{n \geq 1} \sigma_{2k-1}(n) q^n.$$

Therefore, $a_1 = 1$ and $a_n = \sigma_{2k-1}(n) = \sum_{0<d|n} d^{2k-1}$. Since $\widehat{E}_{2k}$ is a modular form for $\mathrm{SL}(2, \mathbb{Z}) = \Gamma_0(1)$, it may also be considered as a form $\widehat{E}_{2k} \in M_{2k}(1, \chi_0) = M_{2k}(\Gamma_0(1))$, where χ_0 is the trivial character modulo 1, i.e., $\chi_0(d) = 1$ for all $d \geq 1$. Thus,

$$a_n = \sigma_{2k-1}(n) \sum_{0<d|n} d^{2k-1} = \sum_{0<d|n} \chi_0(d) d^{2k-1}$$

since $\chi_0(d) = 1$. Also notice that $a_0 = -B_{2k}/4k \neq 0$, so $\widehat{E}_{2k}$ is not a cusp form. Hence, Hecke's Theorem **??** suggests that E_{2k} may be an eigenform; that is, it suggests that E_{2k} is an eigenvector for all T_n, with $n \geq 1$, with eigenvalue a_n. In other words, $T_n(E_{2k}) = \sigma_{2k-1}(n) E_{2k}$ for all $n \geq 1$. This equality is left as an exercise for the reader (see Exercise **??**). $\square$

(31) **Page 117.** Remark 4.4.16 says that Hecke's theorem implies that there is a unique normalized eigenform of $M_{2k}(\Gamma_0(N))$ that is not a cusp form, but what Hecke's theorem truly implies is that there is a unique normalized eigenform of $M_k(\Gamma_0(N), \chi)$ that is not a cusp form. We fix this, and add a note about the first coefficient of such Eisenstein series.

- (**Old text**)

  Example 4.4.16. It follows from Hecke's theorem that, if $k \geq 2$, there is a unique normalized eigenform of $M_{2k}(\Gamma_0(N))$ that is not a cusp form, and it is precisely the Eisenstein series $\widehat{E}_{2k}$, by Example 4.4.12 (and Exercise **??**). $\square$

- (**New text**)

  Example 4.4.16. It follows from Hecke's theorem that, if $k \geq 2$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is a character modulo N, there is a unique normalized eigenform of $M_k(N, \chi)$ that is not a cusp form. This eigenform is precisely the Eisenstein series $\widehat{E}_{k,\chi}$ given by

$$\widehat{E}_{k,\chi}(z) = -\frac{B_{k,\chi}}{2k} + \sum_{n\geq 1}\left(\sum_{0<d|n} \chi(d)d^{k-1}\right) q^n,$$

  where $B_{k,\chi}$ is a generalized Bernoulli number, defined by the following identity:

$$\sum_{d=1}^{N} \frac{\chi(d)\cdot x \cdot e^{dx}}{e^{Nx}-1} = \sum_{k=0}^{\infty} \frac{B_{k,\chi}}{k!}\cdot x^k.$$

  When $N = 1$, and χ is the trivial character modulo 1, i.e., $\chi(d) = 1$ for all $d \geq 1$, then $B_{k,\chi} = B_k$ is the usual Bernoulli number (except $B_{1,\chi} = -B_1 = 1/2$), and $\widehat{E}_{2k,\chi}(z) = \widehat{E}_{2k}(z)$ as in Example 4.4.12. $\square$

(32) **Page 136.** Towards the end of Example 5.3.3., the expression for $(f - 2g)(q)$ should begin with q and not with 1, i.e., it should be

$$(f-2g)(q) = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10} - 5q^{11} + O(q^{12})$$