Typographical Errors in the Second Edition of

Primes of the Form $x^2 + ny^2$

October 9, 2021

Page v, line -8: The title of §1 should be "FERMAT, EULER AND QUADRATIC RECIPROCITY"

Page 25, line above (2.9): "$|b| < a < c$" should be "$|b| \leq a \leq c$"

Page 30, first line of (2.21): "15.23" should be "15, 23"

Page 32, line 2 of Theorem 2.26: "not dividing D." should be "not dividing D," (the period should be a comma)

Page 48, line -13: "$\ker(\chi) \in (\mathbb{Z}/D\mathbb{Z})^*$" should be "$\ker(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^*$"

Page 53, line -1: "property" should be "properly"

Page 61, part (a) of Exercise 3.9: "if and only if a, b or ab has order ≤ 2 in G" should be "if and only if a or b has order ≤ 2 in G"

Page 61, part (b)(ii) of Exercise 3.11: Delete the hint.

Page 61, part (b)(iii) of Exercise 3.11: "See also" should be "See the description of $(\mathbb{Z}/2^{a+2}\mathbb{Z})^*$ given in"

Page 62, line 9: "that Proposition 3.11 and Theorem 3.15 hold for all" should be "that Proposition 3.11 holds for all"

Page 62, part (b) of Exercise 3.12: "$\ker(\Phi)'$" should be "$\ker(\Phi')$"

Page 62, part (a) of Exercise 3.13: "the assigned characters" should be "assigned characters (where $n < 0$ when $D = -4n$ is positive)".

Page 63, part (e) of Exercise 3.13: Replace the hint with "Hint: prove $(2/p) = 1$ if and only if $p \equiv 1, 7 \bmod 8$. For $\Rightarrow$, show that p is properly represented by a form of discriminant 8 and use $-2 \equiv 6 \bmod 8$. For $\Leftarrow$, use the forms $2x^2 + xy + ((1-p)/8)y^2$ of discriminant p (when $p \equiv 1 \bmod 8$) and $2x^2 + xy + ((1+p)/8)y^2$ of discriminant $-p$ (when $p \equiv 7 \bmod 8$). Both represent 2.

Page 65, part (e) of Exercise 3.20: "$f(\alpha x + \beta y, \gamma x + \delta y)$" should be "$f(\alpha x + \gamma y, \beta x + \delta y)$"

Page 65, lines -2 and -1 : "Note also that Lemma 3.25 gives a very quick proof of Exercise 2.27" should be "Note that Lemma 3.25 gives a quick proof of Exercise 2.27(a) for forms of discriminant $-4n$ when $p \nmid n$"

Page 66, part (c) of Exercise 3.24: "supplementary laws:" should be "supplementary laws for P odd:"

Page 75, line 18: "the second memoir. Gauss" should be "the second memoir, Gauss" (the period should be a comma)

Page 81, Exercise 4.10: "Let π be prime in $\mathbb{Z}[\omega]$" should be "Let π be prime of $\mathbb{Z}[\omega]$ not associate to $1 - \omega$"

Page 82, line 2 of Exercise 4.18: "π is prime in $\mathbb{Z}[i]$" should be "π is a prime of $\mathbb{Z}[i]$ not associate to $1 + i$"

Page 91, lines -4 and -3: "$f_i(x)$ are distinct and irreducible modulo $\mathfrak{p}$" with "$f_i(x)$ are monic, and distinct and irreducible modulo $\mathfrak{p}$"

Page 103, line 3 of Exercise 5.2: "it is a finitely generated" should be "it is a nonzero finitely generated"

Page 104, part (f) of Exercise 5.6: "$\mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_K$" should be "$\mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$"

Page 104, part (f) of Exercise 5.6: In the hint, delete the second sentence and replace with "Show that ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_L$ satisfy $\mathfrak{a} \subset \mathfrak{b}$ if and only if $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for some ideal $\mathfrak{c}$. Then apply this to $\mathfrak{p}\mathcal{O}_L \subset I_i \subset \mathfrak{P}_i$."

Page 105, part (d) of Exercise 5.7: It should be "Prove the description of $\mathcal{O}_K$ given in (5.14)"

Page 105, part (c) of Exercise 5.10: Replace the first sentence of the hint with "by part (a) of Exercise 5.1, $\mathfrak{p}$ contains a nonzero integer m, which can be assumed to be positive."

Page 107, Exercise 5.18: "where L and M are" should be "where L is"

Page 109, diagram (6.3): Replace the diagram with the following:

(6.3)

$$\left.\begin{array}{c} L \\ | \\ \tilde{M} \\ | \\ K \\ | \\ \mathbb{Q} \end{array}\right] \text{ Abelian}$$

Page 115, line 5: "35 satisfy" should be "34 satisfy"

Page 116, part (b) of Exercise 6.6: Replace the first two sentence of the hint with "use Proposition 5.10. For a prime $\mathfrak{P}$ of $\mathcal{O}_{LM}$ containing $\mathfrak{p}$, show that if $\sigma \in I_{\mathfrak{P}}$, then the restrictions $\sigma|_L$ and $\sigma|_M$ lie in the inertia groups of $\mathfrak{P} \cap \mathcal{O}_L$ and $\mathfrak{P} \cap \mathcal{O}_M$ respectively."

Page 122, line 4: "principal ideals" should be "nonzero principal ideals"

Page 122, line 4: "*all* ideals" should be "*all* nonzero ideals"

Page 125, line -12: "let $\mathfrak{a}$ be a fractional" should be "let $\mathfrak{a}$ be a proper fractional"

Page 127, one line above (7.16): "$a \cdot \mathfrak{a} = \alpha \cdot a[a, \tau]$" should be "$a \cdot \mathfrak{a} = \alpha \cdot a[1, \tau]$"

Page 133, four lines below (7.26): "$u \in \mathcal{O}$" should be "$u \in \mathcal{O}_K$"

Page 133, line -4: "$[b][c]^{-1}$" should be "$\pm[b][c]^{-1}$"

Page 136, part (a) of Exercise 7.6: "principal ideals" should be "nonzero principal ideals"

Page 136, part (b) of Exercise 7.6: "all ideals" should be "all nonzero ideals"

Page 138, line 2: AM should be MA.

Page 138, line 3: $|M/AM|$ should be $|M/MA|$.

Page 138, part (c) of Exercise 7.15, line 4: "dividing by a by c" should be "dividing a by c"

Page 138, part (d) of Exercise 7.15: $|M/AM|$ should be $|M/MA|$.

Page 138, part (a) of Exercise 7.17: "$\mathfrak{a} = [\alpha, \beta]$ to" should be "$\mathfrak{a} = [\alpha, \beta]$, $\mathrm{Im}(\beta/\alpha) > 0$, to"

Page 138, line -2: $a^2 - 3c^2 = 1$ should be $a^2 - 3c^2 = -1$

Page 140, line 6 of part (d) of Exercise 7.21: "$\mathfrak{a} = \sqrt{d_K}[a, a\tau]$" should be "$\mathfrak{a} = \sqrt{D}[a, a\tau]$"

Page 143, line 1: "any quadratic field" should be "any imaginary quadratic field"

Page 143, line 1: "let f be a positive integer" should be "let $f > 1$ be an integer."

Page 145, second display: "$I_k(\mathfrak{m})/H$" should be "$I_K(\mathfrak{m})/H$"

Page 146, line 15: "mth of unity" should be "mth root of unity"

Page 147, line 4: The citation [62, Chapter V, §6 and Theorem 12.7] refers to the first edition of [62]. For the second edition, the correct citation is [62, Chapter V, §6 and Theorem 11.11].

Page 151, last paragraph of the proof of Theorem 8.12: The proof has a gap. Weak Reciprocity does not apply to the modulus $p\infty$ since p is odd but Theorem 8.11 with $n = 2$ requires an even modulus. Thus the last paragraph of the proof should be replaced with the following:

To apply Theorem 8.11 when $n = 2$, the modulus must be divisible by 2. Since p is odd, $\zeta_{2p} = -\zeta_p$, so $\mathbb{Q}(\zeta_{2p}) = \mathbb{Q}(\zeta_p)$, and by (8.3) and (8.4), $\mathrm{Gal}(\mathbb{Q}(\zeta_{2p})/\mathbb{Q})$ is a generalized ideal class group for the modulus $2p\infty$. It follows that Weak Reciprocity applies to $K/\mathbb{Q}$ for this modulus. However, we have isomorphisms

$$(\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/2p\mathbb{Z})^* \xrightarrow{\sim} I_{\mathbb{Q}}(2p\infty)/P_{\mathbb{Q},1}(2p\infty),$$

where the first map follows since p is odd (a even $\Rightarrow a+p$ is odd) and the second map sends $[a] \in (\mathbb{Z}/2p\mathbb{Z})^*$ to $[a\mathbb{Z}] \in I_{\mathbb{Q}}(2p\infty)/P_{\mathbb{Q},1}(2p\infty)$ when $a > 0$ (see Exercise 8.7). Composing this map with (8.13) shows that $(p^*/\cdot)$ induces a surjective homomorphism from $(\mathbb{Z}/p\mathbb{Z})^*$ to $\{\pm 1\}$. But the Legendre symbol $(\cdot/p)$ is also a surjective homomorphism between the same two groups, and since $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, there is only one such homomorphism. This proves that

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right),$$

and we are done. Q.E.D.

Page 155, lines -18 and -17: "But Exercise 5.9 tells us" should be "But [77, Exercise 4.11(b)] tells us"

Page 158, Exercise 8.4: After the display, add the following new sentences: "Use this to show that if $\mathrm{Gal}(L/K)$ is a generalized ideal class group for $\mathfrak{m}$, then it is also a generalized ideal class group for $\mathfrak{n}$. Hint: use part (i) of Theorem 8.2."

Page 159, part (c) of Exercise 8.7: Delete the current part (c) and replace with the following:

(c) Verify the isomorphisms

$$(\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/2p\mathbb{Z})^* \xrightarrow{\sim} I_{\mathbb{Q}}(2p\infty)/P_{\mathbb{Q},1}(2p\infty)$$

described in the proof of Theorem 8.12.

Page 159, Exercise 8.8: Replace parts (a)–(c) with the following:

(a) Use Exercise 8.2 to construct isomorphisms

$$I_{\mathbb{Q}}(8\infty)/P_{\mathbb{Q},1}(8\infty) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \simeq (\mathbb{Z}/8\mathbb{Z})^*,$$

and conclude that $I_{\mathbb{Q}}(8\infty)/P_{\mathbb{Q},1}(8\infty) = \{[\mathbb{Z}], [3\mathbb{Z}], [5\mathbb{Z}], [7\mathbb{Z}]\}$.

(b) Let $H = \{\mathbb{Z}, 7\mathbb{Z}\}P_{\mathbb{Q},1}(8\infty)$. Show that via the Existence Theorem, H corresponds to $\mathbb{Q}(\sqrt{2})$. Hint: using the arguments of Theorem 8.12 and part (b) of Exercise 8.7, show that H corresponds to one of $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. Then observe that $[7\mathbb{Z}] \in I_Q(8\infty)/P_{\mathbb{Q},1}(8\infty)$ maps to $-1 \in (\mathbb{Z}/8\mathbb{Z})^*$. What element of $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ does this correspond to?

(c) Use Weak Reciprocity to show that $(2/\cdot)$ induces a well-defined homomorphism on $(\mathbb{Z}/8\mathbb{Z})^*$ whose kernel is $\{\pm 1\}$.

(d) Show that $(2/p) = (-1)^{(p^2-1)/8}$.

Page 160, line -2: "$\tilde{S}_{M/K}$" should be "$\tilde{\mathcal{S}}_{M/K}$"

Page 161, part (a) of Exercise 8.12: "$\tilde{S}_{M/K}$ equals the set $S_{M/K}$" should be "$\tilde{\mathcal{S}}_{M/K}$ equals the set $\mathcal{S}_{M/K}$" (two changes)

Page 161, part (b) of Exercise 8.12: "$\tilde{S}_{M/K} \dot{\subset} S_{L/K}$" should be "$\tilde{\mathcal{S}}_{M/K} \subset \mathcal{S}_{L/K}$" (three changes)

Page 161, part (c) of Exercise 8.12: "$S_{M/K} \subset S_{L/K}$" should be "$\mathcal{S}_{M/K} \subset \mathcal{S}_{L/K}$" (two changes)

Page 161, Exercise 8.13, last line: "$N_{\mathfrak{P}}M = M$" should be "$N_{\mathfrak{P}}M = N_{\mathfrak{P}}$"

Page 161, Exercise 8.15: In two places, "$S_{L/K}$" should be "$\mathcal{S}_{L/K}$", and in two places, "$S_{L'/K}$" should be "$\mathcal{S}_{L'/K}$"

Page 161, Exercise 8.16, line 2: "$\tilde{S}_{M/L} = S_{M/K}$" should be "$\tilde{\mathcal{S}}_{M/K} = \mathcal{S}_{M/K}$" (three changes)

Page 161, Exercise 8.16, last line: "of Proposition 8.20" should be "of Proposition 8.20 and Exercise 8.15"

Page 161: Add the following new exercise following Exercise 8.16:

8.17. The definition of $P_{K,1}(\mathfrak{m})$ differs from the standard definition, which uses valuations and multiplicative congruences. See, for example, [62, Chapter IV]. One can show without difficulty that the equivalence of the two definitions reduces to the following claim: $P_{K,1}(\mathfrak{m})$ contains all principal fractional ideals of the form $(a/b)\mathcal{O}_K$ where $a, b \in \mathcal{O}_K$ are relatively prime to $\mathfrak{m}_0$, $a \equiv b \mod \mathfrak{m}_0$, and $\sigma(a/b) > 0$ for all real infinite primes dividing $\mathfrak{m}$.

(a) Let $\sigma_1, \ldots, \sigma_r$ be the real infinite primes dividing $\mathfrak{m}$, and for each i, pick $\epsilon_i \in \{\pm 1\}$. Prove that there is $\lambda \in \mathcal{O}_K$ such that $\lambda \equiv 1 \mod \mathfrak{m}_0$, and $\sigma_i(\epsilon_i \lambda) > 0$ for all i. Hint: by the Approximation Theorem (Theorem 1.1 of [62, Chapter IV]), there is $\alpha \in K^*$ such that $\sigma_i(\epsilon_i \alpha) > 0$ for all i. Argue that α can be chosen to lie in $\mathcal{O}_K$. Then let $\lambda = 1 + d\alpha\beta^2$ where d is a sufficiently large positive integer and β is a nonzero element of $\mathfrak{m}_0$.

(b) Prove the claim made at the beginning of the exercise. Hint: multiply a, b by a suitable $c \in \mathcal{O}_K$ to ensure $a, b \equiv 1 \mod \mathfrak{m}_0$, and then multiply both by λ from part (a) for a suitable choice of ϵ_i to make $\sigma_i(a), \sigma_i(b) > 0$ for all i.

Page 165, line 1: "Lemma 5.21" should be "Corollary 5.21"

Page 167, line 3: "$\mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}$, then "$\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$" should be "$\mathrm{Gal}(M/K) \simeq \mathbb{Z}/3\mathbb{Z}$, then "$\mathrm{Gal}(M/\mathbb{Q}) \simeq S_3$"

Page 167, line 9: "σ is real" should be "α is real"

Page 169, line 1: Replace with "If $\pi = a + bi$ is a primary prime of $\mathbb{Z}[i]$, then"

Page 169, third display: "$I_K(6)/P_{K,\mathbb{Z}}(6)$" should be "$I_K(6)/P_{K,1}(6)$"

Page 171, four lines below third display: $p \nmid (f)$ should be $p \nmid f$

Page 177, Exercise 9.21: Replace parts (c) and (d) with the following:

(c) Consider the natural maps

$$\pi : (\mathcal{O}_K/f\mathcal{O}_K)^* \longrightarrow (\mathcal{O}_K/\mathfrak{m})^*$$
$$\beta : (\mathbb{Z}/f\mathbb{Z})^* \longrightarrow (\mathcal{O}_K/f\mathcal{O}_K)^*.$$

Show that $\ker(\pi) \subset \mathcal{O}_K^* \cdot \mathrm{im}(\beta)$. Hint: use (b) and show that elements of $P_{K,\mathbb{Z}}(f)$ can be represented as $(\gamma/\delta)\mathcal{O}_K$ where $\gamma, \delta \in \mathcal{O}_K$ satisfy $\gamma \equiv c \bmod f\mathcal{O}_K$ for $c \in \mathbb{Z}$ with $\gcd(c, f) = 1$ and $\delta \equiv 1 \bmod f\mathcal{O}_K$.

Page 179, line 2: Add the following hint to part (b) of Exercise 9.23: "Hint: show that $\ker(\pi) \subset \mathcal{O}_K^* \cdot \mathrm{im}(\beta)$ leads to a contraction. Use Exercise 9.22 to reduce to the case where $\ker(\pi) \not\subset \mathrm{im}(\beta)$ and prove that there is an exact sequence

$$1 \longrightarrow \ker(\pi) \cap \mathrm{im}(\beta) \longrightarrow \ker(\pi) \longrightarrow \mathcal{O}_K^*/\big(\mathcal{O}_K^* \cap \mathrm{im}(\beta)\big).$$

Page 186, line -1: At the end of the display, "$z\wp(z)$" should be "$2\wp(z)$"

Page 192, 4 lines below (10.19): "$\pm(z + w_i)$" should be "$\pm(z + w_j)$"

Page 197, Exercise 10.4, second line of the display: "$+\dfrac{24G_4(L)}{z^2}$" should be "$-\dfrac{24G_4(L)}{z^2}$"

Page 199, part (b) of Exercise 10.16: "Theorem 5.25" should be "Theorem 5.30"

Page 199, part (c) of Exercise 10.16: On line 2, "lattices given with" should be "lattices with"

Page 199, part (c) of Exercise 10.16: In the display, "$\displaystyle\sum_{f=1}^{[\mathcal{O}_K:\mathbb{Z}[\alpha]]} h(f^2 d_K)$" should be "$\displaystyle\sum_{f \,|\, [\mathcal{O}_K:\mathbb{Z}[\alpha]]} h(f^2 d_K)$"

Page 200, part (c) of Exercise 10.19: Delete the hint.

Page 203, line -14: "$\gamma \neq \pm 1$" should be "$\gamma \neq \pm I$"

Page 208, line 10: The display should be

$$q(\sigma\tau) = e^{2\pi i(a\tau+b)/d} = e^{2\pi i b/d} q^{a/d}$$

(two errors in the original)

Page 208, line -7: "$j(m\gamma_i, \gamma\tau)$'s" should be "$j(m\gamma_i\gamma\tau)$'s"

Page 210, part (v) of Theorem 1.18: "$(X^P - Y)(X - Y^P)$" should be "$(X^p - Y)(X - Y^p)$" (two errors)

Page 217, line 12: "some prime ideal of $\mathcal{O}$" should be "some prime ideal of $\mathcal{O}_K$"

Page 218, Theorem 11.36: "$\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$" should be "$\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ relatively prime to the conductor of $\mathcal{O}$"

Page 219, line -10: "of class field theory" should be "of complex multiplication"

Page 220, Exercise 11.2: "use (7.9)" should be "use (7.10)"

Page 220, bottom line: "$\mathrm{Re}(\tau) \geq 0$" should be "$\mathrm{Re}(\tau) \leq 0$"

Page 221, second display: The display should be

$$|b| \leq a \leq c, \text{and } b \geq 0 \text{ if either } |b| = a \text{ or } a = c.$$

Page 221, part (b) of Exercise 11.4: Add the following sentences to the hint: "Show that among all forms properly equivalent to a given positive definite forms with real coefficients, there is one with minimal $|b|$. Equation (2.4) is helpful."

Page 221, part (c) of Exercise 11.4: Replace the last sentence with "Furthermore, show that $b = -2a\mathrm{Re}(\tau)$ and $c = a|\tau|^2$."

Page 221, bottom line: "Use (7.9)" should be "Use (7.10)"

Page 222, part (a) of Exercise 11.6: "$\mathrm{SL}(2, \mathbb{Z})$ and that" should be "$\mathrm{SL}(2, \mathbb{Z})$, $\gamma \neq \pm I$, and that"

Page 222, part (c) of Exercise 11.6: Delete the entire Hint.

Page 224, Exercise 11.16: "Let $M = \mathbb{Z}^2$, and" should be "Let $M = \mathbb{Z}^2$, thought of as column vectors, and"

Page 224, Exercise 11.16: "We know from Exercise 7.15" that" should be "Exercise 7.15, applied to the transpose of A, implies that"

Page 227, two lines below the statement of Theorem 12.2: At the end of the line, "by Theorem 12.2." should be "by Theorem 12.2,"

Page 227, three lines below the statement of Theorem 12.2: "$j(\tau)$" should be "$j(\tau_0)$"

Page 228, display (12.5): "$\sum_{n=0}^{\infty} b_n q^n$" should be "$\sum_{n=1}^{\infty} b_n q^n$"

Page 231, second display: "3_{τ_0}" should be "$3\tau_0$"

Page 236, three lines above Corollary 12.19: "see Exercise 2.16" should be "see Exercise 12.16"

Page 240, line 13: "$\mathbb{Q}(\sqrt{-l4})$" should be "$\mathbb{Q}(\sqrt{-14})$"

Page 241, bottom line: "$\zeta_d^a q^{a/d} = \zeta_b^a (q^{1/8})^{a^2}$" should be "$\zeta_d^b q^{a/d} = \zeta_d^b (q^{1/8})^{a^2}$" (three errors)

Page 245, display (12.32): "$\sigma(\mathfrak{f}_1(\sqrt{-14}/2)^2)$" should be '$\sigma(\mathfrak{f}_1(\sqrt{-14})^2)$"

Page 250, bottom line: The display should be "$S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & * \\ a & * \end{pmatrix}$"

Page 251, line 2: The display should be "$T^{\pm 1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a \pm c & * \\ c & * \end{pmatrix}$"

Page 251, bottom line: "$\gamma_3(3\tau)$" should be "$\gamma_2(3\tau)$"

Page 255, part (a) of Exercise 12.14: On the last line of the display, "$\dfrac{f(\tau)^2}{\eta(\tau)^2}$" should be "$\dfrac{\mathfrak{f}(\tau)^2}{\eta(\tau)^2}$"

Page 257, part (b) of Exercise 12.23: Replace the hint with the following: "Hint: show that $\mathfrak{f}_1(\tau)^6$ is a modular function for the group $\tilde{\Gamma}(8)$ defined in Exercise 12.21. Since $\tilde{\Gamma}(8)$ is normal in $\mathrm{SL}(2,\mathbb{Z})$, this implies that $\mathfrak{f}(\tau)^6$ is also invariant under $\tilde{\Gamma}(8)$."

Page 258, line 3 of part (e) of Exercise 12.23: "σ_1 and σ_1" should be "σ_1 and σ_2"

Page 259, part (a) of Exercise 12.28: Immediately after the first display, add "Also show that $2mn - 3n^2 > 0$ and $m^2 - 3n^2 > 0$."

Page 259, part (b)(iii) of Exercise 12.28: In the Hint, "implies $c = 3$" should be "implies $b = c = 1$".

Page 259, part (b)(iv) of Exercise 12.28: In the Hint, "show that $c = 3$" should be "show that $b = c = 1$".

Page 259, part (c) of Exercise 12.28: Delete everything after the first display and replace with the following:

Furthermore, $\gcd(m, n) = 1$ implies $\gcd(k, n) = 1$ and $3 \nmid n$.

(i) Show that $b = 2kn - n^2$ and $c = 3k^2 - n^2$.

(ii) Prove that $c = 3k^2 - n^2$ is impossible since c is a perfect square. Hint: work modulo 3.

Page 261, line 1 of part (a) of Exercise 12.31: "Prove that $P = \sqrt{14}(2/\alpha)$ and $Q = \sqrt{7/2}(\alpha/2)$" should be "Prove that $P = \sqrt{14}/\alpha$ and $Q = \sqrt{7/2}\alpha$"

Page 262, line -10: "important role. The reason for this is the following" should be "important role. Since $\Phi_1(X, Y)$ implies that $\Phi_1(X, X)$ is identically zero, we focus on the case $m > 1$. Then we have the following"

Page 263, line 4: "Thus $\alpha \notin \mathbb{Z}$," should be "Thus $\alpha \notin \mathbb{Z}$ since $m > 1$,"

Page 263, line above first display: "a positive integer m, set" should be "an integer $m > 1$, set"

Page 268, line 1: "compute $H_D(X)$" should be "compute $H_D(X)$ for most D"

Page 268, line -15: "compute any $H_D(X)$" should be "compute $H_D(X)$ for any $D \neq -3k^2$, k odd"

Page 277, part (b) of Exercise 13.2: "fixed m" should be "fixed $m > 1$"

Page 278, part (b) of Exercise 13.6: In four places, "ζ_m^{ab}" should be "ζ_m^{-ab}"

Page 280, line 2 of part (a) of Exercise 13.15: "congrunce" should be "congruence"

Page 280, lines 2 and 3 of part (d) of Exercise 13.15: "$a \mid d_1$, $a \equiv 1 \bmod 4$ ... where $d \equiv 1 \bmod 4$" should be "$a \mid d_1$, $a, b > 0$ and $\gcd(d_1, b) = 1$"

Page 280, part (d)(ii) of Exercise 13.15: Replace everything, including the hint, with "Show that $(d_1/b) = -(\varepsilon a/d_2)$, where $\varepsilon = (-1)^{(a-1)/2}$.

Hint: write $d_1 = \varepsilon ad$ and note that $(d_1/b) = (d_1/4b) = (\varepsilon a/4b)(d/4b)$. Use $4ab = d_1 d_2 - x^2$ to show that $4b \equiv \varepsilon d d_2 \bmod a$ (remember that a has no square factors) and then apply quadratic reciprocity to $(\varepsilon a/d)$."

Page 281, line 1 of part (e) of Exercise 13.16: "$\epsilon(p) = 1$" should be "$\epsilon(p) = -1$"

Page 287, display (14.7): In the second line of the display, "$12x_1 - g_2$" should be "$12x_1^2 - g_2$"

Page 288, three lines above third display: "the order" should be "order"

Page 293, two lines below third display: "Exercise 4.13" should be "Exercise 14.13"

Page 294, line 2: "discriminant" should be "discriminant when $a \neq 0$"

Page 294, line 8: "Theorem 9.4" should be "Theorem 9.4 and Exercise 9.3"

Page 296, line 8: "$2\sqrt{p} \leq a \leq 2\sqrt{p}$" should be "$-2\sqrt{p} \leq a \leq 2\sqrt{p}$"

Page 296, display (14.21): The summation should be "$\displaystyle\sum_{0 \leq |a| \leq 2\sqrt{p}}$"

Page 296, display following (14.21): The first summation should be "$\displaystyle\sum_{0 \leq |a| \leq 2\sqrt{p}}$"

Page 305, display of Exercise 14.7: In two places, "$x + z$" should be "$x + 2$" in the denominator

Page 305, Exercise 14.8: "curve the finite field" should be "curve over the finite field"

Page 306, display of Exercise 14.12: "$Frob_q$" should be "$1 - Frob_q$"

Page 306, line 2 of part (b) of Exercise 14.13: "takes the curve" should be "transforms the curve"

Page 306, Exercise 14.15: "discriminant" should be "conductor"

Page 312, line below (15.10): "$\gamma_p \in \prod_p \mathrm{GL}(2, \mathbb{Z}_p)$" should be "$\gamma_p \in \mathrm{GL}(2, \mathbb{Z}_p)$"

Page 313, line -3: "$(I_L(fm) \cap P_{K,\mathbb{Z}}(f))$" should be "$(I_K(fm) \cap P_{K,\mathbb{Z}}(f))$"

Page 315, six lines above **Theorem 15.16**: "Theorem 7.7" should be "Lemma 7.5"

Page 315, **Theorem 15.16**: "be as above" should be "as above"

Page 317, fourth line of the proof of **Theorem 15.18**: "Theorem 15.17" should be "Theorem 15.16"

Page 317, seventh line of the proof of **Theorem 15.18**: "± 1, 3 and $1 + \sqrt{-m}$" should be "-1, 3 and $1 + \sqrt{-m}$"

Page 318, display (15.19): "$m \equiv 6 \bmod 8$" should be "$m \equiv 6 \bmod 8$ and $3 \nmid m$"

Page 318, two lines below display (15.19): "$m \equiv 3 \bmod 8$" should be "$m \equiv 3 \bmod 4$ and $3 \nmid m$"

Page 318, line -12: "for all proper" should be "for any proper"

Page 320, line 1: "$x_p \in \mathcal{O}_p$" should be "$x_p \in \mathcal{O} \subset \mathcal{O}_p$"

Page 324, line -2: "$\prod_p^*$" should be "$\prod_{\mathfrak{p}}^*$"

Page 328, line 5: "invariant under $\Gamma(8)$ using (12.26)" should be "invariant under the group $\tilde{\Gamma}(8)$ from Exercise 12.21 using (12.26). Note also that $\Gamma(8) \subseteq \tilde{\Gamma}(8)$"

Page 329, Exercise 15.4: "$\gamma_p \in \prod_p \mathrm{GL}(2, \mathbb{Z}_p)$" should be "$\gamma_p \in \mathrm{GL}(2, \mathbb{Z}_p)$"

Page 329, part (c) of Exercise 15.5: "for $a \in \mathbb{Z}$ relatively prime to fm" with "for $a \in \mathbb{Z}$ and α relatively prime to fm"

Page 330, line 1 of Exercise 15.9: "$m \equiv 3 \bmod 8$" should be "$m \equiv 3 \bmod 4$ and $3 \nmid m$"

Page 330, line 2 of Exercise 15.9: "$\mathfrak{f}(\sqrt{-m})^6)$" should be "$\mathfrak{f}(\sqrt{-m})^6$"

Page 330, line 3 of Exercise 15.9: Add a new sentence: "Do the cases $m \equiv 3 \bmod 8$ and $m \equiv 7 \bmod 8$ separately."

Page 330, line 4 of part (b) of Exercise 15.12: "$p^{n_p} x$" should be "$p^{n_p} x_p$"

Page 332, line 1: "$\beta x \equiv 1 \bmod \mathfrak{m}$ for all $\mathfrak{p} \mid \mathfrak{m}$" should be "$\beta x \equiv 1 \bmod \mathfrak{m}$ as defined above"

Page 332, line 2 of part (b) of Exercise 15.18: "the isomorphism takes of" should be "the isomorphism of"

Page 333, Exercise 15.22: "$\zeta_m j(\tau) \in \mathsf{F}_m$" should be "$\zeta_m \in \mathsf{F}_m$"