Typographical Errors in the Second Edition of

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

June 19, 2022

Page v, line −8: The title of §1 should be “FERMAT, EULER AND QUADRATIC RECIPROCITY”

Page 5, line −18: “elemenary” should be “elementary”

Page 25, line above (2.9): “|b| < a < c” should be “|b| ≤ a ≤ c”

Page 26, display (2.12): “$a < \sqrt{(-D)/3}$” should be “$a < \sqrt{-D/3}$”

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(χ) ∈ (Z/DZ)*” should be “ker(χ) ⊂ (Z/DZ)*”

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 $(Z/2^nZ)^*$ 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(Φ)” should be “ker(Φ′)”

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 $p \equiv 1, 7$ mod 8. For $\Rightarrow$, show that $p$ is properly represented by a form of discriminant 8 and use $-2 \equiv 6$ mod 8. For $\Leftarrow$, use the forms $2x^2 + xy + ((1 - p)/8)y^2$ of discriminant $p$ (when
Page 65, part (e) of Exercise 3.20: “f(αx + βy, γx + δy)” should be “f(αx + γy, βx + δy)”

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 | 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 Z[ω]” should be “Let π be prime of Z[ω] not associate to 1 − ω”

Page 82, line 2 of Exercise 4.18: “π is prime in Z[i]” should be “π is a prime of Z[i] not associate to 1 + i”

Page 91, lines −4 and −3: “fi(x) are distinct and irreducible modulo p” should be “fi(x) are monic, and distinct and irreducible modulo p”

Page 94, line 5: “distinct primes” should be “for distinct primes”

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: “pO_L + fi(α)O_K” should be “pO_L + fi(α)O_L”

Page 104, part (f) of Exercise 5.6: In the hint, delete the second sentence and replace with “Show that ideals a, b of O_L satisfy a ⊆ b if and only if a = bc for some ideal c. Then apply this to pO_L ⊆ I_i ⊆ P_i.”

Page 105, part (d) of Exercise 5.7: It should be “Prove the description of 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, 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:

\[
\begin{array}{c}
L \\
| \\
M \\
| \\
K \\
| \\
Q \\
\end{array}
\]

Page 114, 2 lines above (6.17): “[a, b+\sqrt{-n}]” should be “[a, -b+\sqrt{-n}]”

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 \( p \), 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 \( a \) be a fractional” should be “let \( a \) be a proper fractional”

Page 127, one line above (7.16): “\( a \cdot a = \alpha \cdot a[a, \tau] \)” should be “\( a \cdot a = \alpha \cdot a[1, \tau] \)"

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

Page 133, three lines below (7.27): “and \( f\mathcal{O}_K \)” and” should be “\( f\mathcal{O}_K \)” and”

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: “$a = [\alpha, \beta]$ to” should be “$a = [\alpha, \beta], \text{Im}(\beta/\alpha) > 0$, 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: “$a = \sqrt{d_K[a, a\tau]}$” should be “$a = \sqrt{D}[a, a\tau]$”

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: “$I_k(m)/H$” should be “$I_K(m)/H$”

Page 146, line 15: “$m$th of unity” should be “$m$th 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 150, Theorem 8.11: On the line below the first display, “$\mu_n$, is the” should be “$\mu_n$ is the” (remove the comma)

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), $\text{Gal}(\mathbb{Q}(\zeta_{2p})/\mathbb{Q})$ is a generalized ideal class group for the modulus $2p\infty$. It follows that Weak Reciprocity applies to $K/\mathbb{Q}$ for this modulus. This gives a surjective homomorphism

\[ I_{\mathbb{Q}}(2p\infty)/P_{\mathbb{Q},1}(2p\infty) \rightarrow \{\pm 1\}. \]

However, we also 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 $[aZ] \in I_\mathbb{Q}(2p\infty)/P_{\mathbb{Q},1}(2p\infty)$ 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 153, line 6: “Dirichlet $\zeta$-function” should be “Dedekind $\zeta$-function”

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 $\text{Gal}(L/K)$ is a generalized ideal class group for $m$, then it is also a generalized ideal class group for $n$. 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

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

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

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

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 $[7\mathbb{Z}] \in I_\mathbb{Q}(8\infty)/P_{\mathbb{Q},1}(8\infty)$ maps to $-1 \in (\mathbb{Z}/8\mathbb{Z})^*$. What element of $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ 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, part (b) of Exercise 8.10: “(ii)–(iv)” should be “(ii)–(vi)”

Page 160, line −2: “ ˜SM/K” should be “ ˜SM/K”

Page 161, part (a) of Exercise 8.12: “ ˜SM/K equals the set SM/K” should be “ ˜SM/K equals the set SM/K” (two changes)

Page 161, part (b) of Exercise 8.12: “ ˜SM/K ⊂ SL/K” should be “ ˜SM/K ⊂ SL/K” (three changes)

Page 161, part (c) of Exercise 8.12: “SM/K ⊂ SL/K” should be “SM/K ⊂ SL/K” (two changes)

Page 161, Exercise 8.13, last line: “NP M = M” should be “NP M = Np”

Page 161, Exercise 8.15: In two places, “SL/K” should be “SL/K”, and in two places, “SL′/K” should be “SL′/K”

Page 161, Exercise 8.16, line 2: “ ˜SM/L = SM/K” should be “ ˜SM/K = SM/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 PK,1(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: PPK,1(m) contains all principal fractional ideals of the form (a/b)OK where a, b ∈ OK are relatively prime to m0, a ≡ b mod m0, and σ(a/b) > 0 for all real infinite primes dividing m. (a) Let σ1, . . ., σr be the real infinite primes dividing m, and for each i, pick εi ∈ {±1}. Prove that there is λ ∈ OK such that λ ≡ 1 mod m0, and σ(εiλ) > 0 for all i. Hint: by the Approximation Theorem (Theorem 1.1 of [62, Chapter IV]), there is α ∈ K∗ such that σ(εiα) > 0 for all i. Argue that α can be chosen to lie in OK. Then let λ = 1 + dαβ2 where d is a sufficiently large positive integer and β is a nonzero element of m0.

(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 \(\lambda\) from part (a) for a suitable choice of \(\varepsilon_i\) 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: “\(\text{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}\), then \(\text{Gal}(L/\mathbb{Q}) \simeq S_3\)” should be “\(\text{Gal}(M/K) \simeq \mathbb{Z}/3\mathbb{Z}\), then \(\text{Gal}(M/\mathbb{Q}) \simeq S_3\)”

Page 167, line 9: “\(\sigma\) is real” should be “\(\alpha\) 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 \(\ker(\pi) \subset \mathcal{O}_K^* \cdot \text{im}(\beta)\). 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 \(\gamma \equiv c \mod f\mathcal{O}_K\) for \(c \in \mathbb{Z}\) with \(\gcd(c, f) = 1\) and \(\delta \equiv 1 \mod f\mathcal{O}_K\).

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

Page 186, line –1: At the end of the display, “\(z\varphi(z)\)” should be “\(2\varphi(z)\)”

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: “\(+\frac{24G_4(L)}{z^2}\)” should be “\(-\frac{24G_4(L)}{z^2}\)”
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, “\(\sum_{f=1}^{[\mathcal{O}_K: \mathbb{Z}[a]]} h(f^2 d_K)\)” should be “\(\sum_{f \mid [\mathcal{O}_K: \mathbb{Z}[a]]} h(f^2 d_K)\)”

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
\[
q(\sigma\tau) = e^{2\pi i (a\tau + b)/d} = e^{2\pi ib/d} q^{a/d}
\]
(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 1: “\(\equiv 1\)” should be “\(= 1\)”

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: “SL(2\(\mathbb{Z}\))” should be “SL(2, \(\mathbb{Z}\))”

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

Page 220, bottom line: “\(\text{Re}(\tau) \geq 0\)” should be “\(\text{Re}(\tau) \leq 0\)”

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 form 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 $b = -2a\text{Re}(\tau)$ 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: “SL(2,\mathbb{Z}) and that” should be
“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 225, part (a) of Exercise 11.21: “Theorem 5.3” should be “Propo-
sition 5.3”

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: “$3\tau_0$” 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: “$\mathbb{Q}(\sqrt{-14})$” should be “$\mathbb{Q}(\sqrt{14})$”

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

Page 245, display (12.32): “$\sigma(f_1(\sqrt{-14}/2)^2)$” should be “$\sigma(f_1(\sqrt{-14})^2)$”

Page 245, bottom line: “$e^{2.002q}$” should be “$e^{2.004q}$”
Page 245, line 2: “$e^{2.002q}$” should be “$e^{2.004q}$”

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, “$\frac{f(\tau)^2}{\eta(\tau)^2}$” should be “$\frac{\tilde{f}(\tau)^2}{\eta(\tau)^2}$”

Page 257, part (b) of Exercise 12.23: Replace the hint with the following: “Hint: show that $f_1(\tau)^6$ is a modular function for the group $\tilde{\Gamma}(8)$ defined in Exercise 12.21. Since $\tilde{\Gamma}(8)$ is normal in $\text{SL}(2,\mathbb{Z})$, this implies that $f(\tau)^6$ is also invariant under $\tilde{\Gamma}(8)$.”

Page 258, line 3 of part (e) of Exercise 12.23: “$\sigma_1$ and $\sigma_1$” should be “$\sigma_1$ and $\sigma_2$”

Page 259, line 2: “$\mathbb{Z}[\sqrt{-2}]$” should be “$\mathbb{Z}[*\sqrt{-2}]$”

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:”

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, “$\zeta_{ab}^m$” should be “$\zeta_{-ab}^m$”

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

Page 280, lines 2 and 3 of part (d) of Exercise 13.15: “$a \mid d_1$, $a \equiv 1 \mod 4$ . . . where $d \equiv 1 \mod 4$” 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 $4ab = d_1d_2 - x^2$ to show that $4b \equiv \varepsilon dd_2 \mod a$ (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, four lines above third display: “to the” should be “to be”
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 $\sum_{0 \leq |a| \leq 2\sqrt{p}}$

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

Page 303, line 1: “$j \not\equiv 0, 17284$” should be “$j \not\equiv 0, 1728$”

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 1 of **Remark**: “The decomposition” should be “The decomposition”

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

Page 313, line −3: “$(I_L(fm) \cap P_{K, Z}(f))$” should be “$(I_K(fm) \cap P_{K, Z}(f))$”

Page 315, seven lines above **Theorem 15.16**: “Let $K$ be an imaginary quadratic field $K$” should be “Let $K$ be an imaginary quadratic field”

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 315, **Theorem 15.16**: On the second line, “$F_m$ Then” should be “$F_m$. Then” (add a period)

Page 317, fourth line of **Theorem 15.17**: In the display, the right-hand side of the equation should be “$f\tilde{T}_m(u)(\tau_0)$”

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**: “$\pm 1, 3$ 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 “$\prod^*_p$”

Page 327, lines 7 and 8: “Using the description . . . Lemma 15.27, it is easy to see that” should be “Since $x \in \hat{\mathcal{O}}^*$, $g_{\tau_0}(x)$ is easy to describe. Recall that $at_0^2 + bt_0 + c = 0$ where $a, b, c \in \mathbb{Z}$ satisfy gcd$(a, b, c) = 1$ and $a > 0$. Also, $\mathcal{O} = [1, at_0]$ and $[1, \tau_0]$ is a proper $\mathcal{O}$-ideal. As explained in [A23, §3], $g_{\tau_0}(x)$ is the transpose of the matrix representing multiplication by $x$ on $[1, \tau_0] \otimes \mathbb{Z}\hat{\mathcal{O}}$ relative to the basis $\{\tau_0, 1\}$. To get an explicit formula for $g_{\tau_0}(x)$, note that $\hat{\mathcal{O}}^* = \hat{\mathbb{Z}} + \hat{\mathbb{Z}}a\tau_0$, so $x = A + Ba\tau_0$ for $A, B \in \hat{\mathbb{Z}}$. Then a calculation similar to item (iii) in the discussion leading up to Theorem 15.17 shows that

$$g_{\tau_0}(x) = \begin{pmatrix} A - bB & -Bc \\ aB & A \end{pmatrix}.$$  

Note that”

Page 327, two lines below second display: “To prove this, . . . the map $u \mapsto \sigma_u$” should be “Write $u = [\alpha] \in (\mathcal{O}/m\mathcal{O})^*$, where $\alpha$ is relatively prime to $m$ as in the proof of Lemma 15.13. Then the exact sequence (15.14) gives $[\alpha \mathcal{O}_K] \in (I_K(fm) \cap P_{K, \mathbb{Z}}(f))/P_{K, \mathbb{Z}, m}(fm)$, which in turn
gives \( \sigma_u \in \text{Gal}(L_{\mathcal{O}_m}/L_\mathcal{O}) \) via the ideal-theoretic Artin map. The next step is to bring ideles into the picture.”

Page 327, third display: Delete the label (15.38)

Page 327, line following third display to end of the proof of Theorem 15.17: Delete and replace with the following:

The two Artin maps are related by the commutative diagram

\[
\begin{array}{ccc}
\hat{\mathcal{O}}^*/J_{\hat{\mathcal{O}},m}^3 & \xrightarrow{\text{Artin}} & \text{Gal}(L_{\mathcal{O},m}/L_\mathcal{O}) \\
(I_K(fm) \cap P_{KZ}(f))/P_{KZ,m}(fm) & \xrightarrow{\iota} & \\
\end{array}
\]

(15.38)

where \( \iota \) is defined as follows: if \( x = (x_p) \in \hat{\mathcal{O}}^* \) and \( \beta \in K^* \) satisfy \( \beta x_p \in 1 + fm\mathcal{O}_{K,p} \) for all \( p \mid fm \), then \( \iota([x]) = [\beta \mathcal{O}_K] \). Here, \( \mathcal{O}_{K,p} = \mathcal{O}_K \otimes \mathbb{Z} \mathbb{Z}_p \). Exercises 15.20 and 15.21 will give full details about the diagram (15.38).

The strategy will be to construct an idele \( x \in \hat{\mathcal{O}}_K^* \) that maps to \([\alpha \mathcal{O}_K]\) via \( \iota \), so that the Artin map to \( \text{Gal}(L_{\mathcal{O},m}/L_\mathcal{O}) \) takes \( x \) to \( \sigma_u \). Then, if \( x \) maps to \( \sigma \in \text{Gal}(K^{ab}/L_\mathcal{O}) \) via the Artin map, then

\[ \sigma_u = \sigma|_{L_{\mathcal{O},m}}. \]

To construct \( x \), observe that \( \alpha \in \mathcal{O}_p^* \) whenever \( p \mid fm \) since \( \alpha \) is relatively prime to \( fm \). Thus \( \alpha \) has an inverse \( \alpha_p^{-1} \in \mathcal{O}_p^* \) when \( p \mid fm \).

Now consider the idele \( x = (x_p) \in \hat{\mathcal{O}}^* \) where

\[ x_p = \begin{cases} 
1 & p \nmid fm \\
\alpha_p^{-1} & p \mid fm.
\end{cases} \]

Then \( p \mid fm \) implies that \( \alpha x_p = \alpha \alpha_p^{-1} = 1 \in 1 + fm\mathcal{O}_{K,p} \). By the definition of \( \iota \), it follows that \( \iota([x]) = [\alpha \mathcal{O}_K] \), so the Artin map to \( \text{Gal}(L_{\mathcal{O},m}/L_\mathcal{O}) \) takes \( x \) to \( \sigma_u \).

Now take \( f \in F_m \) such that \( f(\tau_0) \) is defined. Then \( f(\tau_0) \in L_{\mathcal{O},m} \) by Theorem 15.16, so that by Shimura reciprocity (Theorem 15.12), we have

\[ \sigma_u(f(\tau_0)) = \sigma(f(\tau_0)) = f^{g_{\tau_0}(x^{-1})}(\tau_0). \]

However, \( f \in F_m \) implies that \( f^{g_{\tau_0}(x^{-1})} \) depends only on \( g_{\tau_0}(x^{-1}) \) modulo \( m \). Recall from the proof of Theorem 15.16 that \( g_{\tau_0}(x^{-1}) \) is the transpose of the matrix representing multiplication by \( x^{-1} \) on \([1, \tau_0] \otimes \mathbb{Z} \hat{\mathbb{Z}}\) relative to the basis \( \{\tau_0, 1\} \).
The definition of $x$ easily implies that $x^{-1} = ((x^{-1})_p)$ is given by

$$(x^{-1})_p = \begin{cases} 1 & p \nmid fm \\ \alpha & p \mid fm, \end{cases}$$

which means that via the isomorphism (15.37), multiplication by $x^{-1}$ on $[1, \tau_0] \otimes \hat{\mathbb{Z}}$ reduces to multiplication by $u = [\alpha]$ on $[1, \tau_0] \otimes \mathbb{Z}/m\mathbb{Z}$. The discussion leading up to Theorem 15.17 shows that $\overline{\gamma}_{\tau_0}(u) \in \text{GL}(2, \mathbb{Z}/m\mathbb{Z})$ is the transpose of the matrix representing this map relative to the basis $\{\tau_0, 1\}$. It follows immediately that $g_{\tau_0}(x^{-1})$ reduces modulo $m$ to $\overline{\gamma}_{\tau_0}(u)$. Thus $\sigma_u(f(\tau_0)) = f^{\overline{\gamma}_{\tau_0}(u)}(\tau_0)$, completing the proof of Theorem 15.17.

Page 328, line immediately above Exercise 6. Exercises: “suprisingly” should be “surprisingly”.

Page 329, 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: “$\gamma_p \in \prod_p \text{GL}(2, \mathbb{Z}_p)$” should be “$\gamma_p \in \text{GL}(2, \mathbb{Z}_p)$”

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

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

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

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

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

Page 331, Exercise 15.15: Replace the existing parts (b), (c) with new parts (b), (c), (d) as follows:

(b) Prove that $K^* \subset \hat{K}^*$ is discrete. By a standard result for Hausdorff topological groups, this implies that $K^*$ is closed in $\hat{K}^*$ (see Proposition 12 of §2.3 of Introduction to Topological Groups by T. Husain, Saunders, Philadelphia, 1966). Hint: first show that $K^* \cap \prod_p \mathcal{O}_{K_p}^{*} = \mathcal{O}_{K}^{*}$.
(c) Use parts (a) and (b) to prove that $\bigcap_m (K^*\mathfrak{m}_K^m/K^*) = K^*(\mathbb{C}^* \times \{1\})/K^*$. Hint: note that the sets $\prod_p U^m_p$ form a neighborhood basis of the identity as we vary over all moduli $m = \prod_p p^{p^m}$.

(d) Theorems 7.1 and 7.3 of [80, §IV.7] imply that for every modulus $m$, there is a finite extension $K_m$ such that $\Phi_K^{-1}(\text{Gal}(K^{ab}/K_m)) = K^*\mathfrak{m}_K^m/K^*$ via the Artin map $\Phi_K : \mathcal{C}_K = \mathfrak{I}_K/K^* \to \text{Gal}(K^{ab}/K)$. Use this and part (b) to show that the kernel of $\Phi_K$ is given by $K^*(\mathbb{C}^* \times \{1\})/K^*$.

---

Page 331, Exercise 15.15: Relabel the existing part (d) as part (c).

Page 331, final paragraph of Exercise 15.15: In the first three lines of this paragraph, replace “The idelic version of . . . an Abelian extension $K_m$ of $K$, called the” with “The Abelian extension $K_m$ of $K$ defined in part (d) is called the”.

Page 331, Exercise 15.16: Replace the entire exercise with the following:

**Exercise 15.16.** This problem concerns the isomorphism (15.34).

(a) The text defines $\hat{K} = K \otimes \mathbb{Z}$ and uses $K \otimes \mathbb{Z} \mathfrak{p} \simeq \prod_{\mathfrak{p} \not\mid m} K_{\mathfrak{p}}$ to show that $\hat{K}^* \simeq \prod_{\mathfrak{p}}^* K_{\mathfrak{p}}^*$ in Exercise 15.12. In a similar way, there is an isomorphism $\mathcal{O}_K \otimes \mathbb{Z} \mathfrak{p} \simeq \prod_{\mathfrak{p}} \mathcal{O}_{K_{\mathfrak{p}}}$ by [A20, Chapter II, Proposition 4]. Use this to prove that for $\hat{\mathcal{O}}_K = \mathcal{O}_K \otimes \mathbb{Z}$, there is an isomorphism $\hat{\mathcal{O}}_K^* \simeq \prod_{\mathfrak{p}} \mathcal{O}_{K_{\mathfrak{p}}}^*$.

(b) Consider the following construction that associates a fractional ideal $x \mathcal{O}_K$ to an idele $x \in \prod_{\mathfrak{p}} K_{\mathfrak{p}}^*$. Given $x = (x_{\mathfrak{p}})$, note that $x_{\mathfrak{p}} \in \mathfrak{p}^n_{\mathfrak{p}}(x) \mathcal{O}_{K_{\mathfrak{p}}}^*$ for a unique $n_{\mathfrak{p}}(x) \in \mathbb{Z}$, where only finitely many $n_{\mathfrak{p}}(x)$ are nonzero. Then define $x \mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}(x)}$. Prove that $a = x \mathcal{O}_K$ satisfies $a \otimes \mathbb{Z} = x \hat{\mathcal{O}}_K$.

(c) Prove that the map $x \mapsto [x \mathcal{O}_K] \in C(\mathcal{O}_K)$ induces an isomorphism $\hat{K}^*/K^*\hat{\mathcal{O}}_K^* \simeq C(\mathcal{O}_K)$. Also show that this isomorphism agrees with the map defined in the discussion following (15.34). Hint: The $x$ constructed in Lemma 15.23 is unique up to multiplication by an element of $\hat{\mathcal{O}}_K^*$.

Page 331, Exercise 15.17: Relabel the existing part (b) as part (c) and add the following new part (b):

(b) Prove that $P_{K,1}(m) = \{\delta \mathcal{O}_K : \delta \in K^*, \delta \equiv 1 \mod m\}$. Hint: in §8, $P_{K,1}(m)$ is defined to be $\{(\alpha_0/\beta_0)\mathcal{O}_K : \alpha_0, \beta_0 \in \mathcal{O}_K, \alpha_0 \equiv \beta_0 \mod m\}$.
\[ \beta_0 \equiv 1 \mod m \}\). The exact sequence from part (a) of Exercise 8.1 will be useful.

Page 332, line 1: “\( \beta x \equiv 1 \mod m \) for all \( p | m \)” should be “\( \beta x \equiv 1 \mod m \) as defined above”

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

Page 332, Exercise 15.20: Delete the existing exercise and replace with the following:

**Exercise 15.20.** Fix a modulus \( m \). In [80, Chapter IV, Proposition (8.2)], Neukirch constructs a commutative diagram

\[
\begin{array}{ccc}
I_K^\text{fin}/K^*I_K^\text{fin} & \xrightarrow{\text{Artin}} & \text{Gal}(K_m/K) \\
\kappa_m \downarrow & & \downarrow \\
I_K(m)/P_{K,1}(m) & \xrightarrow{\text{Artin}} & \\
\end{array}
\]

where \( \kappa_m \) has the property that \( \kappa_m([x]) = [xO_K] \) whenever \( x = (x_p) \in I_K^\text{fin} \) satisfies \( x_p = 1 \) for all \( p | m \). Prove that \( \kappa_m \) equals the map defined in Exercise 15.17. Hint: for a prime \( p \) of \( O_K \) not dividing \( m \), let \( \pi_p \in O_{K_p} \) satisfy \( \pi_p O_{K_p} = pO_{K_p} \). Define \( x(p) \in I_K^m \) to be the idele that has \( \pi_p \) in position \( p \) and 1 in all other positions.

Page 333, Exercise 15.21: Delete the existing exercise and replace with the following:

**Exercise 15.21.** This exercise concerns the diagram (15.38). Fix an order \( \mathcal{O} \subset O_K \) of conductor \( f \) and a positive integer \( m \), and recall the subgroups \( J_{fm} \subset J_{\mathcal{O},m} = K^*J_{\mathcal{O},1,m} \subset \hat{K}^* \) defined in Exercise 15.18.

(a) For \( m = fmO_K \), combine the isomorphism \( \kappa_{fm} : I_K^\text{fin}/K^*I_K^\text{fin,fm} \simeq I_K(fm)/P_{K,1}(fm) \) from Exercise 15.20 with the isomorphism \( \hat{K}^*/J_{fm} \simeq I_K^\text{fin}/K^*I_K^\text{fin,fm} \) from Exercise 15.18 to create a commutative diagram

\[
\begin{array}{ccc}
K^*/\hat{\mathcal{O}}^*/K^*J_{\mathcal{O},m} & \xrightarrow{\text{Artin}} & \text{Gal}(L_{\mathcal{O},m}/L_{\mathcal{O}}) \\
\kappa \downarrow & & \downarrow \\
(I_K(fm) \cap P_{K,z}(f))/P_{K,z,m}(fm) & \xrightarrow{\text{Artin}} & \\
\end{array}
\]

where \( \kappa \) is an isomorphism.

(b) Combine part (a) with the natural map \( \hat{\mathcal{O}}^*/J_{\mathcal{O},m} \rightarrow \hat{\mathcal{O}}^*/K^*J_{\mathcal{O},m} \) to show that the map \( \iota \) defined in the proof of Theorem 15.17 gives the commutative diagram (15.38).
Page 333, Exercise 15.22: “$\zeta_m j(\tau) \in F_m$” should be “$\zeta_m \in F_m$.”

Page 333, Exercise 15.24, end of the sentence: Add two new sentences
“The example following Theorem 15.16 characterized $p = x^2 + y^2$ with $x \equiv 1 \mod 5, y \equiv 0 \mod 5$ using the extended ring class field $L_{O,5}$. Here we explore this example from some other points of view.”

Page 333, Exercise 15.24: Add new parts (c), (d), (e) as follows:

(c) Show that for $p > 5$, $x^4 + x^3 + x^2 + x + 1 \equiv 0 \mod p$ has a solution if and only if $p \equiv 1 \mod 5$, and conclude that for a prime $p$,
$$p = x^2 + y^2, x \equiv 1 \mod 5, y \equiv 0 \mod 5 \iff p \equiv 1 \mod 20.$$

(d) Prove the equivalence of part (c) using Proposition 5.21 and the Artin map (8.4). Hint: see part (a) and the solution to Exercise 15.7.

(e) Give an elementary proof of the equivalence of part (c).