Typographical Errors in the Second Edition of

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

April 15, 2021

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

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$(\chi)$ ∈ $(\mathbb{Z}/D\mathbb{Z})^*$” should be “ker$(\chi)$ ⊂ $(\mathbb{Z}/D\mathbb{Z})^*$”

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 $\leq 2$ in $G$” should be “if and only if $a$ or $b$ has order $\leq 2$ 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 $p \equiv 1, 7 \mod 8$. 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 $p \equiv 1 \mod 8$) and $2x^2 + xy + ((1 + p)/8)y^2$ of discriminant $−p$ (when $p \equiv 7 \mod 8$). 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 $\pi$ be prime in $\mathbb{Z}[\omega]$” should be “Let $\pi$ be prime of $\mathbb{Z}[\omega]$ not associate to $1-\omega$”

Page 82, line 2 of Exercise 4.18: “$\pi$ is prime in $\mathbb{Z}[i]$” should be “$\pi$ 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 $p$” with “$f_i(x)$ are monic, and distinct and irreducible modulo $p$”

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: “$p\mathcal{O}_L + f_i(\alpha)\mathcal{O}_K$” should be “$p\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$”

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

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, $p$ 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:
\[
\begin{array}{c}
L \\
\| \\
M \\
\| \\
K \\
\| \\
Q \\
\end{array}
\]

(6.3)

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 \(O_{LM}\) 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 \(\mathfrak{P} \cap O_L\) and \(\mathfrak{P} \cap O_M\) 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): “\(u \in O\)” should be “\(u \in O_K\)”

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: “\(a = [\alpha, \beta]\) 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 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. However, we have isomorphisms

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

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

\[
\left( \frac{p^*}{q} \right) = \left( \frac{a}{p} \right),
\]

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 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 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/L = 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 165, line 1: “Lemma 5.21” should be “Corollary 5.21”

Page 167, line 3: “Gal(L/K) ≃ Z/3Z, then “Gal(L/Q) ≃ S_3” should be “Gal(M/K) ≃ Z/3Z, then “Gal(M/Q) ≃ S_3”

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

Page 169, line 1: Replace with “If π = a + bi is a primary prime of Z[i], then”

Page 169, third display: “IK(6)/PK,Z(6)” should be “IK(6)/PK,1(6)”

Page 186, line –1: At the end of the display, “zφ(z)” should be “2φ(z)”
Page 192, 4 lines below (10.19): “±(z + w_i)” should be “±(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}[\alpha]]} h(f^2d_K)” should be “…\sum_{f \mid [\mathcal{O}_K:\mathbb{Z}[\alpha]]} h(f^2d_K)”

Page 203, line −14: “γ ≠ ±1” should be “γ ≠ ±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 12: “some prime ideal of \mathcal{O}” should be “some prime ideal of \mathcal{O}_K”

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: “Re(\tau) ≥ 0” should be “Re(\tau) ≤ 0”

Page 221, second display: The display should be

\[ |b| ≤ a ≤ c, \text{and } b ≥ 0 \text{ if either } |b| = a \text{ or } a = c. \]

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 224, Exercise 11.14: “mod p” should be “mod 1 – \zeta_p”

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: “\( 3\tau_0 \)” 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: “\( \zeta_d^a q^{a/d} = \zeta_b^a (q^{1/8})^a q^n \)” should be “\( \zeta_d^b q^{a/d} = \zeta_d(q^{1/8})^a q^n \)” (three errors)

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

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, “\( \frac{f(\tau)^2}{\eta(\tau)^2} \)” should be “\( \frac{f(\tau)^2}{\eta(\tau)^2} \)”
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, part (b)(iii) of Exercise 12.28: In the Hint, “implies $c = 3$” should be “implies $b = c = 1$”.

Page 260, part (c)(iii) of Exercise 12.28: Replace the hint with the following: “Hint: Analyze $\gcd(p^2 + 3q^2, 2pq)$ and use the formula for $\frac{a}{k}$ to conclude that $2n \geq p^2 + 3q^2$. Also note that the result of (ii) implies $p^2 + 3q^2 = u^2 - 3tu + 3t^2$ and recall that $n$ divides $b$.”

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 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 278, part (b) of Exercise 13.6: In four places, “$\zeta_{abm}$” should be “$\zeta_{-abm}$”

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

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 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 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, Exercise 14.15: “discriminant” should be “conductor”

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, 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: “$\pm 1$, 3 and $1 + \sqrt{-m}$” should be “$-1$, 3 and $1 + \sqrt{-m}$”

Page 318, display (15.19): “$m \equiv 6 \text{ mod } 8$” should be “$m \equiv 6 \text{ mod } 8$ and $3 \nmid m$”

Page 318, two lines below display (15.19): “$m \equiv 3 \text{ mod } 8$” should be “$m \equiv 3 \text{ mod } 4$ 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 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: “$\gamma_p \in \prod_p \GL(2, \mathbb{Z}_p)$” should be “$\gamma_p \in \GL(2, \mathbb{Z}_p)$”

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: “$\sqrt[6]{-m}$” should be “$\sqrt[6]{-m}$”

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: “$p^p x$” should be “$p^p x_p$”