Typographical Errors in the Second Edition of

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

May 9, 2020

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$(\chi) \in (\mathbb{Z}/D\mathbb{Z})^*$” 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 $\leq 2$ in $G$” should be “if and only if $a$ or $b$ has order $\leq 2$ in $G$”

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 65, part (c) 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 75, line 18: “the second memoir. Gauss” should be “the second memoir, Gauss” (the period should be a comma)

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 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, “$I_1 \cdots I_g \subset p\mathcal{O}_L$” should be “$(p\mathcal{O}_L)^g \subset I_1 \cdots I_g \subset p\mathcal{O}_L$”

Page 105, part (d) of Exercise 5.7: It should be “Prove the description of $\mathcal{O}_K$ given in (5.14)”
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, line −4: “\( [b][c]^{-1} \)” should be “\( \pm [b][c]^{-1} \)”

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

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

\[
(\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/2p\mathbb{Z})^* \xrightarrow{\sim} I_q(2p \infty)/P_{q,1}(2p \infty),
\]

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 \( [a\mathbb{Z}] \in I_q(2p \infty)/P_{q,1}(2p \infty) \) 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 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 161, Exercise 8.13, last line: “\(N_{\mathbb{P}}M = M\)” should be “\(N_{\mathbb{P}}M = N_{\mathbb{P}}\)”

Page 161, Exercise 8.16, line 2: “\(\tilde{S}_{M/L}\)” should be “\(\tilde{S}_{M/K}\)”

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: “\(\text{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}\), 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 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: In the display, \[ \sum_{f} h(f^2d_K) \] should be \[ \sum_{f \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]} h(f^2d_K) \]

Page 203, line -14: \( \gamma \neq \pm 1 \) should be \( \gamma \neq \pm I \)

Page 208, line 10: The display should be 
\[ q(\sigma \tau) = e^{2\pi i (\alpha \tau + b) / d} = e^{2\pi i b / d} q^{a / d} \]
(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 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(\( \tau \)) \geq 0” should be “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 (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, \text{ and 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 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: “Q(\sqrt{-14})” should be “Q(\sqrt{-14})”

Page 241, bottom line: “c_d a^q/d = c_b (q^{1/8})^{a^2}” should be “c_d a^q/d = c_b (q^{1/8})^{a^2}” (three errors)

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

Page 250, bottom line: The display should be “S\left(\begin{array}{cc} a & b \\ c & c \end{array}\right) = \left(\begin{array}{cc} a & c \\ -c & a \end{array}\right)”

Page 251, line 2: The display should be “T^{\pm 1}\left(\begin{array}{cc} a & b \\ c & c \end{array}\right) = \left(\begin{array}{cc} a \pm c & * \\ c & * \end{array}\right)”

Page 251, bottom line: “γ_3(3τ)” should be “γ_2(3τ)”

Page 255, part (a) of Exercise 12.14: On the last line of the display, “f(τ)^2/η(τ)^2” should be “f(τ)^2/η(τ)^2”

Page 257, part (b) of Exercise 12.23: Replace the hint with the following: “Hint: show that f_1(τ)^6 is a modular function for the group \tilde{Γ}(8) defined in Exercise 12.21. Since \tilde{Γ}(8) is normal in SL(2, Z), this implies that f(τ)^6 is also invariant under \tilde{Γ}(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 (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{n}{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/α) and Q = \sqrt{7/2}(α/2)” should be “Prove that P = \sqrt{14}/α and Q = \sqrt{7/2}α”

Page 268, line 1: “compute HD(X)” should be “compute HD(X) for most D”

Page 268, line -15: “compute any HD(X)” should be “compute HD(X) for any D \neq -3k^2, k odd”
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: “congrunce” should be “congruence”.

Page 281, line 1 of part (e) of Exercise 13.16: “$\epsilon(p) = 1$” should be “$\epsilon(p) = −1$”.

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