Typographical Errors in the first edition softcover of

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

*May 13, 2013*

All of these typos were corrected in the Second Edition of the book, published in 2013.

Page 7, lines 2–3: Replace “three theorems of Fermat” with “three theorems of Fermat for odd primes $p$”

Page 14, line 5: Replace “are of some” with “are some”

Page 16, line 16: Replace “incongruent squares modulo $4N$” with “incongruent squares modulo $4N$ relatively prime to $4N$”

Page 21, Exercise 1.7: Replace “to prove the” with “to prove that”

Page 28, line –18: Replace “$f(p, q)$” and “$f(r, s)$” with “$f(p, r)$” and “$f(q, s)$” respectively

Page 28, line –17: Replace “$(p, q)$” and “$(r, s)$” with “$(p, r)$” and “$(q, s)$” respectively

Page 33, line 6: Replace “29” with “39”

Page 33, line –8: Remove the period at the end of the display

Page 33, line –7: Add “when $p \neq 5$ is odd.” at the beginning of the line

Page 34, line 1: Add “when $p \neq 7$ is odd” at the beginning of the line

Page 35, line 5: Replace “numbers” with “at least one number”

Page 46, line 1 of Exercise 2.24: Replace “is” with “in”

Page 49, line –12: Replace “$X = xz - Czw$” with “$X = xz - Cyw$”

Page 56, lines 2 and 4: In both products, replace “$1 = i$” with “$i = 1$” (two errors)

Page 56, line –2: Replace “in map” with “in the map”

Page 58, line –3: Replace “analagous” with “analogous”

Page 64, line 22: Replace “statment” with “statement”

Page 68, line –8: Replace “$H_1 = H \cap (\mathbb{Z}/)$” with “$H_1 = H \cap ((\mathbb{Z}/)$

Page 70, line 7 of part (d) of Exercise 3.13: Replace “$(x, y) = (0, 4)$” with “$(x, y) = (0, 2)$”

Page 76, line 13: Relace “an one-to-one” with “a one-to-one”

Page 78, line 4: Replace “the that” with “that”

Page 84, line 6: Replace “statment” with “statement”

Page 87, line 16: Replace “Bachman” with “Bachmann”

Page 93, line 1 of Exercise 4.28: Replace “$\zeta^{\mu_1 + \cdots + \mu_f}$” with “$\zeta^{\mu_1 + \cdots + \mu_f}$”

Page 94, display of part (f) of Exercise 4.29: Replace “$-4$” with “+4”

Page 94, line 2 of part (g) of Exercise 4.29: Replace “use (e)” with “use (f)”

Page 103, line 2: Replace “apply apply” with “apply”
7.15. Let $M = \mathbb{Z}^2$ and let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an integer matrix with $\det(A) = ad - bc \neq 0$. Writing $M = [e_1, e_2]$, note that $AM = [ae_1 + ce_2, be_1 + de_2]$. Our goal is to prove that $|M/AM| = |\det(A)|$.

(a) Show that the result is true when $c = 0$. Hint: Use the division algorithm to write an element of $M$ as $ue_1 + ve_2 + w(be_1 + de_2)$ where $u, v, w \in \mathbb{Z}$ and $0 \leq v < |d|$.

(b) Let $B \in \text{GL}(2, \mathbb{Z})$. Show that the result is true for $A$ if and only if it is true for $BA$. Hint: Use the automorphism of $M$ induced by $B$.

(c) Explain how to find $B \in \text{GL}(2, \mathbb{Z})$ such that $BA = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Hint: If $c \neq 0$, prove there exists $B \in \text{GL}(2, \mathbb{Z})$ so that $BA = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ with $|c'| < |c|$. This is easy to do when $|a| < |c|$ (swap rows), and not difficult when $|a| \geq |c|$ (dividing $a$ by $c$ tells you which row operation puts you in the easy case).

(d) Conclude that $|M/AM| = |\det(A)|$.

Page 158, display (*): Replace with $h(d_K) > \frac{\log |d_K|}{7000} \prod_{p|d_K} \left(1 - \frac{[2\sqrt{p}]}{p + 1}\right)$.
Page 161, line –6: replace “not dividing \( m \)” with “not dividing \( m \)”

Page 173, line 16: Replace “\( x_p \in \mathcal{O}_{K_p} \)” with “\( x_p \in \mathcal{O}_{K_p}^* \)”

Page 173, line 18: Replace “[80, §V.2]” with “[80, §IV.2]”

Page 183, line 14: Replace “there is an ideal” with “\( p \) is unramified in \( M \) and there is a prime”

Page 186, fourth line of the proof of Theorem 9.8: Replace “once once” with “once one”.

Page 195, line 4: Replace “\( b > 0 \)” with “\( b \geq 0 \)”

Page 196, part (c) of Exercise 9.21: Replace “Hint: This” with “Hint: this”

Page 197, part (a) of Exercise 9.22: Delete “where \( p \) is the unique integer prime contained in \( p \). Also, in the display, replace the comma at the end with a period.

Page 197, part (b) of Exercise 9.22: Replace “Note that \( N(p) = p \) or \( p^2 \), where \( p \) is the unique integer prime contained in \( p \)” with “Note that \( N(p) = p \) or \( p^2 \), where \( p \) is the unique integer prime contained in \( p \)”.

Page 206, line 1: Replace “\( f(\lambda z) \)” with “\( f(\lambda^{-1}z) \)”

Page 210, proof of Lemma 10.17: Replace “This proof” with “The proof”

Page 211, line 15: Replace “\( w_j - w_i \)” with “\( -w_j - w_i \)”

Page 216, part (b) of Exercise 10.2: Replace “\( \mathbb{Z} \in L \)” with “\( \omega \in L \)”

Page 220, line –2: Replace “\( z \equiv z' \bmod \mathbb{P} \)” with “\( z \equiv z' \bmod L \)”

Page 221, line –2: Replace “\( (\begin{smallmatrix}a & c \\
     b & d \end{smallmatrix}) \)” with “\( (\begin{smallmatrix}a & b \\
     c & d \end{smallmatrix}) \)”

Page 221, line 11: Replace “from in §7” with “from §7”

Page 223, line 8: Replace “\(|\text{Im}(\tau)|\)” with “\(\text{Im}(\tau)\)”

Page 226, line 6: Replace “of a such” with “of such”

Page 227, lines 6 and –15: Replace “\(|\text{Im}(\tau)|\)” with “\(\text{Im}(\tau)\)” (two errors)

Page 239, line 9: Replace “\( S_{L/K} \)” with “\( S_{L/Q} \)”

Page 242, line 1 of Exercise 11.3: Replace “\(|\text{Im}(\tau)|\)” with “\(\text{Im}(\tau)\)”

Page 243, line 2 of Exercise 11.4: Replace “\(|\text{Im}(\tau)|\)” with “\(\text{Im}(\tau)\)”

Page 245, line 4 of Exercise 11.9: Replace “the the” with “the”

Page 244, line 2 of part (a) of Exercise 11.5: Replace “\(|\text{Im}(\tau)|\)” with “\(\text{Im}(\tau)\)”

Page 247, line 1 of part (c) of Exercise 11.16: Replace “prove that that” with “prove that”

Page 250, line 3: Replace “\( -e^{-\eta_2\tau/2} \)” with “\( -e^{-\eta_2\tau/2} \)”

Page 250, line 4: Replace “\( e^{\eta_2(\tau+1)/2} \)” with “\( e^{\eta_2(\tau+1)/2} \)”

Page 260, line –1: Replace “\(-11, -16\)” with “\(-11, -12, -16\)”

Page 269, line 9: Replace “\( f_1(\sqrt{-14})^2 \)” with “\( f_1(\sqrt{-14})^2 \)”

Page 272, line 7: Replace “\( \alpha = \zeta_8 \tau_2(\tau_0)^2 \)” with “\( \alpha = \zeta_8^{-1} \tau_2(\tau_0)^2 \)”.

3
Page 278, line –3: Replace “$e^{-\eta^2 \tau/2}$” with “$-e^{-\eta^2 \tau/2}$”
Page 278, line –2: Replace “$e^{\eta^2 (\tau+1)/2}$” with “$-e^{\eta^2 (\tau+1)/2}$”
Page 279, part (c) of Exercise 12.13: Replace “holmorphic” with “holomorphic”
Page 280, Exercise 12.18: Replace “table 12.20” with “table (12.20)”
Page 282, parts (c), (d), (e) of Exercise 12.23: Replace “$f(\sqrt{-m})^6$” with “$f(\sqrt{-m})^6$” (three errors)
Page 282, line 2 of part (f) of Exercise 12.23: Replace “[4, $\frac{3}{16}$ + $\sqrt{-m}$]” with “[4, $\frac{3}{16}$ + $\sqrt{-m}$]”
Page 294, two lines below the proof of Proposition 13.14: Replace “First note by” with “First note that by”
Page 296, line 18: Replace “§21” with “§12”
Page 298, line –9: Replace “$1 + \sum_{n=1}^{\infty} \sigma_3(n)q^n$” with “$1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n$”
Page 298, display (13.20): Add at period at the end of the last line of the display
Page 298, line –8: Replace “neither $K_1$ or $K_2$” with “neither $K_1$ nor $K_2$”
Page 302, line 8: Replace “$p \equiv 2 \mod p$” with “$p \equiv 2 \mod 3$”
Page 304, part (a) of Exercise 13.7: Replace “$r(-12) = 1$” with “$r(-12, 3) = 1$”
Page 305, line 2 of Exercise 13.12: Replace “$1 + \sum_{n=1}^{\infty} \sigma_3(n)q^n$” with “$1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n$”
Page 305, line 3 of Exercise 13.12: Replace “$(1 - q^n)$” with “$(1 - q^n)^{24n}$”
Page 307, line 4: Replace “$\epsilon(m)$” with “$\epsilon(n)$”
Page 309, line –4: Replace “from the from the” with “from the”
Page 309, line –2: Replace “uniformization” with “the uniformization”
Page 311, first line of (14.6): Replace “$-\frac{1}{4}$” with “$+\frac{1}{4}$”
Page 312, first line of (14.7): Replace “$-x_1 - x_2 - \frac{1}{16}$” with “$-2x_1 + \frac{1}{16}$”
Page 312, line –2: Replace “induces a group” with “a group”
Page 314, line 15: Replace “$\mathrm{End}_K$” with “$\mathrm{End}_K(E)$”
Page 314, lines –12, –11: Replace “$\ker(\alpha) : E(\mathbb{C}) \to E(\mathbb{C})$” with “the kernel of $\alpha : E(\mathbb{C}) \to E(\mathbb{C})$”
Page 318, lines 8 and 9: Replace “see Lang [73, Chapter 13, Theorems 13 and 14]” with “Lemma 8.1 of K. Rubin and A. Silverberg, Point counting on reductions of CM elliptic curves, J. Number Theory 129 (2009), 2903–2923”. I would like to thank Alice Silverberg for this reference.
Page 318, line –2: Replace “an application” with “an application”
Page 319, line –6: Replace “$c \in \mathcal{O}_L$” with “$c \in \mathcal{O}_{L'}$” and replace “$j(E)$” with “$j(E_c)$”
Page 321, lines 4–5: Delete the sentence “Replacing . . . separable”
Page 321, lines 8–15: Delete and replace with the following new material:
\[ \phi \circ \lambda \in \text{End}_{\mathbb{F}_p}(E), \text{ which is commutative since } E \text{ is ordinary. Thus } \text{Frob}_p \circ (\phi \circ \lambda) = (\phi \circ \lambda) \circ \text{Frob}_p, \text{ so that } \phi \circ \lambda \text{ is defined over } \mathbb{F}_p. \text{ Then, given } \sigma \in \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p), \text{ we have } \]
\[ \phi^\sigma \circ \lambda = \phi^\sigma \circ \lambda^\sigma = (\phi \circ \lambda)^\sigma = \phi \circ \lambda, \]
where the last equality holds since \( \phi \circ \lambda \) is defined over \( \mathbb{F}_p \). Since isogenies are surjective over \( \mathbb{F}_p \), it follows easily that \( \phi^\sigma = \phi \). This is true for all \( \sigma \in \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \), which implies that the isomorphism \( \phi : E' \to E \) is defined over \( \mathbb{F}_p \). Q.E.D.

I am grateful to Reinier Bröker for suggesting this argument.

Page 324, line 5: Replace “give us factor” with “give us a factor”
Page 324, two lines below first display: Replace “where is running” with “where the running”
Page 324, line –6: Replace “\( l > 13 \)” with “\( l > 33 \)”
Page 325, line 13: Replace “\( l > 13 \)” with “\( l > 33 \)”
Page 325, line –2: Replace “is a very special” with “is very special”
Page 330, line 2 of Exercise 14.1: Replace “\((x, y, z, )\)” with “\((x, y, z)\)”
Page 331, part (b) of Exercise 14.5: Replace “see 10.13” with “see (10.13)”
Page 332, part (b) of Exercise 14.13: Replace “\((3x, 9(1 - y), 1 + y)\)” with “\((3x, 9(z - y), z + y)\)”
Page 333, line 2 of Exercise 14.19: Replace “usual” with “usual”
Page 334, line 1 of Exercise 14.21: Replace “show when” with “show that when”
Page 338, Reference 49: Replace “as der Theorie” with “aus der Theorie”
Page 345, Index entry for Discriminant: Replace “of a field, see Field” with “of a quadratic field, see Field, quadratic”