Typographical Errors in the softcover edition of

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

July 19, 2007

Page 33, line 6: Replace "29" with "39"

Page 64, line 22: Replace "statment" with "statement"

Page 68, line −8: Replace "$H_1 = H \cap (\mathbf{Z}/$" with "$H_1 = H \cap ((\mathbf{Z}/$"

Page 84, line 6: Replace "statment" with "statement"

Page 111, line 1 of the proof of Proposition 5.29: Replace "By Lemma 5.28, L is Galois over $\mathbf{Q}$, and thus" with "By hypothesis, L is Galois over $\mathbf{Q}$. Thus"

Page 148, line −1: Replace this line with

$$h(d_K) = \frac{-w}{2|d_K|} \sum_{n=1}^{|d_K|-1} \left(\frac{d_K}{n}\right) n, \quad w = \#\text{roots of unity in } \mathcal{O}_K, \tag{7.29}$$

Page 149, third display: Replace the display with "$h(d_K) > \dfrac{\log |d_K|}{7000} \displaystyle\prod_{p|d_K} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right)$,"

Page 150, line −2: Replace "Use (c)" with "Use (b)".

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 221, line −11: Replace "from in §7" with "from §7"

Page 260, line −1: Replace "$-11, -16$" with "$-11, -12, -16$"

Page 272, line 7: Replace "$\alpha = \zeta_8 \mathfrak{f}_2(\tau_0)^2$" with "$\alpha = \zeta_8^{-1} \mathfrak{f}_2(\tau_0)^2$".

Page 279, part c of Exercise 12.13: Replace "holmorphic" with "holomorphic'

Page 296, line 18: Replace "§21" with "§12"

Page 296, 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 302, line 8: Replace "$p \equiv 2 \bmod p$" with "$p \equiv 2 \bmod 3$"

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 321, lines 4–5: Delete the sentence "Replacing ... separable"

Page 321, lines 8–15: Delete and replace with the following new material. I am grateful to Reinier Bröker for suggesting this argument.

$\phi \circ \lambda \in \mathrm{End}_{\overline{\mathbf{F}}_p}(E)$, which is commutative since E is ordinary. Thus $Frob_p \circ (\phi \circ \lambda) = (\phi \circ \lambda) \circ Frob_p$, so that $\phi \circ \lambda$ is defined over $\mathbf{F}_p$. Then, given $\sigma \in \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$, 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 $\mathbf{F}_p$. Since isogenies are surjective over $\overline{\mathbf{F}}_p$, it follows easily that $\phi^\sigma = \phi$. This is true for all $\sigma \in \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$, which implies that the isomorphism $\phi : E' \to E$ is defined over $\mathbf{F}_p$. Q.E.D.