Typographical Errors in the First Printing of

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

January 28, 2009

Page 15, line 8: Replace "$(-1)^{(p-1)/2}$" with "$(-1)^{(p-1)/2}p$".

Page 16, third line of the statement of Lemma 1.14: Replace "not dividing N" with "not dividing D".

Page 17, line 3: Replace "$\left(\frac{N}{n}\right)$" with "$\left(\frac{N}{m}\right)$".

Page 23, line 7: Replace "$(-1)^{(p-1)/2}$" with "$(-1)^{(q-1)/2}q$".

Page 25, line 13: Replace "$(f(p,s) + f(r,q))xy$" with "$(2apr + bps + brq + 2cqs)xy$".

Page 26, second line of the proof of Lemma 2.5: Replace "$2bxy$" with "bxy".

Page 28, line -10: Replace "earliers" with "earlier".

Page 32, line 6: Replace "$r \geq 6$" with "$s \geq 6$".

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

Page 33, line -2: Replace "29" with "39".

Page 35, line -4: Replace "Gauss," with "Gauss".

Page 35, line -2: Replace "odd or even" with "even or odd".

Page 36, top formula of (2.28): Replace "mod 12" with "mod 24".

Page 39, lines -18 and -17: Replace "Lagrange" with "Legendre".

Page 39, line -1: Replace "Theoremé Generalé" with "Théorème General".

Page 40, line 11: Replace "Theoremé" with "Théorème".

Page 40, line 20: Replace "It's" with "Its".

Page 40, line -7: Replace "one Legendre's" with "one of Legendre's".

Page 42, line 10: Replace "$C = 5x^2 + 6xy + 10y^2$" with "$C = 5x^2 + 4xy + 9y^2$ ".

Page 45, line -2: Replace "$(x^{4k} - 1)^2 + 2x^{4k}$" with "$((x^{2k} - 1)^2 + 2x^{2k})(x^{4k} - 1)$"

Page 49, line 9: Replace "$2Bxy$" with "Bxy".

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

Page 54, line -7: Replace "2^{μ}" with "$2^{\mu-1}$".

Page 55, line -5: Replace "$m \in 1$" with "$m \geq 1$".

Page 60, line -6: Replace "37,38" with "37,58".

Page 63, line 21: Replace "Reiger" with "Rieger".

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

Page 68, part (i) of Exercise 3.11 (b): Replace "$H \cap (\{1\} \times (\mathbf{Z}/m\mathbf{Z})^*)$" with "$H \cap ((\mathbf{Z}/2^{a+2}\mathbf{Z})^* \times \{1\})$".

Page 69, first line of part (a) of Exercise 3.12: Replace "can classified" with "can be classified".

Page 71, line 6: Replace "Lemma 2.5" with "Lemma 2.3".

Page 73, line 9: Replace "Exercise" with "Exercise 3.21".

Page 73, line -7: Replace "P is" with "P is not".

Page 82, equation (4.20): Replace "$=$" with "$\equiv$".

Page 83, line -8: Replace "proof Euler's" with "proof of Euler's".

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

Page 87, line 16: Replace "Reiger" with "Rieger".

Page 89, line 8: Replace "acheivement" with "achievement".

Page 90, line -1: Replace "$(a+3\sqrt{-3})/2$" with "$(a+3\sqrt{-3}b)/2$".

Page 91, line 9: Replace "result of (c)" with "result of (d)".

Page 92, line -1: Replace "$i^{ab/4}$" with "$i^{ab/2}$".

Page 98, line -6: Replace "a free" with "is a free".

Page 100, line -9: Replace "$\mathcal{O}_K$" with "$\mathcal{O}_L$".

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 112, line -2: Replace "field K of" with "field of".

Page 122, line 6: Replace "$M \subset L$" with "$\tilde{M} \subset L$".

Page 122, display (6.3): Replace the long bracket (]) going from $\mathbf{Q}$ to L with a long bracket going from $\mathbf{Q}$ to $\tilde{M}$.

Page 124, line 1: Replace "a quadratic" by "an imaginary quadratic".

Page 124, line 3: Replace "$a\ d_K$" with "$a \mid d_K$"

Page 129, first line of Exercise 6.8: Replace "a quadratic" by "an imaginary quadratic".

Page 130, first line of part (i) of Exercise 6.9 (c): Replace "(b)" with "(a)".

Page 130, second line of part (i) of Exercise 6.9 (c): Replace "Exercise 6.7" with "Exercise 6.8".

Page 131, line 7: Replace "ϵ" with "δ".

Page 131, line -6: Replace "τ" with "$\sigma\tau$".

Page 132, line -3: Replace "fields" with "field".

Page 134, line 19: Replace "$\mathbf{Z}[\sqrt{-4n}]$" with "$\mathbf{Z}[\sqrt{-n}]$".

Page 135, third line of Lemma 7.5: Replace "proper ideal" with "proper fractional ideal".

Page 136, line 5: Replace "proper ideals" with "proper fractional ideals".

Page 140, line -8: Replace "need study" with "need to study".

Page 142, line -15: Replace "orders" with "order".

Page 148, line -1: Replace this line with

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

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

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

Page 157, display in part (a) of Exercise 7.29: The exponent "n_i" should be inside the parentheses.

Page 163, third line of the proof of Corollary 8.7: Replace "$\Phi_{L/K,m}$ and $\Phi_{M/K,m}$" with "$\ker(\Phi_{L/K,m})$ and $\ker(\Phi_{M/K,m})$".

Page 163, fourth line of the proof of Corollary 8.7: Replace "Exercise 5.13" with "Exercise 5.16".

Page 167, line 1: Replace "$(-1)^{(p-1)/2}$" with "$(-1)^{(p-1)/2}p$".

Page 167, line 10: Replace "$\Phi_{\mathbf{Q}(\sqrt{p^*})/\mathbf{Q},p\infty}$" with "$\ker(\Phi_{\mathbf{Q}(\sqrt{p^*})/\mathbf{Q},p\infty})$"

Page 167, line -3: Replace "relatively to" with "relatively prime to".

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 187, running head: Replace "$_F[\sqrt{-64}]$" with "$\mathbf{Z}[\sqrt{-64}]$".

Page 188, statement of Theorem 9.12: "$\frac{1}{h(D)}$" and "$\frac{1}{2h(D)}$" need to be interchanged.

Page 202, second display: Replace the first "$\leq$" with "$=$".

Page 202, second display: Replace the denominator "$|\omega|^2(\frac{1}{2}|\omega|^2)$" with "$|\omega|^2(\frac{1}{2}|\omega|)^2$".

Page 203, line -9: Replace "$-60G_4(L)\wp(z) - 140G_6(L)\wp(z)$" with "$+60G_4(L)\wp(z) + 140G_6(L)\wp(z)$".

Page 206, line 1: Replace "$f(\lambda z)$" with "$f(\lambda^{-1}z)$".

Page 206, line 10: Replace "x^3" with "$4x^3$".

Page 209, statement of Theorem 10.14: Replace "$\wp$ function" with "$\wp$-function".

Page 210, line −3: Replace "proposition" with "theorem".

Page 211, line −9: Replace "mutiplication" with "multiplication".

Page 220, line −2: Replace "$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$" with "$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbf{Z})$".

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

Page 222, lines −14 to −3: Replace the statement and proof of Lemma 11.4 with the following:

Lemma 11.4. *Every* $\tau \in \mathbf{h}$ *is* $\mathrm{SL}(2, \mathbf{Z})$*-equivalent to a point* τ' *which satisfies* $|\mathrm{Re}(\tau')| \leq 1/2$ *and* $\mathrm{Im}(\tau') \geq 1/2$.

Proof. If $\mathrm{Im}(\tau) \geq 1/2$, then there is an integer m such that $\tau' = \tau + m$ satisfies $|\mathrm{Re}(\tau')| \leq 1/2$ and $\mathrm{Im}(\tau') \geq 1/2$. Since $\tau' = \tau + m = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)\tau$, we are done in this case.

If $\mathrm{Im}(\tau) < 1/2$, then by the argument of the previous paragraph, we can assume $|\mathrm{Re}(\tau)| \leq 1/2$. It follows that $|\tau| < 1/\sqrt{2}$, so that

$$\mathrm{Im}\Big(\frac{-1}{\tau}\Big) = \frac{\mathrm{Im}(\tau)}{|\tau|^2} > 2\,\mathrm{Im}(\tau).$$

Since $-1/\tau = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\tau$, we can more than double the imaginary part of τ by using an element of $\mathrm{SL}(2, \mathbf{Z})$. Repeating this process as often as necessary, we must eventually obtain a $\mathrm{SL}(2, \mathbf{Z})$-equivalent point $\tau' \in \mathbf{h}$ which satisfies $\mathrm{Im}(\tau') \geq 1/2$. Q.E.D.

Page 223, line 2: Replace "Theorem 2.9" with "Theorem 2.8".

Page 225, line 4: In the summation, replace "$n = 1$" with "$n = 0$".

Page 225, line 11: Replace "multiple" with "divisor".

Page 226, line 5: Replace "negative coefficients" with "coefficients for negative exponents".

Page 229, line 10: In the summation, replace "$n = 1$" with "$n = 0$".

Page 229, line 10: Replace "z^n" with "q^n".

Page 229, equation (11.13): In the summation, replace "$n = 1$" with "$n = 0$".

Page 230, line 2: Replace "finitely many" with "finitely many negative".

Page 231, line −7: Replace "$\Phi_m(X, Y) = \Phi_m(Y, X)$" with $\Phi_m(X, Y) = \Phi_m(Y, X)$ if $m > 1$".

Page 232, line 10: In the summation, replace "$n = 1$" with "$n = 0$".

Page 232, line 14: In the summation, replace "$n = 1$" with "$n = 0$".

Page 233, line −10: In the two summations, replace "$n = 1$" with "$n = 0$".

Page 233, line −6: In the summation, replace "$n = 1$" with "$n = 0$".

Page 234, line 10: Replace "$\mathbf{Z}((q))$" with "$\mathbf{Z}((q))[X]$".

Page 235, line 7: Replace "given the" by "given by the".

Page 239, line 12: Replace "$\mathcal{O}$" with "$\mathcal{O}_K$".

Page 239, line 14: Replace "$\mathbf{a} \cap \mathcal{O}$" with "$\mathbf{p} \cap \mathcal{O}$".

Page 244, line -5: Replace "γ" with "γ with $m \neq 0$".

Page 245, third line of Exercise 11.8: In the formula for $C(m)$, replace "c" with "0".

Page 246, line 11: Replace "$\Psi(m)$" with "$|C(m)|$".

Page 249, line -1: Replace "disciminant" with "discriminant".

Page 250, first line of *Proof of Theorem 12.2*: Replace "the Theorem 11.1" with "Theorem 11.1".

Page 250, second line of *Proof of Theorem 12.2*: Replace "of of" with "of".

Page 251, line 3: In the summation, replace "$n = 1$" with "$n = 0$".

Page 251, equation (12.5): In the summation, replace "$n = 1$" with "$n = 0$".

Page 252, line -4: In the summations, replace "$i = 1$" and "$k = 1$" with "$i = 0$" and "$k = 0$".

Page 252, line -3: Replace "$Q(Y) ==$" with "$Q(Y) =$".

Page 252, line -3: In the summation, replace "$l = 1$" with "$l = 0$".

Page 253, line 2: In the summations, replace "$i = 1$" and "$k = 1$" with "$i = 0$" and "$k = 0$".

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

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

Page 274, line 8: Replace "(iv)" with "(i)".

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

Page 280, second and third lines of Exercise 12.19: Replace "$\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$" with "$\mathbf{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7})$".

Page 285, line -1: Replace "$2^{20} \cdot 3 \cdot 11^6 \cdot 21323$" with "$2^{20} \cdot 3 \cdot 11^6 \cdot 19 \cdot 21323$".

Page 295, lines -10 and -8: Replace "$pu + i$" with "$pu - i$" in two places.

Page 296, line 1: Replace "$\Phi(X, j(\tau))$" with "$\Phi_p(X, j(\tau))$".

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 315, line -9: Replace "$|E(\mathbf{F}_q|$" with "$|E(\mathbf{F}_q)|$" .

Page 316, statement of Proposition 14.15: Replace "Then" with "If $p > 3$, then".

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.

Page 324, line –6: Replace "$l > 13$" with "$l > 33$"

Page 325, line 13: Replace "$l > 13$" with "$l > 33$"

Page 328, first display: Replace "$1 - O(2^{-k^{1/\ln\ln k}})$" with "$(1 - O(2^{-k^{1/\ln\ln k}})) \times 100$".

Page 329, second line of the proof of Proposition 14.30: replace "$\prod_{i=1}^h (X - j(\mathbf{a}_i)$" with "$\prod_{i=1}^h (X - j(\mathbf{a}_i))$".

Page 336, reference 28: Replace "Vieweg Brunswick" with "Vieweg, Braunschweig".

Page 339, reference 84: Replace "Reiger" with "Rieger".

Page 340, reference 102: Replace "Braunschwieg" with "Vieweg, Braunschweig".

Page 341, reference 111: Replace "Quadratiche" with "Quadratische".

Page 350, index entry for Reiger, G. J.: Correct the spelling to "Rieger, G. J." and move to after the index entry for Residue.