Errata et Addenda to the First Printing of the Book
Advanced Topics in Computational Number Theory
by **Henri Cohen**
(20000615 Version)

Graduate Texts in Mathematics 193, Springer-Verlag, 2000
First Printing 2000, XV + 578 pages.
ISBN 0-387-98727-4 Springer-Verlag New York Berlin Heidelberg

p. 23 line 8, instead of "Corollary 1.2.11" read "Corollary 1.3.9"
p. 31 line -11, instead of "$\mathfrak{c}_j = \mathfrak{g}_{n+1-j}\mathfrak{g}_{n-j}^{-1}$" read "$\mathfrak{c}_j = \mathfrak{g}_j\mathfrak{g}_{j+1}^{-1}$"
p. 31 line -7, instead of "$\mathfrak{g}_j(A) = \mathfrak{c}_{n+1-j}\cdots\mathfrak{c}_n$" read "$\mathfrak{g}_j(A) = \mathfrak{c}_j\cdots\mathfrak{c}_n$"
p. 44 line 3 of step 4 of Algorithm 1.7.3, exchange "$a_{i,j}$" with "$a_{i,i}$" (twice)
p. 44 line 3 of step 7 of Algorithm 1.7.3, instead of "$a_{j,i}A'_j - A'_i$" read "$A'_j - a_{j,i}A'_i$" and instead of "$a_{j,i}V'_j - V'_i$" read "$V'_j - a_{j,i}V'_i$"
p. 45 line 13, instead of "$\mathfrak{c} = \sum_i \mathfrak{a}'_i\mathfrak{b}'_i$" read "$\mathfrak{c} = \sum_i \mathfrak{a}'_i\mathfrak{b}'^{-1}_i$"
p. 45 line 17, instead of "$(n-i)\times(n-i)$" read "$(n+1-i)\times(n+1-i)$"
p. 45 line -7, instead of "step 5" read "step 2"
p. 46 line 3 of Exercise 1, exchange "$1/|\mathcal{N}(x)|$" and "$|\mathcal{N}(x)|$"
p. 60 line 10, instead of "$\theta_1 = -R'(X)/R'_Z(X,k)$" read "$\theta_1 = -R'_Z(X,k)/R'(X)$"
p. 60 line 15, instead of "$\theta_1^i\theta_2^j$" read "$\theta_1^{i_1}\theta_2^{i_2}$"
p. 62 line -5 and line -4, instead of "$L_1(X)$" read "$L_1[X]$"
p. 65 line -8, instead of "$\sum_{0\le j<n_1} c_{i,j}a_j = b_i$" read "$\sum_{0\le j<n_1} c_{i,j}b_j = a_i$"
p. 65 line -3 (twice) and line -1 (once), instead of "α" read "θ_2"
p. 66 line 3 of step 2 of Algorithm 2.1.12, instead of "$(1,0,\dots,0)^t$" read "$(0,1,0,\dots,0)^t$"
p. 85 line 8, instead of "α_j" read "γ_j"
p. 88 line 1 of Lemma 2.3.7, instead of "$\alpha\in K$" read "$\alpha\in L$"
p. 88 line -12, instead of "$\mathcal{N}_{L/K}(I)\in I$" read "$\mathcal{N}_{L/K}(I)\subset I$"
p. 92 lines 8 and 9, exchange "$\mathfrak{P}$ is unramified" with "$\mathfrak{P}$ is ramified"
p. 99 Replace steps 3 and 4 of Algorithm 2.3.21 by the following:

3. [Terminate] Using Algorithm 1.5.1, compute an HNF pseudo-basis $(\gamma_i,\mathfrak{c}_i)$ for the intersection $I^{-1}\leftarrow I_1\cap I_2$.

p. 106 line -1, instead of "$\mathbb{Z}_K \smallsetminus \mathfrak{p}^{-1}$" read "$\mathfrak{p}^{-1}\smallsetminus\mathbb{Z}_K$"
p. 110 lines 5 and 6 of Algorithm 2.4.12, replace twice "$\sum_{1\le k\le n}$" by "$\sum_{0\le k\le n}$"
p. 114 line 19, instead of "$\theta\in K$" read "$\theta_1\in K$"
p. 131 Exercise 33, instead of "proof given in" read "proof of"
p. 131 Exercise 34, replace twice "t_i" by "T_i", and replace four times "r_i" by "R_i"
p. 131 Exercise 36, instead of "$\omega^2(\omega+3)$" read "$\omega^2(-\omega-3)$"
p. 135 line -5, instead of "$\rho(\alpha) = \big(\overline{\alpha},(\mathrm{sign}(\sigma_i(\alpha))_{\sigma_i\in\mathfrak{m}_\infty}\big)$" read "$\rho(\alpha) = \big(\overline{\alpha},(\mathrm{sign}(\sigma_i(\alpha)))_{\sigma_i\in\mathfrak{m}_\infty}\big)$"
p. 161 Exercise 7 d), instead of "necessary" read "necessarily"
p. 161 Exercise 15 a), add the property "$\mathfrak{d}(L/K)\mid\mathfrak{m}_0^{\ell^r-1}$"
p. 187 line 1, instead of "$\phi\big(\overline{\beta}\big)=\overline{\beta}$, and" read "$\phi\big(\overline{\beta}\big)=\overline{\beta}$, and"

p. 201 line 3 of step 2 of Algorithm 4.2.16, instead of "$\beta \leftarrow \beta \prod_i (1+\gamma_{a,i}^{-y_{a,i}})$" read $\beta \leftarrow \beta \prod_i (1+\gamma_{a,i})^{-y_{a,i}}$"

p. 212 line -14, instead of "$(\mathbb{Z}/\mathfrak{m})^*$" read "$(\mathbb{Z}_K/\mathfrak{m})^*$"

p. 221 Exercise 18 c), instead of "prime ideal below" read "prime number below"

p. 226 line 9, instead of "field K, a congruence" read "field K and a congruence"

p. 230 middle, instead of "the next section" read "Section 5.2.4"

p. 255 line -3, instead of "$\gamma \in K^{*\ell}$" read "$\gamma \in K^*$"

p. 260 line -10, instead of "Thus," read "Hence,"

p. 293 Exercise 4 a), instead of "exists" read "exist" (twice)

p. 308 line 3, instead of "$(-i)^{f_\infty}$" read "$(-i)^{|\mathfrak{f}_\infty|}$"

p. 308 step 5 of Algorithm 6.2.4, instead of "$(-i)^{|f_\infty|}$" read "$(-i)^{|\mathfrak{f}_\infty|}$"

p. 315 middle, instead of "elliptic function $j(\tau)$" read "modular function $j(\tau)$"

p. 318 middle, instead of "$\left(\dfrac{2i\pi}{\omega_2}\right)^{24}$" read "$\left(\dfrac{2i\pi}{\omega_2}\right)^{12}$"

p. 345 Remove Exercise 8 (it is Exercise 15 d)

p. 346 Exercise 25, put the parenthetical statement "(where as usual we set $\mathfrak{f} \cap \mathbb{Z} = f\mathbb{Z}$)" at the end of the sentence, without parentheses

p. 425 line 2 of step 9, instead of "$d_3 \leftarrow \lceil (b-s)/2 \rceil - 1$, $d_4 \leftarrow \lfloor (b+s)/2 \rfloor + 1$" read "$d_3 \leftarrow \lceil (b-s)/2 \rceil$, $d_4 \leftarrow \lfloor (b+s)/2 \rfloor$"

p. 434 line 11, instead of "α/α'" read "$(\alpha/\alpha')\mathbb{Z}_K$"

p. 434 line -13, instead of "whose prime factors are only prime ideals above 2" read "dividing 2"

p. 439 line 2 of (4), instead of "they will" read "it will"

p. 439 line 5 of (4), instead of "repeat" read "recompute"

p. 439 middle, instead of "the case of prime degree" read "the prime degree case"

p. 444 line -8, instead of "G_{18}^+, G_{18}^-, G_{36}, and G_{72}" read "G_{36}^+, G_{36}^-, and G_{72}"

p. 451 line -3, instead of "Schwartz's" read "Cauchy–Schwarz's"

p. 455 line 1, instead of "Schwartz's" read "Cauchy–Schwarz's"

p. 469 replace Exercise 6 b) by the following: "Let R_1 denote an even integer such that $0 \le R_1 \le 2r_1$. Show that the number of K-isomorphism classes of quadratic extensions L/K with $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{d}(L/K)) \le x$ and R_1 real embeddings is asymptotic to $(\binom{r_1}{R_1/2}/2^{r_1}) Q_K \cdot x$, where Q_K is as above."

p. 470 line 1 of Exercise 14, replace " and" by ", "

p. 471 Exercise 16 a), instead of "Schwartz's" read "Cauchy–Schwarz's"

p. 471 Exercise 16 a), instead of "show that" read "prove *Lagrange's identity*"

p. 483 line -6, instead of "$\theta_k(\tau)(\theta_0(\sigma)^k - 1) = 0$" read "$(\theta_0(\sigma)^k - 1)\theta_k(\tau) = 0$"

p. 484 line -12, instead of "$\mathfrak{D}(L/K) = \mathbb{Z}_L^*$" read "$\mathbb{Z}_L^* = \mathfrak{D}(L/K)^{-1}$"

p. 488 middle, instead of "$v_{\mathfrak{P}}(\mathfrak{f}_2)$ is even" read "$v_{\mathfrak{P}}(\mathfrak{f}_2)$ is even when $\mathfrak{p}$ is ramified in K_2/K"

p. 520 rewrite Exercise 12 as follows: "Let L/K be an extension of number fields, let P be a monic polynomial with coefficients in K, let $\mathfrak{p}$ be a prime ideal of K, and let $\alpha \in L$ be a root of P. Assume that the $\mathfrak{p}$-adic valuations of all the coefficients of P are nonnegative. Show that $v_{\mathfrak{P}}(\alpha) \ge 0$ for any prime ideal $\mathfrak{P}$ of L above $\mathfrak{p}$."

p. 520 line 1 of Exercise 15, instead of "let ℓ is a prime number" read "ℓ a prime number"

p. 558 add at the appropriate place "Γ_∞: group of integer translations, 122"

p. 573 add at the appropriate place "Lagrange's identity, 471"