Errata et Addenda to the First Printing of the Book
Advanced Topics in Computational Number Theory
by **Henri Cohen**
(20000211 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. 131 Exercise 33, instead of "proof given in" read "proof of"
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 "$\phi(\overline{\beta}) = \overline{\beta}$, and" read "$\phi(\overline{\beta}) = \overline{\beta}$, and"
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 $v_{\mathfrak{P}}(\alpha) \geq 0$ 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”