Errata et Addenda to the Second Printing of the Book
A Course in Computational Algebraic Number Theory
by **Henri Cohen**
(19940607 version)

Graduate Texts in Mathematics 138, Springer-Verlag, 1993, XXI + 534 pages.
ISBN 3-540-55640-0 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-55640-0 Springer-Verlag New York Berlin Heidelberg

p. 4 line -2, instead of "$a * b$" read "$a \cdot b$"
p. 55 line 20, instead of "$p_m(X) = \ldots$" read "$p_m(X) \leftarrow \ldots$"
p. 60 line 3, instead of "$X_i^{\prime}$" read "$M_i^{\prime}$, $X_i^{\prime}$" and instead of "X)" read "M, X)"
p. 79 line 1, instead of "for all" read "for all non-zero"
p. 82 line 4, instead of "exists" read "exist"
p. 88 line 11, instead of "Gram-Schmidt" read "Gram"
p. 88 line 13, instead of "so that statements ... removed" read "and the updating of the vectors $\mathbf{b}_i$ done in Sub-algorithms RED and SWAP must be done directly on the Gram matrix"
p. 89 line 13, instead of "to be LLL" read "from being LLL"
p. 93 line 3 of Algorithm REDI, after "$H_k \leftarrow H_k - qH_l$," insert " $\mathbf{b}_k \leftarrow \mathbf{b}_k - q\mathbf{b}_l$,"
p. 93 line 1 of Algorithm SWAPI, after "H_k and H_{k-1}," insert " exchange $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$,"
p. 93 line 4 of Algorithm SWAPI, instead of "$t + \lambda\lambda_{i,k}/B$" read "$(Bt + \lambda\lambda_{i,k})/d_k$"
p. 94 line 2 of step 2, instead of "$\mu_{k,j} = 0$" read "$\mu_{k,j} \leftarrow 0$"
p. 120 line 13, instead of "$\ell(A)^{2m-2}$" read "$\ell(A)^{m-1+\deg(A')}$"
p. 120 line -8, instead of "a^{2m-1}" read "$a^{m+\deg(A')}$"
p. 120 line -7, instead of "proposition." read "proposition. Note that we have $\deg(A') = m-1$ except when the characteristic of R is non-zero and divides m."
p. 131 line 3 of Step 1, add " $\pmod{A(X)}$" at the end of the formula
p. 135 line -15, instead of "any factor of A" read "up to sign, any factor of A"
p. 137 line -12, instead of "find" read "finds"
p. 154 line 7, instead of "More generally, for" read "For"
p. 155 line 17, instead of "a polynomial" read "an irreducible polynomial"
p. 197 line -11, instead of "Z_K" read "$\mathbb{Z}_K$"
p. 211 line 8, instead of "Although more ... preferred." read "Although Algorithm 4.9.10 is more pleasing to the mind, Algorithm 4.9.9 is considerably faster and should therefore be preferred in practice."
p. 283 line -11, instead of "and it is easy to check that this distance Δ_C belongs to one of the hyperplanes $\sum_i x_i = 2ik\pi$ for $k \in \mathbb{Z}$" read "and it is clear that the real part of Δ_C lies in the hyperplane $\sum_i x_i = 0$"
p. 348 line 3, instead of "an ideal" read "a vector v as above and an ideal"
p. 348 line 3, instead of " this" read ", this"
p. 349 line 7, instead of "a $(r_1+$" read "an $(r_1+$"
p. 349 line 15, instead of "$\mathfrak{p}_i^{e_i}$" read "$\mathfrak{p}_i$"
p. 349 line 22, instead of "the zero vector" read "v equal to the zero vector"
p. 349 line -5, instead of "step 5" read "step 4"
p. 350 line 18, instead of "step 10" read "step 9"
p. 350 line 20, instead of "MC" read "M_C"
p. 376 lines 4, 6, 7, 8, 9, 10, 16, 18, instead of "))/2)" read ")/2)"
p. 376 lines 16 and 17, instead of the given formula for $j((1+i\sqrt{15})/2)$ read

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

$$
\begin{aligned}
j((1+i\sqrt{15}))/2) &= \frac{-191025-85995\sqrt{5}}{2} \\
&= \frac{1-\sqrt{5}}{2}\left(\frac{75+27\sqrt{5}}{2}\right)^3 = 1728-3\left(\frac{273+105\sqrt{5}}{2}\right)^2
\end{aligned}
$$