Errata et Addenda to the Second Printing of the Book
A Course in Computational Algebraic Number Theory

by **Henri Cohen**

(19940924 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. VII line -1, instead of "Vallee" read "Vallée"
p. 43 line 3 of Exercise 16, instead of "$\mathbb{Q}(\zeta)$" read "$\mathbb{Z}[\zeta]$"
p. 43 line 5 of Exercise 16, instead of "$(-1)^{(p-1)/2}$" read "$(-1)^{(p-1)/2}p$"
p. 73 line -1, instead of "lowest" read "least"
p. 156 line -3, instead of "$\mathbb{Z}[\alpha]$" read "$\mathbb{Q}(\alpha)$"
p. 185 line 4, instead of "lowest" read "least"
p. 190 middle, add a third item to the statement of the proposition:

"(3) *If α and β are in K, then $I = \alpha\mathbb{Z}_K + \beta\mathbb{Z}_K$ if and only if for every prime ideal $\mathfrak{p}$ we have*

$$\min(v_{\mathfrak{p}}(\alpha), v_{\mathfrak{p}}(\beta)) = v_{\mathfrak{p}}(I)$$

where $v_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-adic valuation at the prime ideal $\mathfrak{p}$."

p. 191 line -17, add the proof of (3) as follows:

"For (3) recall that the sum of ideals correspond to GCD, and that the GCD is computed by taking the minimum of the $\mathfrak{p}$-adic valuations."

p. 192 middle, replace everything starting with the statement of Lemma 4.7.9 until the end of the section by the following.

Lemma 4.7.9. *Let $\mathfrak{p}$ be a prime ideal above p of norm p^f (f is called the residual degree of $\mathfrak{p}$ as we will see in the next section), and let $\alpha \in \mathfrak{p}$. Then we have $\mathfrak{p} = (p, \alpha) = p\mathbb{Z}_K + \alpha\mathbb{Z}_K$ if and only if $v_p(\mathcal{N}(\alpha)) = f$ or $v_p(\mathcal{N}(\alpha + p)) = f$, where v_p denotes the ordinary p-adic valuation.*

Proof. This proof assumes some results and definitions introduced in the next section. Assume first that $v_p(\mathcal{N}(\alpha)) = f$. Then, since $\alpha \in \mathfrak{p}$ and $\mathcal{N}(\mathfrak{p}) = p^f$, for every prime $\mathfrak{q}$ above p and different from $\mathfrak{p}$ we must have $v_{\mathfrak{q}}(\alpha) = 0$ otherwise $\mathfrak{q}$ would contribute more powers of p to $\mathcal{N}(\alpha)$. In addition and for the same reason we must have $v_{\mathfrak{p}}(\alpha) = 1$. It follows that for any prime ideal $\mathfrak{q}$, $\min(v_{\mathfrak{q}}(p), v_{\mathfrak{q}}(\alpha)) = v_{\mathfrak{q}}(\mathfrak{p})$ and so $\mathfrak{p} = (p, \alpha)$ by Proposition 4.7.7 (3).

If $v_p(\mathcal{N}(\alpha + p)) = f$ we deduce from this that $\mathfrak{p} = p\mathbb{Z}_K + (\alpha + p)\mathbb{Z}_K$, but this is clearly also equal to $p\mathbb{Z}_K + \alpha\mathbb{Z}_K$.

Conversely, let $\mathfrak{p} = p\mathbb{Z}_K + \alpha\mathbb{Z}_K$. Then for every prime ideal $\mathfrak{q}$ above p and different from $\mathfrak{p}$ we have $v_{\mathfrak{q}}(\alpha) = 0$, while for $\mathfrak{p}$ we can only say that $\min(v_{\mathfrak{p}}(p), v_{\mathfrak{p}}(\alpha)) = 1$.

Assume first that $v_{\mathfrak{p}}(\alpha) = 1$. Then clearly $v_p(\mathcal{N}(\alpha)) = v_p(\mathcal{N}(\mathfrak{p})) = f$ as desired. Otherwise we have $v_{\mathfrak{p}}(\alpha) > 1$, and hence $v_{\mathfrak{p}}(p) = 1$. But then we will have $v_{\mathfrak{p}}(\alpha + p) = 1$ (otherwise $v_{\mathfrak{p}}(p) = v_{\mathfrak{p}}((p + \alpha) - \alpha) > 1$), and still $v_{\mathfrak{q}}(\alpha + p) = 0$ for all other primes $\mathfrak{q}$ above p, and so $v_p(\mathcal{N}(\alpha + p)) = f$ as before, thus proving the lemma. ☐

Note that the condition $v_p(\mathcal{N}(\alpha)) = f$, while sufficient, is not a necessary condition (see Exercise 20).

Note also that if we write $\alpha = \sum_{1 \le i \le k} \lambda_i \gamma_i$ where the γ_i is some generating set of $\mathfrak{p}$, we may always assume that $|\lambda_i| \le p/2$ since $p \in \mathfrak{p}$. In addition, if we choose $\gamma_1 = p$, we may assume that $\lambda_1 = 0$.

This suggests the following algorithm, which is simple minded but works quite well.

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

Algorithm 4.7.10 (Two-Element Representation of a Prime Ideal). Given a prime ideal $\mathfrak{p}$ above p by a system of $\mathbb{Z}_K$-generators γ_i for $(1 \le i \le k)$, this algorithm computes a two-element representation (p, α) for $\mathfrak{p}$.

We assume that one knows the norm p^f of $\mathfrak{p}$ (this is always the case in practice, and in any case it can be obtained by computing the HNF of $\mathfrak{p}$ from the given generators), and that $\gamma_1 = p$ (if this is not the case just add it to the list of generators).

1. [Initialize] Set $R \leftarrow 1$.
2. [Set coefficients] For $2 \le i \le k$ set $\lambda_i \leftarrow R$.
3. [Compute α and check] Let $\alpha \leftarrow \sum_{2 \le i \le m} \lambda_i \gamma_i$, $n \leftarrow \mathcal{N}(\alpha)/p^f$, where the norm is computed, for example, using the sub-resultant algorithm (see Section 4.3). If $p \nmid n$, then output (p, α) and terminate the algorithm. Otherwise, set $n \leftarrow \mathcal{N}(\alpha + p)/p^f$. If $p \nmid n$ then output (p, α) and terminate the algorithm.
4. [Decrease coefficients] Let j be the largest $i \le k$ such that $\lambda_i \ne -R$ (we will always keep $\lambda_2 \ge 0$ so j will exist). Set $\lambda_j \leftarrow \lambda_j - 1$ and for $j + 1 \le i \le m$ set $\lambda_i \leftarrow R$.
5. [Search for first non-zero] Let j be the smallest $i \le k$ such that $\lambda_i \ne 0$. If no such j exists (i.e. if all the λ_i are equal to 0) set $R \leftarrow R + 1$ and go to step 2. Otherwise go to step 3.

Remarks. 1) Steps 4 and 5 of this algorithm represent a standard backtracking procedure. What we do essentially is to search for $\alpha = \sum_{2 \le i \le k} \lambda_i \gamma_i$, where the λ_i are integers between $-R$ and R. To avoid searching both for α and $-\alpha$, we add the condition that the first non-zero λ should be positive. If the search fails, we start it again with a larger value of R. Of course, some time will be wasted since many old values of α will be recomputed, but in practice this has no real importance, and in fact $R = 1$ or $R = 2$ is usually sufficient. The remark made after Lemma 4.7.9 shows that the algorithm will stop with $R \le p/2$.

2) It is often the case that one of the γ_i for $2 \le i \le k$ will satisfy one of the conditions of step 3. Thus it is useful to test this before starting the backtracking procedure.

We refer to [Poh-Zas] for extensive information on the use of two-element representations."

p. 195 instead of "*If* $p = \prod_{i=1}^{g} \mathfrak{p}_i$ *is an unramified prime in* K" read "*If* p *is an unramified prime in* K *with* $p\mathbb{Z}_K = \prod_{i=1}^{g} \mathfrak{p}_i$"

p. 199 middle, instead of "$p^{-1} = R + aR$" read "$\mathfrak{p}^{-1} = R + aR$"

p. 203 line -4 until p. 204 line -12, replace completely by the following.

"To compute the inverse of an ideal I given by a $\mathbb{Z}$-basis γ_j represented by an $n \times n$ matrix M on the integral basis as above, we thus proceed as follows. Computing T^{-1} we first obtain a basis of the codifferent $\mathfrak{d}(K)^{-1}$. We then compute the *ideal* product $I\mathfrak{d}(K)^{-1}$ by Hermite reduction of an $n \times n^2$ matrix as explained in Section 4.7.1. If N is the HNF matrix of this ideal product, then by Proposition 4.8.19, the columns $(N^tT)^{-1}$ will form a $\mathbb{Z}$-basis of the ideal $(I\mathfrak{d}(K)^{-1})^{-1}\mathfrak{d}(K)^{-1} = I^{-1}$, thus giving the inverse of I after another HNF. In paractice, it is better to work only with integral ideals, and since we know that $\det(T) = d(K)$, this means that we will replace $\mathfrak{d}(K)^{-1}$ by $d(K)\mathfrak{d}(K)^{-1}$ which is an integral ideal.

This leads to the following algorithm.

Algorithm 4.8.21 (Ideal Inversion). Given an integral basis $(\omega_i)_{1 \le i \le n}$ of the ring of integers of a number field K and an integral ideal I given by an $n \times n$ matrix M whose columns give the coordinates of a $\mathbb{Z}$-basis γ_j of I on the ω_i, this algorithm computes the HNF of the inverse ideal I^{-1}.

1. [Compute $d(K)\mathfrak{d}(K)^{-1}$] Compute the $n \times n$ matrix $T = (t_{i,j})$ such that $t_{i,j} = \mathrm{Tr}_{K/\mathbb{Q}}(\omega_i \omega_j)$. Set $d \leftarrow \det(T)$ (this is the determinant $d(K)$ of K hence is usually available with the ω_i already). Finally,

call δ_j the elements of $\mathbb{Z}_K$ whose coordinates on the ω_i are the columns of dT^{-1} (thus the δ_j will be a $\mathbb{Z}$-basis of the integral ideal $d(K)\mathfrak{d}(K)^{-1}$).

2. [Compute $d(K)I\mathfrak{d}(K)^{-1}$] Let N be the HNF of the $n \times n^2$ matrix whose columns are the coordinates on the integral basis of the n^2 products $\gamma_i\delta_j$ (the columns of N will form a $\mathbb{Z}$-basis of $d(K)I\mathfrak{d}(K)^{-1}$).

3. [Compute I^{-1}] Set $P \leftarrow d(K)(N^tT)^{-1}$, and let e be a common denominator for the entries of the matrix P. Let W be the HNF of eP. Output (W, e) as the HNF of I^{-1} and terminate the algorithm.

Remarks.

(1) If many ideal inversions are to be done in the same number field, step 1 should of course be done only once. In addition, it may be useful to find a two-element representation for the integral ideal $d(K)\mathfrak{d}(K)^{-1}$ since this will considerably speed up the ideal multiplication of step 2. Algorithm 4.7.10 cannot directly be used for that purpose since it is valid only for prime ideals, but similar algorithms exist for general ideals (see Exercise 30). In addition, if $\mathbb{Z}_K = \mathbb{Z}[\theta]$ and if $P[X]$ is the minimal monic polynomial of θ, then one can prove (see Exercise 29) that $\mathfrak{d}(K)$ is the principal ideal generated by $P'(\theta)$, so the ideal multiplication of step 2 is even simpler.

(2) If we want to compute the HNF of the different $\mathfrak{d}(K)$ itself, we apply the above algorithm to the integral ideal $d(K)\mathfrak{d}(K)^{-1}$ (with $M = d(K)T^{-1}$) and multiply the resulting inverse by $d(K)$ to get $\mathfrak{d}(K)$.”

p. 217 **Addendum.** Add the following exercises.

“29. Let $\mathfrak{p}$ be a prime ideal above the prime 2 in a number field K such that $e(\mathfrak{p}/2) = 2$. Show that the congruences $x^2 \equiv a \pmod{\mathfrak{p}^3}$ have a solution for $a = -1$ and $a = -2$.

30. Let I be an integral ideal in a number field K and let $\ell(I)$ be the positive generator of $I \cap \mathbb{Z}$.

a) Show that

$$\ell(I) = \prod_{p \mid \mathcal{N}(I)} p^{\max_{\mathfrak{p}\mid p} \lceil v_{\mathfrak{p}}(I)/e(\mathfrak{p}/p)\rceil} \quad .$$

b) Let $\alpha \in I$ be such that $(\mathcal{N}(I), \mathcal{N}(\alpha)/\mathcal{N}(I)) = 1$. Show that

$$I = \ell(I)\mathbb{Z}_K + \alpha\mathbb{Z}_K = \mathcal{N}(I)\mathbb{Z}_K + \alpha\mathbb{Z}_K$$

(this is a partial generalization of Lemma 4.7.9).

c) Deduce from this an algorithm for finding a two-element representation of I analogous to Algorithm 4.7.10.

31. Let $\mathfrak{p}$ be a prime ideal in a number field K, and denote by p the prime number below $\mathfrak{p}$, by $e = e(\mathfrak{p}/p)$ the ramification index, and by $f = f(\mathfrak{p}/p)$ the residual degree of $\mathfrak{p}$. The goal of this exercise is to find the Abelian group structure of $\mathbb{Z}_K/\mathfrak{p}^k$ and also of $(\mathbb{Z}_K/\mathfrak{p}^k)^*$ in a number of cases.

a) Let $k \geq 1$ be an integer, and let $k - 1 = qe + r$ be the Euclidean division of $k - 1$ by e, with $0 \leq r < e$. Show that we have the Abelian group isomorphism

$$\mathbb{Z}_K/\mathfrak{p}^k \simeq \left(\mathbb{Z}/p^{q+1}\mathbb{Z}\right)^{f(r+1)} \times \left(\mathbb{Z}/p^q\mathbb{Z}\right)^{f(e-r-1)} \quad .$$

b) Let $k \geq 1$ be an integer, and let $k-2 = qe+r$ be the Euclidean division of $k-2$ by e, with $0 \leq r < e$. Assume that $p \geq \min(k, e+2)$. Show that we have the Abelian group isomorphism

$$\left(\mathbb{Z}_K/\mathfrak{p}^k\right)^* \simeq \left(\mathbb{Z}/(p^f - 1)\mathbb{Z}\right) \times \left(\mathbb{Z}/p^{q+1}\mathbb{Z}\right)^{f(r+1)} \times \left(\mathbb{Z}/p^q\mathbb{Z}\right)^{f(e-r-1)} \quad ,$$

where the left hand side is a multiplicative group and the right hand side an additive group (note that the formula for the p-part of this formula is the same as in a) but with different values of q and r).

c) Assume that $e = 1$, i.e. that $\mathfrak{p}$ is an unramified prime ideal. The above isomorphism gives the structure of $(\mathbb{Z}_K/\mathfrak{p}^k)^*$ for $p \geq 3$. Show that for $p = 2$,

$$\left(\mathbb{Z}_K/\mathfrak{p}^k\right)^* \simeq \left(\mathbb{Z}/(p^f-1)\mathbb{Z}\right) \times \left(\mathbb{Z}/p^{k-1}\mathbb{Z}\right)^{f-1} \times \mathbb{Z}/p^{k-2}\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \ .$$

d) Assume on the contrary that e is large, say $e \geq k(p-1)/p$. Set $u_m = \lfloor (k-1)/p^m \rfloor$ for all $m \geq 0$, so that $u_m = 0$ for m sufficiently large. Show that

$$\left(\mathbb{Z}_K/\mathfrak{p}^k\right)^* \simeq \left(\mathbb{Z}/(p^f-1)\mathbb{Z}\right) \times \prod_{m \geq 1} \left(\mathbb{Z}/p^m\mathbb{Z}\right)^{f(u_{m-1}-2u_m+u_{m+1})} \ .$$

e) Assume that e is not divisible by $p-1$. Show that there exists an Abelian group G of order p^{k-1} such that

$$\left(\mathbb{Z}_K/\mathfrak{p}^k\right)^* \simeq \left(\mathbb{Z}/(p^f-1)\mathbb{Z}\right) \times G^f \ .$$

f) Determine the structure of $(\mathbb{Z}_K/\mathfrak{p}^k)^*$ for $1 \leq k \leq 5$. The results can be expressed solely as functions of p, k, e and f, and also in the case $p = 3$, $e = 2$ and $4 \leq k \leq 5$, of ε where $\varepsilon = 1$ if there exists a solution of $x^2 \equiv -3 \pmod{\mathfrak{p}^3}$, $\varepsilon = 0$ otherwise.

32. Given a prime ideal $\mathfrak{p}$ in a number field K and a positive integer k, write an algorithm which computes the Abelian group structure of $(\mathbb{Z}_K/\mathfrak{p}^k)^*$ as a product of cyclic groups.

33. Let $K = \mathbb{Q}[\theta]$ be a number field, where θ is an algebraic integer whose minimal monic polynomial is $P(X) \in \mathbb{Z}[X]$. Assume that $\mathbb{Z}_K = \mathbb{Z}[\theta]$. Show that the different $\mathfrak{d}(K)$ is the principal ideal generated by $P'(\theta)$.

34. Let I and J be two integral ideals in a number field K given by their HNF matrices M_I and M_J. Assume that I and J are coprime, i.e. that $I + J = \mathbb{Z}_K$. Give an algorithm which finds $i \in I$ and $j \in J$ such that $i + j = 1$.

35. a) Using the preceding exercise, give an algorithm wich finds explicitly the element $\beta \in \mathbb{Z}_K$ whose existence is proven in Proposition 4.7.8.

b) Deduce from this an algorithm which finds a two-element representation $I = \alpha\mathbb{Z}_K + \beta\mathbb{Z}_K$ of an integral ideal I given a non-zero element $\alpha \in I$.

c) In the case where $\alpha = \ell(I)$, compare the theoretical and practical performance of this algorithm with the one given in Exercise 30."

p. 237 line 8, instead of "lowest" read "least"

p. 243 line 2 of step 4 of Algorithm 5.4.8, instead of "step 2" read "step 3"

p. 243 step 3 of Algorithm PARTEUCL, instead of "Let $q \leftarrow \lfloor d/v_3 \rfloor$ and simultaneously $t_3 \leftarrow d \bmod v_3$" read "Let $d = qv_3 + t_3$ be the Euclidean division of d by v_3 with $0 \leq t_3 < |v_3|$"

p. 285 lines -9 to page 286 line 9, replace completely by the following:

"We thus obtain a matrix $A = (a_{i,j})$ with $n+1$ rows and k columns, whose entries in the first n rows are integers and the entries in the last row are real numbers. Note that by definition, for every $j \leq k$ we have

$$\delta(\mathbf{1}, \prod_{1 \leq i \leq n} f_{p_i}^{a_{i,j}}) \equiv a_{n+1,j} \pmod{R(D)} \ .$$

Since the distance function that we have chosen is exactly additive, it follows that when performing column operations on the complete matrix A, this relation between the $n+1$-st component and the others is preserved.

Hence we apply Hermite reduction to the matrix formed by the first n rows, but performing the corresponding column operations also the entries of the last row. The first $k-n$ columns of the resulting matrix will thus have only zero entries, except perhaps for the entry in the $n+1$-st row. By the remark made above, for $1 \le j \le k-n$ we will thus have

$$a_{n+1,j} = \delta(\mathbf{1},\mathbf{1}) \equiv 0 \pmod{R(D)} \ ,$$

in other words $a_{n+1,j}$ is equal to a multiple of the regulator $R(D)$ for $1 \le j \le k-n$.

If k is large enough, it follows that in a certain sense the GCD of the $a_{n+1,j}$ for $1 \le j \le k-n$ should be exactly equal to $R(D)$. We must be careful in the computation of this "GCD" since we are dealing with inexact real numbers. For this purpose, we can either use the LLL algorithm which will give us a small linear combination of the $a_{n+1,j}$ for $1 \le j \le k-n$ with integral coefficients, which should be the regulator $R(D)$, or use the "real GCD" Algorithm 5.9.3 as described below."

p. 292 line -14, instead of "the similarly" read "similarly"

p. 293 end of Exercise 5, instead of "and to my knowledge...assumption" read "the complete result without the randomness assumption has only recently been proved by Duke [Duk]."

p. 293 line -1, instead of "in terms of" read "as a function of"

p. 302 line 8, instead of "lowest" read "least", and remove "(lcm)"

p. 302 line 9, instead of "PID" read "PID,"

p. 313 line 15, instead of "lowest" read "least"

p. 319 middle, replace "$\mathbb{Z}/3\mathbb{Z}$" by "C_3" and "$(A_3,+)$" by "$(C_3,+)$"

p. 339 line 6, instead of "we take in step 9" read "in step 9 we take"

p. 342 Corollary 6.4.15, in (3) and in (4), instead of "If $p \equiv 1 \pmod 3$" read "If $p \nmid a$, $p \equiv 1 \pmod 3$", and in (5) instead of "If $p = 3$" read "If $p = 3$ and $p \nmid a$"

p. 349 line 1, instead of "the sum... $2i\pi$" read "the components x_i of this vector satisfy $\sum_{1 \le i \le r_1} x_i + \sum_{r_1 < i \le r_1+r_2} \Re(x_i) = 2ik\pi$ for some $k \in \mathbb{Z}$"

p. 357 Exercise 7, instead of " Find also" read ". Find also"

p. 359 Exercise 26, instead of "Let ω_i" read "Let $(\omega_i)_{1 \le i \le n}$"

p. 411 end of Exercise 9, replace "[Mes3]" by "[Nag]" and replace "rank 12" by "rank 13"

p. 422 line -2, instead of "[Mon1]" read "[Mon2]"

p. 432 line 14, instead of "lowest" read "least"

p. 433 line 6, instead of "occurs (in step 6)" read "occurs in step 6"

p. 441 line -7, instead of "$y = tx$" read "$x = ty$"

p. 446 line 5, -12 (twice) and line -8, instead of "n" read "N"

p. 448 line 7, instead of "$an = p^{v_p(a)-v_p(b)}b$" read "$an = p^{v_p(a)-v_p(b)}bm$"

p. 456 line 1, instead of "If $p \ge 3$" read "If $p \ge 3$ or $p = 2$ and $k = 2$"

p. 456 line 7, instead of "$j^2\left(\chi_{2,q}^{2^{k-3}}, \chi_{2,q}^{2^{k-3}}\right)$" read "$j^2\left(\chi_{2,q}^{2^{k-3}}, \chi_{2,q}^{3\cdot 2^{k-3}}\right)$"

p. 457 line 4, instead of "$2\delta_N$" read "δ_N"

p. 474 line 5, instead of "[Coh-Len1]" read "(see Section 5.10.1 and [Coh-Len1])"

p. 497 Exercise 8, instead of "$x \in \mathbb{Z}_K$" read "$x = a + b\theta \in \mathbb{Z}_K$" and at the end replace "." by ", where $\left(\frac{x}{\mathfrak{p}}\right)$ is defined in Exercise 19 of Chapter 4."

p. 497 line 1 of Exercise 9, instead of "numbers the" read "numbers, the"

p. 523 line -2, before [Duv] insert the following reference:

"[**Duk**] W. Duke, *Hyperbolic distribution functions and half-integral weight Maass forms*, Invent. Math. **92** (1988), 73–90."

p. 530 insert index entry "Duke, W.", 293