Errata et Addenda to the Third and Fourth Corrected Printings of A Course in Computational Algebraic Number Theory

by **Henri Cohen**

(20001127 version)

Warning. The errata presented here are of course to be taken into account for the first and second printing, but the page and line numbering given here corresponds to the third and fourth printings and is quite different from that of the preceding printings.

Graduate Texts in Mathematics 138, Springer-Verlag, 1993,
Third, Corrected Printing 1996, XX + 545 pages.
ISBN 3-540-55640-0 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-55640-0 Springer-Verlag New York Berlin Heidelberg

p. VI at Shanks, add the footnote "Daniel Shanks died on September 6, 1996"

p. VI middle and p. VII line 11, instead of "Francois Dress" read "François Dress"

p. VI line -1, instead of "Jean-Francois Mestre, Francois Morain" read "Jean-François Mestre, François Morain"

p. 11 just before "Quite a different way" insert the following long text

"Perhaps surprisingly, we can easily improve on Algorithm 1.2.4 by using a flexible window of size at least k bits, instead of using a window of fixed size k. Indeed, it is easy to see that any positive integer N can be written in a unique way as

$$N = 2^{t_0}(a_0 + 2^{t_1}(a_1 + \cdots + 2^{t_e}a_e))$$

where $t_i \geq k$ for $i \geq 1$ and the a_i are odd integers such that $1 \leq a_i \leq 2^k - 1$ (in Algorithm 1.2.4 we took $t_0 = 0$, $t_i = k$ for $i \geq 1$, and $0 \leq a_i \leq 2^k - 1$ odd or even).

As before, we can precompute g^3, g^5, … , g^{2^k-1} and then compute g^N by successive squarings and multiplications by g^{a_i}. To find the a_i and t_i, we use the following immediate sub-algorithm.

Sub-Algorithm 1.2.4.1 (Flexible Base 2^k Digits). Given a positive integer N and $k \geq 1$, this sub-algorithm computes the unique integers t_i and a_i defined above. We use $[N]_{b,a}$ to denote the integer obtained by extracting bits a through b (inclusive) of N, where bit 0 is the least significant bit.

```
1. [Compute $t_0$] Let $t_0 \leftarrow v_2(N)$, $e \leftarrow 0$ and $s \leftarrow t_0$.
2. [Compute $a_e$] Let $a_e \leftarrow [N]_{s+k-1,s}$.
3. [Compute $t_e$] Set $m \leftarrow [N]_{\infty,s+k}$. If $m = 0$, terminate the sub-algorithm. Otherwise, set $e \leftarrow e+1$, $t_e \leftarrow v_2(m)+k$, $s \leftarrow s+t_e$ and go to step 2.
```

The flexible window algorithm is then as follows.

Algorithm 1.2.4.2 (Flexible Left-Right Base 2^k). Given $g \in G$ and $n \in \mathbb{Z}$, this algorithm computes g^n in G. We write 1 for the unit element of G.

```
1. [Initialize] If $n = 0$, output 1 and terminate. If $n < 0$ set $N \leftarrow -n$ and $z \leftarrow g^{-1}$. Otherwise, set $N \leftarrow n$ and $z \leftarrow g$.
```

2. [Compute the a_i and t_i] Using the above sub-algorithm, compute a_i, t_i and e such that $N = 2^{t_0}(a_0 + 2^{t_1}(a_1 + \cdots + 2^{t_e}a_e))$ and set $f \leftarrow e$.
3. [Precomputations] Compute and store z^3, z^5, ... , z^{2^k-1}.
4. [Loop] If $f = e$ set $y \leftarrow z^{a_f}$ otherwise set $y \leftarrow z^{a_f} \cdot y$. Then repeat t_f times $y \leftarrow y \cdot y$.
5. [Finished?] If $f = 0$, output y and terminate the algorithm. Otherwise, set $f \leftarrow f - 1$ and go to step 4.

We have used above the word "surprisingly" to describe the behavior of this algorithm. Indeed, it is not a priori clear why it should be any better than Algorithm 1.2.4. An easy analysis shows, however, that the average number of multiplications which are not squarings is now of the order of $2^{k-1} + \lg|n|/(k+1)$ (instead of $2^{k-1} + \lg|n|/k$ in Algorithm 1.2.4), see Exercise 33. The optimal value of k is the smallest integer satisfying the inequality $\lg|n| \le (k+1)(k+2)2^{k-1}$.

In the above example where n has 100 decimal digits, the flexible base 2^5 algorithm takes on average $(3/4)332 + 16 + 332/6 \approx 320$ multiplications, another 3% improvement. In fact, using a simple modification, in certain cases we can still easily improve (very slightly) on Algorithm 1.2.4.2, see Exercise 34."

p. 11 line -11, instead of "the 2^k algorithm" read "the flexible 2^k algorithm"

p. 17 in Algorithm 1.3.7, remove the initializations "$A \leftarrow 1$, $B \leftarrow 0$, $C \leftarrow 0$, $D \leftarrow 1$" from step 1 and put them instead at the end of step 2

p. 45 add the following exercises.

"33. Show that, as claimed in the text, the average number of multiplications which are not squarings in the flexible left-right base 2^k algorithm is approximately $2^{k-1} + \lg|n|/(k+1)$, and that the optimal value of k is the smallest integer such that $\lg|n| \le (k+1)(k+2)2^{k-1}$.

34. Consider the following modification to Algorithm 1.2.4.2. We choose some odd number L such that $2^{k-1} < L < 2^k$ and precompute only z, z^3, ... , z^L. Show that one can write any integer N in a unique way as $N = 2^{t_0}(a_0 + 2^{t_1}(a_1 + \cdots + 2^{t_e}a_e))$ with a_i odd, $a_i \le L$, and $t_i \ge k - 1$ for $i \ge 1$, but $t_i = k - 1$ only if $a_i > L - 2^{k-1}$. Analyze the resulting algorithm and show that, in certain cases, it is slightly faster than Algorithm 1.2.4.2."

p. 52 line -1, instead of "column" read "column, with $k+1 \le i \le n$"

p. 69 step 4 of Algorithm 2.4.5, instead of "set $k \leftarrow k+1$ and go to step 5" read "set $k \leftarrow k+1$, and if $l > 1$ and $i = l$ set $l \leftarrow l - 1$, then go to step 5"

p. 72 line 4 of step 4 of Algorithm 2.4.8, instead of "$W_j \leftarrow W_j - qW_i$" read "$W_j \leftarrow W_j - qW_i \bmod R$"

p. 73 line -3, instead of "last $n - r + 1$" read "last $n - r$"

p. 129 line 4, instead of "$p = 2$" read "$p > 2$"

p. 129 line -20, instead of "$U \circ T$" read "$U \circ T \bmod A$"

p. 156 line -17, instead of "$A_1(b) < 0$ when" read "$A_1(b) < 0$ if and only if"

p. 157 line -8, instead of "Proposition 4.8.6" read "Theorem 4.8.6"

p. 159 line -5, instead of "$r_{i,k}$" read "$r_{k,i}$"

p. 159 line -4, instead of "$(r_{0,k}, r_{1,k}, \ldots, r_{n-1,k}, 1)$" read "$(r_{k,0}, r_{k,1}, \ldots, r_{k,n-1}, 1)$" and instead of "$r_{i,k}$" read "$r_{k,i}$"

p. 159 line -3, instead of "$r_{i,0}$" read "$r_{0,i}$"

p. 160 line 10, instead of "$r_{i,j}$" read "$r_{k,i}$"

p. 161 middle, instead of “This will in practice be considered as a $r_1 + 2r_2 = n$-uplet of real numbers. Now operations” read “Operations”

p. 168 line 8 and 9, instead of “p is an odd prime” read “p is a prime”

p. 176 lines 12 to 15, replace the four lines of the end of the

proof starting with “If we set γ...” by “It follows that the vector of the $(P(\beta_i))$ and of the $\alpha_{\phi(i)}$ are both solutions of the linear system $\sum_{1\le i\le n} v_i\beta_i^h = s_h$, and since the β_i are distinct this system has a unique solution, so the vectors are equal, thus proving the proposition.”

p. 179 line -3 and p. 180 line -11, instead of “a^{m-1}” read “a^{n-1}”

p. 184 line -8, instead of “so $M \subset M'$” read “so M annihilates IH/IJ hence $M \subset M'$”

p. 193 line 11, add “Note that this is simply the proof of the Chinese remainder theorem for ideals.”

p. 195 line 2 of Algorithm 4.7.10, instead of “$\mathbb{Z}_K$-generators” read “$\mathbb{Z}$-generators”

p. 195 line 1 of step 3 of Algorithm 4.7.10, instead of “$2 \le i \le m$” read “$2 \le i \le k$”

p. 195 line 2 of step 4 of Algorithm 4.7.10, instead of “$j + 1 \le i \le m$” read “$j + 1 \le i \le k$”

p. 200 line 14, instead of “$e_i = f_i$” read “$d_i = e_i$”

p. 201 line -5, instead of “Then $y \notin xR$ and $y\mathfrak{p} \subset xR$, hence $a = y/x$” read “Since $y\mathfrak{p} \subset xR$, the element $a = y/x$”

p. 202 line -10, instead of “ $\displaystyle\sum_{1\le\le n}$ ” read “ $\displaystyle\sum_{1\le i\le n}$ ”

p. 204 line 3 of step 3, instead of “0” read “0”

p. 204 line 1 of step 5, instead of “If $p \nmid A_{n,n}$,” read “Using Algorithm 2.4.8, replace A by its HNF. Then, if $p \nmid A_{n,n}$,”

p. 206 line -7, instead of “determinant $d(K)$” read “discriminant $d(K)$”

p. 211 line -13 and -12, instead of “where $\|x\|$ denotes the absolute value of x when x is real and the square of the modulus of x when x is complex” read “where $\|\sigma(x)\| = |\sigma(x)|$ if σ is a real embedding and $\|\sigma(x)\| = |\sigma(x)|^2$ if σ is a complex embedding”

p. 216 line 1, instead of “$\dfrac{1}{6}$” read “$\dfrac{1}{60}$”

p. 217 line -4, instead of “$A \leftarrow 8b - 3a^2$” read “$A \leftarrow 3a^2 - 8b$” and line -2, instead of “$(r_1, r_2) = (0, 4)$ iff $D > 0$ and $AB < 0$” read “$(r_1, r_2) = (0, 2)$ iff $D > 0$ and either $A \le 0$ or $B \le 0$”

p. 224 line -2, replace 4 times small parentheses by larger ones

p. 227 line 1, instead of “$(-b + \sqrt{D})/2a$” read “$(-b + \sqrt{D})/(2a)$”

p. 234 line -6, instead of “$H(0) = -1/12$” read “$H(N) = -1/12$”

p. 237 line -13, instead of “Let D be a negative fundamental discriminant” read “Let D be a negative discriminant (not necessarily fundamental)”

p. 237 line -10 and -9, instead of “entire function satisfying” read “entire function. If in addition D is a fundamental discriminant, this function satisfies the functional equation”

p. 240 line 4, instead of “time” read “average time”

p. 246 line 7, instead of “$I_i = a_i\mathbb{Z} + \tau_i\mathbb{Z}$” read “$I_i = a_i(\mathbb{Z} + \tau_i\mathbb{Z})$”

p. 246 line 9, instead of “$\tau_3 = ua_1\tau_2 + va_2\tau_1 + w\tau_1\tau_2$” read “$\tau_3 = (d/d_0)(u\tau_2 + v\tau_1 + w\tau_1\tau_2)$”

p. 248 line 2 of step 3 of Algorithm 5.4.8, instead of “$c_2 = c_2 + gd_1$” read “$c_2 \leftarrow c_2 + gd_1$”

p. 249 line 2 of step 6 of Algorithm 5.4.9, instead of “$c_3 \leftarrow v_3 d + gd_1$” read “$c_3 \leftarrow v_3 f + gd_1$”

p. 250 line -16, instead of “guess that $h(D)$” read “guess that, for $D < -4$, $h(D)$”

p. 252 line 7, instead of “[McCur-Haf]” read “[Haf-McCur1]”

p. 262 line -5, instead of “reduced form” read “quadratic form”

p. 262 line -3, after (1) insert “If (a, b, c) is reduced, then”

p. 262 line -2, instead of “More precisely” read “More precisely, if (a, b, c) is reduced”

p. 276 line -7, add a white square at the end of the line

p. 280 line -6, instead of “positive norm.” read “positive norm. By abuse of notation, we will again denote by $\delta(f, g)$ the unique representative belonging to the interval $[0, R^+[$, and similarly for the distance between ideals.”

p. 282 line -16, instead of “very small.” read “very small. More precisely, it can be proved (see [Len1]) that $\delta(f, \rho^2(f)) > \ln 2$, hence the number of reduction steps is at most $4\ln(D)/\ln 2$.”

p. 289 line -19, instead of “$\delta(\mathbf{1}, f) = (eL\ln 2 + \ln R)/2$” read “$\delta(f_0, f) = (eL\ln 2 + \ln R)/2$ for some fixed form f_0 equivalent to f”

p. 290 line 20, instead of “$\delta(\mathbf{1}, f)$” read “$\delta(\prod_{p\le P} f_p^{e_p}, f)$”

p. 290 line -6, instead of “$g = \prod_{p\le P} f_p^{v_p}$” read “$g = \prod_{p\le P} f_p^{\varepsilon_p v_p}$”

p. 290 line -1, instead of “$f_{p_i}^{a_{i,j}}$” read “$f_{p_i}^{-a_{i,j}}$”

p. 291 line 9, instead of “$a_{n+1,j} =$” read “$a_{n+1,j} \equiv$”

p. 304 lines -12 and -11, instead of “again by the binomial theorem” read “using this time the multinomial theorem instead of the binomial theorem”

p. 321 step 9, instead of “s” read “f” (3 times)

p. 322 step 14, instead of “r” read “s” (7 times) and instead of “d” read “r” (3 times)

p. 340 line 3, instead of “$(\overline{f}, \overline{gh}) = 1$” read “$(\overline{f}, \overline{g}, \overline{h}) = 1$”

p. 343 line 3 of Corollary 6.4.12, instead of “$\dfrac{-3v \pm u}{6v}$” read “$\dfrac{-3v \mp u}{6v}$”

p. 359 line 4 of step 5, instead of “the matrix is not of maximal rank” read “one of the matrices H or C is not of maximal rank”

p. 368 and following major correction (oversight in all the previous printings): exchange in most places “ω_1” and “ω_2”, except p. 415 where the “ω_2” is correct. In particular, the canonical basis (ω_1, ω_2) for a real elliptic curve is now such that ω_2 is real and ω_1 is in the upper half plane. Specifically, the corrections are p. 368, p. 370, p. 378, twice p. 395, five times page 396, twice p. 398 and p. 412 replace “ω_2/ω_1” by “ω_1/ω_2”, twice p. 395 and twice p. 396 replace “$2\pi/\omega_1$” by “$2\pi/\omega_2$”, twice p. 396 replace “$c\omega_2 + d\omega_1$” by “$c\omega_1 + d\omega_2$”, twice p. 396 and p. 398 replace z/ω_1 by z/ω_2, three times p. 396, six times p. 398, twice p. 399 and p. 412 replace an isolated “ω_1” by “ω_2”, twice p. 398 and five times p. 399 (but *not* p. 415) replace an isolated “ω_2” by “ω_1”. Although not mathematically necessary, it is then more aesthetic to replace everywhere “$\mathbb{Z} + \mathbb{Z}\tau$” by “$\mathbb{Z}\tau + \mathbb{Z}$”.

p. 392 line -16, instead of “$n \ge 2$” read “$n \le 2$”

p. 395 line -1, add the following: “**Warning.** The condition $m \ge 1$ in step 3 should in practice be implemented as $m > 1 - \varepsilon$ for some small $\varepsilon > 0$ depending on the current accuracy. If this precaution is not taken the algorithm may loop indefinitely, and the cost is simply that the final τ may land very close to but not exactly in the standard fundamental domain, and this has absolutely no consequence for practical computations."

p. 407 line 2 of step 3, instead of "set $c \leftarrow 1$" read "set $c \leftarrow \nu$"

p. 408 line 1 of step 9, instead of "$a_4 and p^3$" read "a_4 and p^3"

p. 408 line 2 of step 9, instead of "a^6" read "a_6"

p. 408 line 1 of step 11, instead of "$X^2+a_3/p^2X+a_6/p^4$" read "$X^2+a_3/p^2X-a_6/p^4$"

p. 408 line -1, instead of "$c \leftarrow 1\ T \leftarrow II^*$" read "$c \leftarrow 1$, $T \leftarrow II^*$"

p. 416 line -4, instead of "$f_1(\sqrt{D})$" read "$f_1(\sqrt{D/4})$"

p. 417 line 4 of Exercise 1, instead of "and $b_2 \equiv 0$,... respectively" read "and $b_2 \equiv -c_6 \pmod{12}$"

p. 425 line 3 of Section 8.4, instead of "may be factor" read "may be a factor"

p. 432 line 8, instead of "Proposition 8.5.3" read "Proposition 8.5.4"

p. 435 line -3, instead of "corresponding to $\mathfrak{b}$" read "corresponding to $\mathfrak{b}^{-1}$"

p. 436 line 1, instead of "$\delta(g_1, g) =$" read "$\delta(g_1, g^{-1}) =$"

p. 440 line 19, instead of "It is also however also" read "It is however also"

p. 440 line -10, instead of "We must show how are we going" read "We must explain how we are going"

p. 452 line -6, instead of "$\max(e, k+1))$" read "$\max(e, k+u))$ where u is as in Lemma 9.1.10"

p. 452 line -5, instead of "Proposition 9.1.8" read "Lemma 9.1.8"

p. 453 middle, after "prime r dividing N" insert "(by Lemma 9.1.10 and our choice of ℓ)"

p. 454 line -16, instead of "of order" read "of order dividing"

p. 462 line 3 of the proof of Lemma 9.1.24, instead of "$j_3(\chi,\chi,\chi) =$" read "$j_3(\chi,\chi,\chi)^\gamma =$"

p. 474 step 4 of Algorithm 9.2.4, instead of "$(x+3y)$" read "$(x+3y)/2$" (twice) and instead of "$(x-3y)$" read "$(x-3y)/2$" (twice)

p. 476 line 3 of Exercise 7. instead of "$\chi(x) \neq 1$" read "$\chi(x) \neq 0$ and 1"

p. 476 Exercise 7, add the following question.

" c) Show that if χ is a primitive character modulo q which is not necessarily a prime, we still have $|\tau(\chi)| = \sqrt{q}$."

p. 478 line 5, instead of "$\varepsilon = 0$ or 1" read "$\varepsilon_k = 0$ or 1"

p. 480 line 2 of the second remark, instead of "a follows" read "as follows"

p. 482 lines 4, 14, 16, 19, instead of "$1/2a$" read "$1/(2a)$"

p. 487 middle, instead of "$t = 0 \pmod{N}$" read "$t \equiv 0 \pmod{N}$"

p. 490 line -12, instead of "we note than one can" read "we note that one can"

p. 490 line -1, instead of "Pomerance ," read "Pomerance,"

p. 494 line -4, instead of "is t is the" read "if t is the"

p. 499 line 9, instead of "$\mathcal{N}(a+b\theta)$" read "$\ln(\mathcal{N}(a+b\theta))$"

p. 500 line 19, instead of "Let V is the column" read "Let V be the column"

p. 528 before [Lang1], add the following: "One can find at the URL

`http://www-cs-faculty.stanford.edu/~knuth/index.html`

nearly 350 pages of corrections and additions to [Knu1], [Knu2] and [Knu3], absolutely necessary for those having the older editions of Knuth's books. This has been incorporated in a new 3 volume set which came out in 1996."

p. 535 in [Len-Len2], instead of "nmber field" read "number field"

p. 538 instead of “[**de Weg**] de Weger B.,” read “[**deWeg**] B. de Weger,”