**Errata et Addenda to the Book**

**A Course in Computational Algebraic Number Theory**

by **Henri Cohen**

(19940513 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 add "Andrew Odlyzko," after "Nicolas,"
p. X line -7, instead of "algorithms" read "an algorithm"
p. XIII e-mail address, remove "`ecole.`"
p. XIII end, add the following:
"In addition, a regularly updated errata file is available by anonymous ftp from `megrez.ceremab.u-bordeaux.fr (147.210.16.17)`, directory `pub/cohenbook`."
p. XX 8.4., instead of "Lehmann" read "Lehman"
p. 1 line -13, instead of "is that it is" read "that it is"
p. 2 line -4, instead of "easily" read "easy"
p. 2 line -2 replace "Cayley/Magma" by "Magma" and insert after "Macsyma"
p. 3 line 16, instead of "not." read "not)."
p. 10 lines 1 and 2, instead of "$O(\ln m \ln |n|)$ instead of $O(\ln^2 m \ln\ln |n|)$ for" read "in average up to 1.5 times faster than"
p. 10 step 1 of Algorithm 1.2.4, instead of "$z \leftarrow g$ and $f \leftarrow e$." read "$z \leftarrow g$. Finally, set $f \leftarrow e$."
p. 13 step 1 of Algorithm 1.3.3, instead of "simple precision" read "single precision"
p. 17 step 2 of Algorithm 1.3.7, instead of "simple precision" read "single precision"
p. 20 line -4, instead of "$x_i =$" read "$x_i$"
p. 22 line 13, instead of "$\ldots]$." read "$\ldots]$)."
p. 22 replace step 3 of Algorithm 1.3.13 by the following:

"3. [Output quotient] Set $a_i \leftarrow q$ and output $a_i$, then set $i \leftarrow i+1$, $a \leftarrow b$, $b \leftarrow r$, $a' \leftarrow b'$ and $b' \leftarrow r'$. If $b$ and $b'$ are non-zero, go to step 2. If $b = b' = 0$, terminate the algorithm. Finally, if $b = 0$ set $q \leftarrow \infty$ and $q' \leftarrow \lfloor a'/b' \rfloor$ while if $b' = 0$ set $q \leftarrow \lfloor a/b \rfloor$ and $q' \leftarrow \infty$."

p. 37 line 14, instead of "custom" read "special-purpose"
p. 37 steps 1 and 3, instead of "above" read "below"
p. 37 replace step 2 by the following:

"2. [Small degree?] If $\deg(A) = 0$, terminate the algorithm.If $\deg(A) = 1$, and $A(X) = a_1X + a_0$, output $-a_0/a_1$ and terminate the algorithm. If $\deg(A) = 2$ and $A(X) = a_2X^2 + a_1X + a_0$, set $d \leftarrow a_1^2 - 4a_0a_2$, compute $e \leftarrow \sqrt{d}$ using Algorithm 1.5.1, output $(-a_1+e)/(2a_2)$ and $(-a_1-e)/(2a_2)$, and terminate the algorithm. (Note that $e$ will exist.)"

p. 41 line 13 to line -1, replace completely by the following:

"The idea is to use the following proposition.

**Proposition 1.7.4.** *Let $n = p^k$ be a prime power. Then*

(1) *For any $a$ we have $p \mid (a^n - a, n)$.*
(2) *If $k \ge 2$ and $p > 2$, let $a$ be a witness to the compositeness of $n$ given by the Rabin-Miller test 8.2.2, i.e. such that $(a, n) = 1$, and if $n - 1 = 2^t q$ with $q$ odd, then $a^q \not\equiv 1 \pmod{n}$ and for all $e$ such that $0 \le e \le t-1$ then $a^{2^e q} \not\equiv -1 \pmod{n}$. Then $(a^n - a, n)$ is a non-trivial divisor of $n$ (i.e. is different from 1 and $n$).*

Typeset by $\mathcal{AMS}$-TeX

*Proof.* By Fermat's theorem, we have $a^n \equiv a \pmod{p}$, hence (1) is clear. Let us prove (2). Let $a$ be a witness to the compositeness of $n$ as defined above. By (1), we already know that $(a^n - a, n) > 1$. Assume that $(a^n - a, n) = n$, i.e. that $a^n \equiv a \pmod{n}$. Since $(a, n) = 1$ this is equivalent to $a^{n-1} \equiv 1 \pmod{n}$, i.e. $a^{2^t q} \equiv 1 \pmod{n}$. Let $f$ be the smallest non-negative integer such that $a^{2^f q} \equiv 1 \pmod{n}$. Thus $f$ exists and $f \le t$. If we had $f = 0$, this would contradict the definition of a witness ($a^q \not\equiv 1 \pmod{n}$). So $f > 0$. But then we can write

$$p^k \mid (a^{2^{f-1}q} - 1)(a^{2^{f-1}q} + 1)$$

and since $p$ is an odd prime, this implies that $p^k$ divides one of the two factors. But $p^k \mid (a^{2^{f-1}q} - 1)$ contradicts the minimality of $f$, and $p^k \mid (a^{2^{f-1}q} + 1)$ contradicts the fact that $a$ is a witness (we cannot have $a^{2^e q} \equiv -1 \pmod{n}$ for $e < t$), hence we have a contradiction in every case thus proving the proposition. □

This leads to the following algorithm.

**Algorithm 1.7.5** (Prime Power Test). Given a positive integer $n > 1$, this algorithm tests whether or not $n$ is of the form $p^k$ with $p$ prime, and if it is, outputs the prime $p$.

1. [Case $n$ even] If $n$ is even, set $p \leftarrow 2$ and go to step 4. Otherwise, set $q \leftarrow n$.

2. [Apply Rabin-Miller] By using Algorithm 8.2.2 show that either $q$ is a probable prime or exhibit a witness $a$ to the compositeness of $q$. If $q$ is a probable prime, set $p \leftarrow q$ and go to step 4.

3. [Compute GCD] Set $d \leftarrow (a^q - a, q)$. If $d = 1$ or $d = q$, then $n$ is not a prime power and terminate the algorithm. Otherwise set $q \leftarrow d$ and go to step 2.

4. [Final test] (Here $p$ is a divisor of $n$ which is almost certainly prime.) Using a primality test (see Chapters 8 and 9) prove that $p$ is prime. If it is not (an exceedingly rare occurence), set $q \leftarrow p$ and go to step 2. Otherwise, by dividing $n$ by $p$ repeatedly, check whether $n$ is a power of $p$ or not. If it is not, $n$ is not a prime power, otherwise output $p$. Terminate the algorithm.

We have been a little sloppy in this algorithm. For example in step 4, instead of repeatedly dividing by $p$ we could use a binary search analogous to the binary powering algorithm. We leave this as an exercise for the reader (Exercise 4)."

p. 48 line 1 of step 5 of Algorithm 2.2.1, instead of "$k > l$" read "$k > j$"

p. 51 replace the last two lines of Proposition 2.2.5 by the following:

"Finally, let $c_n = a_{n,n}^{(n-1)}$. Then all the divisions by $c_{k-1}$ are exact; we have $\det(M_k) = c_k^{n-k-1}\det(M_0)$, and in particular $\det(M_0) = c_n$."

p. 51 line -15, instead of "$k + 1 \times k + 1$" read "$(k+1) \times (k+1)$"

p. 51 line -4 instead of "$sM_{n,n}$" read "$sm_{n,n}$"

p. 59 line -2 instead of "a $m \times r$" read "an $m \times r$"

p. 59 line -2 instead of "$r \le n \le m$" read "$n \le m$"

p. 59 line -1 instead of "a $n \times r$" read "an $n \times r$"

p. 61 lines 5 to 8, replace step 4 by the following:

"4. [Modify basis and eliminate] Set $B_t \leftarrow B_s$ (if $t \ne s$), then set $B_s \leftarrow M_s$. Then for $j = s+1$, ... ,$k$, do as follows. Exchange $m_{s,j}$ and $m_{t,j}$ (if $t \ne s$). Set $m_{s,j} \leftarrow dm_{s,j}$. Then for all $i \ne s$ and $i \ne t$, set $m_{i,j} \leftarrow m_{i,j} - m_{i,s}m_{s,j}$. Finally, go to step 2."

p. 61 line 2 of Algorithm 2.3.7, instead of "column" read "columns"

p. 71 lines -6 to -1, replace step 4 by the following:

"4. [Next row] Using Euclid's extended algorithm, find $(u, v, d)$ such that $ua_{i,k} + vR = d = \gcd(a_{i,k}, R)$. Set $W_i \leftarrow uA_k \bmod R$ (here taken in the interval $[0, R-1]$). If $w_{i,i} = 0$ set $w_{i,i} \leftarrow R$. For $j =$

$i+1, \ldots, m$ set $q \leftarrow \lfloor w_{i,j}/w_{i,i} \rfloor$ and $W_j \leftarrow W_j - qW_i$. If $i = 1$, output the matrix $W = (w_{i,j})_{1 \le i,j \le m}$ and terminate the algorithm. Otherwise, set $R \leftarrow R/d$, $i \leftarrow i-1$, $k \leftarrow k-1$, $j \leftarrow k$, and if $a_{i,k} = 0$ set $a_{i,k} \leftarrow R$. Go to step 2."

p. 73 line 2 of step 4 of Algorithm 2.4.10, instead of "step 6" read "step 5"

p. 87 line 6, instead of "set", read "set (in this order)"

p. 87 line 6, just before "$B_k \leftarrow B_{k-1}B_k/B$" insert "$\mathbf{b} \leftarrow \mathbf{b}^*_{k-1}$, $\mathbf{b}^*_{k-1} \leftarrow \mathbf{b}^*_k + \mu\mathbf{b}$, $\mathbf{b}^*_k \leftarrow -\mu_{k,k-1}\mathbf{b}^*_k + (B_k/B)\mathbf{b}$, "

p. 94 just before step 1, instead of "$\mathbf{r} \cdot \mathbf{b}_i = 0$ for all $i$" read "$\sum_{1 \le i \le n} r_i \mathbf{b}_i = 0$"

p. 94 line -5, after "echange $B_k$ and $B_{k-1}$", insert ", exchange $\mathbf{b}^*_k$ and $\mathbf{b}^*_{k-1}$"

p. 94 line -3, after "$B_{k-1} \leftarrow B$", insert ", $\mathbf{b}^*_{k-1} \leftarrow \mu\mathbf{b}^*_{k-1}$"

p. 94 line -1, after "$\mu_{k,k-1} \leftarrow \mu t$" insert "$\mathbf{b} \leftarrow \mathbf{b}^*_{k-1}$, $\mathbf{b}^*_{k-1} \leftarrow \mathbf{b}^*_k + \mu\mathbf{b}$, $\mathbf{b}^*_k \leftarrow -\mu_{k,k-1}\mathbf{b}^*_k + (B_k/B)\mathbf{b}$, "

p. 95 line 10, instead of "it itself" read "is itself"

p. 101 line 7, instead of "$n+1 \times n$" read "$(n+1) \times n$"

p. 106 Exercise 28, instead of "In" read "in"

p. 106 line -3, instead of "accordingly" read "accordingly."

p. 107 line 2, instead of "Chapter 3.)" read "Chapter 3)."

p. 108 line 3, instead of "[Knu1]" read "[Knu2]"

p. 110 last line of Algorithm 3.1.1, instead of "got to" read "go to"

p. 114 line -4, instead of "$s = \prod_p p^{v_p(s)}$" read "$s = u\prod_p p^{v_p(s)}$"

p. 114 line -3, instead of "where" read "where $u$ is a unit,"

p. 117 lines 12 to 16, replace the two sentences starting with "We can still divide" and ending with "algorithm." by

"We could still try to divide $A$ and $B$ by their content from time to time (say every 10 iterations), but this would usually be a very bad idea (see Exercise 4)."

p. 117 end of step 1, instead of ", $h \leftarrow 1$ and $c \leftarrow 0$." read " and $h \leftarrow 1$.

p. 117 replace completely step 3 by

"3. [Reduce remainder] Set $A \leftarrow B$, $B \leftarrow R/(gh^\delta)$, $g \leftarrow \ell(A)$, $h \leftarrow h^{1-\delta}g^\delta$ and go to step 2. (Note that all the divisions which may occur in this step give a result in the ring $\mathcal{R}$.)"

p. 121 lines 1 to 3, suppress the two sentences "Contrary to ... Exercise 4)."

p. 124 lines -10 and -9, replace the sentence "For $k \ge 2$,...$T_k = T_{k-1}/V_k$." by

"For $k \ge 1$, set $V_{k+1} = (T_k, V_k)$ if $p \nmid k$, $V_{k+1} = V_k$ if $p \mid k$, and $T_{k+1} = T_k/V_{k+1}$."

p. 125 line 1, instead of "$A =\in \mathbb{F}_p[X]$" read "$A \in \mathbb{F}_p[X]$"

p. 125 line -6, instead of " and go to step 2" read ". Go to step 2."

p. 126 line 3, instead of "(see Knu2])" read "(see [Knu2])"

p. 128 lines 1 and 2 of step 2, instead of "Set $C \leftarrow T \ldots C \leftarrow C + D$." read "Set $C \leftarrow T$ and then repeat $d-1$ times $C \leftarrow T + C^2 \bmod A$."

p. 128 line -21 to -19, instead of "Knuth gives ... power of 2" read "Knuth gives $C \leftarrow C + C^2 \bmod A$, but this should be instead, as above, $C \leftarrow T + C^2 \bmod A$"

p. 132 line 2, instead of "degree $n$," read "degree $n$ (with $p \ge 3$),"

p. 132 line 2 of step 4 of Algorithm 3.4.11, instead of "$\deg(D) > 1$" read "$\deg(D) > 0$"

p. 132 line 3 of step 4 of Algorithm 3.4.11, instead of "computations" read "computation"

p. 132 end of Algorithm 3.4.11, put the "3" on the same line as "go to step" (this is not a misprint, but an important TEXnical change)

p. 136 line -9, instead of "$S \equiv (VD \bmod A_e) \pmod p$ and $T \equiv (UD \bmod B_e) \pmod p$" read "$S \equiv VD + WA_e \pmod p$ and $T \equiv UD - WB_e \pmod p$ for some polynomial $W$"

p. 143 line 1, instead of "$n$" read "$m$"

p. 143 line 4, instead of "$1 \leq j \leq n$" read "$1 \leq j \leq m$"
p. 143 line 14, instead of "$N_i^n$" read "$N_i^m$"
p. 143 line 14, instead of "$N_i^{n'}$" read "$N_i^{m'}$"
p. 143 line 15, instead of "$n' \leq n$" read "$m' \leq m$"
p. 147 replace Exercise 4 by the following.

"4. Modify Algorithm 3.3.1 so that $A$ and $B$ are divided by their respective contents every 10 iterations. Experiment and convince yourself that this modification leads to polynomials $A$ and $B$ having much larger coefficients later on in the Algorithm, hence that this is a bad idea."

p. 147 Exercise 5, instead of "$r \times (A, B)$" read "$r \cdot (A, B)$"
p. 162 line -13, instead of "$Z$" read "$\mathbb{Z}$"
p. 163 line -9, instead of "independent" read "dependent"
p. 185 middle, instead of "$N_{K/\mathbb{Q}}(x)$" read "$\mathcal{N}_{K/\mathbb{Q}}(x)$"

p. 189 **Addendum.** Line -9, replace the 4 lines starting with "We can always assume" and ending with "(see Exercise 17)." by the following.

"We do however have the following corollary:

**Corollary 4.7.6.5.** *Let $R$ be an order in $K$ containing $\theta$, let $\omega_1, \dots, \omega_n$ be the HNF basis of $R$ with respect to $\theta$, and let $d_1 = 1, d_2, \dots, d_n$ be the integers defined in the preceding corollary. Further, let $M$ be an $R$-module of rank $n$ over $\mathbb{Z}$ and let $(A, d)$ be its HNF with respect to the basis $\omega_1, \dots, \omega_n$, where $d$ is the denominator and $A = (a_{i,j})$ is an integral matrix in upper triangular HNF. Then for every $i$ and $j$ with $i \leq j$, $a_{j,j}$ divides $a_{i,j}$ and $a_{j,j}$ divides $\frac{d_j}{d_i} a_{i,i}$. In other words, the HNF basis of $M$ has the form*

$$\alpha_j = \frac{z_j}{d}\left(\omega_j + \sum_{1 \leq i < j} h_{i,j}\omega_i\right) \quad ,$$

*where the $z_j$ are positive integers such that $z_j \mid \frac{d_j}{d_i} z_i$ for $i < j$ and the $h_{i,j}$ satisfy $0 \leq h_{i,j} < z_i/z_j$ for $i < j$. Furthermore, $z_1$ is the smallest positive element of $dM \cup \mathbb{Z}$.*

*Proof.* Let $M_R$ be the HNF matrix of $R$ on the powers of $\theta$, and $(B, d)$ be the HNF matrix of the module $M$ on the powers of $\theta$. It is clear that we have $A = M_R^{-1} B$, and the corollary follows immediately by expanding the matrix product and using Theorem 4.7.5 and Corollary 4.7.6. $\square$"

p. 197 line 18, instead of "$\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta)$" read $\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta)\mathbb{Z}_K$"
p. 198 line -11, instead of "$\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta)$" read $\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta)\mathbb{Z}_K$"
p. 205 middle, instead of "in the case of quadratic fields in Chapter 5." read
"for quadratic fields in Chapter 5 and for general number fields in Chapter 6."
p. 208 line 6, instead of "$R$" read "$\mathbb{R}$"
p. 211 line -1, instead of "$r_1$" read "$r_1 + r_2$"

p. 216 lines -9 to -7, instead of "If $x \in \mathbb{Z}_K \dots x - y \in p\mathbb{Z}_K$" read "If $x \in \mathbb{Z}_K$, show that there exists a unique $\varepsilon \in \{-1, 0, +1\}$ such that

$$x^{(\mathcal{N}\mathfrak{p}-1)/2} \equiv \varepsilon \pmod{\mathfrak{p}},$$

where we write $x \equiv y \pmod{\mathfrak{p}}$ if $x - y \in \mathfrak{p}$"

p. 217 Exercise 25 line 4, instead of "$\alpha$" read "$\alpha^k$"
p. 217 **Addendum.** Add the following exercise.

"28. Let $\mathfrak{p}$ be a (non-zero) prime ideal in $\mathbb{Z}_K$ for some number field $K$, let $e = e(\mathfrak{p}/p)$ be its ramification index, let $\mathfrak{p} = p\mathbb{Z}_K + \alpha\mathbb{Z}_K$ be a two-element representation of $\mathfrak{p}$, and finally let $v = v_{\mathfrak{p}}(\alpha)$. Let $a \geq 1$ and $b \geq 1$ be integers. By computing $\mathfrak{q}$-adic valuations for each prime ideal $\mathfrak{q}$, show that

$$p^a\mathbb{Z}_K + \alpha^b\mathbb{Z}_K = \mathfrak{p}^{\min(ae,bv)} \ .$$

Deduce from this formulas for computing explicitly $\mathfrak{p}^k$ for any $k \geq 1$."

p. 225 middle, replace "$\longmapsto$" by "$\longrightarrow$" four times
p. 225 line -6, instead of "$\leq 0$" read "$\leq 1$"
p. 226 line -9, instead of "i.e" read "i.e."
p. 226 line -7, instead of "to $f$" read "to $(a, b, c)$"
p. 226 line -5, instead of "$[-\frac{1}{2}, \frac{1}{2})$" read "$[-\frac{1}{2}, \frac{1}{2}[$"
p. 226 line -3, instead of "class of" read "class of positive definite"
p. 227 line 1 of Lemma 5.3.4, instead of "is a" read "be a"
p. 229 line 8, instead of "occurs for" read "occurs only for"
p. 230 line -9, insert "For $D = -N$, " before "Algorithm"
p. 230 line -7, instead of "adapted" read "adapted to compute $H(N)$ itself, "
p. 236 step 6 of Algorithm 5.4.1, replace by:

"6. [Initialize order] Set $n \leftarrow hn$.

7.[Compute the order of $g$ mod $L \cdot S$] (Here we know that $g^n \in L \cdot S$). For each prime $p$ dividing $n$, do the following: set $S_1 \leftarrow g^{n/p} \cdot S$ and sort $S_1$. If there exists a $z \in L$ such that $z \in S_1$, set $n \leftarrow n/p$ and go to step 7."

p. 236 line -7, instead of "7." read "8."
p. 236 line -6, instead of "$q \leftarrow \lfloor\sqrt{n}\rfloor$" read "$q \leftarrow \lceil\sqrt{n}\rceil$"
p. 236 line -4, instead of "Note that the" read "The"
p. 236 line -1, instead of "step 7" read "step 8"
p. 237 line 3, remove "in that case"
p. 237 line 4, instead of "step 7" read "step 8"
p. 237 line -20, instead of "and step 6" read "and step 7"
p. 238 lines 6 and 7, instead of "step 6" read "step 7"
p. 243 line -11, instead of "involves" read "involve"
p. 246 line 3, instead of "mod $p$ using" read "mod $4p$ by a simple modification of"
p. 246 step 1, instead of "Using Algorithm 1.5.1 ... $\left(\frac{D}{p}\right) = 1$." read "For the first $b$ values of $p$ such that $\left(\frac{D}{p}\right) = 1$, compute $b_p$ such that $b_p^2 \equiv D \pmod{4p}$ using Algorithm 1.5.1 (and modifying the result to get the correct parity)."
p. 247 line 9, instead of "[Buc-Dul]" read "[Buc-Dül]"
p. 249 line 4, instead of "[McCur-Haf]" read "[Haf-McCur1]"
p. 249 line -3 and -2, instead of "[Buc-Dul]" read "[Buc-Dül]"
p. 253 line 14, instead of "[Buc-Dul]" read "[Buc-Dül]"
p. 265 line 1 after Algorithm 5.7.1, instead of "note that the" read "the"
p. 274 line 18, instead of "Shanks" read "Shanks's"
p. 274 line 18, instead of "an algorithm in $O(D^{1/4+\epsilon})$" read "a $O(D^{1/4+\epsilon})$ algorithm"
p. 275 line 1, instead of "*distance*" read "distance"
p. 282 line 11, instead of "any number field" read "the representation of algebraic numbers (and not only units), and to any number field"
p. 283 middle, instead of

$$L_C(x) = (\ln\sigma_1(x), \ldots, \ln\sigma_{r_1}(x), \ln\sigma_{r_1+1}(x), \ldots, \ln\sigma_{r_1+r_2}(x)) \ ,$$

read

$$L_C(x) = (\ln \sigma_1(x), \dots, \ln \sigma_{r_1}(x), 2\ln \sigma_{r_1+1}(x), \dots, 2\ln \sigma_{r_1+r_2}(x)) \ ,$$

p. 291 lines 10 and 13 instead of "$C$" read "$A$"
p. 292 line -4 instead of "$C$" read "$A$"
p. 292 line -3, instead of "$m(Z/5\mathbb{Z})$" read "$m(\mathbb{Z}/5\mathbb{Z})$"
p. 294 suppress Exercise 24 (it is solved in the text)
p. 296 **Addendum.** End of Exercise 27, add the following:

"c) Using the Polya-Vinogradov inequality (see Exercise 8 of Chapter 9), give a better explicit upper bound for $h(D)$, asymptotic to $\frac{1}{2\pi}\sqrt{f}\ln f$."

p. 304 line -10, instead of "$\gamma_i$" read "$\overline{\gamma_i}$"
p. 304 line -5, instead of "$\gamma_j$" read "$\overline{\gamma_j}$"
p. 305 step 3 of Algorithm 6.1.8, instead of "$\omega_i$," read "$\omega_i$ (which will be the inverse of an integer by Corollary 4.7.6),"
p. 305 step 3 of Algorithm 6.1.8, instead of "$d \leftarrow D/G^2$" read "$d \leftarrow D \cdot G^2$"
p. 313 line 2, instead of "*(deterministic)*" read "*probabilistic*"
p. 313 lines -2 and -1, instead of "The details are left to the reader" read
"This will be done in the algorithm given below."
p. 316 replace steps 13 to 15 of Algorithm 6.2.9 by the following.

"13.[Factor $m(X)$] (We know that $m(X)$ is a squarefree product of linear polynomials.) By using one of the final splitting methods described in Section 3.4, or simply by trial and error if $p$ is small, factor $m(X)$ into linear factors as $m(X) = m_1(X) \cdots m_k(X)$.

14. [Split $H$] Let $d = \dim_{\mathbb{F}_p}(\overline{H})$. For $r = 1, \dots, k$ do as follows. Set $\beta_r \leftarrow m_r(\alpha)$, let $M_r$ be the $n \times (d+n)$ matrix over $\mathbb{F}_p$ whose first $d$ columns give the basis of $\overline{H}$ and the last $n$ express $\omega_i\beta_r$ on the integral basis. Finally, let $\overline{H_r}$ be the image of $M_r$ computed using Algorithm 2.3.2.

15. [Update list] Remove $\overline{H}$ and add $\overline{H_1}, \dots, \overline{H_k}$ to the list $\mathcal{L}$, set $c \leftarrow c + k - 1$ and go to step 8."

p. 316 line 13, add: "The validity of steps 14 and 15 of the algorithm is left as an exercise for the reader (Exercise 27)."
p. 323 line -7, instead of "The one" read "The algorithm"
p. 327 line 10, instead of "7, 8, 9 and 10" read "7, 8, 9, 10 and 11"
p. 332 line 5, instead of "$b_k + 2a_k$" read "$m_k + 2l_k$"
p. 341 line 1, instead of "we cannot" read "when $3 \mid m$ we cannot"
p. 341 line 7, instead of "prime" read "primes"
p. 344 line -6, instead of "$,(\omega - b(2+a^2)/3)\mathbb{Z}$" read "$+(\omega - b(2+a^2)/3)\mathbb{Z}$"
p. 345 line 5, instead of "$\mathfrak{p}_1 \in \mathfrak{p}_1 p_2$" read "$\mathfrak{p}_1 \subset \mathfrak{p}_2$"
p. 345 line 16, instead of "$a^2b^4 \equiv 1 \mod 27$" read "$a^2b^4 \equiv 1 \pmod{27}$"
p. 354 middle, instead of "Hermite reductions" read "Smith reduction matrices"
p. 356 line 2 of Step 7, instead of "$r_1 \le i \le r_u$" read "$r_1 < i \le r_u$"
p. 356 replace Exercise 3 by the following:

"3. (F. Diaz y Diaz.) With the notations of Theorem 6.1.4, show that a restatement of the Dedekind criterion is the following. Let $r_i(X)$ be the remainder of the Euclidean division of $T(X)$ by $t_i(X)$. We have evidently $r_i \in p\mathbb{Z}[X]$. Set $d_i = 1$ if $e_i \ge 2$ and $r_i \in p^2\mathbb{Z}[X]$, $d_i = 0$ otherwise. Then in (3) we can take $U(X) = \prod_{1 \le i \le k} t_i^{e_i - d_i}$. In particular, $\mathbb{Z}[\theta]$ is $p$-maximal if and only if $r_i \notin p^2\mathbb{Z}[X]$ for every $i$ such that $e_i \ge 2$."

p. 357 Exercise 10, question c) should be on the next line
p. 359 add the following exercise:

"27. Let $m(X) = m_1(X)\cdots m_k(X)$ be the decomposition of $m(X)$ obtained in step 13 of Algorithm 6.2.9. For $1 \le r \le k$, let $e_r$ be a lift to $\mathcal{O}$ of $m_r(\alpha)$, and set $H_r = H + e_r\mathcal{O}$. Show that $H = H_1 \cdots H_r$, and hence that steps 14 and 15 of Algorithm 6.2.9 are valid. (Note: the $e_r$ are *not* orthogonal idempotents.)"

p. 369 line 6, instead of "[Kam]" read "([Kam])"

p. 369 lines 6-7, instead of "and it is possible ... fields" read "and finally for all number fields in 1994 by Merel ([Mer])"

p. 373 line -14, instead of "*There exists a unique isogeny* $\hat{\phi}$" read "*Let* $\phi$ *be an isogeny from* $E$ *to* $E'$. *There exists a unique isogeny* $\hat{\phi}$ *from* $E'$ *to* $E$"

p. 384 line 3, instead of "$f$ *is equal to* $(2\pi)^{-s}\Gamma(s)L(E,s) = N^{-s/2}\Lambda(E,s)$" read "$f(it/\sqrt{N})$ *is equal to* $\Lambda(E,s)$"

p. 384 line 14, instead of "tables)." read "tables.)"

p. 384 line -1 and 385 line 1, instead of "$f_E(\tau) = \sum_{n\ge1} a_n q^n$ *the inverse Mellin transform of* $(2\pi)^{-s}\Gamma(s)L(E,s)$" read "*let* $f_E(\tau) = \sum_{n\ge1} a_n q^n$, *so that the Mellin transform of* $f_E(it/\sqrt{N})$ *is equal to* $\Lambda(E,s)$"

p. 385 the 2 middle paragraphs must of course be completely rewritten in view of Wiles's proof of the Taniyama-Weil conjecture in the semistable case

p. 387 lines 11 to 15 instead of "J.-F. Mestre ... (see

[Fer])" read "Using a construction of J.-F. Mestre (see [Mes3] and Exercise 9), Mestre and Nagao have obtained infinite families of curves of rank greater or equal to 13 (see [Mes5] and [Nag]), and using Mestre's construction, several authors have obtained individual curves of much higher rank, the current record being rank 21 by Nagao and Kouya (see [Mes4], [Fer] and [Nag-Kou])"

p. 389 middle, instead of "[Sil]" read "the first printing of [Sil]"

p. 394 line -3, instead of "$\lambda X + A$" read "$\lambda X + B$"

p. 395 step 1 line 3, replace "The assignments ... values)." by the following: "The assignments given in this algorithm for these maps and for $g$ are formal, i.e. we assign polynomials or rational functions, not values. In addition, it is understood that the modifications of $g$ imply the modifications of the coefficients $s_i$.)"

p. 395 replace the first five lines of step 2 by the following:

"2.

2.[Send $P_0$ to $(0:0:1)$] If $w_0 \ne 0$, set $(m_1,m_2,m_3) \leftarrow (w_0m_1 - u_0m_3, w_0m_2 - v_0m_3, w_0m_3)$, $(n_1,n_2,n_3) \leftarrow (w_0n_1 + u_0n_3, w_0n_2 + v_0n_3, w_0n_3)$, $g \leftarrow g(w_0U + u_0W, w_0V + v_0W, w_0W)$ and go to step 3. Otherwise, if $u_0 \ne 0$, set $(m_1,m_2,m_3) \leftarrow (u_0m_3, u_0m_2 - v_0m_1, u_0m_1)$, $(n_1,n_2,n_3) \leftarrow (u_0n_3, u_0n_2 + v_0n_3, u_0n_1)$, $g \leftarrow g(u_0W, u_0V + v_0W, u_0U)$ and go to step 3. Finally, if"

p. 395 replace lines -2 and -1 by the following: "$(m_1,m_2,m_3) \leftarrow (c_3m_1 + c_2m_3, c_3m_2 + \lambda c_2m_3, c_3m_3)$, $(n_1,n_2,n_3) \leftarrow (c_3n_1 - c_2n_3, c_3n_2 - \lambda c_2n_3, c_3n_3)$, $g \leftarrow g(c_3U - c_2W, c_3V - \lambda c_2W, c_3W)$ and go to step 5."

p. 396 lines 4 and 5, replace by "$(m_3, m_2 - \lambda m_1, m_1)$, $(n_1,n_2,n_3) \leftarrow (n_3, n_2 + \lambda n_3, n_1)$ $g \leftarrow g(W, V + \lambda W, U)$, then set $\lambda \leftarrow 0$.

p. 396 line 10, instead of "$c_2(m_1,m_2)m_3$" read "$c_2(m_1,m_2)m_3)$"

p. 397 middle instead of "$p > 19$" read "$p > 457$"

p. 397 line 2 of Algorithm 7.4.12 instead of "$p \ge 13$" read "$p > 457$"

p. 398 line 14, instead of "100, say" read "457. Note that one can prove that 457 is best possible, but it is easy to modify slightly the algorithm so that it works for much lower values of $p$."

p. 398 line -2 and -1, replace the last sentence by "Using recent new ideas of Elkies, Atkin has been able to deal with a 200-digit prime. Finally, combining this with an idea of Couveignes and Morain, Morain has dealt with a 250-digit prime."

p. 400 line -1, instead of "$t1$" read "$t_1$"

p. 401 line 1, instead of "$r_1 * a_1$" read "$r_1 a_1$"

p. 401 line 3 of step 15, instead of "goto step 1" read "goto step 2"

p. 408 line 10, instead of ", $a \leftarrow b$, and if $a \leq 1$, set $a \leftarrow 1$ and go to step 4." read "and $a \leftarrow \max(b,1)$."

p. 409 Exercise 1, replace the first sentence by "Given $c_4$ and $c_6$ computed by Formulas (7.1), we would like to recover the $b_i$ and $a_i$, where we assume that the $a_i$ are in $\mathbb{Z}$."

p. 415 line -9, instead of "possible" read "usually possible"

p. 415 line -8, instead of "finite set" read "reasonably small finite set"

p. 418 lines 8, 16, 19 and -6, instead of "Lehmann" read "Lehman"

(the last three corrections are not necessary if the big change below is made)

p. 418 line -8, instead of "*(*)*" read "$(*)$"

(not necessary if the big change below is made)

p. 418 **Addendum.** Line 14 to the end of Section 8.4, replace completely by:

"Although several methods were introduced to improve trial division (which is, we recall, a $O(N^{1/2+\epsilon})$ algorithm), the first method which has a running time which could be proved to be substantially lower was introduced by Lehman (see [Leh1]). Its execution time is at worst $O(N^{1/3+\epsilon})$, and it is indeed faster than trial division already for reasonably small values of $N$. The algorithm is as follows.

**Algorithm 8.4.1** (Lehman). Given an integer $N \geq 3$, this algorithm finds a non-trivial factor of $N$ if $N$ is not prime, or shows that $N$ is prime.

1. [Trial division] Set $B \leftarrow \lfloor N^{1/3} \rfloor$. Trial divide $N$ up to the bound $B$ using Algorithm 8.1.1. If any non-trivial factor is found, output it and terminate the algorithm. Otherwise set $k \leftarrow 0$.

2. [Loop on $k$] Set $k \leftarrow k+1$. If $k > B$, output the fact that $N$ is prime and terminate the algorithm. Otherwise, set $r = 1$ and $m = 2$ if $k$ is even, $r = k+N$ and $m = 4$ if $k$ is odd.

3. [Loop on $a$] For all integers $a$ such that $4kN \leq a^2 \leq 4kN + B^2$ and $a \equiv r \pmod{m}$ do as follows. Set $c \leftarrow a^2 - 4kN$. Using Algorithm 1.7.3, test whether $c$ is a square. If it is, let $c = b^2$, output $\gcd(a+b, N)$ (which will be a non-trivial divisor of $N$) and terminate the algorithm. Otherwise, use the next value of $a$ if any. If all possible values of $a$ have been tested, go to step 2.

*Proof.* (D. Zagier) If no factors are found during step 1, this means that all the prime factors of $N$ are greater than $N^{1/3}$ hence $N$ has at most two prime factors.

Assume first that $N$ is prime. Then the test in step 3 can never succeed. Indeed, if $a^2 - 4kN = b^2$ then $N \mid a^2 - b^2$ hence $N \mid (a-b)$ or $N \mid (a+b)$ so $a+b \geq N$, but this is impossible since the given inequalities on $k$ and $a$ imply that $a < 2N^{2/3} + 1$ and $b < N^{1/3}$ so $N \leq 13$. An easy check shows that for $3 \leq N \leq 13$, $N$ prime the test in step 3 does not succeed (note that for $N = 2$, $k = 1$ and $a = 3$ it does).

Assume now that $N$ is composite, so that $N = pq$ with $p$ and $q$ not necessarily distinct primes. We may assume that $p \leq q$, hence $N^{1/3} < p \leq q$, or in other words $1 \leq q/p < N^{1/3}$. Consider the continued fraction expansion of $q/p$. The successive convergents $u_n/v_n$ are such that $u_n$ and $v_n$ form an increasing sequence. Let $n$ be the unique index such that $u_n v_n < N^{1/3} < u_{n+1} v_{n+1}$ (since $pq > N^{1/3}$ such an $n$ exists), and set $r = u_n$, $s = v_n$, $r' = u_{n+1}$, $s' = v_{n+1}$. Then, using the elementary properties of continued fractions, we have

$$\left| \frac{q}{p} - \frac{r}{s} \right| \leq \left| \frac{r'}{s'} - \frac{r}{s} \right| = \frac{1}{ss'} \ ,$$

but also, since $s/r$ and $s'/r'$ are successive convergents to $p/q$, we have

$$\left|\frac{p}{q}-\frac{s}{r}\right| \le \left|\frac{s'}{r'}-\frac{s}{r}\right| = \frac{1}{rr'} \ .$$

Thus we obtain $|pr-qs| \le p/s'$ from the first inequality, $|pr-qs| \le q/r'$ from the second, and taking the geometric mean this gives

$$|pr-qs| \le \sqrt{\frac{pq}{r's'}} < N^{1/3} \ .$$

If we set $k = rs$ and $a = ps + qr$, we have $a^2 - 4kN = (ps - qr)^2$. The congruences for $a$ are easily checked, and so we see that step 3 succeeds with these values, thus proving the validity of the algorithm. $\square$

For each value of $k$ there are at most $1/2(\sqrt{4kN + N^{2/3}} - \sqrt{4kN}) \approx N^{1/6}k^{-1/2}/8$ values of $a$, and since $\sum_{k\le x} k^{-1/2} \approx 2x^{1/2}$, the running time of the algorithm is indeed $O(N^{1/3+\epsilon})$ as claimed.

We refer to [Leh1] for ways of fine tuning this algorithm, which is now only of historical interest."

p. 419 lines 10, 13 and -7, replace "Lehmann" by "Lehman"

(the first two are not necessary if the big change above is made)

p. 424 lines 1 and middle, replace "(*)" by "$(*)$"

p. 431 line 11 instead of "step 8" read "step 9"

p. 432 middle, remove the sentence "We also use ... time to time"

p. 432 step 1 of Algorithm 8.8.2, suppress "$P \leftarrow 1$, "

p. 432 step 2 and step 4 of Algorithm 8.8.2, instead of $(P, N)$ read $(x-1, N)$

p. 432 step 3 of Algorithm 8.8.2, suppress "$P \leftarrow P \cdot (x-1) \bmod N$, "

p. 432 step 3 of Algorithm 8.8.2, instead of "$c < 20$" read "$c < 200$"

p. 440 lines 13 and -11, instead of "$x \ne 1 \pmod q$" read "$x \not\equiv 1 \pmod q$"

p. 445 line -14, instead of "$l_p(r, \max(k_1, k_2)$" read "$l_p(r, \max(k_1, k_2))$"

p. 457 line -12, instead of "Otherwise," read "Otherwise" and line -11 instead of ", then output" read ", output"

p. 458 line 14, instead of "$s > n^{1/3}$" read "$s > N^{1/3}$"

p. 461 line 5, instead of "i.e" read "i.e."

p. 462 line 3 of step 7, instead of "i.e" read "i.e."

p. 463 line -13, instead of "Miller" read "Elkies"

p. 467 line -2, instead of "$p$ is prime" read "$p$ is an odd prime"

p. 468 **Addendum.** Add the following exercises:

"7. Let $\chi$ be a character modulo $q$, where $q$ is not necessarily prime. We will say that $\chi$ is *primitive* if for all divisors $d$ of $q$ such that $d < q$, there exists an $x$ such that $x \equiv 1 \pmod d$ and $\chi(x) \ne 1$. Set $\zeta = e^{2i\pi/q}$, and $\psi(a) = \sum_{x\in(\mathbb{Z}/q\mathbb{Z})^*} \chi(x)\zeta^{ax}$.

a) Let $a$ be such that $d = (a, q) = 1$. Show that $\psi(a) = \overline{\chi}(a)\tau(\chi)$.

b) Assume that $\chi$ is a primitive character and that $d = (a, q) > 1$. Show that there exists a $u \in (\mathbb{Z}/q\mathbb{Z})^*$ such that $au = d$. Deduce from this that $\psi(a) = 0$, and hence that the formula $\psi(a) = \overline{\chi}(a)\tau(\chi)$ is still valid.

8. Let $\chi$ be a primitive character modulo $q$, as defined in the preceding exercise, and set $S(x) = \sum_{n\le x} \chi(n)$.

a) Using the preceding exercise, give an explicit formula for $\tau(\chi)S(x)$.

b) Deduce that

$$\sqrt{q}\,|S(x)| \le \sum_{1\le m<q,\ m\ne q/2} \frac{1}{\sin\frac{\pi m}{q}} \ .$$

c) Show finally the *Polya-Vinogradov inequality*

$$|S(x)| = \left|\sum_{1\le n\le x} \chi(x)\right| \le \sqrt{q}\log q \ .''$$

p. 470 line -15, instead of "$kN$" read "$\sqrt{kN}$"
p. 482 line -10, instead of "this" read "this (see [Chu])"
p. 482 line -5, instead of "1993" read "1994"
p. 484 middle, instead of "simple precision" read "single precision"
p. 487 line 4, before "The basic idea" insert "For complete details I refer to [Len-Len2]"
p. 495 line 3 of step1, instead of "$A(X^2) = S(X)S(-X)$" read "$A(X^2) = \pm S(X)S(-X)$"
p. 495 step 2, remove the sentence "If $R(X)$ is ... algorithm."
p. 497 line 3 of Exercise 10, instead of "$A(X^2) = S(X)S(-X)$" read "$A(X^2) = \pm S(X)S(-X)$"
p. 498 the second paragraph has been rewritten and now reads as follows:

"Most general-purpose symbolic algebra packages have been written primarily for applied mathematicians, engineers and physicists, and are not always well suited for number theory. These packages roughly fall into two categories. In the first category one finds computer algebra systems developed in the 1970's, of which the main representatives are Macsyma and Reduce. Because of their maturity, these systems have been extensively tested and have probably less bugs than more recent systems. In addition they are very often mathematically more robust. In the second category, I include more recent packages developed in the 1980's of which the most common are Mathematica, by Wolfram Research, Inc., Maple, by the University of Waterloo, Canada, and more recently Axiom, developed by IBM and commercialized by NAG. These second-generation systems being more recent have more bugs and have been less tested. They are also often more prone to mathematical errors. On the other hand they have been aggressively commercialized and as a consequence have become more popular. However, the older systems have also been improved, and in particular recently Macsyma was greatly improved in terms of speed, user friendliness and efficiency and now compares very favorably to more recent packages. Mathematica has a very nice user interface, and its plotting capabilities, for example on the Macintosh, are superb. Maple is faster and often simpler to use, and has my preference. Axiom is a monster (in the same sense that ADA is a monster as a programming language). It certainly has a large potential for developing powerful applications, but I do not believe that there is the need for such power (which is usually obtained at the expense of speed) for everyday (number-theoretic) problems."

p. 499 middle, instead of "Cayley/Magma, GAP, Kant" read "GAP, Kant, Magma, Simath"
p. 499 middle, replace the description of the Cayley system by the following:

"The Magma system is designed to support fast computations in algebra (groups, modules, rings, polynomial rings over various kinds of coefficient domains), number theory and finite geometry. It includes general machinery for classical number theory (for example the ECM program of A.K. Lenstra), finite fields and cyclotomic fields and facilities for computing in a general algebraic number field. It will eventually include a MPQS factoring algorithm, a Jacobi sum-type primality test and a general purpose elliptic curve calculator. According to the developers, it should eventually include "just about all of the algorithms of this book". Simath, developed at the university of Saarbrucken, is another system for number-theoretic computations which is quite fast and has a nice user interface called simcalc."

p. 500 middle and p. 501 line 1, replace "Symbolics Macsyma" by "Macsyma"
p. 500 line -17, instead of "Cayley" read "Magma"

p. 501 line 5, instead of "Symbolics version" read "commercial version"

p. 501 lines 7 to 10, replace the Macsyma ordering information by the following: "Macsyma Inc., 20 Academy Street, Suite 201, Arlington MA 02174-6436, phone (617) 646-4550 or 1-800-MACSYMA (free from the U.S.), fax (617) 646-3161, e-mail `info-macsyma@macsyma.com`."

p. 501 line -12, instead of "forthcoming" read "also available"

p. 502 lines 1, 3 and 11, replace "Cayley" by "Magma"

p. 502 line 4, instead of "Appolo" read "HP, Appolo"

p. 502 For Kant, change address to "`pohst@math.tu-berlin.de` and `daberkow@math.tu-berlin.de`"

p. 502 middle, add "You can obtain Simath by anonymous ftp from `ftp.math.uni-sb.de`"

p. 502 middle, add "You can obtain Kant by anonymous ftp from `ftp.math.tu-berlin.de` directory /pub/algebra/Kant"

p. 502 add "`ftp.math.uni-sb.de` (134.96.32.23)" to the list of sites from where you can get Simath

p. 502 add "`megrez.ceremab.u-bordeaux.fr` (147.210.16.17)" to the list of sites from where you can get Pari by anonymous ftp

p. 502 line -2, instead of "128.146.7.200" read "128.146.110.30"

p. 502 line -1, instead of "Ubasic, CC4, Frenz-Calc" read "Most packages"

p. 517 in [H-W], instead of "*5-th ed.*" read "5-th ed."

p. 517-528 replace where necessary "ed" by "ed." and "eds" by "eds."

p. 521-528 due to a TEX mistake on my part, a number of dates and page numbers which were in the TEX source have not been printed. They are as follows:

In [Arn] "(1991)"; in [Atk1] "(1990)"; in [Atk2] "(1991)"; in [Bre1] "(1985)";
in [Buc-Dul] "(1991) pp. 53–72"; in [Ford3] "(1991) pp. 129–138"; in [LLMP] "(1991)";
in [Mor1] "(1989)"; in [Poh4] "(1991) pp. 173–182"; in [Pom] "(1983) pp. 89–139"

p. 520 remove the four lines concerning [**Len-Poh**], and insert after the paragraph concerning [Poh-Zas] the following:

"[**Poh5**] M. Pohst, *Computational Algebraic Number Theory*, DMV Seminar **21**, Birkhäuser, Boston, 1993.

Writeup of a course given by the author in 1990. This can be considered as an update to parts of [Poh-Zas]."

p. 521 in [Was], after the title add "Graduate texts in Math. **83**, "

p. 521 in [Adl-Hua] change title to "Primality testing and Abelian varieties over finite fields"

p. 521 in [APR], instead of "Ann of Math." read "Ann. of Math."

p. 521 in [AGP], instead of "in preparation" read "*There are infinitely many Carmichael numbers*, Ann. of Math. (1994), to appear

p. 521 replace the reference [Arn] by

"[**Arn**] F. Arnault, *The Rabin-Miller primality test: composite numbers which pass it*, Math. Comp., to appear."

p. 521 in [Atk-Mor], instead of "(to appear)" read "**61** (1993), 29–68"

p. 522 instead of "[Buc-Dul]" read "[Buc-Dül]"

p. 522 replace the entry for [BFP] by

"[**BFP**] J. Buchmann, D. Ford and M. Pohst, *Enumeration of quartic fields of small discriminant*, Math. Comp. **61** (1993), 873–879."

p. 525 replace the entry for [Kam] by

"[**Kam**] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229."

p. 525 replace the entry for [LaM-Odl] by

"[**LaM-Odl**] B. LaMacchia and A.M. Odlyzko, *Solving large sparse linear systems over finite fields*, in Advances in cryptology: Crypto 90, A. Menezes and S. Vanstone (eds.), LN in Comp. Sci. **537**, Springer-Verlag (1991), 109–133"

p. 525 in [Leh1] instead of "Lehmann" read "Lehman"

p. 525 instead of "[Len-Len]" read "[Len-Len1]"

p. 525 after [Len-Len] insert

"[**Len-Len2**] A. K. Lenstra and H. W. Lenstra (eds.), *The development of the number field sieve*, LN in Math. **1554**, Springer-Verlag, Berlin, Heidelberg, New-York, 1993."

p. 525 in [LLMP], replace "manuscript" by "in [Len-Len2], pp. 11–42

p. 525 after [McKay] insert

"[**Mer**] L. Merel, *in preparation*"

p. 525 after [Mes4] add the following reference:

"[**Mes5**] J.-F. Mestre, private communication."

p. 525 in [Mol-Wil], replace "(to appear)" by "**41** (1992) 259–308"

p. 526 after [Mor-Nic], add the following references:

"[**Nag**] K. Nagao, *An example of elliptic curve over* $\mathbb{Q}(T)$ *with rank* $\geq 13$, to appear"

"[**Nag-Kou**] K. Nagao and T. Kouya, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* $\geq 21$, to appear"

p. 526 in [Nic], instead of "A. Lenstra" read "A. K. Lenstra"

p. 527 in [Schn-Euch], add " **529**" after "Sci.", and replace "(to appear)" by "(1991), 68–85"

p. 527 replace reference [Sey2] by the following:

"[**Sey2**] M. Seysen, *Simultaneous reduction of a lattice basis and its reciprocal basis*, Combinatorica **13** (1993), 363–376."

p. 527 in [Star] add "(1973)"

p. 529-534 add index entries for "Chinese remainder theorem, 19", "continued fraction, 260, 264, 418", "Elkies, N., 463", "Fermat's little theorem, 414, 432, 442", "Fermat's last theorem, 150, 451", "Newton's method, 38, 44", "$p$-adic factorization, 357", "powering algorithms, 42, 458", "prime number theorem, 212", "prime ideal theorem, 212", "pseudo-prime, 414", "square root, in $\mathbb{Z}$, 38, modulo $p$, 31", "Weil conjectures, 380", "Wieferich congruence, 451"

p. 531 instead of "Lehmann, S." read "Lehman, S."

p. 532 instead of "Manin, Y" read "Manin, Y."

p. 532 remove page 463 to the entry for Miller, V.