Modern Computer Algebra

Addenda and corrigenda for the May 1999 edition

2 February 2004

JOACHIM VON ZUR GATHEN
and
JÜRGEN GERHARD

Universität Paderborn

CAMBRIDGE
UNIVERSITY PRESS

Page v line 3: *Cappuccino* instead of Cappucino (WERNER KRANDICK, 28. 1. 1999)

Chapter 1

Page 8 line 2: the first quote is actually due to *Arthur C. Clarke (1972)* (JEFFREY SHALLIT, 3. 1. 2000)

Page 12 Figure 1.4: *right* angles instead of straight (26. 8. 1999)

Page 15 line 9: insert *coprime to* $\varphi(N)$ before the comma (BENNO FUCHSSTEINER, 17. 12. 2001)

line –10: this line should read

$$2 \cdot 26^0 + 0 \cdot 26^1 + 4 \cdot 26^2 + 18 \cdot 26^3 + 0 \cdot 26^4 + 17 \cdot 26^5 = 202\,302\,466.$$

(HEIKO KÖRNER, 13. 11. 2002)

line –3: Euler's theorem only applies when x and N are coprime, but the conclusion $x^* \equiv x \bmod N$ is true for any x; see Exercise 20.5 (BENNO FUCHSSTEINER, 17. 12. 2001)

Page 17 lines 1–2: $l+1$ *times* instead of "l times" and *factor of* $l+1$ instead of "factor of l" (ANDREAS OESTERHELT, 18. 1. 2000)

Chapter 2

Page 33 line 14, Algorithm 2.3: replace the summation range $0 \leq i \leq m$ by $0 \leq i \leq n$ (11. 5. 1999)

Page 35 line 13, Algorithm 2.4: $b = (-1)^t \sum_{0 \leq i \leq m} b_i 2^{64i}$ (THOMAS LÜCKING, 10. 5. 1999)

line 16, step 1 of Algorithm 2.4: replace b by $|b|$ (ANDREAS OESTERHELT, 9. 2. 2000)

line 17, step 2 of Algorithm 2.4: replace the summation range $0 \leq i \leq m$ by $0 \leq i \leq n$ (THOMAS LÜCKING, 10. 5. 1999)

Page 38 line 17: 260, not 26 (OLAV GEIL, 12. 10. 2003)

Page 40 line 10, Exercise 2.4: picoseconds should be *nanoseconds* ($= 10^{-9}$ *sec.)* (WERNER KRANDICK, 28. 1. 1999)

line –10, Exercise 2.10: replace $f =$ by $a =$ (DANIEL PANARIO, 14. 6. 2001)

Chapter 3

Page 42 line –3, quote by Augustus de Morgan: *writers* instead of "writings" (16. 4. 2000)

Page 44 line –14, Definition 3.3: $u \in R$ instead of $b \in R$ (THOMAS LÜCKING, 10. 5. 1999)

Page 47 line –12: insert *for* $1 \le i \le \ell$ after integers (THOMAS LÜCKING, 17. 12. 1999)

Page 49 line –12, proof of Lemma 3.9: replace this line by

$$Q_i \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ \rho_{i+1}^{-1} & -q_i\rho_{i+1}^{-1} \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} r_i \\ (r_{i-1} - q_i r_i)\rho_{i+1}^{-1} \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix},$$

(THOMAS LÜCKING, 10. 5. 1999)

Page 51 line –15: remove once $> n_\ell$ (21. 5. 2001)

Page 52 lines 4–5, proof of Lemma 3.10: the formula for s_2 should read $s_2 = (s_0 - q_1 s_1)/\rho_2 = (\rho_0^{-1} - q_1 \cdot 0)/\rho_2 = (\rho_0\rho_2)^{-1}$ (HEIKO KÖRNER, 28. 11. 2002)

Page 53 lines 3–5: replace these lines by

$$\begin{aligned} 2\sum_{2\le i\le m+1}(n-m+i-1+n-m+i) &= 4m(n-m) + 2\sum_{0\le i<m}(2i+3) \\ &= 4m(n-m) + 2(m^2-m) + 6m \\ &= 4nm - 2m^2 + 4m. \end{aligned}$$

(24. 5. 2001)

line –12: $\ell > 2$ instead of $\ell \ge 2$ (HEIKO KÖRNER, 17. 12. 2002)

Page 54 line 4: add *if* $n \ge 1$ (HEIKO KÖRNER, 17. 12. 2002)

Page 60 line –17, Algorithm 3.14: replace $a \ge b > 0$ by $a, b > 0$ (DIRK JUNG, 11. 2. 2000)

Chapter 4

Page 65 line –3: replace $\{f \bmod n: f \in R\}$ by $\{f \bmod m: f \in R\}$ (SEYED HESAMEDDIN NAJAFI, 16. 2. 2000)

Page 67 line –8, Example 4.3: $x^3 - x + 2$ instead of $x^3 - x + 1$ (DANIEL PANARIO, 14. 6. 2001)

Page 68 line 6, Lemma 4.4: K is an extension field of F (HEIKO KÖRNER, 19. 2. 2003)

line 11, Example 4.5: insert *is* before irreducible (29. 5. 2001)

line 14, Example 4.5: $x^3 - x + 2$ instead of $x^3 - x + 1$ (DANIEL PANARIO, 14. 6. 2001)

Page 69 line –12, step 2 of Algorithm 4.8: replace twice b_{i-1} by b_{i+1}

line –2: replace this line by

$$8^{13} \equiv ((8^2 \cdot 8)^2)^2 \cdot 8 \equiv ((-4 \cdot 8)^2)^2 \cdot 8$$

(ANDREAS HIRN, 14. 12. 1999)

Page 73 line 11: remove "is unique" (1. 6. 2001)

Page 74 line –2: replace approximate by *approximating* (29. 5. 2001)

Page 78 Table 4.4, line 3: replace $-1' \, 01''$ by $-1' \, 11''$ (MICHAEL NÜSKEN, 20. 3. 2001)

Page 81 line 11: replace (1996) by *(1997)*, also on pages **210** line 9, **272** line 17, **316** line 10, and **330** line 14. (ARNOLD SCHÖNHAGE, 3. 6. 1999)

line –12, Notes 4.5: Exercise *16.7*, not 16.6 (9. 5. 2001)

Page 82 lines –10 and –9, Notes 4.6: the title of al-Khwārizmī's book is *al-kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala* (DANIEL MÜLLER, 15. 2. 2000)

Page 85 line 1, Exercise 4.6: f must be monic (ANDREW KLAPPER, 6. 2. 2002)

line –7, Exercise 4.17 (i): replace the last sentence by *Prove that* $p_{S,T} = q^{-\#S}(1-q^{-1})^{\#T}$. (MARTIN LOTZ, 21. 11. 2001)

Page 87 line 21, Exercise 4.30 (i): replace $\max\{\nu(f), \nu(g)\}$ by $\min\{\nu(f), \nu(g)\}$ (KATHY SHARROW, 21. 2. 2002)

Chapter 5

Page 91 Figure 5.3: the arrow pointing down left and marked "lifting" should be replaced by a vertical down arrow "modular computation $R/\langle p \rangle \longrightarrow R/\langle p \rangle$" plus a horizontal arrow "lifting $R/\langle p^l \rangle \longleftarrow R/\langle p \rangle$" (MICHAEL CLAUSEN, 25. 5. 1999)

Page 94 line –5, Theorem 5.1: $7n^2 - 7n$ instead of $7n^2 - 8n + 1$ (HEIKO KÖRNER, 19. 2. 2003)

line –1, proof of Theorem 5.1: this formula should read

$$\sum_{1 \leq i < n} 2i = n^2 - n$$

(HEIKO KÖRNER, 19. 2. 2003)

Page 95 lines 1–5, proof of Theorem 5.1: replace this paragraph by:

arithmetic operations. Then for each i, we divide m by m_i, taking $2n-2$ operations (Exercise 5.3), evaluate m/m_i at u_i, taking at most $2n-3$ operations since m/m_i is monic, and divide v_i by that value. This amounts to $4n^2 - 4n$ operations for all i. Finally, computing the linear combination (3) takes another $2n^2 - 2n$ operations, and the estimate follows by adding up.

(HEIKO KÖRNER, 19. 2. 2003)

Page 98 line 5, Algorithm 5.4: there is a linebreak missing before c_i (THOMAS LÜCKING, 10. 5. 1999)

line 7: the reference should be to *Section 3.1* instead of 2.4 (OLAV GEIL, 12. 10. 2003)

Page 101 lines –8 through –4: insert *The entries* $a_{ij}^{(1)} = a_{ij}$ *are the entries of the original matrix A.* The inequality on line –7 should read "$|a_{ij}| \le b_1$", the formula on line –5 becomes

$$b_k \le 2b_{k-1}^4 \le 2^{1+4} b_{k-2}^{4^2} \le \cdots \le 2^{1+4+\cdots+4^{k-2}} b_1^{4^{k-1}} = 2^{(4^{k-1}-1)/3} b_1^{4^{k-1}},$$

and the formula on line –4 should read "$n^2 \lambda(b_1) \approx n^2 \log_{2^{64}} b_1$". (MICHAEL CLAUSEN, 25. 5. 1999)

line –5: see page 132 for a justification of this formula (HUANG YONG, 9. 4. 2002)

Page 105 line –8: replace the sentence by *Thus for* $f \in \mathbb{Z}[x]$ *and* $u \in \mathbb{Z}$, $f^{(i)}(u)/i!$ *is always an integer.* (29. 5. 2001)

Page 106 line 3, Equation (14): u_i instead of u (THOMAS LÜCKING, 10. 5. 1999)

line 8: $v_1 = f(1) + f'(1)(x-1) = 1$ (DAVID THEIWES, 9. 4. 1999)

Page 112 line 14: $t = x/2$, not $t = -x/2$ (HEIKO KÖRNER, 19. 2. 2003)

Page 117 line 13: $t = \alpha t_j^*$ instead of $t = \alpha t_j$ (HEIKO KÖRNER, 19. 2. 2003)

Page 119 line 2: $q = 2$ instead of $q = 1$ (HEIKO KÖRNER, 19. 2. 2003)

Page 120 line 11, proof of Lemma 5.29: replace (33) by (34) (HEIKO KÖRNER, 19. 2. 2003)

Page 117 line –4, Theorem 5.26 (iii): $|t_j^*| \le m/k$ instead of $t_j^* \le m/k$ (29. 5. 2001)

Page 118 line 11: $|t_j^*| \le m/k$ instead of $t_j^* \le m/k$ (29. 5. 2001)

Page 121 line –11: replace $g_{i,2}$ by $g_{i,2}^*$ (OLAF MÜLLER, 15. 5. 2000)

line –5: insert $\bmod m_i$ before "for all i" (29. 5. 2001)

Page 122 line –14, Notes 5.3: replace "the use" by *to use* (DIRK JUNG, 11. 2. 2000)

Page 123 lines 5–6, Notes 5.5: replace Svoboda & Valach (1955, 1957) by *Svoboda & Valach (1955), Svoboda (1957)* (21. 5. 2001)

Page 128 line 24, Exercise 5.35: The f as required is a (one-dimensional) cubic spline, not a Bézier curve. A two-dimensional cubic spline, for example, interpolating a set of points $(x_0, y_0), \ldots, (x_n, y_n) \in \mathbb{R}^2$, is obtained by applying the exercise twice, once with with $u_i = i$ and $v_i = x_i$ for all i, and once with $u_i = i$ and $v_i = y_i$ for all i. This yields a parametric curve $(x(t), y(t))$ for $0 \le t \le n$ such that for each $i \in \{0, \ldots, n-1\}$, $x(t)$ and $y(t)$ are fixed cubic polynomials in t on the interval $[i, i+1]$. We can rewrite these two polynomials as a Bézier curve

$$\begin{aligned}(x(t), y(t)) = {} & (x_i, y_i) \cdot (i+1-t)^3 + P_i \cdot 3(t-i)(i+1-t)^2 \\ & + Q_i \cdot 3(t-i)^2(i+1-t) + (x_{i+1}, y_{i+1}) \cdot (t-i)^3\end{aligned}$$

on the interval $[i, i+1]$, where $P_i, Q_i \in \mathbb{R}^2$ are **control points**. In this form, $(x(t), y(t))$ is a (cubic) Bézier spline interpolating $(x_0, y_0), \ldots, (x_n, y_n)$ and with control points $P_0, Q_0, \ldots, P_{n-1}, Q_{n-1}$. (20. 5. 1999)

Chapter 6

Page 132 line –17: replace $\mathbb{Q}$ by $\mathbb{Q} \setminus \{0\}$

line –15: replace $b_i \in \mathbb{N}_{\geq 1}$ by $b \in \mathbb{N}_{\geq 1}$, and $\gcd(a_0, \ldots, a_n) = 1$ by $\gcd(a_0, \ldots, a_n, b) = 1$

(DANIEL LAUER, 22. 5. 2000)

Page 146 line –4: replace Gauß' lemma 6.6 by *Corollary 6.10* (HEIKO KÖRNER, 25. 4. 2003)

Page 147 line 8, proof of Corollary 6.21: replace Corollary 6.48 by *Corollary 6.15* (HEIKO KÖRNER, 25. 4. 2003)

Page 148 line –15, Lemma 6.25: replace $\overline{\mathrm{lc}(f)} \neq 0$ by $\overline{\mathrm{lc}(f)}$ *is not a zero divisor* (WINFRIED BRUNS, 10. 6. 2003)

Page 153 lines 10 and 11: replace $\deg_y w = \deg_y v > \deg_y h$ by $\deg_x w = \deg_x v > \deg_x h$ (DAVID GOLDBERG, 14. 11. 2000)

Page 154 line –4: replace $\mathsf{M}(f) \geq 1$ by $\mathsf{M}(f) \geq |\mathrm{lc}(f)|$ (PETER BÜRGISSER, 16. 1. 2002)

Page 157 line 9, proof of Theorem 6.35: $f^* w \equiv bf \bmod p$, not $f^* \equiv bf \bmod p$ (31. 5. 2001)

line 15, proof of Theorem 6.35: replace 4^n by 4^{n^2} (PETER BÜRGISSER, 16. 1. 2002)

Page 161 line 10: replace $O^{\sim}(n \log A)$ by $O^{\sim}(n^2 + n \log A)$ (31. 5. 2001)

Page 164 line –12, Example 6.41: *pink curve* instead of blue curve (DIRK JUNG, 11. 2. 2000)

Page 165 lines 8–10: replace "of algebraic extensions" by *in an algebraic extension E* and replace $(\alpha+\beta, \beta) \in F^2$ by $(\alpha+\beta, \beta) \in E^2$ (ANDREAS HIRN, 14. 12. 1999)

Page 169 line –7, proof of Corollary 6.48: *imply* instead of implies (10. 4. 2001)

Page 170 line 7: replace $(u_{n+m-k-1}, \ldots, u_k)$ by $(u_{n+m-k-1}, \ldots, u_k)^T$ (DIRK JUNG, 11. 2. 2000)

Page 171 lines –2 and –1, continuation of Example 6.1: replace these two lines by

```
S[4] := submatrix(S[3], 1 .. 1, [2]);
```

$$S_4 := \left[\ 216\ \right]$$

(DIRK JUNG, 11. 2. 2000)

Page 172 line 8, continuation of Example 6.1: replace 824 by 216 (DIRK JUNG, 11. 2. 2000)

Page 173 line 6: replace $2B$ by $2(n+1)^{1/2}B$ (31. 5. 2001)

line 14: $|\sigma_{n_i}^k \sigma_{n_{i-1}}|$ instead of $|\sigma_{n_i}^k \sigma_{n_i - 1}|$ (31. 5. 2001)

Page 173 line –9: replace (1997) by *(1996)*, also on pages **188** line 22 and **310** line –9. (4. 5. 2001)

Page 174 line 6, Theorem 6.53 (ii): even C^{m+2} is correct, by the solution to Exercise 6.47 (29. 1. 1999)

Page 175 line –2, Theorem 6.54 (ii): even $(m+2)$ is correct, by the solution to Exercise 6.48 (29. 1. 1999)

Page 176 line 5, Theorem 6.55: Replace $0 \le i \le \ell$ by $2 \le i \le \ell$. Moreover, the definition of subresultants and the proof of the theorem have to be modified so that $\deg f < \deg g$ is allowed and the kth subresultant is defined for $k < \deg f$ or $k < \deg g$ as well, similarly to Lemma 6.25. (DANIEL LAUER, 22. 5. 2000)

Page 178 line –10: $n^2 \log_{2^{64}} B$ instead of $n^2 \log_{2^6 4} B$ (DIRK JUNG, 11. 2. 2000)

Page 181 line 7: replace "number" by *polynomial* (30. 11. 1999)

Page 182 line –13: replace numerators by *denominators* (31. 5. 2001)

line –5: The address of the NTL homepage has changed and is now `http://www.shoup.net/ntl/` (2. 5. 1999)

Page 184 Figure 6.5: replace "heuristic with $u = 2^n$" by *heuristic with u a power of* 2. Moreover, the caption should be changed to:
Various gcd *algorithms in* $\mathbb{Z}[x]$ *for pseudorandom polynomials of degree* $2n-2$ *with nonnegative coefficients less than* $n2^{2n}$*, for* $1 \le n \le 32$ *and for* $32 \le n \le 4096$. (see also the description of the experiments on page 183) (THOMAS LÜCKING, 7. 1. 2000)

Page 185 Figure 6.6: the caption should be changed to:
The small primes modular gcd *algorithm in* $\mathbb{Z}[x]$ *of NTL for various pseudorandom polynomials of degree* $2n-2$ *with* $2k$*-bit coefficients.* Accordingly, the input size is $4n \cdot k$, and all labels on the horizontal axis of the diagram should be multiplied by 4 (see also the description of the experiments on page 183) (THOMAS LÜCKING, 7. 1. 2000)

Page 187 line –23, Notes 6.6: insert *and* $g \mid f$ before "such that" (PETER BÜRGISSER, 16. 1. 2002)

Page 192 line –16, Exercise 6.36 (i): replace $\mathbb{Q}[y]$ by $\mathbb{Q}[x]$ (DANIEL LAUER, 22. 5. 2000)

Page 193 line 6, Exercise 6.41: $0 \le k \le \deg g$ should be replaced by $0 \le k < \deg g$ (5. 2. 1999)

line –15, Exercise 6.44 (i): $\|a_i\|_\infty$ instead of $|a_i|$ (THOMAS LÜCKING, 9. 12. 1999)

line –7, Exercise 6.45: remove *and with max-norm* $\|f\|_\infty, \|g\|_\infty \le A$ (25. 8. 2000)

Page 194 line 3, Exercise 6.45 (iii): insert *if* f, g *are in* $\mathbb{Z}[x]$ *with max-norms at most* A at the end of the sentence (25. 8. 2000)

Page 194 line –4, Exercise 6.49 (ii): the sentence should read: *Prove that both the numerator and the denominator of* α_i *are absolutely at most* $(2B)^i$. (DANIEL LAUER, 22. 5. 2000)

Chapter 7

Page 202 line –5, Example 7.4 (continued): the Padé approximant is v/u and not u/v (OLGA MENDOZA, 18. 4. 2003)

Chapter 8

Page 210 line –16: replace "inside front cover" by *inside back cover*, also on pages **232** line –10, **281** line 13, **357** line –8, **411** line 10, **494** line 19, **519** line 6, and **600** line 7 (7. 5. 1999)

Page 212 Lemma 8.2 is correct but not general enough to cover its application in Theorem 12.2. If you are interested in that Theorem, you may replace Lemma 8.2 and its proof by:

LEMMA 8.2. *Let* $b, c \in \mathbb{R}_{>0}$, $d \in \mathbb{R}_{\geq 0}$, $S, T : \mathbb{N} \longrightarrow \mathbb{N}$ *be functions with* $S(2n) \geq cS(n)$ *for all* $n \in \mathbb{N}$, *and*

$$T(1) = d, \quad T(n) \leq bT(n/2) + S(n) \text{ for } n = 2^i \text{ and } i \in \mathbb{N}_{\geq 1}.$$

Then for $i \in \mathbb{N}$ *and* $n = 2^i$ *we have*

$$T(n) \leq \begin{cases} dn^{\log b} + S(n)\log n & \text{if } b = c, \\ dn^{\log b} + \frac{c}{b-c}S(n)(n^{\log(b/c)} - 1) & \text{if } b \neq c. \end{cases}$$

In particular, if $n^{\log c} \in O(S(n))$, *then* $T(n) \in O(S(n)\log n)$ *if* $b = c$, *and* $T(n) \in O(S(n)n^{\log(b/c)})$ *if* $b > c$.

PROOF. Unraveling the recursion, we obtain inductively

$$\begin{aligned} T(2^i) &\leq bT(2^{i-1}) + S(2^i) \leq b(bT(2^{i-2}) + S(2^{i-1})) + S(2^i) \\ &= b^2T(2^{i-2}) + bS(2^{i-1}) + S(2^i) \leq \cdots \\ &\leq b^iT(1) + \sum_{0\leq j<i} b^jS(2^{i-j}) \leq d2^{i\log b} + S(2^i)\sum_{0\leq j<i}\left(\frac{b}{c}\right)^j, \end{aligned}$$

where we have used that $S(2^{i-j}) \leq c^{-j}S(2^i)$ in the last inequality. If $b = c$, then the last sum simplifies to $S(2^i) \cdot i$. If $b \neq c$, then we have a geometric sum

$$\sum_{0\leq j<i}\left(\frac{b}{c}\right)^j = \frac{(\frac{b}{c})^i - 1}{\frac{b}{c} - 1} = \frac{c}{b-c}(2^{i(\log(b/c))} - 1),$$

and the first claim follows. □

(29. 11. 2003)

Page 215 line 15: replace $b \in R$ by *nonzero* $b \in R$ (MICHAEL BARNETT and KEVIN PERRY, 26. 10. 1999)

line 16: insert *(unless R is the trivial ring* $\{0\}$*)* before the period (4. 11. 1999)

Page 216 line 4, Lemma 8.7: replace $1 < \ell < n$ by $1 \leq \ell < n$ (OLAV GEIL, 27. 10. 2003)

line –5, proof of Lemma 8.7: replace "$s, t \in \mathbb{Z}$ so that $s\ell + tn = g$" by $u, v \in \mathbb{Z}$ *so that* $u\ell + vn = g$ (DIRK JUNG, 11. 2. 2000)

line –3: replace $m = nt/g$ by $m = n/tg$ (11. 3. 2000)

line –2: $b \cdot (\omega^g - 1)$ instead of $b \cdot (w^g - 1)$ (16. 4. 2000)

Page 217 lines 1 and 2, proof of Lemma 8.7: replace s and t by u and v, respectively (DIRK JUNG, 11. 2. 2000)

line 12, Lemma 8.8: insert *as defined on page 67* at the end of the line (MICHAEL BARNETT, 26. 10. 1999)

line –2: replace c by h (ANDREAS BESCHORNER, 3. 12. 1999, and DIRK JUNG, 11. 2. 2000)

Page 218 line 13, Example 8.10: $3x^3 + 4x + 2$ instead of $3x^2 + 4x + 2$ (THOMAS LÜCKING, 10. 5. 1999)

line –7: $R[x]$, not $F[x]$ (OLAV GEIL, 27. 10. 2003)

line –2: insert *is* after this (THOMAS LÜCKING, 10. 5. 1999)

Page 230 line –6: 2^{64}*-ary* instead of 64-adic (MICHAEL NÜSKEN, 25. 1. 2000)

Page 231 line 5: 2^t*th root of unity* instead of tth root of unity (26. 8. 1999)

Page 234 line 12: replace this line by

$$f \cdot g \equiv f(y^{2d-1}, y) \cdot g(y^{2d-1}, y) = h(y^{2d-1}, y) = \sum_{0 \leq i \leq 2n-2} h_i y^{(2d-1)i} \equiv h \bmod x - y^{2d-1},$$

(MARTIN LOTZ, 21. 11. 2001)

Page 235 line 5, Notes 8.3: add *Schönhage showed that n-bit integers can be multiplied on random access machines (with cost m to access an m-bit address) using* $O(n \log n)$ *word operations (see Knuth (1998), §4.3.3 C).* (ARNOLD SCHÖNHAGE, 3. 6. 1999)

Page 236 line 7, Exercise 8.6: replace $n \log n$ by $n^{\log 3}$ (27. 6. 2001)

Page 237 line 10, Exercise 8.9 (ii): replace DFT_ω^{-1} by $\mathrm{DFT}_{\omega^{-1}}$ (MICHAEL NÖCKER, 9. 6. 2000)

Page 237 line 17, Exercise 8.10 (iv): replace $V_1\alpha, V_1\beta$ by $V_1 f, V_1 g$ (identifying the polynomials f, g with their coefficient vectors) (OLAV GEIL, 12. 10. 2003)

Page 239 line –20, Exercise 8.24 (ii): the parenthesis should be closed after the word *algorithm* (29. 1. 1999)

Page 240 line –22, Exercise 8.30: The text of the exercise contains several typos; see the solutions for a corrected version. (29. 1. 1999)

Page 241 line –7, Exercise 8.36 (ii): the (i) should be removed (29. 1. 1999)

Chapter 9

Page 245 Figure 9.1: the blue formula for the tangent should be replaced by

$$y = \varphi'(g_i) \cdot z + \varphi(g_i) - \varphi'(g_i) g_i$$

(HELMUT MEYN, 20. 7. 1999)

Page 246 line –8, proof of Theorem 9.4: replace fg_i by fg_{i-1} (TOM KOORNWINDER, 6. 3. 2003)

Page 249 line 8, Theorem 9.12: replace $\deg p < l \deg p$ by $\deg f < l \deg p$ (DIRK JUNG, 11. 2. 2000)

Page 253 line –5, proof of Lemma 9.21: replace p^k by p^{2k} (18. 4. 2001)

Page 261 line –1: The starting condition is *not* necessary: e.g., $v(\varphi(3)) = 1$, when $\varphi = y^3 - 1$ and v is the 7-adic valuation, but the first iteration of Newton iteration yields $3 - \varphi(3)/\varphi'(3) \equiv 1 \bmod 7$, so Newton iteration converges. (MICHAEL NÜSKEN, 20. 3. 2001)

Page 263 lines 6–7: $y^3 - 1$, not $x^3 - 1$. Moreover, only the white points in the middle do not converge, since there derivative $\varphi' = 3y^2$ of $\varphi = y^3 - 1$ vanishes modulo 7 and Newton iteration is not applicable. However, the points $g \in \mathbb{Z}_{(7)}$ with $g \equiv 3, 5, 6 \bmod 7$ converge, despite the fact that they are no roots of φ modulo 7. (MICHAEL NÜSKEN, 20. 3. 2001)

line 9: $4 + 2 \cdot 7 + \cdots$ instead of $4 + 2 \cdot 6 + \cdots$ (MICHAEL NÜSKEN, 20. 3. 2001)

Page 272 line 8: The address of Victor Shoup's homepage has changed and is now `http://www.shoup.net` (2. 5. 1999)

line 15, Notes 9.1: replace $3.75\,\mathsf{M}(n)$ by $2.9375\,\mathsf{M}(n)$ (ARNOLD SCHÖNHAGE, 3. 6. 1999)

line 22, Notes 9.4 and 9.5: *Muḥammad* instead of Muhammad (DANIEL MÜLLER, 15. 2. 2000)

Chapter 10

Page 282 line –10, step 4 of Algorithm 10.5: replace $r_1(u_n - 1)$ by $r_1(u_{n-1})$ (DIRK JUNG, 11. 2. 2000, and SEYED HESAMEDDIN NAJAFI, 3. 3. 2000)

Page 285 line 6, step 1 of Algorithm 10.11: replace $u_0, \ldots, u_{n-1}$ by $x - u_0, \ldots, x - u_{n-1}$ (DIRK JUNG, 11. 2. 2000)

Page 286 line –7, step 4 of Algorithm 10.14: replace r_1 rem $m_r - 1$ by r_1 rem m_{r-1} (SEYED HESAMEDDIN NAJAFI, 3. 3. 2000, and RUCHIRA DATTA, 5. 9. 2000)

Page 289 line –16, step 3 of Algorithm 10.22: call Algorithm *10.20*, not 10.9 (SEYED HESAMEDDIN NAJAFI, 3. 3. 2000)

Page 290 line –13, Exercise 10.4 (ii): Use $\ln x \leq x - 1$ for all *positive* $x \in \mathbb{R} \ldots$ (19. 2. 1999)

Page 291 line –20, Exercise 10.6: *Suppose* instead of suppose (19. 2. 1999)

Chapter 11

Page 295 line –10: replace l by ℓ (10 times) (MICHAEL NÜSKEN, 25. 1. 2000)

Page 297 line –11, Example 11.2: replace $3x$ by $3x^2$
line –8: replace $3x^5$ by $3x^6$
(DIRK JUNG, 11. 2. 2000)

Page 300 line –7, continuation of Example 11.2: replace $3x$ by $3x^2$ (DIRK JUNG, 11. 2. 2000)

Page 304 line –5, proof of Theorem 11.7: replace $t_\ell/\mathrm{lc}(f)$ by $t_\ell/\mathrm{lc}(g)$ (31. 5. 2001)

Page 305 line 2: replace the bound by $(10\,\mathsf{M}(n) + O(n)) \log n$ (25. 5. 1999)

Page 307 line –3, Theorem 11.13: replace n, m by $n \geq m$ (11. 4. 2001)

Chapter 12

Page 314 line -2, proof of Theorem 12.2: Lemma 8.2 is not general enough to imply the first claim; see the correction for page 212. (MURRAY BREMNER, 29. 10. 2003)

Page 319 line –2: replace c_j by f_j (HELMUT MEYN, 13. 1. 2000)

Page 320 line 2: replace c_j by f_j (HELMUT MEYN, 13. 1. 2000)

Page 326 line 6, Theorem 12.15: In fact, the cost is $2n\,c(A) + O(kn^2)$ with storage for $2n^2$ field elements, and $3kn\,c(A) + O(kn^2)$ with linear storage (ERICH KALTOFEN, 31. 5. 1999)

Page 327 line –17, Formula (10): $F^{\mathbb{N}}$ instead of F^n (HELMUT MEYN, 14. 1. 2000)

Page 328 line –16, Theorem 12.18: In fact, the expected cost is $2n\,c(A) + O(n^2)$ with storage for $2n^2$ field elements, and $6n\,c(A) + O(n^2)$ with linear storage (ERICH KALTOFEN, 31. 5. 1999)

Page 330 line 11, Notes 12.1: replace 2.609 by 2.548 (ARNOLD SCHÖNHAGE, 3. 6. 1999)

Page 332 lines 9–10, Exercise 12.10 (i): insert *over* F after β and also after $E^{\mathbb{N}}$ (19. 2. 1999)
line 11, Exercise 12.10 (ii): F*-linear map* instead of linear map (19. 2. 1999)

Chapter 13

Page 338 line –15, Example 13.3: the displayed equation should read as follows.

$$\widehat{f}(1) = -\pi i = -\widehat{f}(-1), \quad \widehat{f}(10) = -\frac{1}{10}\pi i = -\widehat{f}(-10).$$

(29. 1. 1999)

Page 344 lines –11 to –9, Exercise 13.1: The statement is wrong for signals $f : \mathbb{R} \longrightarrow \mathbb{C}$. For example, the characteristic function of the rational numbers, with $f(t) = 1$ if $t \in \mathbb{Q}$ and $f(t) = 0$ otherwise, has precisely the rational numbers as periods. (28. 6. 2001)

Chapter 14

Page 355 line –6: A instead of An (MICHAEL NÖCKER, 6. 5. 1999)

Page 361 line 15, step 1 of Algorithm 14.8: **if** $a \in \mathbb{F}_q$ instead of **if** $a \in F$ (HELMUT MEYN, 29. 5. 1999)

line –6, Theorem 14.9: remove "an expected number of" (MICHAEL NÜSKEN, 20. 3. 2001)

Page 365 line –15, Algorithm 14.13: replace "a prime power" by *an odd prime power* (DIRK JUNG, 11. 2. 2000)

line –4, step 3 of Algorithm 14.13: insert *with input g and i* before "to compute" (PETER BÜRGISSER, 16. 1. 2002)

Page 366 lines 14–15, proof of Theorem 14.14: replace k by r (PETER BÜRGISSER, 21. 12. 2001)

Page 374 line –17: $a_{n-1}, \ldots, a_0$ instead of $a_{n-1}, \ldots, 0$ (HELMUT MEYN, 29. 5. 1999)

Page 375 line –6: insert *operations* before "in R" (4. 3. 1999)

Page 387 line –13, Corollary 14.44: *uniformly* instead of uniform (25. 2. 2000)

Page 389 line 9, Lemma 14.47 (ii): replace "if n is odd" by *if* $n \geq 3$ *is odd* (ABHIJIT DAS, 10. 10. 2001)

line 10, Lemma 14.47 (iii): replace "if k and n are coprime" by *if k is a prime not dividing n* (5. 3. 1999)

line –6, proof of Theorem 14.49: replace the formula by

$$f_r(x^{n/m}) = \Phi_m(x^{n/m}) = \Phi_n,$$

(TOM KOORNWINDER, 6. 3. 2003)

Page 390 line 14, proof of Lemma 14.50: replace $q^d - 1 = \mathbb{F}_{q^d}^\times$ by $q^d - 1 = \#\mathbb{F}_{q^d}^\times$ (HELMUT MEYN, 30. 5. 1999)

line –5: replace the factor (x^2+2+1) by (x^2+x+1) (HELMUT MEYN, 30. 5. 1999)

Page 391 line 8, Equation (12): this line should read

$$i \sim j \iff \exists l \in \mathbb{Z}\colon iq^l = j$$

(9. 3. 1999)

Page 397 line –10, Exercise 14.6 (i): replace this formula by

$$\gcd\Big(\prod_{a \le d < b} (x^{q^d} - x), f\Big)$$

(5. 3. 1999)

line –7, Exercise 14.6 (i): replace the formula by

$$\gcd\Big(\prod_{a \le d < b} (x^{q^b} - x^{q^{b-d}}), f\Big)$$

(5. 3. 1999)

Page 398 line 22, Exercise 14.11 (iii): *Hint:* $\mathbb{F}_q^\times$ *is cyclic (Exercise 8.16).* (5. 2. 1999)

line –13, Exercise 14.14: see Exercise 18.16 (5. 2. 1999)

Page 399 line 10, Exercise 14.16 (i): replace $T(\alpha)$ by $T_m(\alpha)$ twice (4. 4. 2001)

line –25, Exercise 14.17: The text of the exercise contains several typos; see the solutions for a corrected version. (5. 2. 1999)

Page 401 line 15, Exercise 14.27: insert *monic* before irreducible (19. 2. 1999)

line 17, Exercise 14.27 (ii): $w = u/\gcd(u, v^n)$ (MARTIN LOTZ, 15. 1. 2002)

line –7, Exercise 14.30 (iii): insert *(iv)* after Exercise 14.27 (5. 3. 1999)

Page 402 lines 6–7, Exercise 14.32 (i): Every *monic* polynomial ... a squarefree *monic* polynomial h. (4. 3. 1999)

line 16, Exercise 14.35: replace $O(n \log d)$ by $O(\mathsf{M}(d) + n \log d)$ (4. 3. 1999)

Page 403 line –17, Exercise 14.42: The text of the exercise contains some typos; see the solutions for a corrected version. (5. 3. 1999)

Chapter 15

Page 412 line –13: the expected cost of step 2 is $O((\beta^2 + \mathsf{M}(n)\log n)\mathsf{M}(\beta)\log\beta)$ word operations (PETER BÜRGISSER, 16. 1. 2002)

Page 415 line 18: insert *if p does not divide the discriminant of f* after quadratic (10. 5. 1999)

Page 419 line –1, Algorithm 15.10: insert $\mathrm{lc}(f)$ *is not a zero divisor modulo m* at the beginning of the line (PETER BÜRGISSER, 16. 1. 2002)

Page 420 line 2, Algorithm 15.10: replace s^*t^* by s^*g^* (DIRK JUNG, 11. 2. 2000)

Page 421 line 13, proof of Theorem 15.11: at most $2n$ (PETER BÜRGISSER, 16. 1. 2002)

Page 425 line –15, Theorem 15.18: this should read $O(\mathsf{M}(n)\log r \cdot \mathsf{M}(l \log m))$; similarly on line –13 (8. 3. 1999)

Page 431 lines 14–16, proof of Theorem 15.21: replace $n \log \gamma$ by $n\gamma$ twice (20. 6. 2001)

Page 436 Figure 15.9: the last two abort degrees **46372** and **47536** should be interchanged (13. 11. 1999)

Page 442 line 3, Exercise 15.3: insert *the monic polynomial* after of (8. 3. 1999)

line 20, Exercise 15.8: add *if p does not divide its discriminant* (8. 3. 1999)

Page 443 line 4, Exercise 15.10 (v): $a_{n,r} = 0$ instead of $a_{nr} = 0$ (HELMUT MEYN, 9. 9. 2003)

line 6, Exercise 15.10 (v): replace $1 \le k \le n \le 8$ by $1 \le r \le n \le 8$ (HELMUT MEYN, 9. 9. 2003)

line 10, Exercise 15.13: insert *the monic polynomial* after "Suppose that" (8. 3. 1999)

Page 444 line -23, Exercise 15.21: replace $f - gh$ by $gh - f$

line -20, Exercise 15.21 (ii): insert *such that* $\mathrm{lc}(f)$ *is a unit modulo m* after $m \in R$

(8. 3. 1999)

line –8, Exercise 15.25 (iii): remove *and only if.* See the solutions for a correct version of this claim.

line –5, Exercise 15.25 (iv): remove *conclude*

(8. 3. 1999)

Page 445 lines 7–8, Exercise 15.26: replace the sentence after the comma by *with monic $h_1, \ldots, h_k \in \mathbb{Z}[x]$ that are squarefree and pairwise coprime modulo p, and $h_k \neq 1$.* (13. 4. 1999)

Chapter 16

Page 447 line –4, Definition 16.1: replace "The vectors $f_1, \ldots, f_n$" by *If these vectors are linearly independent, then they* (15. 6. 1999)

Page 451 line 8: The formula in the proof of Theorem 16.6 should read:

$$\left|\det\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}\right| = \left|\det\begin{pmatrix} f_1^* \\ \vdots \\ f_n^* \end{pmatrix}\right| = \|f_1^*\| \cdots \|f_n^*\| \le \|f_1\| \cdots \|f_n\|.$$

(MICHAEL CLAUSEN, 25. 5. 1999)

Page 453 Table 16.3, line 2: $-$ *row* 1 instead of $+$ row 1
line 4: -3 *row* 1 instead of $-$ row 1
(DIRK JUNG, 11. 2. 2000)

Page 455 line 8, proof of Lemma 16.12 (ii): $\mu_{ij} - \lambda\mu_{jj}$ instead of $\mu_{ij} - \lambda\mu_{ij}$ (THOMAS LÜCKING, 22. 7. 1999)

Page 456 line 14, Lemma 16.14: $1 < k < i$ instead of $1 \leq k < i$ (THOMAS VIEHMANN, 19. 3. 2001)

Page 457 line –6: replace this line by

$$D_0 = \|f_1^*\|^{2(n-1)}\|f_2^*\|^{2(n-2)}\cdots\|f_{n-1}^*\|^2 \leq \|f_1\|^{2(n-1)}\|f_2\|^{2(n-2)}\cdots\|f_{n-1}\|^2 \leq A^{n(n-1)},$$

(EVA MIERENDORFF, 17. 3. 2001)

Page 462 line 12: replace $q^* = q^{**}u + r^{**}$ by $r^* = q^{**}u + r^{**}$ (EUGENE LUKS, 1. 12. 2002)

Page 469 line 2: replace "no solution is known" by *no direct "sparse" solution is known, but the arithmetic circuit and black box representations discussed below solve the problem* (ERICH KALTOFEN, 31. 5. 1999)

Page 471 line 2, Notes 16.2 and 16.3: insert *is* after "it" (STEFAN GERHOLD, 16. 7. 2003)

Page 472 line 16, Exercise 16.3: $f \star g$ instead of $(f \star g)(x)$ (20. 3. 1999)
line 19, Exercise 16.3 (ii): replace the last sentence by *(The resulting polynomials are the monic associates of the first four* ***Chebyshev polynomials of the second kind****).* (20. 3. 1999)
line –12, Exercise 16.7: The definition of the Hermite normal form is wrong. In addition to being lower triangular, the Hermite normal form is required to have positive diagonal entries, and the entries below the diagonal must be reduced modulo the diagonal element in the same column. These additional assumptions make the Hermite normal form of a nonsingular square matrix with integer entries unique. Algorithm 16.26 only computes a lower triangular matrix, but not necessarily the Hermite normal form. However, it is easy to compute the Hermite normal form from any lower triangular matrix: multiply some rows by -1 to make all diagonal elements positive if necessary, and then reduce the elements below the diagonal modulo the diagonal element in each column. (4. 2. 2001)

Page 473 line 2, step 5 of Algorithm 16.26: *row index* instead of column index (4. 2. 2001)
line –5, Exercise 16.9: $\mathbb{R}h_{i-1}$ instead of $\mathbb{R}h_{n-1}$ (20. 3. 1999)

Page 474 line 5, Exercise 16.12: the text of this exercise contains several errors; see the solutions for a corrected version (20. 3. 1999)

Page 475 line –1, Exercise 16.17: replace the last sentence in parenthesis by *As mentioned in Section 16.6, one can factor polynomials in random polynomial time both in the arithmetic circuit and in the black box representation* (ERICH KALTOFEN, 31. 5. 1999)

Chapter 18

Page 494 line –18: remove "or a Carmichael number". The Fermat test may return "composite" for Carmichael numbers, namely when $\gcd(a,N) > 1$. (EVA MIERENDORFF, 17. 3. 2001)

Page 495 line –3: replace "algorithms" by *algorithm* (FRIEDRICH EISENBRAND, 16. 8. 2000)

Page 496 lines 15–19: The argument that $0 \notin I$ can be simplified by noting that $(-1)^m = -1 \neq 1$ (FRIEDRICH EISENBRAND, 16. 8. 2000)

Page 500 line –4: replace $|M| \leq e^{B/6} < B$ by $|M| \leq \lfloor e^{B/6} \rfloor \leq B$ (THOMAS VIEHMANN, 11. 3. 2001)

Page 503 line –10: insert *distinct* before "odd" (THOMAS VIEHMANN, 11. 3. 2001)

Page 504 line –15: It is not known whether the inclusion $\mathcal{BPP} \subseteq \mathcal{NP} \cap \text{co-}\mathcal{NP}$ holds true. The best known upper bound appears to be $\mathcal{BPP} \subseteq \mathcal{MA} \subseteq \Sigma_2^p \cap \Pi_2^p$. (MICHAEL NÜSKEN and MITCH HARRIS, 23. 9. 1999)

Page 509 line 1, Notes 18.6: *1997* instead of 1998a (16. 10. 2002)

line –16, Exercise 18.4 (i): Since $\gcd((N-1)/2, p-1) = 2$, the statement is wrong. (HELMUT MEYN, 23. 11. 1999)

Page 510 line –20, Exercise 18.12 (i): replace the whole sentence after "Carmichael number N" by *Your algorithm should take a confidence parameter $c \in \mathbb{N}$ as additional input, such that each factor in the output is prime with probability at least $1 - 2^{-c}$, and it should use an expected number of $O((c + \log N) \log N \cdot \mathsf{M}(\log N))$ word operations.* (29. 3. 1999)

Page 511 line 14, Exercise 18.18 (i): replace $x/2\ln x$ by $x/(2\ln x)$ (MICHAEL NÜSKEN, 20. 3. 2001)

line –10, Exercise 18.20: replace $\gcd(a, p_i)$ by $\gcd(p, p_i)$ (MICHAEL NÜSKEN, 20. 3. 2001)

Page 512 line 6, Exercise 18.21 (i): replace "$O(n^4 \log^2(nB))$ and $O(n^4 \log^2(nA))$" by $O(n^4 \log(nB) \operatorname{loglog}(nB) + n^3 \log^2(nB))$ *and* $O(n^3 m \log^2(nA))$ (9. 4. 1999)

line 7, Exercise 18.21 (ii): add *(ii)* after Corollary 18.12 (12. 4. 1999)

line 16, Exercise 18.23 (i): this line should be replaced by

$$\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right), \quad \left(\frac{a}{MN}\right) = \left(\frac{a}{M}\right)\left(\frac{a}{N}\right)$$

(12. 4. 1999)

Page 513 line –4, Exercise 18.27 (iv): replace co-$\mathcal{NP}$ by $\mathcal{NP} \cap \text{co-}\mathcal{NP}$ (22. 4. 1999)

line –2, Research problem 18.28: This research problem was solved in August 2002 by Manindra Agrawal, Neeraj Kayal and Nitin Saxena: primality can be tested deterministically in polynomial time. See `http://www.cse.iitk.ac.in/news/primality.pdf`. (16. 10. 2002)

Chapter 19

Page 514 lines 16–17, quote by Maurice Kraïtchik: add translation *The equation* $x^2 - y^2 = N$ *is of paramount importance in the factorization problem* (5. 3. 1999)

Page 517 line 5: the factored number is $2^{599} - 1$ (PAUL ZIMMERMANN, 27. 5. 1999)

Page 519 line –2: *prime divisor of* N instead of p (MANTSIKA MATOOANE, 18. 9. 1999)

Page 520 line 4: $\gcd(x_t - x_{t+l}, N)$ instead of $\gcd(x_{t+l} - x_l, N)$ (ANDREAS HIRN, 14. 12. 1999)

lines –11 and –10: replace these lines by

$$\begin{aligned}\mathcal{E}(s) &= \sum_{j\geq 1} \mathrm{prob}(s \geq j) \leq 1 + \sum_{j \geq 0} e^{-j^2/2p} \leq 2 + \int_0^\infty e^{-x^2/2p} dx \\ &\leq 2 + \sqrt{2p} \int_0^\infty e^{-x^2} dx = 2 + \sqrt{\frac{p\pi}{2}}\end{aligned}$$

(OLAF MÜLLER, 1. 9. 2000)

Page 522 line 2: *Since* $y_i = x_{2i}$ *for all* i, not $y_{2i} = x_i$ (MANTSIKA MATOOANE, 18. 9. 1999)

Page 526 line –10: replace b^2 rem N by *the least absolute residue of* b^2 *modulo* N (THOMAS VIEHMANN, 19. 3. 2001)

Page 528 line 8, Proof of Lemma 19.14, first paragraph: insert *(Exercise 14.8)* before the end of the sentence (5. 2. 1999)

Page 530 line 8: this is the expected number of trials for finding *one* B-number, but we need h of them.

(THOMAS VIEHMANN, 19. 3. 2001)

The following 11 lines should be replaced by:

We need $h+1$ *B-numbers, and the expected number* k *of loop iterations satisfies* $k \leq n^{2r}(h+1)$. *Plugging this into (4) and using* $n < h < B$, *we obtain a total cost of*

$$O(B^3 + B^2 n^{2r} \mathsf{M}(n)) \tag{7}$$

word operations. Ignoring the factor $\mathsf{M}(n)$ *and equating the logarithms of the two factors* $B^2 = e^{n/r}$ *and* $n^{2r} = e^{2r \ln n}$ *gives* $r^2 \approx n/(2\ln n)$, *and we set*

$$r = \left\lceil \sqrt{\frac{n}{2\ln n}} \right\rceil. \tag{8}$$

Then $B \leq e^{\sqrt{n(\ln n)/2}}$, *and using*

$$L(N) = e^{\sqrt{\ln N \ln\ln N}}, \tag{9}$$

we obtain the following result by substituting (8) in (7).

THEOREM 19.15.
Dixon's random squares method factors an integer N with an expected number of $O^{\sim}(L(N)^{2\sqrt{2}})$ word operations.

Page 533 line 9: insert *and* $v = ru + s$ before the closing curly brace (THOMAS VIEHMANN, 19. 3. 2001)

Page 535 line –2: replace $\nu \in \mathbb{F}_q$ by $c \in \mathbb{F}_q$ (HELMUT MEYN, 30. 5. 1999)

Page 539 lines 11–14, Theorem 19.24: the additional condition $\#S \geq 3$ is needed, and the constant c is independent of p and S (EVA MIERENDORFF, 17. 3. 2001)

lines –5 to –1, Corollary 19.25: the additional condition $\sigma \geq 3$ is needed, and the constant c_1 is independent of p, N, and B (EVA MIERENDORFF, 17. 3. 2001)

Page 540 lines 5–7: replace these lines by

$$\left(1 - \frac{M}{N^3}\right)^m \leq \left(1 - \frac{sc_1}{\ln p}\right)^m \leq \left(1 - \frac{sc_1}{\ln C}\right)^m \leq e^{-msc_1/\ln C} \leq \varepsilon,$$

when we choose $m \geq \ln(1/\varepsilon)\ln(C)/(sc_1)$*, where* c_1 *is as in the previous corollary.* (THOMAS VIEHMANN, 11. 3. 2001)

Page 543 line –23: Exercise 19.1 is about the 159-digit factor N of $2^{599} - 1$, from page 517 (PAUL ZIMMERMANN, 27. 5. 1999)

line –2, Exercise 19.5 (iii): replace $0 \leq i \leq k$ by $1 \leq i \leq k$ (12. 4. 1999)

Page 544 line 6, Exercise 19.8: Three *positive* integers (12. 4. 1999)

line –14, Exercise 19.10: $-S_i \subseteq \mathbb{Z}^{\times}_{q^{l_i}}$ instead of $-S \subseteq \mathbb{Z}^{\times}_{q^{l_i}}$ (HELMUT MEYN, 9. 12. 1999)

Page 545 line –5, Exercise 19.18 (iv): $\mathcal{E}(X)$ should be replaced by $\mathcal{E}(|X|)$ (13. 4. 1999)

Chapter 20

Page 547 line 7: The "ElGacryp" should be removed (22. 4. 1999)

Page 548 lines 20/21: *parametrized* instead of parameterized (11. 3. 2000)

Page 550 line –9: replace "nonconstant polynomials $g, h \in F[x]$" by *polynomials* $g, h \in F[x]$ *of degree at least* 2 (THOMAS VIEHMANN, 11. 3. 2001)

Page 556 line –20, Exercise 20.3 (iii): insert *, and assume that* r *is coprime to* $\operatorname{char} F$ before the period (22. 4. 1999)

Chapter 21

Page 567 line –9, Example 21.2: replace this line by

$$(u - x, v - y) = CS = 2SR = (-2u + 1, -2v),$$

(9. 4. 2001)

Page 569 line 13: replace f,g,h by f,g,h^* (MICHAEL BARNETT, 1. 11. 1999)

Page 570 line 1: $\{u_1,\ldots,u_d\}$ instead of $\{u_1,\ldots,u_s\}$ (MICHAEL BARNETT, 1. 11. 1999)

Page 572 line 6, Definition 21.7 (i): $c_\alpha \boldsymbol{x}^\alpha$ instead of $c_\alpha x^\alpha$ (MICHAEL BARNETT, 1. 11. 1999)

Page 574 line –13, Example 21.10 (continued): this should read $-(x^2y-x)$, not $-(xy^2-x)$ (VOLKER KRUMMEL, 19. 2. 2003)

Page 575 lines –7 and –6, proof of Lemma 21.15: replace this sentence by *There is at least one term $q_i\boldsymbol{x}^{\alpha_i}$ in which $\boldsymbol{x}^\beta$ occurs, and then $\boldsymbol{x}^{\alpha_i} \mid \boldsymbol{x}^\beta$.* (THOMAS VIEHMANN, 11. 3. 2001)

Page 576 line –3, proof of Theorem 21.18: $(\alpha_1,\ldots,\alpha_n)\in B$, not $\in A$ (TOM KOORNWINDER, 24. 4. 2003)

Page 585 lines –9 and –8: *a $g^{**}\in G$ such that* $\mathrm{lt}(g^{**}) \mid \mathrm{lt}(g^*)$. *Since G is minimal, we have* $\mathrm{lt}(g)=\mathrm{lt}(g^*)=\mathrm{lt}(g^{**})\in\mathrm{lt}(G^*)$*, ...* (THOMAS VIEHMANN, 11. 3. 2001)

Page 586 lines –5 and –4: replace these two lines by

$$S(f_1,g_3) \text{ rem } (f_1,f_2,g_3) = \frac{1}{3}uy^2 - v^2x - v^2 \text{ rem } (f_1,f_2,g_3) = 0,$$
$$S(f_2,g_3) \text{ rem } (f_1,f_2,g_3) = \frac{1}{3}uy^2 - v^2x + 2v^2 - vy \text{ rem } (f_1,f_2,g_3) = 0,$$

(MICHAEL BARNETT, 1. 11. 1999)

Page 592 line 8, Notes 21.6: replace $g_2\in I$ by $g_2\notin I$ (9. 4. 2001)

Chapter 22

Page 603 line –8, Example 22.6 (continued): The blank entry in row 5, column 4 of the matrix is zero. (29. 6. 2003)

Page 607 line 3, Exercise 22.5: The text of this exercise contains some errors; see the solutions for a corrected version (22. 4. 1999)

Chapter 23

Page 610 line 12: replace the minus by a plus in the product rule (21. 7. 2003)

Page 621 line –5, proof of Theorem 23.12: replace this and the following line by *If we let $f_{i+1}=g_i$ for $1\le i<m$, then (13) proves that f_1 in (12) is indeed a polynomial, and (F1) and (F2) are satisfied for $(f_1,\ldots,f_m)$.* (30. 4. 1999)

Page 628 line 11: $\log_{2^{64}} n$ instead of $\log_{2^64} n$ (16. 3. 2001)

Page 635 line –8, Exercise 23.4 (iii): This line should read

$$f = \sum_{0\le i<n} \frac{(\Delta_h^i f)(0)}{h^i i!} x(x-h)\cdots(x-ih+h),$$

(OLAF MÜLLER, 12. 8. 2003)

Page 635 line –4, Exercise 23.5 (i): $\mathbb{R}_{>0}$ instead of $\mathbb{R}_{\geq 0}$ (23. 4. 1999)

Page 636 line 12, Exercise 23.8: The text of this exercise contains several typos; see the solutions for a corrected version. (30. 4. 1999)

Page 637 line 6, Exercise 23.10: *for* $m, n \in \mathbb{N}$. (30. 4. 1999)

line –13, Exercise 23.14: $f \sim g$ instead of $f \equiv g$ (4. 2. 2001)

Page 638 line 10, Exercise 23.19: replace "hypergeometric terms are" by *the set of hypergeometric terms is* (6. 5. 1999)

line –17, Exercise 23.23: $n \in \mathbb{N}_{\geq 1}$, and neither of the two sums is hypergeometric (30. 4. 1999)

line –7, Exercise 23.24: $\mathbb{Q}[x]$ instead of $Q[x]$, similarly $\mathbb{Q}[x]$ instead of $F[x]$ on line –6 (6. 5. 1999)

Page 639 line 8, Exercise 23.28: replace $\deg f > 0$ by $\deg g > 0$ (30. 4. 1999)

lines –9 and –8, Exercise 23.29 (iii): Replace nonconstant by *nonzero*. Moreover, it is not true that this representation is unique. For example, for $a = x$ and $b = x^2 - 1$, both $(r,s,u,v) = (1, x+1, 1, x-1)$ and $(r,s,u,v) = (1, x-1, x, 1)$ satisfy the conditions.

line –4, Exercise 23.29 (iv): Both implications are wrong. A counterexample for the "if" direction is $a = x+1$ and $b = x$, where in fact $(r,s,u,v) = (1,1,1,x)$ is the unique respresentation as in (iii), but there do not exist polynomials c, d such that $\Delta(c/d) = a/b = 1 + 1/x$, by Lemma 23.5. A counterexample for the "only if" part is $a = 2x+1$ and $b = 1$, where $(r,s,u,v) = (2x+1, 1, 1, 1)$ is the unique representation as in (iii), and for $c = x^2$ and $d = 1$ we have $\Delta(c/d) = a/b$.

However, the following is true: there exist nonzero coprime monic polynomials $c, d \in F[x]$ such that $E(c/d) = a/b$ if and only if $r = s = 1$ for all representations as in (iii), and in fact $(r,s,u,v) = (1,1,d,c)$ is the unique respresentation in this case (see S. A. ABRAMOV and M. PETKOVŠEK (2001), Canonical Representations of Hypergeometric Terms, *Formal Power Series and Algebraic Combinatorics (FPSAC01)*, to appear.)

line –2, Exercise 23.29 (v): replace "the extended" by *an extended*
(SERGEĬ ABRAMOV, 22. 3. 2000)

Chapter 24

Page 656 line 12: *multiple of* g_1, not of g (MICHAEL BARNETT, 28. 10. 1999)

Page 662 line –5, Exercise 24.3: Replace the sentence by *Prove (6) for all nonnegative integers* $n \geq w \geq s$ *by double induction on* w *and* n. (23. 4. 1999)

Chapter 25

Page 670 line 13: replace $\{r \bmod i : r \in R\}$ by $\{r \bmod I : r \in R\}$ (MICHAEL BARNETT, 26. 10. 1999)

Page 684 line 3: *Chapter 3* instead of Chapter 2 (EMRULLAH DURUCAN, 15. 1. 2001)

Page 687 Figure 25.3: It is not known whether the inclusion $\mathcal{BPP} \subseteq \mathcal{NP} \cap \text{co-}\mathcal{NP}$ holds true. The best known upper bound appears to be $\mathcal{BPP} \subseteq \mathcal{MA} \subseteq \Sigma_2^p \cap \Pi_2^p$. (MICHAEL NÜSKEN and MITCH HARRIS, 23. 9. 1999)

Sources of quotations

Page 689 line –17, quote by al-Kāshī in the Introduction: the correct title of al-Kāshī's book is *miftāḥ al-ḥisāb, The key to computing* (DANIEL MÜLLER, 15. 2. 2000)

line –15, quote attributed to Paul Theroux in Chapter 1: actually this quote is due to **Arthur Charles Clarke** (*1917), can be found in his *Report on Planet Three and Other Speculations*, ch. 14: Technology and the Future, Harper & Row, New York, Evanston, San Francisco, London, 1972, p. 139, and is called *Clarke's Third Law* (JEFFREY SHALLIT, 3. 1. 2000)

Page 690 line 27, quote by al-Khwārizmī in Chapter 4: the title of al-Khwārizmī's book is *al-kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala* (DANIEL MÜLLER, 15. 2. 2000)

line –6, quote by Michael Crichton in Chapter 7: insert *Reprinted with kind permission of Alfred A. Knopf Incorporated, New York, and Random House, Inc., New York.* (19. 2. 1999)

Page 691 line 1, quote by Richard Feynman in Chapter 8: the following should be inserted after "New York": *and Random House UK Limited, London* (19. 2. 1999)

line 3, quote by Arnold Schönhage in Chapter 8: replace "(*1935)" by *(*1934)* (ARNOLD SCHÖNHAGE, 3. 6. 1999)

Page 692 line 23, quote by Maj Sjöwall and Per Wahlöö in Chapter 18: insert *Reprinted with kind permission of Norstedts Förlag AB, Stockholm.* (19. 2. 1999)

line –31, quote by Richard Feynman in Chapter 19: the following should be inserted after "New York": *and Random House UK Limited, London* (19. 2. 1999)

Page 693 line –12: the quote is from **Al-Qur'ān**, *Sūra 27 al-naml* (28. 5. 2001)

References

Page 700 line –25, References, Berggren, Borwein & Borwein: the year *(1997)* is missing (1. 6. 1999)

Page 701 line 27, References, Brassard & Bratley (1996): *Practice* instead of Prectice (HELMUT MEYN, 30. 5. 1999)

Page 702 line 11, References, Buchberger & Winkler: the year *(1998)* is missing (ERICH KALTOFEN, 31. 5. 1999)

line 17, References, Bürgisser, Clausen & Shokrollahi: the correct year is 1997 (ARNOLD SCHÖNHAGE, 3. 6. 1999)

Page 714 line 14, References, Krylov (1931): определятся should be replaced by определяются (26. 2. 1999)

line –19, References, Lagrange (1759): replace this line by

Taurinensia **1**. *Œuvres*, publiées par J.-A. SERRET, vol. 1, 1867, Gauthier-Villars, Paris, 1–20.

(16. 3. 2001)

Page 716 line –20, References, Lickteig & Roy (1997): the correct year is *1996* (4. 5. 2001)

Page 718 line –23, References, Mihăilescu (1998a): the correct year is *1997* (16. 10. 2002)

Page 723 line –17, References, Schubert (1793): the correct pages are *172–186* (19. 2. 1999)

line –2, References, Schwenter (1636): *Mathematicæ* instead of Mathematiæ (8. 8. 2003)

Page 725 line –30, References, Svoboda & Valach (1957): the author is only Antonín Svoboda (21. 5. 2001)

Index

Page 730 line –6, Index, left column: Bernoulli, Jakob (*1654*–1705) (3. 5. 2001)

Page 731 line 20, Index, left column: Brauer, Alfred *Theodor* (DON KNUTH, 30. 6. 1999)

Page 732 line –8, Index, right column: Corless, Robert *Malcolm* (ROB CORLESS, 26. 7. 1999)

Page 735 line 31, Index, left column: the correct Greek spelling of Euclid's name is Εὐκλείδης (16. 4. 2000)

line –8, Index, left column: *Κνίδιος*, not Κγίδιος (IOANNIS EMIRIS and ILIAS KOTSIREAS, 25. 7. 2001)

Page 737 line –5, Index, right column: Glover, Roderick *Edward* (ROD GLOVER, 30. 7. 1999)

Page 738 line –13, Index, right column: Caliph *Hārūn* al-Rashīd (هارون الرشيد) (28. 5. 2001)

Page 739 line 28, Index, right column: replace Ἰαμβλίχος by *Ἰάμβλιχος* (ILIAS KOTSIREAS, 13. 8. 2001)

Page 740 line –23, Index, right column: Kalorkoti, Kyriakos *(Καλορκότη, Κυριάκος)* (KYRIAKOS KALORKOTI, 29. 1. 1999)

Page 741 line 15, Index, left column: al-Khwārizmī, Abū Jaʿfar Muḥammad bin Mūsā (ابو جعفر محمّد بن موسى الخوارزمي) (DANIEL MÜLLER, 15. 2. 2000)

Page 742 line 20, Index, right column: Lloyd, Daniel *Boone, Jr.* (DANIEL BRUCE LLOYD, 28. 1. 1999)

Page 750 line 12, Index, left column: Shokrollahi, *Mohammad* Amin (MICHAEL CLAUSEN, 25. 5. 1999)

Page 754 lines 1–2, end of Index: the correct quote is

وَ مَا مِنْ غَآئِبَةٍ فِى السَّمَآءِ وَ الْاَرْضِ اِلَّا فِىْ كِتَبٍ مُّبِيْنٍ

The Holy Qur'ān (732)

(28. 5. 2001)

inside back cover Radix conversion takes time $O(\mathsf{M}(n)\log n)$, according to Theorem 9.15. For the special case of Taylor expansion, as in Corollary 9.16, Aho, Steiglitz & Ullman (1975) give an $O(\mathsf{M}(n))$ algorithm; see also Schönhage, Grotefeld & Vetter (1994), page 284. (ARNOLD SCHÖNHAGE, 3. 6. 1999)