Modern Computer Algebra

Addenda and corrigenda
2013 edition (and usually earlier editions)

7 April 2016

JOACHIM VON ZUR GATHEN
and
JÜRGEN GERHARD

Bonn and Waterloo

CAMBRIDGE
UNIVERSITY PRESS

1. 2013 edition (and usually earlier editions)

Page 102 last line of Theorem 5.1: replace $7ny$ by $7n$. (XIANGUI ZHAO, 14. 10. 2013)

Page 291 Exercise 9.34: The second part of this exercise, computing a square root of 2 modulo 3^8, cannot be solved: 2 has no square root modulo 3, and therefore no solution exists modulo any power of 3, either. This should be changed to, e.g., "compute a square root of 2 modulo 7^8". 1999 edition: page 276; 2003 edition: page 287. (XIANGUI ZHAO, 2. 12. 2013)

Page 319 line 3 of Step 8: There is a typographical error in the leading exponent of t_5; the correct polynomial (i.e., the top right entry of the matrix) is $3x^4+3x^3+4x+1$. (DEREJE KIFLE, 30. 5. 2014)

Page 321 Step 3 of Example 11.2 (continued): The numbers to the right of the $\upharpoonright$ truncation operator are inccorect. This should read $r_0 \upharpoonright (2\cdot 3-2) = r_0 \upharpoonright 4 = x^4+5x^3+3x^2+5$, $r_1 \upharpoonright (4-(8-7)) = r_1 \upharpoonright 3 = x^3+4x^2+2x+2$ and ... (DEREJE KIFLE, 30. 5. 2014)

Page 330 lines –6 and –5, Example 11.17: The quotients q_2 and q_3 are incorrect. The correct calculations are as follows:

$$\begin{aligned} r_0 &= q_1r_1+r_2 = \left(\frac{1}{3}x+\frac{4}{9}\right)r_1+\frac{16}{9}x+\frac{32}{9}, \\ r_1 &= q_2r_2+r_3 = \left(\frac{27}{16}x-\frac{9}{4}\right)r_2+9, \\ r_2 &= q_3r_3 = \left(\frac{16}{81}x+\frac{32}{81}\right)r_3. \end{aligned}$$

(ROMAIN LEBRETON, 12. 2. 2016)

Page 467 Exercise 15.2: The suggested prime $p=5003$ does not satisfy the inequality $2B<p<4B$ in step 2 of Algorithm 15.2. The factorization will still succeed with that prime. Alternatively, use $p=199999$, which lies within then required bounds. 1999 edition: page 442; 2003 edition: page 455. (WEIXI GU, 10. 3. 2014)

Page 474 lines 2-3, Lemma 16.2: The conclusion is trivial over $\mathbb{R}$, and should be replaced by the following: Then $\det(g_{ij})_{1\le i,j\le n}$ is an integer multiple of $\det(f_{ij})_{1\le i,j\le n}$. 1999 edition: page 448; 2003 edition: page 462. (ALBERT HEINLE, 20. 1. 2015)

Page 509 lines 8-9, Notes 17.1: The Chor-Rivest cryptosystem was broken by Vaudenay (1998). 1999 edition: page 483; 2003 edition: page 497. (DANIEL PANARIO, 12. 11. 2012)

Page 599 lines 4-5: This should be "$\mathrm{lt}(f_1)$ or $\mathrm{lt}(f_2)$", instead of "$\mathrm{lc}(f_1)$ or $\mathrm{lc}(f_2)$". (XIANGUI ZHAO, 10. 3. 2014)

2. 2003 edition (and usually 1999 edition)

Page 11 line -8: replace $6+6+3=15$ by $6+6+1=13$. (PETER NILSSON, 28. 12. 2008)

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

Page 45 line 5: remove the superfluous last parenthesis in "$\gcd(\gcd(a,b),c))$". 1999 edition: page 45, line 4. (MASAAKI KANNO, 24. 3. 2004)

Page 51 line –8: $\ell > 2$ instead of $\ell \geq 2$ (HEIKO KÖRNER, 17. 12. 2002)

Page 52 line 9: add *if* $n \geq 1$

line 10, equation (8): $\ell = n-1$, not $\ell = n$

(HEIKO KÖRNER, 17. 12. 2002)

Page 54 line -1 should read "the product of the normal forms". 1999 edition: page 46, line 2. (MASAAKI KANNO, 24. 3. 2004)

Page 60 Exercise 3.2 (page 57 in 1999 edition): Replace "ring" by *integral domain*. There are rings with zero divisors in which the claim is false. Victor Shoup pointed out to us the following counterexample from Anderson, Axtell, Forman & Stickles (2004), originally due to Kaplansky. R is the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$, with pointwise addition and multiplication. We define $a,b \in R$ by $a(x) = b(x) = x$ for $x < 0$, $a(x) = b(x) = 0$ for $0 \leq x \leq 1$, and $a(x) = -b(x) = x-1$ for $x > 1$. Then $a \mid b$ and $b \mid a$, but there is no unit $c \in R^\times$ with $a = bc$. (VICTOR SHOUP, 13. 1. 2005)

Page 63 Exercise 3.20. The correct claim in (ii) is $c_{i+2}(0,0,x_2,\ldots,x_i) = Tc_i$, and in (iii) it is

$$R_i = \begin{pmatrix} Tc_{i-1} & T_{c_i} \\ c_i & c_{i+1} \end{pmatrix}$$

for $i \geq 1$. (CHARLES-ANTOINE GIULIANI, 16. 02. 2008) .

Page 72 line 14, Lemma 4.5: K is an extension field of F (HEIKO KÖRNER, 19. 2. 2003)

Page 76 line -9: replace $\det f$ by $\deg f$. 1999 edition: page 72, line 16. (STEFAN DREKER, 15. 07. 2003)

Page 92 line –16, Exercise 4.30 (i): replace $\max\{\nu(f),\nu(g)\}$ by $\min\{\nu(f),\nu(g)\}$ (KATHY SHARROW, 21. 2. 2002)

Page 93 line 11, Exercise 4.33 (i): replace nonconstant by *nonlinear* (OLAF MÜLLER, 12. 8. 2003)

Page 100 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 101 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 104 line 13: the reference should be to *Section 3.1* instead of 2.4 (OLAV GEIL, 12. 10. 2003)

Page 108 line 10: see page 140 for a justification of this formula (HUANG YONG, 9. 4. 2002)

Page 115 line 13: change "Lemma 3.15 (vii)" to *Lemma 3.15 (vi).* (OLAV GEIL, 17. 03. 2006)

Page 117 line 7: change "Chinese Remainder Theorem 5.3" to *Chinese Remainder Theorem, Corollary 5.3.* 1999 edition: page 97.

line -10: change "Lemma 3.15 (vii)" to *Lemma 3.15 (vi).* 1999 edition: page 239, line 1. (OLAV GEIL, 17. 3. 2006)

Page 119 line 1: $t = x/2$, not $t = -x/2$ (HEIKO KÖRNER, 19. 2. 2003)

Page 124 line 6: $t = \alpha t_j^*$ instead of $t = \alpha t_j$ (HEIKO KÖRNER, 19. 2. 2003)

Page 125 line –9: $q = 2$ instead of $q = 1$ (HEIKO KÖRNER, 19. 2. 2003)

Page 127 line 4, proof of Lemma 5.29: replace (34) by (33) (HEIKO KÖRNER, 19. 2. 2003)

Page 134 Exercise 5.32, first two lines: replace "quadratic matrix" by *square matrix* and remove "for all i". 1999 edition: page 127. (MASAAKI KANNO, 24. 3. 2004)

Page 147 line -17: replace "irreducibles of $R[x]$" by *irreducibles of R.* 1999 edition: page 139, line -17. (STEFAN DREKER, 30. 12. 2004)

Page 148 line 5: replace K by $K\setminus\{0\}$. 1999 edition: page 140, line 5. (STEFAN DREKER, 30. 12. 2004)

Page 155 line 1: replace Gauß' lemma 6.6 by *Corollary 6.10* (HEIKO KÖRNER, 25. 4. 2003)

Page 156 line –5, 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 159 line –6: Solovay & Strassen's primality test (Section 18.5). Also on page 196, line 20. 1999 edition: pages 151 and 187. (26. 06. 2011)

Page 174 line -6: remove the superfluous "when $\#S \geq d$". 1999 edition: page 166, line 12. (HEIKO KÖRNER, 7. 07. 2004)

Page 208 line 10: replace $d(r-c)$ by $w(r-c)$. 1999 edition: page 198, line 10. (HEIKO KÖRNER, 7. 07. 2004)

Page 210 line 3: replace "$+a_1 + a_0$" by "$+a_1\beta + a_0$". 1999 edition: page 200 (SEBASTIAN GRIMSELL, 23. 11. 2005)

Page 212 line –5, Example 7.4 (continued): the Padé approximant is v/u and not u/v (OLGA MENDOZA, 18. 4. 2003)

Page 222 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

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

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 226 line 6, Lemma 8.7: replace $1 < \ell < n$ by $1 \leq \ell < n$ (OLAV GEIL, 27. 10. 2003)

Page 228 line –7: $R[x]$, not $F[x]$ (OLAV GEIL, 27. 10. 2003)

Page 240 line 14: Write $3^\lambda fg$ instead of $2^\lambda fg$. 1999 edition: page 230. (HEIKO KÖRNER, 18. 10. 2004)

Page 241 line 18 (Input of Algorithm 8.25): change "64-adic" to 2^{64}-*adic*. 1999 edition: page 231. (MASAAKI KANNO, 24. 3. 2004; HEIKO KÖRNER, 18. 10. 2004)

Page 243 lines 12 and 18: replace "64-adic" by 2^{64}-*adic*. 1999 edition: page 233, lines 9 and 15. (MASAAKI KANNO, 24. 3. 2004; HEIKO KÖRNER, 18. 10. 2004)

Page 247 line –22, 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 254 line 8: the constant term of rev(a) is a_n, not a_0. (HELMUT MEYN, 26. 6. 2005; OLAV GEIL, 12. 05. 2006; SEBASTIAN GRIMSELL, 18. 01. 2008)

Page 256 line –8, proof of Theorem 9.4: replace fg_i by fg_{i-1} (TOM KOORNWINDER, 6. 3. 2003)

Page 263 Lemma 9.20: We may simplify the first sentence to: *Let* $\varphi \in R[y]$ *and* $g \in R$. This removes the notational collision with the φ_i in line 5. (HELMUT MEYN, 26. 06. 2005; OLAV GEIL, 12. 05. 2006)

line 6: read $\varphi = \sum_{2\le i\le n} \varphi_i (y-g)^{i-2}$. 1999 edition for both corrections: page 253. (HELMUT MEYN 21.06.2005; OLAV GEIL 12 MAY 2006)

Page 264 lines 3 and 5: h is being substitued for y, and $\psi(h-g)$ must be replaced by $\psi(h)$. (OLAV GEIL, 12. 05. 2006);

Page 284 Exercise 9.10: in characteristic 2 the cost of algorithm 9.3 drops to $2\mathsf{M}(l)+2l$ because the cost for the ith step is at most $2^i + \mathsf{M}(2^i)$. 1999 edition: page 273. (GUILLERMO MORENO-SOCÍAS, 22. 05. 2006)

Exercise 9.12(ii): s should be the inverse of f modulo r (so that $sf \equiv 1 \bmod r$), instead of the inverse of r modulo f. 1999 edition: page 273. (HOWARD CHENG, 29. 6. 2005)

Page 302 Theorem 10.25, last line: write *word operations* instead of "operations in F". 1999 edition: page 290. (MASAAKI KANNO, 24. 3. 2004, ALLAN STEEL, 28. 04. 2006)

Page 309-325 The fast Euclidean algorithm in the 1999 and 2003 editions contained an error. Much of Chapter 11 has been rewritten for the 2013 edition.

Page 328 line -2, proof of Theorem 12.2: Lemma 8.2 is not general enough to imply the first claim; see the correction for page 222. (MURRAY BREMNER, 29. 10. 2003)

Page 376 Figure 14.5: The labels in this figure are left-shifted too far. The figure with correct labels is:

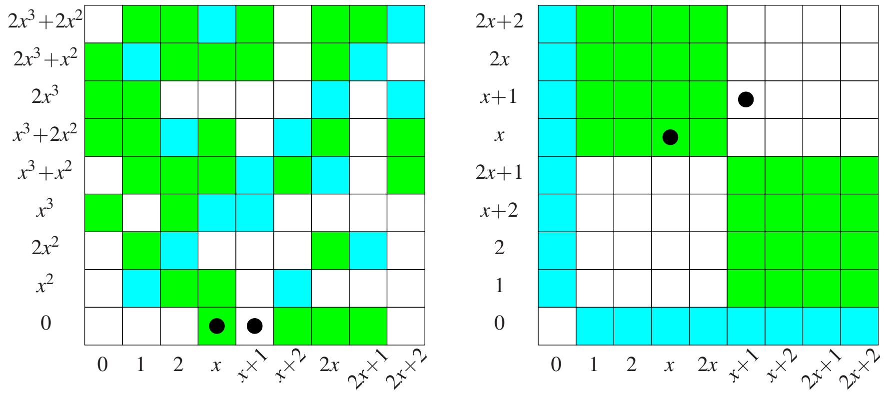

FIGURE 14.5: The lucky and unlucky choices for factoring $x^4+x^3+x-1 \in \mathbb{F}_3[x]$.

(8. 8. 2003)

Page 392-393 Algorithm 14.31: In the output specification, replace "an irreducible factor" by "a proper factor". Replace the condition in step 5 by "if $g_1 \neq 1$ and $g_1 \neq f$". Replace the first paragraph of the proof, starting at "If $g_1 = 1$", by the following: In order to analyze the failure probability, we note that a is a uniformly random element of $\mathcal{B}$, so that $u_i \equiv a \bmod f_i$ for $1 \leq i \leq r$ are independent random elements of $\mathbb{F}_q$ (via its embedding in $\mathbb{F}_q[x]/\langle f_i \rangle$). If some u_i is zero and some u_j nonzero, a factor is returned in step 5. With probability q^{-r}, all u_i's are zero. All u_i's are nonzero with probability $(1-q^{-1})^r$, and then each $v_i = u_i^{(q-1)/2}$ is 1 or -1 with probability 2^{-1} for either case, and all v_i's are equal with probability $2 \cdot 2^{-r}$. This failure occurs in step 7 with probability $t = q^{-r} + (1-q^{-1})^r \cdot 2^{-r+1} < 2^{-1}$, since this holds for $r = 2$, $r \geq 2$ and t is monotonically decreasing in r. 1999 edition: pages 378-379. (EVAN JINGCHI CHEN, 19. 04. 2005; CHRISTIAAN VAN DE WOESTIJNE, 3. 02. 2006)

Page 394 Algorithm 14.33, step 1: Replace "choose two row vectors" by "choose two column vectors". 1999 edition: page 380. (MICHAEL NÜSKEN, 19. 4. 2006)

Page 395 line -1: Replace "given in Notes 14.9" by *given in Notes 14.8*. 1999 edition: page 381. (MICHAEL NÜSKEN, 19. 4. 2006)

Page 404 line 4, 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 417 Exercise 14.38(i): Insert before the comma: *with at most one exception*. 1999 edition: page 402. [Solution: In the vector space representation, as in Figure 14.8, we let $c_{ij} = b_j \text{ rem } f_i \in \mathbb{F}_2$ be the ith component of the basis element b_j.

Thus $c_j = (c_{1j}, \ldots, c_{rj})$ for $1 \le j \le r$ form a basis of $\mathbb{F}_2^r$. Suppose there were two indices i, say $i = 1$ and $i = 2$ for simplicity, for which the conclusion fails. Then $c_{1j} = c_{2j}$ for all j and for every vector in the space spanned by $c_1, \ldots, c_r$, the first coordinate would equal the second one. This contradiction proves the claim.

Note. For $q > 2$, the statement of (i) is false. We may take some $u \in \mathbb{F}_q$ with $u \ne 0, 1$, the unit vectors $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with a 1 in the ith position, $b_1 = (1, \ldots, 1) = \sum_{1 \le i \le r} e_i$, and $b_i = ub_1 + e_i$ for $2 \le i \le r$. Then $b_1, \ldots, b_r$ form a basis of $\mathbb{F}_q^r$, since $e_i = b_i - ub_1$ for $i \ge 2$ and $e_1 = (1 - ru + u)b_1 + \sum_{2 \le i \le r} b_i$.] (GIULIO GENOVESE, 11. 5. 2004)

Page 434 Example 15.8 (Continued): Replace the values of b, c and d by $b = -5x^2 - 10x - 5$, $c = 10x - 10$ and $d = -10$. 1999 edition: page 420. (EVAN JINGCHI CHEN, 19.04.2005, ROBERT SCHWARZ, 1. 06. 2008)

Page 456 Exercise 15.10 (v): $a_{n,r} = 0$ instead of $a_{nr} = 0$. Replace $1 \le k \le n \le 8$ by $1 \le r \le n \le 8$ (HELMUT MEYN, 9. 9. 2003)

Page 467 Example 16.3 (continued), last paragraph of this page: "...on the lattice of Example 16.3, later.) and Figure 16.3 depicts...", the "later.)" part is spurious. 1999 edition page 453. (JOHN R. BLACK, 06. 01. 2005)

Page 476 line 12: replace $q^* = q^{**}u + r^{**}$ by $r^* = q^{**}u + r^{**}$ (EUGENE LUKS, 1. 12. 2002)

Page 485 line 2, Notes 16.2 and 16.3: insert *is* after "it" (STEFAN GERHOLD, 16. 7. 2003)

Page 590 line 13, Example 21.10 (continued): this should read $-(x^2y - x)$, not $-(xy^2 - x)$ (VOLKER KRUMMEL, 19. 2. 2003)

Page 592 line –11, proof of Theorem 21.18: $(\alpha_1, \ldots, \alpha_n) \in B$, not $\in A$ (TOM KOORNWINDER, 24. 4. 2003)

Page 611 Exercise 21.25, lines 23–25: replace this sentence by: if $\nabla f = (f_x, f_y)$ and $\nabla g = (g_x, g_y)$ are the Jacobians of f and g, respectively, where $f_x = \partial f / \partial x$ and f_y, g_x, g_y are defined analogously, then the equality $\nabla f = \lambda \nabla g$ holds at a local maximum or minimum of f on S for some $\lambda \in \mathbb{R}$. 1999 edition: page 595. (15. 2. 2004)

Page 614 line 12: in Lemma 22.2 (iv), add *for* $n \ge 1$. 1999 edition: page 598, line 12. (STEFAN DREKER, 30. 12. 2004)

Page 619 line –8, Example 22.6 (continued): The blank entry in row 5, column 4 of the matrix is zero. (29. 6. 2003)

Page 623 line 8, Example 22.13 (ii): replace $2x \cdot \exp(x)$ by $2x \cdot \exp(x^2)$ (20. 6. 2003)

Page 624 line 13: replace the right-hand side bv' by bv (19. 6. 2003)

Page 625 line –11, Example 22.16: replace the equation by

$$\frac{g'}{g} = \frac{(3x^2+2x)\exp(x)+(x^3+x^2)\exp(x)}{(x^3+x^2)\exp(x)} = \frac{x^2+4x+2}{x^2+x},$$

(29. 6. 2003)

Page 636 line 12: replace the minus by a plus in the product rule (21. 7. 2003)

Page 637 line -7: in Definition 23.2, replace $f(x+m-1)$ by $f(x-m+1)$. 1999 edition: page 611, line -7. (STEFAN DREKER, 15. 07. 2003)

Page 649 line 16, Example 23.17 (ii): replace F by $\mathbb{Q}$ twice. 1999 edition: page 623, line 14. (STEFAN DREKER, 15. 07. 2003)

Example 23.17 (iv), line -5: replace "We compute" by *Using the shift operator E, we compute.* 1999 edition: page 623, line -4. (STEFAN DREKER, 30. 12. 2004)

Page 661 line –4, 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 686 In equation (29), the constant term of the numerator should be 34, and the correct expression is:

$$w = \frac{-9u^2v-6u^2-6uv+20u+23v+34}{9u^2+6u-23}$$

1999 edition: page 660. (JENS KUNERLE, 04. 10. 2004)

Page 753 line 32, References, Schwenter (1636): *Mathematicæ* instead of Mathematiæ (8. 8. 2003)

Page 768 Joseph Diaz Gergonne (28. 04. 2006)

Solutions to selected exercises

Page 21 Solution to Exercise 6.44, line 10: Replace $O(mk^2d^2)$ by $O(mk^2\beta^2)$, and assume $\alpha \le \beta$. (MASAAKI KANNO, 24. 3. 2004)

inside front cover The following figure is missing: (8. 8. 2003)

Fast multiplication

multiplication algorithm	time $\mathsf{M}(n)$
classical	$2n^2$
Karatsuba	$O(n^{1.59})$
Schönhage & Strassen	$O(n \log n \log\log n)$
Fürer	$n \log n \cdot 2^{O(\log^* n)}$

Fast integer and polynomial arithmetic

task	time
multiplication (§8.1) division with remainder (§9.1) modular multiplication (§9.1)	$O(\mathsf{M}(n))$
radix conversion (§9.2) multipoint evaluation (§10.1) interpolation (§10.2) reduction modulo several moduli (§10.3) Chinese Remainder Algorithm (§10.3) Extended Euclidean Algorithm (§11.1) modular inversion (§11.1)	$O(\mathsf{M}(n) \log n)$

Classical arithmetic: time $O(n^2)$ for all tasks (Chapters 2–5)

3. 1999 edition only

Page 51 line 2: $(2n_i+1)(n_{i-1}-n_i+1)$ instead of $2n_i(n_{i-1}-n_i+1)$. The following calculations must be changed accordingly. This is corrected in the second edition, but it does not appear in the addenda and corrigenda. (MASAAKI KANNO, 24. 3. 2004)

Page 73 line 11: Remove " unique and". This corrects the correction in the addenda and corrigenda for the 1999 edition. The sentence is correct in the 2003 edition. (MASAAKI KANNO, 24. 3. 2004)

Page 230 line 4: $3^{l-1} < n \leq 3^l$, not 3^ℓ. (HEIKO KÖRNER, 18. 10. 2004)

Page 249 Exercise 8.23, page 239, line 1: Replace 66537 by 65537. (OLAV GEIL, 17. 03. 2006; R. GREGORY TAYLOR, 11. 04. 2006)

References

The numbers in brackets at the end of a reference are the pages on which it is cited. Names of authors and titles are usually given in the same form as on the article or book.

D. D. ANDERSON, M. AXTELL, S. J. FORMAN, and JOE STICKLES (2004), When are Associates Unit Multiples? *Rocky Mountain Journal of Mathematics* **34**(3), 811–828. [3]

SERGE VAUDENAY (1998), Cryptanalysis of the Chor-Rivest cryptosystem. In *Advances in Cryptology: Proceedings of CRYPTO '98*, Santa Barbara, CA, vol. 1462, ed. H. KRAWCZYK. Springer-Verlag, Berlin, Heidelberg, 243–256. [2]