# Modern Computer Algebra

## Addenda and corrigenda, 2003 edition

30 November 2003

JOACHIM VON ZUR GATHEN
and
JÜRGEN GERHARD

Universität Paderborn

CAMBRIDGE
UNIVERSITY PRESS

**Murray Bremner**

**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)

**Winfried Bruns**

**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)

**Olav Geil**

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

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

**Stefan Gerhold**

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

**Tom Koornwinder**

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

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

**Heiko Körner**

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

**Page 100** 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 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 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 (33) by (34) (HEIKO KÖRNER, 19. 2. 2003)

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

**Volker Krummel**

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

**Eugene Luks**

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

**Olga Mendoza**

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

**Helmut Meyn**

**Page 456** line –20, Exercise 15.10 (v): $a_{n,r} = 0$ instead of $a_{nr} = 0$ (HELMUT MEYN, 9. 9. 2003)

line –18, Exercise 15.10 (v): replace $1 \leq k \leq n \leq 8$ by $1 \leq r \leq n \leq 8$ (HELMUT MEYN, 9. 9. 2003)

### Olaf Müller

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

**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)

### Kathy Sharrow

**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)

### Huang Yong

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

### The authors

**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 | $O(n \log n \log\log n)$ |

## Fast integer and polynomial arithmetic

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

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

**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

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

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

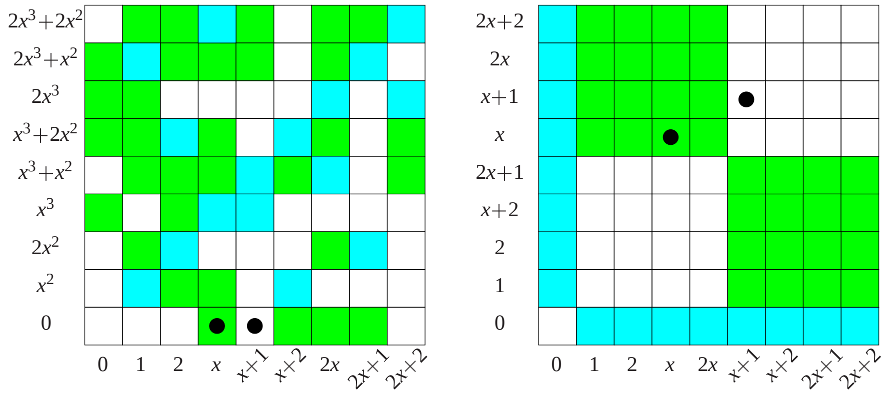


FIGURE 14.5: The lucky and unlucky choices for factoring $x^4+x^3+x-1 \in \mathbb{F}_3[x]$.

(8. 8. 2003)

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