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^n". 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 truncation operator are incorrect. 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:

  $r_0 = q_1 r_1 + r_2 = \left(\frac{1}{3}x + \frac{4}{9}\right) r_1 + \frac{16}{9}x + \frac{32}{9}$,

  $r_1 = q_2 r_2 + r_3 = \left(\frac{27}{16}x - \frac{9}{4}\right) r_2 + 9$,

  $r_2 = q_3 r_3 = \left(\frac{16}{81}x + \frac{32}{81}\right) r_3$.

  (Romain Lebreton, 12. 2. 2016)

Page 467

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

Page 509

Page 599
- lines 4-5: This should be "lt($f_1$) or lt($f_2$)" instead of "lc($f_1$) or lc($f_2$)". (Xiangui Zhao, 10. 3. 2014)

Modern Computer Algebra, Joachim Von zur Gathen and Jurgen Gerhard, version 7 April 2016

Page 11  

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. (Masaki 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 $n \geq 1$

Page 54  

Page 60  
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 $c \in R^*$ with $a = bc$. (Victor Shoup, 13. 1. 2005)

Page 63  
Exercise 3.20. The correct claim in (ii) is $c_{i+2}(0,0,x_2,\ldots,x_i) = T c_i$, and in (iii) it is
\[
R_i = \begin{pmatrix} 1 & T_{ci-1} \\ c_i & T_{ci} \\ c_i & c_{i+1} \end{pmatrix}
\]
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  

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  

Page 117  


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

Page 124  
line 6: $t = \alpha t^*$ 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  

Page 147  

Page 148  

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 $\overline{\text{lc}}(f) \neq 0$ by $\overline{\text{lc}}(f)$ 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  

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

Modern Computer Algebra, Joachim von zur Gathen and Jürgen Gerhard, version 7 April 2016
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 $b, c \in \mathbb{R}_{>0}, d \in \mathbb{R}_{\geq 0}, S, T : \mathbb{N} \to \mathbb{N}$ 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

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

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

$$T(2^i) \leq bT(2^{i-1}) + S(2^i) \leq b(bT(2^{i-2}) + S(2^{i-1})) + S(2^i)$$

$$= b^2T(2^{i-2}) + bS(2^{i-1}) + S(2^i) \leq \ldots$$

$$\leq b^iT(1) + \sum_{0 \leq j < i} b^j S(2^{i-j}) \leq d2^{i\log b} + S(2^i) \sum_{0 \leq j < i} \left( \frac{b}{c} \right)^j,$$

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

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

and the first claim follows. □

(29. 11. 2003)
Page 240  line 14: Write $3^\lambda f g$ instead of $2^\lambda f g$. 1999 edition: page 230. (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 $f g_i$ by $f g_{i-1}$ (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 $\varphi_i$ in line 5. (HELMUT MEYN, 26. 06. 2005; OLAV GEIL, 12. 05. 2006)

Page 264  lines 3 and 5: $h$ is being substituted 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 $2M(l) + 2l$ because the cost for the $i$th step is at most $2^i + M(2^i)$. 1999 edition: page 273. (GUILLERMO MORENO-SOCIAS, 22. 05. 2006)


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

(8. 8. 2003)

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 $B$, so that $u_i \equiv a \mod f_i$ 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)


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 $i$th component of the basis element $b_j$.]
Thus $c_j = (c_{1j}, \ldots, c_{rj})$ for $1 \leq j \leq r$ form a basis of $F_r^n$. 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 $u \in F_q$ with $u \neq 0, 1$, the unit vectors $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with a 1 in the $i$th position, $b_1 = (1, \ldots, 1) = \sum_{1 \leq i \leq r} e_i$, and $b_1 = ub_1 + e_i$ for $2 \leq i \leq r$. Then $b_1, \ldots, b_r$ form a basis of $F_q^n$, since $e_i = b_1 - ub_1$ for $i \geq 2$ and $e_1 = (1 - ru + u)b_1 + \sum_{2 \leq i \leq r} b_i$.]

(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): $a_{nr} = 0$ instead of $a_{nr} = 0$. Replace $1 \leq k \leq n \leq 8$ by $1 \leq r \leq n \leq 8$ (HELMUT MEYEN, 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 $- (\lambda^2 y - x)$, 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 $\nabla f = (f_s, f_t)$ and $\nabla g = (g_s, g_t)$ are the Jacobians of $f$ and $g$, respectively, where $f_s = \partial f/\partial x$ and $f_t, g_s, g_t$ 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


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 $bv^2$ by $bv$ (19. 6. 2003)

Page 625

line –11, Example 22.16: replace the equation by
\[
g' = \frac{(3x^2 + 2x)\exp(x) + (x^3 + x^2)\exp(x)}{(x^3 + x^2)\exp(x)} = \frac{x^2 + 4x + 2}{x^2 + x},
\]

(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


Page 661
line –4, Exercise 23.4 (iii): This line should read

\[
f = \sum_{0 \leq i < n} \frac{(\Delta_i f)(0)}{h^i i!} x(x-h) \cdots (x-ih+h),
\]

(OLAF MÜLLER, 12. 8. 2003)

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

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


Page 753

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 \( \alpha \leq \beta \). (MASAAKI KANNO, 24. 3. 2004)
The following figure is missing: (8. 8. 2003)

**Fast multiplication**

<table>
<thead>
<tr>
<th>multiplication algorithm</th>
<th>time $M(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>classical</td>
<td>$2n^2$</td>
</tr>
<tr>
<td>Karatsuba</td>
<td>$O(n^{1.59})$</td>
</tr>
<tr>
<td>Schönhage &amp; Strassen</td>
<td>$O(n \log n \log \log n)$</td>
</tr>
<tr>
<td>Fürer</td>
<td>$n \log n \cdot 2^{O(\log^* n)}$</td>
</tr>
</tbody>
</table>

**Fast integer and polynomial arithmetic**

<table>
<thead>
<tr>
<th>task</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>multiplication (§8.1)</td>
<td>$O(M(n))$</td>
</tr>
<tr>
<td>division with remainder (§9.1)</td>
<td>$O(M(n))$</td>
</tr>
<tr>
<td>modular multiplication (§9.1)</td>
<td>$O(M(n) \log n)$</td>
</tr>
<tr>
<td>radix conversion (§9.2)</td>
<td></td>
</tr>
<tr>
<td>multipoint evaluation (§10.1)</td>
<td></td>
</tr>
<tr>
<td>interpolation (§10.2)</td>
<td></td>
</tr>
<tr>
<td>reduction modulo several moduli (§10.3)</td>
<td></td>
</tr>
<tr>
<td>Chinese Remainder Algorithm (§10.3)</td>
<td></td>
</tr>
<tr>
<td>Extended Euclidean Algorithm (§11.1)</td>
<td></td>
</tr>
<tr>
<td>modular inversion (§11.1)</td>
<td></td>
</tr>
</tbody>
</table>

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.
