Remarks and Errata to the Second Edition of *A Concrete Introduction to Higher Algebra*, published by Springer-Verlag New York, 1995 (first edition, 1979), second printing, September, 1997

Lindsay N. Childs

Reviews

The following telegraphic review appeared in the *American Mathematical Monthly*, vol. 103 (Feb. 1996), p. 282:

> New edition of a durable and well-regarded text. Admirers needn't feel concern — the essential elements and appeal of the first edition have survived intact despite substantial revision. [A review of the first edition appeared in the Monthly of October, 1983.] Changes include more emphasis on elementary group theory, more treatment of computational number theory and primality testing, new coverage of quadatric reciprocity, use of the discrete Fourier transform.

Errata (as of 6/12/98)

These are corrections to the first and second printings of the second edition. Those marked by '#' remain errata (or comments) for the second printing, which came out in late summer, 1997.

Names in parentheses following the errata refer to the discoverer.

Concerning the unattributed errata for the first printing, Prof. Donald Crowe of the University of Wisconsin, Madison, kindly provided a dozen of them, which he estimated to be only 10% of the total he found. He suggested that the careful reader may find many more. My thanks to him for his assistance. Thanks also to Richard Ehrenborg of Cornell for several errata, and to Olav Hjortås[1] of Bergen for all but one of the errata to the first printing between pages 264 and 355.

Thanks also to Margaret Readdy and her student Chris Jeuell of Cornell for nearly all of the errata which remain in the second printing. My thanks also to Prof. Readdy for her comments noted below.

Any additional errata will be greatly appreciated. Please send them to

`lc802@math.albany.edu`.

[1] URI: http://www.lstud.ii.uib.no/~s771/indexeng.html

p. 8, line -6

"Then $P(n)$ is true ..."

# p. 9 (line -14)

Delete "(1)". (Chris Jeuell)

# p. 9 (line -5)

"n uses" should be replaced by "$n - n_0$ uses". (Jamie Bessich)

# p. 10 (line -12)

The expression $(k^3 + 3k^2 + 3k + 1)$ should not itself be cubed. Similarly, $(k^2 + 2k + 1)$ should not be squared. (Chris Jeuell)

p. 12,

E12 is defective and should be omitted (it appears impossible to prove either part by induction).

# p. 12 (E14):

"theorem" and "proof" should be in quotes. (Chris Jeuell)

# p. 14 (line 10)

"for some number r" should be replaced by "for some natural number r".

# p. 16 (line -7)

Replace "Example 6, above" by "Example 1 (from section 2B)". (Chris Jeuell)

# p. 20 (line 2)

a/b should be replaced by b/a in the *floor* and *fraction* expressions. (Chris Jeuell)

# p. 20 (line 8)

"$7 + 10$" should be "7×10" in the decimal expansion of 1976. (Chris Jeuell)

# p. 24 (E4)

Italicize "n" in "Which n would be appropriate?" (Chris Jeuell)

# p. 26 (line 10)

Italicize "a" in "to mean a does not divide ...". (Chris Jeuell)

# pp. 31 - 32

Margaret Readdy writes: "Use matrix notation to give a nicer presentation for gcd and Bezout."

# p. 32 (line -10)

q should be q_1, as in: $r_1 = b \cdot 1 + a \cdot (-q_1)$. (Chris Jeuell)

# p. 36 (line -6)

"... after 128 divisions ..." (Chris Jeuell)

# p. 37 (line 12)

"If the quotients $q_1, q_2, \ldots q_n$ are large ..." (Chris Jeuell)

# P. 38 line 10

“for any $n > 1$, , $a_{n+1} = a_n + a_{n-1}$” (Margaret Readdy)

# p. 39 (sentence before the Corollary)

“... with d digits satisfies $a < a_{5d+2} \ldots$” (Chris Jeuell)

p. 45, line 22 and E4

This is slightly incorrect. The algorithm applied to $\sqrt{19}$ shows that d can be larger than $\sqrt{19}$. Suppose $0 < c < \sqrt{m}$, $0 < d < \sqrt{m} + c$, d divides $m - c^2$, and one performs a step of the algorithm, namely: write $(\sqrt{m} + c)/d = q + r$ where $0 < r < 1$, then rationalize the denominator of $1/r$ to get $(\sqrt{m} + c')/d'$. Then $0 < c' < \sqrt{m}$, d' divides $m - c'^2$, and $0 < d' < \sqrt{m} + c'$, not $d' < \sqrt{m}$. So always $0 < d' < 2\sqrt{m}$. Hence the number of pairs (c, d) which can arise in the algorithm is bounded by $2m$. Thanks to Bill Hammond for finding this error.

# p. 51 Proof of Thm 1

“If not, $\sqrt{2} = b/a$, with a, b natural numbers. Multiplying both sides by a and squaring, we get ...” (Margaret Readdy)

p. 54, E24

“Using the last two exercises and E20, prove ...”

# p. 55 (E1)

In the hint, p_1 should be italicized. (Chris Jeuell)

p, 58, line -15

“by Proposition 2” (not Proposition 1), (found by Morris Orzech)

# p. 67 E9 (ii)

“$(a_1 + ... + a_n)^2 \equiv \ldots$” (Margaret Readdy)

# p. 71, line 13.

Wiles’ proof appeared in the *Annals of Mathematics*, May, 1995. The story of how it was proved has been the subject of several popular books. One is: *Fermat’s Enigma*, by Simon Singh, Walker & Co., 1997. An excerpt from Singh’s book appears in the February, 1998 issue of *Math Horizons*, the MAA journal about mathematics for undergraduates.

p. 80, E2:

change the reference to (iiia), p. 66; also, in the second line of the proof of (ii) of Proposition 1, change “$=$” to congruence.

p. 82, line 3 should read:

if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then $a + b \equiv a' + b' \pmod{m}$.

# p. 106 (line -10):

“with $1 \leq m < n < 2\sqrt{p}$” (Chris Jeuell)

# p. 109 (E3):

“(iv) Find other values of x_0 for which N divides $x_{12} - x_6$, and values of x_0 for which N doesn’t divide $x_{12} - x_6$.” (Chris Jeuell)

# p. 119 (line -10):

“c” should be italicized. (Chris Jeuell)

# p. 119 (line -8):

“a” should be italicized in “for all *a*”. (Chris Jeuell)

p. 123, Proposition 2:

Tat-Hung Chan of Fredonia observed that the ring $\mathbf{Z}/4\mathbf{Z}$ contradicts Proposition 2 on p.123. The proof breaks down because the only values for a and b are $a = b = 2$, so that $a, b, a+b, 0$ reduce to $2, 2, 0, 0$. Richard Ehrenborg and Steve Chase noted that the ring $\mathbf{F}_2[x]/(x^2)$ is the only other counterexample.

# p. 123 (line -10):

In “if such a number b exists”, the “a” should not be italicized. (Chris Jeuell)

# p. 126 (line 6):

The last “a” before “(s factors)” should be italicized. (Chris Jeuell)

# p. 127, line 3:

“Find the order of i+1”.

# p. 129, line 2 of proof of Proposition 2:

“If $f(a) = 0$, then $1 =$ ” (Olav Hjortaas has very sharp eyes!)

p. 135, lines 11, 13 and -7:

roman “a” should be italic “a”, also on line 1 of the next page. (The typesetter changed virtually all the italic “a”s within the text in the final manuscript to roman, and I obviously didn’t find them all!)

# p. 141 (E8):

The expression $p - 1!$ should be $(p-1)!$ (Chris Jeuell).

p. 143, line above E3:

“set of units of $\mathbf{Z}/m\mathbf{Z}$”

p. 153, line -12:

$m < g_0$ should be $m \leq g_0$.

p. 157, line -4:

$= (.46, 58, 17, 8, 34, 17, 8, \dots)$

p. 161, line -11:

$r/s = .q_1 \dots$

Section 10B, p. 164ff.:

Margaret Readdy writes: “There is no need to put all of these restrictions on RSA. There are four cases, namely $(w, N) = 1$, $(w, N) = p$, $(w, N) = q$, and $(w, N) = N$. The second and third cases are not hard to prove for the students and thus one has the full strength of RSA available. See Rivest, Shamir and Adleman article in Communications of ACM.”

# p. 169 lines -9, -8:

"…then for any integer a relatively prime to n, n divides $a^{n-1} - 1$". (Margaret Readdy)

# p. 169.:

An interesting commentary on Hardy's remarks appears in a paper of the eminent number theorist L. J. Mordell: Hardy's "A Mathematician's Apology", American Mathematical Monthly, vol. 77 (1970), pp. 831-835.

# p. 169, Exercise 3:

Saab Yaqub Hassan of Cornell observed that once encoded, the message cannot be decoded!

# p. 171, line -5:

The December, 1997 issue of Focus, the Mathematical Association of America's newsletter, reported a new largest prime: it was the Mersenne number $2^p - 1$ where $p = 2,976,221$. The discoverer was Gordon Spence of England. Elsewhere on the UAlbany Math. Dept.'s web page (and also in Keith Devlin's Focus article reporting on Spence's discovery) is a discussion of a world-wide ongoing search for more Mersenne primes, so Spence's prime is not likely to remain the largest for long.

In fact, a week after I wrote the above paragraph came an announcement that $2^p - 1$ is prime where $p = 3,021,377$. The discoverer was Roland Clarkson, a sophomore at California State Univ. at Dominguez Hills. For recent information on Mersenne primes, check `http://www.mersenne.org/` and

`http://www.utm.edu/research/primes/notes/3021377/`.

p. 172, Proposition 2:

"... then $m = \dots$ is a perfect number" (all in italics)

# p. 196 (line 12):

"Then $x = 3x_1 + 6x_2 + (-1)x_3 = -3946\dots$" (Chris Jeuell)

p. 200, line -4:

"$0 \leq a_2 \leq m_2$"

p. 240, line 13:

$s > 0$ should be $s \geq 0$.

p. 243, line -3:

"an element", not "a element".

p. 249, E 10:

"with $f(x)r(x) + g(x)s(x) = d(x)$"; E 12, "for all $r \neq 0, 1$" (found by Bill Hammond).

p. 253, line -8:

the last factor of $x^3 - 2$ in $C[x]$ should be $x - (\omega^2)2^{(1/3)}$.

p, 264, line 2:

the square root sign should not cover the x.

p. 271, line -2:

$D = \{z : |z| \leq R\}$.

p. 279, line -5:

italicize the x in "x^3".

# **p. 287, line -2:**

Clearer language would be: "Suppose $f(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are in $\mathbf{Q}[x]$. Then ..."

# **p. 288 (line 5):**

The coefficient of x^2 should be -4, not -3, as the computations below show. The polynomial $x^4 - 3x^2 + 9$ is factorable over the integers; to see this, write it as $(x^4 + 6x^2 + 9) - 9x^2$, which is the difference of two squares. (Chris Jeuell)

# **p. 289 line -4:**

Change second term to $a_{n-1}r^{n-1}s$. (Margaret Readdy)

p. 292, line 7:

"Hence $\phi_p(g(0)) = \phi_p(h(0)) = 0$" [wrong subscript on the second ϕ]

p. 298, line 4:

"new", not "nwe".

p. 303, line 4 of Example 2:

$\deg r(x) < \deg m(x)$.

p. 308, line 1 of Section B:

modulo a polynomial [all roman]

# **p. 303 line 12:**

In Exercise 1 change "root" to "remainder". (Margaret Readdy)

# **p. 305 line -1:**

The (*) refers to the equation at line -8, which should be labeled with (*)
(Margaret Readdy)

# **p. 306 line 8:**

Delete extra comma. (Margaret Readdy)

# **p. 309 E2 (ii):**

The first modulus should be $x^4 + x + 1$, not $x^4 + x + x$. (Margaret Readdy)

# **p. 313, Section 21B:**

Margaret Readdy writes: As a comment, I showed the 4×4 and 8×8 Fast Fourier Transform matrix decompositions to my class, as well as explained butterfly diagrams to them (and piping, to speed up the process).

p. 317, line -10:

the coefficient of x in $f(x)$ should be $(a_1 + a_3x^2)$

# p. 320, fifth line after the matrix:

the second entry of the vector should be ω^{-i}, not ω^{-1}. (Chris Jeuell)

# p. 322 E6 (ii):

The $(i, j)^{\text{th}}$ entry should be 5^{ij}. Also, the notation "$(i - j)^{\text{th}}$ entry" should be "$(i, j)^{\text{th}}$ entry". (Margaret Readdy)

p. 326, line 5 of Example 1(continued):

$r_1(x) = x^2$

p. 326, line -3:

"The equation (3) becomes"

# p. 350, line 8:

the first strategy on line 9 was not used in the example above (but is useful in other examples).

p. 351, line 2:

the italic a should be roman (see comment on p. 135)

p. 353, line 3 of section A:

omit the).

p. 354, Proposition 1:

"A finite group G of order n is cyclic if and only if ..."

p. 355, lines 2-3:

Omit: "Assume in this next theorem that the group operation is multiplication"

p. 355, lines 11-12:

"Then $a^s = a^{dq} * a^r$, so $a^r = a^s * (a^d)^{-q}$ is a product ..."

# p. 355, line -10:

"... distinct. To do this"

p. 355, line -7:

"d divides n. ..."

# p. 369 line 22:

Comma after a^r. (Margaret Readdy)

p. 418, E13, line 2:

"many", not "may".

# p. 421 (E4):

There should be a left parenthesis after the slash, i.e., $\mathbf{F}_2[x]/(x^4 + \dots)$. (Chris Jeuell)

# p. 429 (line 8):

The left parenthesis in $p(x)$ should not be italicized. (!)(Chris Jeuell)

# p. 431 E5 (i):

Change “root” to “roots”. Delete comma after “are”. (Margaret Readdy).

p. 431, E5, (ii):

“Why does this not contradict the theorem that a polynomial of degree 4 cannot have more than four roots in a field.”

# p. 442, line 5:

Change first α to a.

# p. 442, line -6:

Change subscript on $C_1(x)$ to capital I (twice).

# p. 442, line -5:

Change minus to plus. (Margaret Readdy)

# p. 444 line -3:

Delete 1 in denominator of $\alpha + 1$, that is, change expression in parenthesis to $(\alpha + 1 + 1)$. (Margaret Readdy)

p. 447, line -5:

“... evaluates $R(x)$ at α^i, $i = 1, \ldots, 6$. Since $C(\alpha^i) = 0$, $i = 1, \ldots, 6$, ...”

# p. 448, Conditions for rank S starting at line -11:

Margaret Readdy writes: The “shortcut” conditions for the rank of **S** are really wrong. You cannot compute the rank of a matrix by looking at the upper left-hand square minors. For example, in Code V if you have error polynomial $E(x) = x^{11} + x^8 + x^7$, one has $E(\alpha) = 0$, and thus no errors, by the shortcut condition for rank.

# p. 450 E19 a:

Missing digit. We substituted (10110). (Margaret Readdy)

p. 487, Section 6D, E1:

(a) and (d) are, (b, (c) and (e) are not.

p. 494, line 5:

E4 (a) should be $x^4 + x^2 + 1$, and E5 (b) should be $2x^5 + 2x^3 + 2x^2 + 2$.

p. 505, E7 (b)(ii):

the answer should be $2\alpha^2 + \alpha + 2$.

Last update, June 12, 1998