AN INTRODUCTION TO
THE THEORY OF NUMBERS

Fifth Edition, First and Second Printings
by
Ivan Niven
Herbert S. Zuckerman
Hugh L. Montgomery

John Wiley (New York), 1991

ALTERATIONS FOR THE FIRST AND SECOND PRINTINGS

PAGE/LINE	
v/-15ff	The publisher no longer distributes the Solutions Manual. A lab manual and soft
v/-8	for ‘(Section 2.4)’ read ‘(Section 2.5)’
v/-7	for ‘Hansel’ read ‘Hensel’
vi/7	for ‘Appendixes’ read ‘Appendices’
vi/-4	after ‘C. Pomerance’ insert ‘J. Rickert’
vi/-3	between ‘H.’ and ‘C. Williams’ delete ‘J. Rickert’
vii/7	for ‘Bionomial’ read ‘Binomial’
1/12,13	replace ‘natural number such as’ by ‘natural number greater than 1 such as’
1/−2	replace ‘any exponent’ by ‘any integral exponent’
2/5	replace ‘natural numbers’ by ‘integers’
2/-11	for ‘135’ read ‘133’
3/−10,−11	replace ‘is a logical consequence of the first’ by ‘is logically equivalent to the first’
4/18	for ‘$\{-2,-1,0,1,2,\ldots\}$’ read ‘$\{\ldots,-2,-1,0,1,2,\ldots\}$’
6/19	for ‘$a = 248$’ read ‘$a = 428$’
18/3	between ‘of’ and ‘integers’ insert ‘two or more’.
27/2	for ‘Let $\mathcal{N}$ denote’ read ‘Let N denote’
29/-7	replace ‘an’ by ‘a positive’
29/−3	replace ‘numbers n’ by ‘numbers $n \geq 4$’
	[Thanks to Art Benjamin for pointing this out.]
33/-11	As of July, 1992, the largest prime known is M_{756839}.
52/-16	for ‘asserts’ read ‘is equivalent to the assertion’
52/-16	after ‘x’ insert ‘ $\pmod{m}$’
52/-15	after ‘a’ insert ‘ $\pmod{m}$’
52/-14	after ‘$\overline{a}$’ insert ‘ $\pmod{m}$’

NZM corrections, continued

53/4	for ‘$(p-1)\equiv -1$’ read ‘$(p-1)!\equiv -1$’
56/2	for ‘$ac+bc$’ read ‘$ad+bc$’
57/Exercise 14	replace ‘all n’ by ‘all $n\ge 0$’
72/-1	for ‘p^{α_r}’ read ‘p^{α_i}’
83/12	replace ‘Let’ by ‘Suppose that m is an odd integer >1, and let’
84/-13	for ‘reduced residues’ read ‘relatively prime to m’
86/9	for ‘***4.**’ read ‘**4.**’
86/12	for ‘***5**’ read ‘**5.**’
88/5	after ‘x^2+x+47’ insert ‘$\equiv 0$’
88/7	for ‘$a=1$’ read ‘$a\equiv 1$’
88/-17	for ‘$x^2+x+7 \pmod{81}$’ read ‘$x^2+x+7\equiv 0 \pmod{81}$’
88/-16	for ‘$x^2+x+7 \pmod{3}$’ read ‘$x^2+x+7\equiv 0 \pmod{3}$’
91/15	replace ‘$f(a)\overline{f'(a)}\equiv 1 \pmod{p^{2j}}$’ by ‘$f(a)\overline{f'(a)}\equiv 1 \pmod{p^{j}}$’
102/1	The term ‘quadratic residue’ is defined in Definition 3.1 on page 131.
107/3	insert ‘and $k>0$’
107/-12	after ‘if and only if’ insert ‘m is composite and’
108/-8	for ‘(mod m)’ read ‘(mod q)’
110/14	for ‘$x^2\equiv a \pmod{p}$’ read ‘$v^2\equiv k \pmod{p}$’
110/-2	The term ‘quadratic nonresidue’ is defined in Definition 3.1 on page 131.
114/-11	for ‘$x^2\equiv a$’ read ‘$(x-r)^2\equiv k$’
129/16	Delete the paragraph that begins ‘Before 1970,...’ and replace it by the following:

Methods for factoring numbers have developed considerably during the twentieth century. Some of the algorithms employed involve quite sophisticated mathematics, as in the case of the elliptic curve method of Hendrik Lenstra, which we discuss in Section 5.8. During the past decade, the most impressive factorizations were achieved by means of elaborations of the *quadratic sieve* method, proposed by Carl Pomerance in 1982. However, a new strategy called the *general number field sieve* is yielding good results, and offers great promise for the future. Further discussion of factoring techniques can be found in the publications of Pomerance, of Riesel, and of Bressoud, listed in the General References. For the general number field sieve one should see A. K. Lenstra and H. W. Lenstra, Jr., *The development of the number field sieve*, Lecture Notes in Math. 1554, Springer-Verlag (Berlin), 1993.

NZM corrections, continued

130/25	for ‘Corollary 2.29’ read ‘Corollary 2.30’
137/*$\mathbf{22}$.	Replace ‘$(p+1)^{1/2}$’ by ‘$p-1$’
141/Problem 18	replace ‘1111111111111’ by ‘1111118111111’ (in two places)
142/3	before ‘.’ insert ‘and that $p>2$’
153/10	insert ‘g.c.d.$(m_1, m_2) = 1$’
153/-11	for ‘if $\left(\frac{d}{p}\right) = 1$.’ read ‘if $p\|d$ or $\left(\frac{d}{p}\right) = 1$.’
153/-8	for ‘$\left(\frac{d}{p}\right) = 1$’ read ‘$\left(\frac{d}{p}\right) = 1$ or 0’ (in two places)
157/-4	Replace ‘$ax^2 + bxy + y^2$’ by ‘$ax^2 + bxy + cy^2$’
161/15	To the end of the definition append: ‘(*When $d<0$, we count* /it only the positive definite forms.)’
162/18	after ‘and only if’ insert ‘$p=2$, $p=5$, or’
162/-6	after ‘$\left(\frac{p}{5}\right) = 1$’ insert ‘or 0’
162/-3	after ‘if and only if’ insert ‘$p=5$ or’
162/-1	after ‘if and only if’ insert ‘$p=2$ or’
181/10	for ‘$-x = n-1+1-\nu$’ read ‘$-x = -n-1+1-\nu$’
182/1	Replace ‘*de Plignac’s formula.*’ by ‘(Legendre)’
189/2	after ‘$p^\beta\|n$’ add ‘, $\beta > 0$’
195/6	Replace ‘Theory’ by ‘Theorem’
195/Problem 5	Replace first ‘.’ by ‘,’
196/6	for ‘Theory’ read ‘Theorem’
197/-8	for ‘Slow’ read ‘Show’
205/Problem 14	after ‘distinct’ insert ‘and non-consecutive’
207/13	Replace ‘permits’ by ‘permutes’
219/3	after ‘solvable’ insert ‘and $b \neq 0$’
233/-9	for ‘v’ read ‘y’
237/10	Replace ‘$(-1,1),(0,1),(3,11),$’ by ‘$(-1,\pm1),(0,\pm1),(3,\pm11)$’
245//7	for ‘$b=1$’ read ‘$b=-1$’
245/7	for ‘$y=-1$’ read‘$y=1$’
249/2	after ‘$N(p) = 2p^2 - p$’ add ‘, except that $N(2) = 4$’
249/3	before ‘**8.**’ insert ‘*’
279/17	for ‘b is odd’ read ‘b is even’
293/-20	replace ‘Section 1.1’ by ‘Section 1.2’ [Thanks to Harley Flanders for pointing this out.]
302/-2	for ‘at’ read ‘a’
308/6	Replace ‘$\sqrt{5}$’ by ‘$\sqrt[3]{5}$’
318	Between Corollary 6.27 and its proof, insert the following paragraph:

NZM corrections, continued

With a small amount of calculation one can show that 33 is not the sum of five positive perfect squares, but that every integer n, $34 \le n \le 169$, is the sum of five positive squares. Hence the constant 169 in the corollary above can be replaced by 33, but not by any smaller number. [Thanks to P. T. Bateman for suggesting this.]

321/12	Wrong font: ‘$\mathbf{b}f_1 = g$’ should be ‘$\mathbf{bf}_1 = g$’
323/1	for ‘207’ read ‘210’
330/-3	for ‘$i \ge 1$’ read ‘$i > 1$’.
333/-14	for ‘$a_0 > 0$’ read ‘$a_0 \ge 0$’.
340/-15	for ‘integers x and all y’ read ‘pairs of integers x, y’
340/-14	for ‘to ξ’ read ‘h_n/k_n to ξ with $n > 0$’
344/Problem 4	replace ‘$\xi - \frac{h}{k}$’ by ‘$\lvert\xi - \frac{h}{k}\rvert$’
356/−7	replace ‘$x_2 = y_2\sqrt{d}$’ by ‘$x_2 + y_2\sqrt{d}$’
448/−1	replace ‘$q^e(n) = q^o(n)$’ by ‘$q^e(n) - q^o(n)$’
456/-7	for ‘$\sum\limits_{k=0}^{p(k)} x^k$’ read ‘$\sum\limits_{k=0}^{\infty} p(k)x^k$’
500/8	after the reference to Borevich and Shafarevich, insert the following new reference:

D. M. Bressoud, *Factorization and primality testing*, Springer-Verlag, (New York), 1989.

502/-15	before ‘Birkhäuser’ insert ‘Second Edition,’ and replace ‘1985’ by ‘1994’
502/-9, -10	replace ‘Spartan (Washington), 1962’ by ‘fourth edition, Chelsea (New York), 1993’
508/-7	after ‘Recall’ insert ‘the Remark on p. 132 and ’
512/7	for ‘3360’ read ‘3660’.
514/-17	for ‘1, 4, 7 (mod 27)’ read ‘4, 13, 22 (mod 27)’
515/7	for ‘(b) $(x+1)^2 \equiv 4$’ read ‘(b) $(x-6)^2 \equiv 4$’
515/8	for ‘(d) $(2x+1)^2 \equiv 5$’ read ‘(d) $(x-6)^2 \equiv 11$’
515/9	for ‘$x \equiv \pm 5 \pmod{19}$’ read ‘$x \equiv \pm 9 \pmod{19}$’
516/§3.1;**6.**(a)	for ‘$\pm 1, \pm 2, \pm 3 \pmod{13}$’ read ‘$\pm 1, \pm 3, \pm 4 \pmod{13}$’
518/-15	insert ‘(7, 24, 25), (24, 7, 25)’.