Errata and Addenda for
Algorithmic Number Theory
Volume I: Efficient Algorithms
by Eric Bach and Jeffrey Shallit
MIT Press, 1996

[This list last updated August 17 2014]

[This list available on the world wide web at
`http://www.math.uwaterloo.ca/~shallit/anterrata.html` .]

(Doug Tygar; November 19 1996) Page facing the title page: the author of *Realistic Compiler Generation* is Peter Lee, not Robert Lee. (Not our fault!)

(JOS; June 5 2002) Pages 1 and 13: about Goldbach's conjecture: Jean-Marc Deshouillers, Yannick Saouter and Herman te Riele (`Herman.te.Riele@cwi.nl`) have now verified Goldbach's conjecture to 10^{14}: "New experimental results concerning the Goldbach conjecture", in *Algorithmic Number Theory*, Lecture Notes in Computer Science, Vol. 1423 (1998), 204–215.

(Steven Myers; March 26 1997) Page 9: In line -4, replace "computer" with "compute".

(JOS; February 28 2005) Page 10: Replace the sentence in line 10 with: "We now know 42 Mersenne primes, the largest being $2^{25964951} - 1$, a number of 7816230 decimal digits." Similarly, on page 274, replace the "33" in line -3 with "42", and append 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, and 25964951 to the end of the list on page 275. Finally, add the following lines to the end of the table on page 309:

3 Sep 1996	$2^{1257787} - 1$	378632	Slowinski & Gage (reference TBA)
13 Nov 1996	$2^{1398269} - 1$	420921	Armengaud (reference TBA)
1 Sep 1997	$2^{2976221} - 1$	895932	Spence & Woltman (reference TBA)
27 Jan 1998	$2^{3021377} - 1$	909526	Clarkson, Woltman, Kurowski, et. al.
1 Jun 1999	$2^{6972593} - 1$	2098960	Hajratwala, Woltman, Kurowski, et al.
14 Nov 2001	$2^{13466917} - 1$	4053946	Cameron et al.
2 Dec 2003	$2^{20996011} - 1$	6320430	Shafer et al.
28 May 2004	$2^{24036583} - 1$	7235733	Findley et al.
18 Feb 2005	$2^{25964951} - 1$	7816230	Nowak et al.

For the discovery of $2^{6972593} - 1$, see G. Woltman, On the discovery of the 38th known Mersenne prime, *Fib. Quart.* **37** (1999), 367–370.

(M. Pohst; June 14 1999) Page 11: The sentence citing the paper of Hollinger and Serf should instead refer to a paper describing the SIMATH system, or Kaltofen and Grabmeier's new book on computer algebra.

(EB; October 5 2012) Page 32: The last line of the first paragraph should read, "If $(R - \{0\}, \cdot)$ forms a group, then R is called a *division ring*."

(EB; October 5 2012) Page 33: The first line of Section 2.8.3 should read "A *field* is a division ring containing at least 2 elements.".

(EB; June 17 1997) Update to Page 39: Using the Brent-McMillan algorithm and fast arithmetic, Bruno Haible and Thomas Papanikolaou computed 1 million digits of Euler's constant. [Announced on number theory net, 4/2/97; see

`http://listserv.nodak.edu/archives/nmbrthry.html`

for archives.]

(JOS; August 15 1996 & March 6 1997) Page 64: Notes to section 3.2 should also cite the following papers:

D. Zuras, More on squaring and multiplying large integers, *IEEE Trans. Comput.* **43** (1994), 899–908.

B. S. Fagin, Large integer multiplication on hypercubes, *J. Parallel Distrib. Comput.* **14** (1992), 426–430.

(Joachim von zur Gathen; October 10 1996) Page 96: Replace Cook [1985] by reference to A. Borodin, J. von zur Gathen, and J. Hopcroft, Fast parallel matrix and GCD computations, *Proc. 23rd Annual Symposium on Foundations of Computer Science*, IEEE Press, 1982, pp. 65–71.

(JOS; October 14 1997) Page 96: In line −5, replace "Theorem 4.2.2" with "Corollary 4.2.2".

(JOS; August 8 1996) Page 97: Add a citation of the paper of Peter Schreiber, A supplement to J. Shallit's paper "Origins of the analysis of the Euclidean algorithm", *Historia Math.* **22** (1995), 422–424.

(EB; June 17 1997) Page 118: In line 12, change "triangles" to "triangle".

(Yvo Desmedt; January 16 2004) Page 119: In Exercise 45, part (b), remove the word "left".

(M. Elqabbany; June 11 1998) Page 120: In exercise 47, for "Theorem 4.2.2", read "Corollary 4.2.2.".

(JOS; March 6 1997) Page 121: The citation to de Melo and Svaiter [1995] should be changed to [1996], and the reference on page 449 should be corrected to *Proc. Amer. Math. Soc.* **124** (1996), 1377–1378.

(Donald Knuth; July 1 1996) Page 122: Due to a confusion over what was a first and what was a last name, the paper attributed to Kangsheng [1988] should really be Shen [1988]. The bibliography entry on page 433 should be changed, as well as the index entry on page 499.

(EB; October 10 2000) Page 123: Add a reference to

H. Schwarz, *Elemente der Zahlen-Theorie*, H. W. Schmidt, Halle, 1855, p. 268

where Eisenstein's algorithm is discussed.

(Helmut Meyn; July 6 1999) Page 135: Replace second sentence by

For the second, note that if $n > 1$ we have

$$\sum_{d|n} \mu(d) q^{n/d} \leq q^n - q^{n/\ell} + \sum_{1 \leq i < n/\ell} q^i \leq q^n,$$

if ℓ is the smallest prime dividing n.

(Helmut Meyn; July 2 1999) Page 139: In line -8 replace max with min.

(Helmut Meyn; July 16 2001) Page 142: In line -12 eplace "v_i is monic" by "u_i is monic".

(EB; October 29 1997) Page 143: In the statement of Exercise 6 (c), delete "using can be done".

(Robert Silverman; August 1 1997) Page 150: In the notes to Section 6.4, add a reference to

R. D. Silverman, Parallel polynomial arithmetic over finite rings, *J. Parallel Distrib. Comput.* **10** (1990), 265–270.

(Joachim von zur Gathen; October 10 1996) Page 151: There is an NC algorithm to compute a (not necessarily monic) associate of the gcd in $\mathbb{F}_q[X]$. In particular, one can decide if $\gcd(f, g) = 1$ with an NC algorithm.

(EB; August 23 1996) Page 152: The following recently-published paper gives estimates for error terms in the theorem of Bilharz [1937]: F. Pappalardi and I. Shparlinski, On Artin's conjecture in function fields, *Finite Fields and their Applications* **1** (1995), 399–404.

(Klaus Huber, September 30 1997) Update to Page 159: In a finite field of order 2^m, square roots can be computed using $O(m^2)$ bit operations, as follows. Suppose that $k = \mathbb{F}_2[X]/(f)$ with f irreducible. Write $f = f_1^2 + X f_2^2$ with $\deg f_i \leq m/2$. Since f is irreducible, $f_2 \neq 0$. The square root of $a = a_1^2 + X a_2^2$ is $b = a_1 + (f_2/f_1)a_2$. See K. Huber, *Elect. Lett.* **32** (1996), 102–103.

(D. E. Knuth, June 5 1997) Page 172: Line -3 should read "a randomized...".

(EB, June 5 1997) Page 179, line -13 should read "there must be a j..." Also, in line -6, change $\log r$ to $e \log r$ in bound on q.

(EB; October 8 1996) Page 186: Line -13: Add right paren after $\varphi(n)$.

(EB; March 25 1997) Page 194, Notes to 7.1: The essential step in a Tonelli-style algorithm is to locate x in the chain

$$G_0 \subset G_1 \subset \cdots \subset G_k,$$

in the sense that $x \in G_i - G_{i-1}$. We have followed Tonelli in doing this top-down (i.e., testing $x \in G_i$ for decreasing i). The contribution of Shanks [1972] is to go bottom-up, looking for the least i for which $x \in G_i$. On average, this cuts out about half of the tests. The paper of Lindhurst [1995] was presented at the 5th meeting of the Canadian Number Theory Association and appeared in *Number Theory*, CRM Proc. Lecture Notes, 19, Amer. Math. Soc., 1999, pp. 231–242.

(EB; March 25 1997) Page 196, paragraph 4: Some of the ideas of Berlekamp's algorithm appeared in E. Prange, An algorism [sic] for factoring $X^n - 1$ over a finite field, Technical Report AFCRC-TN-59-775, Air Force Cambridge Research Center, Bedford, Mass., October 1959. In particular, Prange exhibited a basis B for the Berlekamp algebra of $\mathbb{F}_q[X]/(X^n - 1)$ and observed that the set $\{(b - \alpha)^{q-1} : b \in B,\ \alpha \in \mathbb{F}_q\}$, has enough nontrivial idempotents to factor $X^n - 1$. He used linear algebra rather than the gcd to obtain the factors. F. Montoya, J. Muñoz, and A. Peindao [A factoring algorithm in $\mathbb{F}_2[X]$, manuscript 1996] found a procedure similar to Berlekamp's, using the mapping $a \mapsto a^2 + aX$.

(Joachim von zur Gathen; Aug 13 1996) Page 197: The running time estimates in von zur Gathen and Shoup [1992a, 1992b] and Kaltofen and Shoup [1995] are incomparable. (The first is better for large q and the second better for small q.) The essential idea in these algorithms is a new way to compute the Frobenius map $x \mapsto x^q$ on $R = k[X]/(f)$. Let $\beta(X)$ denote the polynomial $X^q \bmod f$. Then if $\alpha(X)$ is any other element of R, we have $\alpha^q = \alpha(\beta(X))$.

(Joachim von zur Gathen; April 8 1997) Page 199: add reference to A. L. Chistov, Algorithm of polynomial complexity for factoring polynomials over local fields, *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR* **192** (1991) 112–148. In Russian. English translation in *J. Mathematical Sciences* **70** (1994) 1912–1933. Von zur Gathen states [personal communication] that a randomized polynomial-time algorithm for p-adic factoring results if one replaces the initial step of factoring mod p, which Chistov does deterministically, by a randomized procedure such as the Cantor-Zassenhaus algorithm.

(EB; June 17 1997) Update to Page 199: In the notes to §7.7, add: For a discussion of factoring polynomials mod p^n, see J. von zur Gathen and S. Hartleib, Factoring modular

polynomials, *Proc. ISSAC 96*, pp. 10–17. Also, on page 199, paragraph -3: add reference to J. D. Dixon, Exact solution of linear equations using P-adic expansions, *Numer. Math.* **40** (1982) 137–141.

(Eric Skaug; February 20 2005) Page 205: In line −8, delete the word "is" before "reflects".

(Dipankar Gupta; February 23 1996) Page 210: Line −3: It should read "It therefore suffices to show $\psi_1(x) \sim x^2/2$ ..."

(D. E. Knuth, June 5 1997) Page 215: in the second displayed equation, = should be $\leq$. Even better, replace the entire equation by

$$\left|\psi_1(x) - x^2/2\right| \leq \left(\frac{\log B}{\pi B} + O(1/B)\right) x^2 + O(x^{3/2}).$$

(EB; January 9 2012; JOS, August 17 2014) Theorem 8.5.7 can be now improved to 5.18 (from 11/2), based on T. Xylouris, On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions, *Acta Arith.* **150** (2011), 65–91. And in his thesis `http://bib.math.uni-bonn.de/downloads/bms/BMS-404.pdf` an Xylouris improves this to 5.00.

(EB; March 7 1997) Page 224: Line 5: should read "what these results for **the** problem of actually...".

(EB; August 22 1996 and JOS; March 12 1997) Update to Page 225: P. Ribenboim [Prime Number Records, *Nieuw Arch. v. Wiskunde* (4) **12**, 53–95] cites unpublished work of S. Weintraub, who found 863 composite numbers following the prime $p = 6505941701960039$. Ed Pegg, Jr. states on page 121 of the March 1997 issue of *College Math. J.* that there is a prime gap of size 1411 between $131 \cdot 10^{55} - 51$ and $131 \cdot 10^{55} + 1361$. Harvey Dubner (`hdubner1@compuserve.com`) and Harry Nelson have found a prime gap of size 18828; the gap ends with a prime of 607 digits.

(Victor Shoup; July 8 1999) Page 230: Line 1 should read "relatively prime to the discriminant of f".

(EB; June 17 1997) Page 232: The bound of Theorem 8.7.13 should read

$$q = O(p^{2e}(\log n + e \log p)).$$

(Change this at top of next page too.) Line -2, replace p^{p^e} by p^{ep^e}. Line -1 should read $|\Delta| N\mathbf{f} \leq p^{(1+e)p^e} n^{p^e}$.

(C. Pomerance; January 24 2000) Page 235: Theorem 8.8.18 should have been stated only for $n > 2$, since Oesterlé's estimate (used on p. 263) only applies when the nth cyclotomic field is a proper extension of Q. It is, however, true for $n = 2, x \geq 2$, and $n = 1, x \geq 2.0625$.

(B. Richmond; August 31 2003) Page 237: In the right side of the equation of exercise 4 (a), replace $\log p$ by $\log x$.

(D. E. Knuth; June 5 1997) Page 241: In exercise 29, "decideable" should read "decidable".

(EB; June 9 2004) Page 249: In the first displayed equation, li should be li_0.

(EB; January 10 1997) Page 250: the index entries corresponding to Table 8.1 (e.g., Gram, Backlund, etc.) should be corrected to read 250 instead of 249.

(EB; March 25 1997) Page 254: Bach [1995] will appear in *Math. Comp.*, October 1997.

(EB; March 25 1997) Page 255: Update Bach [1994] to E. Bach, The complexity of number-theoretic constants, *Info. Proc. Letters*, **62** (1997), 145–152.

(EB; January 9 1997) All index entries on pages 255–264 should be decreased by 1.

(JOS; March 6 1997) Page 256: The result of R. C. Baker and G. Harman appeared in *Proc. London Math. Soc.* **72** (1996), 261–280.

(Gudmund Frandsen; May 14 1997) Page 256: In the displayed formula, replace $\liminf$ with $\limsup$.

(JOS; February 4 1997) Update to Page 257, paragraph -5: The largest twin primes currently known are $242206083 \times 2^{38880} \pm 1$, found by K.-H. Indelkofer and A. Ja'rai. See the postscript to the article

Tony Forbes, A large pair of twin primes, *Math. Comp.* **66** (1997), 451–455.

(Serge Lang, September 26 1997) Page 258: The Bateman-Horn conjecture was stated incorrectly. One must exclude sets of polynomials for which $\nu(p) = p$ for some prime p.

(EB, September 30 1997) Update to Page 259: Dedekind's work is now available in English: R. Dedekind, *Theory of Algebraic Integers*, Cambridge University Press, 1996. Translation of *Sur La Théorie des Nombres Entiers Algébriques*, Gauthier-Villars, Paris, 1877. (= Bull. Sci. Math. Astron. (1), v. 1.)

(Victor Shoup; July 8 1999) Page 261: In line 2, replace Δ_K by $\mathrm{disc}(f)$.

(EB, June 5 1997) Page 262: In line 11, change $\leq$ to "O".

(John Brillhart; August 16 1996 & Donald Knuth; May 20 1997) Page 265: Line 10 should read, "Euler proved that if a number $n > 1$ with $n \equiv 1 \pmod 4$ can be written..."

(EB; February 10 1997) Pages 268–269: It should be stated that the Fellows-Koblitz algorithm works for odd $n > 3$. This is because Theorem 8.8.11 on page 234, used in the proof of Theorem 9.1.3, is valid only for $x \geq 4$.

(Troy Vasiga; March 28 2000) Page 274: In line 11, "section 6.6.5" should read "section 6.5". Also, replace "$f(x)$" on line 10 with "$f(X)$".

(EB; December 31 1997) Page 282: In line 15, change "If $j \geq 2$" to "If $j = 2$".

(EB; June 5 1997) Page 292: In line 9, change "Lemma" to "Theorem".

(EB; October 22 1996) Page 296: Line 5: Remove the word "consecutively".

(M. Balazard; March 22 2002) Page 308: In exercise 50 (a), remove the word "composite".

(JOS; September 3 1997) Page 310: The discussion of odd perfect numbers is misplaced; it should appear under the notes to Section 9.2. Furthermore, the the technical report of Brent, Cohen, and te Riele [1989] has now appeared, and should be replaced here and on page 399 by

> R. P. Brent, G. L. Cohen and H. J. J. te Riele, Improved techniques for lower bounds for odd perfect numbers. *Math. Comp.* **57** (1991), 857–868.

(JOS; August 1 2000) Page 314: The notes to section 9.4 should cite the following paper:

> M. M. Artjuhov, Certain criteria for the primality of numbers connected with the little Fermat theorem, *Acta Arith.* **12** (1967), 355–364

which anticipates the analysis of Solovay-Strassen and Lehmer.

(Dave Hamm; April 12 1996) Page 315: The reference Alford, Granville, and Pomerance [1994b] is cited on this page, but is missing on page 390. It should be:

> W. R. Alford, A. Granville, and C. Pomerance, On the difficulty of finding reliable witnesses, in *Algorithmic Number Theory, 1st International Symposium, ANTS-I*, L. M. Adleman and M.-D. Huang, eds., Lect. Notes in Comp. Sci. Vol. 877, Springer-Verlag, 1994, pp. 291–322.

(JOS; March 6 1997) Page 318: Add the following references to the list of papers on computationally useless formulas for primes:

> S. Kahan, On the smallest prime greater than a given positive integer, *Math. Mag.* **47** (1974), 91–93;
>
> S. Weintraub, On an Nth prime formula, *J. Recreational Math.* **27** (1995), 252–254.

(EB; September 22 1996) Page 322: In exercise 24, at the bottom of the page, change $O(1/c)$ to $O(1/x)$ (two times).

(EB; August 23 1996) Page 326: Solution to Exercise 3.4: add reference to B. Balasubramanian and S. V. Nagaraj, Perfect power testing, *Info. Proc. Lett.* **58** (1996), 59–63.

(Lars Hesel Christensen; October 29 2003) Page 326: Solution to Exercise 3.12: The sample encoding should read 000101110100.

(JOS; August 9 1996) Page 329: In exercise 30, change the first period in the last line to a comma.

(Peter Caven; July 10 2004) Page 336: In the algorithm Power2, change the second while loop to read "while $f \geq 1$".

(Ian Skoch; May 3 2014) Page 337: in the solution to exercise 5.6, the 2nd row of the matrix M should be [0 1].

(JOS; March 5 1997) Page 340: In the solution to exercise 5.22, add a reference to Solomon Golomb's Problem 10311, *Amer. Math. Monthly* **100** (1993), 499, and solution in **104** (1997), 71–72.

(EB; October 25 2002) Page 350: The reference to algorithms for constructing normal bases should be to exercise 24 of *Chapter 7*.

(EB; September 30 1997) Update to Page 351: Add the following reference on normal bases. M. Wang and I. F. Blake, Normal Basis of the Finite Field $F_{2^{(p-1)p^m}}$ over $\mathbb{F}_2$, *IEEE Trans. Info. Theory* **43**, 1997, 737–739.

(EB; February 20 1997) Page 355: In exercise 7.17, the two big-O expressions are missing a left parenthesis.

(EB; October 14 1996) Page 370: Line 7, delete "is increased".

(EB; June 18 1997) Page 372: Line 15, replace "The first result follows" with "The second result follows"

(EB; August 7 1996) Page 376: in the solution to exercise 8.46, the p in the last summation should be in italic, not bold.

(JOS; April 7 1997) Pages 381–382: in the solution to exercise 9.24, also refer to Lucas [1876b] and [1878a, pp. 230–231].

(Jud McCranie; January 3 1997) Page 382: in the solution to exercise 9.33, the 3rd to last line of the algorithm Segment2 should read "for $i \leftarrow 1$ to Δ do".

(D. G. Malm; June 25 1998) Page 390: The volume number for Alford, Granville, and Pomerance [1994a] is incorrect. It should be 139.

(J. von zur Gathen; August 13 1996) Page 391: in reference [Artin and Schreier 1927], replace "Kennseichnung" with "Kennzeichnung".

(J. von zur Gathen; October 11 1996) Page 393: replace "teilerfremnd" with "teilerfremd" in Backlund [1929].

(JOS; August 8 1996) Page 394: remove third-from-last comma in line 2 of reference Bassalygo [1978].

[EB, June 30 1997] Page 395: Berlekamp [1972] is in *Congr. Numer.* VI, not VII.

(EB; August 23 1996) Page 401: Buchmann and Shoup [1991] has now appeared in journal form: J. Buchmann and V. Shoup, Constructing nonresidues in finite fields and the extended Riemann hypothesis, *Math. Comp.* **65** (1996), 1311–1326.

(JOS; August 14 1996) Page 409: the page numbers in [Curtze 1899] should be 257–306, and the citation on page 308 should be revised to read Curtze [1899, pp. 288–289].

(JOS; September 19 1996) Pages 409–410: Reorder the references involving Damgård so they are in the correct order. Also, the year cited in Damgård and Landrock [1993] should be 1993, not 1991.

(Helmut Meyn; August 26 1999) Page 413: Replace "Dornsetter" with "Dornstetter".

(J. von zur Gathen; October 11 1996) Page 421: remove semicolon in title of Gauss [1876].

(G. Frandsen; December 1 1997) Page 428: the reference Hensel [1888] has incorrect page numbers; the correct ones are 230–237.

(JOS; December 31 1997) Page 436: the reference Konyagin and Pomerance [1994] has now appeared:

> S. Konyagin and C. Pomerance, On primes recognizable in deterministic polynomial time, in R. L. Graham and J. Nešetřil, eds., *The Mathematics of Paul Erdős*, Springer-Verlag, 1997, pp. 176–198.

(JOS; April 7 1997) Page 445: In the reference Lucas [1878a], correct the page numbers to read "184–240; 289–321".

(EB; August 7 1996) Page 447: in reference [von Mangoldt 1905], the word "verteilung" should be capitalized.

(EB; June 13 1997) Page 447: page numbers for Massey [1969] should be 122–127.

(EB; June 30 1997) Page 469: H. Williams [1972] is in *Congr. Numer.* VI, not VII.

(Donald E. Knuth, June 25 1997) Page 469: Shanks [1972] was published in the Second Manitoba Conference on Numerical Mathematics.

(J. von zur Gathen; October 11 1996) Page 463: replace "Gessammelte" with "Gesammelte" and "Grosse" with "Grösse" in Riemann [1860].

(EB; October 29 1997) Page 472: In references Sispánov [1941, 1942], add accents to the journal name: *Boletín Matemático*.

(JOS; August 7 1996) Page 486: in reference [Zheng 1994], the initials and names of Yao and Knuth should be capitalized.

(EB; January 9 1997) Page 487: in the Index to Notation, Jacobsthal's function is mentioned on page 257, not page 258.

(J. von zur Gathen; October 11 1996) Page 500: Index entry to Lehman at the bottom of the page should read "2, 13, 250" in place of "2, 13, 249".

(EB; January 9 1997) Page 504: the last index entry for p-adic numbers should read "199, 261" in place of "199–262".

(Jud McCranie; July 11 1998) Pages 505–506: some of the index entries for prime numbers are messed up. For example, consolidate the entries "in an arithmetic progression" and "in arithmetic progressions"; move the entry under "primes, explicit estimates for functions of" to under "prime numbers", and add index entries for "primes, sum of"; "primes, product of", and "primes, largest known throughout history"; "prime ideals", "density" and "density of".