Update # 4 to *Factorizations of* $b^n \pm 1$

Samuel S. Wagstaff, Jr.

The following tables present the updates made to *Factorizations of* $b^n \pm 1$ from October 23, 1982, when the book went to press, to July 3, 1986. All new factorizations reported in earlier updates are included in Update # 4. Earlier updates may be discarded. This update reports a total of 1812 factorizations.

Date	Update	Number of New Factorizations
July 20, 1983	1	244
August 27, 1984	2	296
June 30, 1985	3	196
July 3, 1986	4	1076

We show the lines which have been changed in each main table. Next we list the new primes and probable primes added to Appendix A. As we will explain later, Appendix B no longer will be updated. However, we do repeat the additions to Appendix B which appeared in Update # 1. All of the numbers listed in the original Appendix C have been factored. In fact, the smallest composite cofactors in the updated tables have 71 digits. We list the composites of 71 to 88 digits as the new Appendix C. We have not updated the short tables; the new factors of $2^{211} - 1$, $2^{212} + 1$, $2^{224} + 1$, $10^{67} - 1$, $10^{71} - 1$, $10^{79} - 1$ and $10^{64} + 1$ may be found easily in the updated lines for the main tables and in Appendix A.

The "Introduction to the Main Tables" describes developments in three areas—technology, factorization and primality testing—which contributed to the tables. Further progress in each of these areas has been achieved since the book was published [13, 24, 30, 31, 37, 40], although some of this progress does not relate directly to progress in these tables.

1. Technology. The factoring group at Sandia National Laboratories [11, 12, 13] has used the quadratic sieve factoring method on a Cray-1 computer and a Cray XMP computer to obtain the original Ten "Most Wanted" Factorizations. Wunderlich [41, 42] is programming the continued fraction factoring method on various parallel processors. te Riele has programmed the quadratic sieve algorithm on a Cyber 205.

Smith and Wagstaff [28, 35, 37] have built a special processor, the Extended Precision Operand Computer, to factor numbers with the continued fraction method. This machine has a 128-bit word length and several remaindering units to perform the trial division quickly. Dubner and Dubner [14] have built a special computer which rapidly performs arithmetic with large integers. They use it for various number-theoretic calculations, including factoring large numbers and seeking large primes of special form. A group at LSU [32] is building a 256-bit processor for the CPS [7, 33] factoring method. Pomerance, Smith and Tuler [27] are building a special machine for factoring by the quadratic sieve algorithm.

Silverman [34] has factored many large numbers using the quadratic sieve algorithm running on a star network of SUN microcomputers. Each SUN sieves a different interval and reports its results to the central machine, which determines when it has enough information to factor the number. No doubt the use of supercomputers and networks of microcomputers for factoring will continue, as will the construction of special processors for factoring.

2. Factorization algorithms. See [4, 6] for Brent's variation of Pollard's Monte Carlo factorization method. See [25, 28, 29] for the "early abort strategy," which accelerates the continued fraction algorithm. See [39] for the $p + 1$ analog of the Pollard $p - 1$ method (cf. p. xlii). Baillie has completed a factor search of all the composite numbers in the project using the $p - 1$ method with high limits. Montgomery has found ways to accelerate the Pollard methods [21] and, at a more basic level, modular multiplication [20].

The quadratic sieve factoring method developed by C. Pomerance [25, 26] was mentioned on page lviii of the "Introduction." It was used [15] to factor only one number whose factors appear in the book. The Sandia group [11, 12, 13] has used the method to factor more than a dozen numbers reported in this update. In the past year Silverman [34] has factored hundreds of numbers with this method. Recently, Niebuhr and te Riele have also used it. The time-consuming elimination step limits the size of the factor base in the quadratic sieve (and some other) factoring methods. Several researchers [23, 38] have suggested techniques for speeding up this step.

C. P. Schnorr and H. W. Lenstra, Jr. have invented a new factoring method [33] called the CPS method. It did not produce any factorization reported in this update. See also [7]. Two other new factoring algorithms, the residue list sieve [10] and the cubic sieve [10, 22] have not produced any result in this update.

H. W. Lenstra, Jr. has invented another new factoring algorithm, called the elliptic curve method. At this writing it has been described only in preprints and technical reports [19, 2, 5, 8, 21, 37]. Montgomery and Silverman each have used it to factor hundreds of numbers reported in this update.

3. Primality testing algorithms. Thanks to the efforts [1, 9] of L. M. Adleman, C. Pomerance, R. S. Rumely, H. Cohen and H. W. Lenstra, Jr. we can now test a 200-digit number for primality in a reasonable time. A. K. Lenstra and A. Odlyzko have proved primality of all PRP's in Appendix A (both old and update PRP's) up to 212 digits as well as some larger ones. Several authors [3, 8, 16] have invented primality tests which use elliptic curves. Atkin has implemented a practical primality test based on elliptic curves and has used it to prove the primality of several cofactors of between 212 and 343 digits. As a result of all this work, only 36 PRP's lack rigorous primality proofs. I hope someone finishes these primality proofs soon. The new techniques do not produce summaries like those in Appendix B. Thus, although the proofs have been done, there is nothing to add to Appendix B. In the tables below, we have not listed lines whose only update is the change of "PRP" to "P".

4. Status of the project and of important factorizations. All of the Ten "Most Wanted" Factorizations on page lviii and the Fifteen "More Wanted" Factorizations on page lix have been done. New "Wanted" lists were prepared for Updates # 2 and 3. Of the numbers on those two lists, only 2,512+ and 5,128+ remain unsplit. The other numbers on those lists, the original "Wanted" numbers and many numbers on other "Wanted" lists issued between updates were factored by Atkin and Rickert, Davis and Holdridge, Montgomery, Niebuhr, Silverman, te Riele and Wagstaff. Here are the current "Most" and "More Wanted" lists:

Ten "Most Wanted" Factorizations

1.	2,512+	C148	6.	10,97−	C89
2.	5,128+	C87	7.	10,97+	C96
3.	7,128+	C95	8.	3,178+	C84
4.	2,311−	C87	9.	12,89+	C92
5.	10,94+	C88	10.	11,97+	C97

Twenty-Four "More Wanted" Factorizations

2,349−	C93	3,194+	C89	7,127−	C99	11,101−	C105
2,634L	C95	3,256+	C111	7,104+	C82	11,107−	C96
2,332+	C95	5,139−	C84	7,116+	C82	11,109−	C113
2,1024+	C291	5,146+	C83	10,101−	C101	11,104+	C100
3,199−	C86	6,131−	C92	10,106+	C95	11,128+	C118
3,181+	C82	6,121+	C83	10,109+	C93	12,92+	C87

All of the original Mersenne numbers $M_p = 2^p - 1$, $p \le 257$, have now been factored completely. D. Slowinski found two more Mersenne primes, namely, M_{132049} and M_{216091}.

Several more prime factors of Fermat numbers have been discovered. The new factors $k \cdot 2^n + 1$ of $F_m = 2^{2^m} + 1$ are listed in the following table. G. B. Gostin found the factors of F_m for $m =$ 25, 27, 61, 64, 75, 122, 142 and 906. H. Suyama found the factor of F_{2089} and W. Keller found the other nine. We are grateful to the discoverers for their permission to list the factors here. See [17, 18, 36] for some of the factors.

k	n	m	k	n	m
1522849979	27	25	22347	279	275
430816215	29	27	27609	341	334
21626655	54	52	120845	401	398
54985063	66	61	38039	419	416
17853639	67	64	11969	643	637
3447431	77	75	57063	908	906
5234775	124	122	431	2099	2089
8152599	145	142	9	9431	9428
232905	207	205	5	23473	23471

If you factor any numbers in the tables, please send the factors to:

Professor Samuel S. Wagstaff, Jr.
Department of Computer Sciences
Purdue University
West Lafayette, IN 47907 USA.

They will be checked and included in the next update. The factors reported in this update were discovered by ("&" connects members of one team) A. O. L. Atkin & N. W. Rickert, R. J. Baillie, R. P. Brent, J. A. Davis & D. B. Holdridge, H. Dubner, P. L. Montgomery, W. Niebuhr, R. Silverman, J. W. Smith & S. S. Wagstaff, Jr., H. Suyama, H. J. J. te Riele and S. S. Wagstaff, Jr. The program which checked the factors and inserted them into the tables was written by Jonathan W. Tanner. We are grateful to those who sent new factors and to the computer centers where their work was done.

Several typographical errors were corrected in the second printing of the book. We list the changes here for those who have the first printing. We thank those who reported errors to us.

Page	Line	Correction
xli	−16	Change "Rick" to "Rich".
xlii	5	Change "CDC 7600" to "CDC 6500".
xliii	−13	Change "*N*" to "an odd number *N*".
lii	−2	Change "by an asterisk." to "by an asterisk, except when $p = n = 2$."
liii	3	Change "just once." to "just once, if $m > 2$."
lvii	−5	Change "probably prime" to "probable prime".
lx	4	Prepend another "1" to k of the second factor of F_7. That k should be 11141971095088142685.
62	"399"	Change "(1,7,17,133)" to "(1,7,19,133)".
98	"209"	Change "(1,3,7,21)" to "(1,19)".
107	8	Change "label P or PRP" to "label, P or PRP".

The Computer Museum mentioned on page lviii has moved from Marlboro, Mass., to 300 Congress Street, Boston, Mass. 02210.

REFERENCES

1. L. M. Adleman, Carl Pomerance and R. S. Rumely, "On distinguishing prime numbers from composite numbers," *Ann. of Math.*, 117 (1983), 173-206.

2. Eric Bach, "Lenstra's algorithm for factoring with elliptic curves, Exposé," Computer Sciences Department, University of Wisconsin, Madison, February, 1985.

3. W. Bosma, "Primality testing using elliptic curves," Report 85-12, Mathematisch Instituut, Universiteit van Amsterdam, 1985.

4. R. P. Brent, "An improved Monte Carlo factorization algorithm," *BIT*, 20 (1980), 176-184.

5. R. P. Brent, "Some integer factorization algorithms using elliptic curves," Research report CMA-R32-85, The Australian National University, Canberra, September, 1985.

6. R. P. Brent and J. M. Pollard, "Factorization of the eighth Fermat number," *Math. Comp.*, 36 (1981), 627-630.

7. Duncan A. Buell, "The expectation of success using a Monte Carlo factoring method—some statistics on quadratic class numbers," *Math. Comp.*, 43 (1984), 313-327.

8. D. V. Chudnovsky and G. V. Chudnovsky, "Sequences of numbers generated by addition in formal groups and new primality and factorization tests," Research report RC 11262 (#50739), IBM Research Center, Yorktown Heights, July, 1985.

9. H. Cohen and H. W. Lenstra, Jr., "Primality testing and Jacobi sums," *Math. Comp.*, 42 (1984), 297-330.

10. D. Coppersmith, A. M. Odlyzko and R. Schroeppel, "Discrete logarithms in $\mathbf{GF}(p)$," *Algorithmica*, 1 (1986), 1-15.

11. J. A. Davis and D. B. Holdridge, "Factorization using the quadratic sieve algorithm," in *Advances in Cryptology, Proceedings of Crypto* 83, David Chaum, ed., Plenum Press, New York (1984), 103-113.

12. J. A. Davis and D. B. Holdridge, "Most wanted factorizations using the quadratic sieve," Sandia National Laboratories Report SAND 84-1658, August, 1984.

13. J. A. Davis, D. B. Holdridge and G. J. Simmons, "Status report on factoring (at the Sandia National Labs)," in *Advances in Cryptology*, *Proceedings of EUROCRYPT* 84, T. Beth, N. Cot and I. Ingemarsson, eds., Springer-Verlag Lecture Notes in Computer Science v. 209 (1985),183-215.

14. H. Dubner and R. Dubner, "The development of a powerful, low-cost computer for number theory applications," *J. Rec. Math.*, 18 (1986), 81-86.

15. J. L. Gerver, "Factoring large numbers with a quadratic sieve," *Math. Comp.*, 41 (1983), 287-294.

16. S. Goldwasser and J. Kilian, "A provably correct and probably fast primality test," preprint, M. I. T., December, 1985; Proc. Eighteenth Annual ACM Symp. on the Theory of Computing (STOC), Berkeley, May 28-30, 1986.

17. G. B. Gostin and P. B. McLaughlin, "Six new factors of Fermat numbers," *Math. Comp.*, 38 (1982), 645-649.

18. Wilfrid Keller, "Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$," *Math. Comp.*, 41 (1983), 661-673.

19. H. W. Lenstra, Jr., "Factoring integers with elliptic curves," preprint, May, 1986.

20. Peter L. Montgomery, "Modular multiplication without trial division," *Math. Comp*., 44 (1985), 519-521.

21. Peter L. Montgomery, "Speeding the Pollard methods of factorization," preprint, December, 1985.

22. A. M. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance," in *Advances in Cryptology*, *Proceedings of EUROCRYPT* 84, T. Beth, N. Cot and I. Ingemarsson, eds., Springer-Verlag Lecture Notes in Computer Science v. 209 (1985), 224-314.

23. D. Parkinson and M. Wunderlich, "A compact algorithm for Gaussian elimination over $\mathbf{GF}(2)$ implemented on highly parallel computers," *Parallel Computing*, 1 (1984), 65-73.

24. Carl Pomerance, "Recent developments in primality testing," *Math. Intelligencer*, 3 (1981), 97-105.

25. Carl Pomerance, "Analysis and comparison of some integer factoring algorithms," in *Computational Methods in Number Theory*, Part 1, H. W. Lenstra, Jr. and R. Tijdeman, eds., Math. Centrum Tract 154, Amsterdam (1982), 89-139.

26. Carl Pomerance, "The quadratic sieve factoring algorithm," in *Advances in Cryptology*, *Proceedings of EUROCRYPT* 84, T. Beth, N. Cot and I. Ingemarsson, eds., Springer-Verlag Lecture Notes in Computer Science v. 209 (1985), 169-182.

27. Carl Pomerance, J. W. Smith and Randy Tuler, "A pipe-line architecture for factoring large integers with the quadratic sieve algorithm," preprint, December, 1985.

28. Carl Pomerance, J. W. Smith and S. S. Wagstaff, Jr., "New ideas for factoring large integers," in *Advances in Cryptology, Proceedings of Crypto* 83, David Chaum, ed., Plenum Press, New York (1984), 81-85.

29. Carl Pomerance and S. S. Wagstaff, Jr., "Implementation of the continued fraction integer factoring algorithm," *Congressus Numerantium*, 37 (1983), 99-118.

30. Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.

31. Hans Riesel, "Modern factorization methods," *BIT*, 25 (1985), 205-222.

32. W. G. Rudd, Duncan A. Buell and Donald M. Chiarulli, "A high performance factoring machine," *Proceedings of the Eleventh International Symposium on Computer Architecture*, 1984.

33. C. P. Schnorr and H. W. Lenstra, Jr., "A Monte Carlo factoring algorithm with linear storage," *Math. Comp.*, 43 (1984), 289-311.

34. Robert D. Silverman, "The multiple polynomial quadratic sieve," preprint, August, 1985.

35. J. W. Smith and S. S. Wagstaff, Jr., "An extended precision operand computer," *Proceedings of the Twenty-First Southeast Region ACM Conference*, (1983), 209-216.

36. Hiromi Suyama, "Searching for prime factors of Fermat numbers with a microcomputer," *bit*, 13 (1981), 240-245 (in Japanese).

37. S. S. Wagstaff, Jr. and J. W. Smith, "Methods of factoring large integers," Report CSD-TR-585, Department of Computer Sciences, Purdue University, March, 1986.

38. D. Wiedemann, "Solving sparse linear equations over finite fields," *IEEE Trans. Info. Theory*, 32 (1986), 54-61.

39. H. C. Williams, "A $p + 1$ method of factoring," *Math. Comp.*, 39 (1982), 225-234.

40. H. C. Williams, "An overview of factoring," in *Advances in Cryptology, Proceedings of Crypto* 83, David Chaum, ed., Plenum Press, New York (1984), 71-80.

41. Marvin C. Wunderlich, "Factoring numbers on the Massively Parallel Computer," in *Advances in Cryptology, Proceedings of Crypto* 83, David Chaum, ed., Plenum Press, New York (1984), 87-102.

42. Marvin C. Wunderlich, "Implementing the continued fraction factoring algorithm on parallel machines," *Math. Comp.*, 44 (1985), 251-260.