Update # 5 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 first edition went to press, to June 21, 1987, the cut-off date for the second edition. All new factorizations reported in earlier updates are included in Update # 5. Earlier updates may be discarded. If you have the second edition of the book, you do not need this update. But if you have the first edition, you should keep this update *and* the most recent later update (2.1 or 2.2 or 2.3, etc.) This update reports a total of 2045 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
June 21, 1987	5	233

The tables below contain 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 some 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 80 digits. The composites of 80 to 100 digits are listed 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. There has been enormous progress [14, 26, 32, 33, 41, 44] in each of these areas since the first edition was published, although some of this progress does not relate directly to progress in these tables.

1. Advances in Technology. The factoring group at Sandia National Laboratories [12, 13, 14] 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 [46, 47, 48] has programmed the continued fraction factoring method on various parallel processors. te Riele has programmed the quadratic sieve algorithm on a Cyber 205. Young and Buell [49] used a Cray-2 to determine that the twentieth Fermat number is composite. They checked this calculation with a Cray XMP.

Smith and Wagstaff [30, 39, 41] 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 [15] 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. Rudd, Buell and Chiarulli [34] are building a 256-bit processor for the CPS [7, 36] factoring method. Pomerance, Smith and Tuler [29] are building a special machine for factoring by the quadratic sieve algorithm.

Silverman [37, 38] 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. Advances in Factorization Algorithms. See [4, 6] for Brent's variation of Pollard's Monte Carlo factorization method. See [27, 30, 31] for the "early abort strategy," which accelerates the continued fraction algorithm. Williams and Wunderlich [46] describe the changes in the continued fraction algorithm needed to make it run efficiently on a parallel computer. See [43] for the $p + 1$ analogue of the Pollard $p - 1$ method (cf. p. xlii). (Page references are to the first edition, of course.) Baillie has completed a factor search of all the composite numbers in the project using the $p - 1$ method with limits 200000 for Step 1 and 10200000 for Step 2. Montgomery has found ways to accelerate the Pollard and elliptic curve methods [23] and modular multiplication [22].

The quadratic sieve factoring method of Pomerance [27, 28] was mentioned on page lviii of the "Introduction." It was used [16] to split only one number whose factors appear in the first edition. The Sandia group [12, 13, 14] has used the method to factor more than a dozen numbers reported in this update. Silverman [37, 38] has factored hundreds of numbers with this method. Niebuhr, te Riele and Wagstaff 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 [25, 42] have suggested techniques for speeding up this step.

C. P. Schnorr and H. W. Lenstra, Jr. have invented a new factoring method [36] 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 [11] and the cubic sieve [11, 24] have not produced any result in this update. In fact, to our knowledge, these methods have never been programmed.

H. W. Lenstra, Jr. has invented another new factoring algorithm, called the elliptic curve method. See [21, 2, 5, 8, 23, 41]. Montgomery and Silverman each have used it to factor hundreds of numbers reported in this update. Brent, Kida, Suyama and Wagstaff have used it, too. Most of the tables have been searched by the two-step elliptic curve method with several curves and bounds ranging from 200000 and 10000000 for small numbers (80-100 digits) to 50000 and 2500000 for large numbers (300-360 digits).

3. Advances in Primality Testing Algorithms. Thanks to the efforts [1, 9, 10, 35] of L. M. Adleman, C. Pomerance, R. S. Rumely, H. Cohen, H. W. Lenstra, Jr. and A. K. Lenstra we can now test a 200-digit number for primality in a reasonable time. A. K. Lenstra and A. M. Odlyzko have proved primality of all PRP's in Appendix A (both old and update PRP's) up to 210 digits as well as some larger ones. Several authors [3, 8, 17] 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 the following 35 PRP's lack rigorous primality proofs:

2,1958M	PRP222	2,2290L	PRP264	2,2338M	PRP284	2,1093+	PRP315
2,1594M	PRP228	2,1858M	PRP265	2,1096+	PRP284	2,2314L	PRP315
2,1874M	PRP228	2,2054M	PRP266	2,2102M	PRP286	2,1117+	PRP319
2,808+	PRP236	2,1169–	PRP268	2,1049–	PRP288	2,1112+	PRP321
2,979–	PRP237	2,1966L	PRP268	2,2126L	PRP294	2,2234M	PRP324
2,883+	PRP237	2,2198M	PRP271	2,2122L	PRP296	2,2342L	PRP327
2,1886L	PRP237	2,1906L	PRP277	2,1061+	PRP301	2,2258L	PRP332
2,844+	PRP245	2,1934L	PRP279	2,2242M	PRP307	2,2374M	PRP334
2,911+	PRP260	2,2134L	PRP284	2,1189+	PRP312		

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, 3 and 4. Many 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, Kida, 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.	2,353+	C106
2.	7,128+	C95	7.	2,349−	C93
3.	12,89+	C92	8.	10,101−	C101
4.	11,97+	C97	9.	10,106+	C95
5.	2,332+	C95	10.	6,131−	C92

Twenty-One "More Wanted" Factorizations

2,311−	C87	5,160+	C90	10,109+	C93
2,353−	C101	6,137+	C99	11,107−	C96
2,674M	C87	7,137−	C101	11,104+	C100
2,1024+	C291	7,121+	C89	11,128+	C118
3,199−	C86	7,122+	C87	12,92+	C87
3,194+	C89	10,97−	C89	12,104+	C89
5,157−	C89	10,94+	C88	12,106+	C99

All of the original Mersenne numbers $M_p = 2^p - 1$, $p \le 257$, have been factored completely. Haworth [19] has determined that the only Mersenne primes M_p with $p < 100000$ are the 28 primes listed on page lix. D. Slowinski found two more Mersenne primes, namely, M_{132049} and M_{216091}.

After years of effort, Williams and Dubner [45] have proved that the repunit R_{1031} is prime.

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. W. Keller found the factors of F_m for $m =$ 52, 205, 275, 334, 398, 416, 637, 9428 and 23471. R. J. Baillie found the fifth factor of F_{12}, H. Suyama found the factor of F_{2089} and G. B. Gostin found the other fifteen. We are grateful to the discoverers for their permission to list the factors here. See [18, 20, 40] for some of the factors. Recently, Young and Buell [49] used Pépin's test to prove that F_{20} is composite. Baillie has checked that the cofactors of F_{12} (the new one), F_{15} and F_{16} are composite.

k	n	m	k	n	m
76668221077	14	12	733251	377	375
1522849979	27	25	810373	378	376
430816215	29	27	120845	401	398
21626655	54	52	38039	419	416
54985063	66	61	77377	550	547
17853639	67	64	11969	643	637
76432329	74	72	57063	908	906
3447431	77	75	25835	1125	1123
5234775	124	122	13143	1454	1451
8152599	145	142	431	2099	2089
232905	207	205	501	3508	3506
22347	279	275	9	9431	9428
27609	341	334	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, G. B. Gostin, Y. Kida, 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. Although H. W. Lenstra, Jr. and Carl Pomerance sent us no new factors, they contributed exciting new ideas used by many of those mentioned above. We are in their debt, too.

Several typographical errors were corrected in the second printing (1985) of the book. We list the changes here for those who have the first printing (1983). 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. At this writing, D. H. Lehmer's sieves are in storage and temporarily not on display. Ask the Museum staff if you want to see them.

An error discovered since the second printing of the first edition was that the composite number 1223165341640099735851 was listed as a prime factor of $6^{175} - 1$. Atkin noticed that this number is 34840572551.35107498301. The correct entry for this number is given on page 28 of this update.

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. H. Cohen and A. K. Lenstra, "Implementation of a new primality test," *Math. Comp.*, 48 (1987), 103-121.

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

12. 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.

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

14. 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.

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

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

17. S. Goldwasser and J. Kilian, "A provably correct and probably fast primality test," Proc. Eighteenth Annual ACM Symp. on the Theory of Computing (STOC), Berkeley, May 28-30, 1986.

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

19. G. McC. Haworth, "Primality testing Mersenne numbers (II)," Abstract 86T-11-57, *Abstr. Amer. Math. Soc*. 7 (1986), 224-225.

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

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

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

23. Peter L. Montgomery, "Speeding the Pollard and elliptic curve methods of factorization," *Math. Comp*., 48 (1987), 243-264.

24. 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.

25. 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.

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

27. 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.

28. 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.

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

30. 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.

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

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

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

34. 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.

35. Robert Rumely, "Recent advances in primality testing," *Notic. Amer. Math. Soc*. 30 (1983), 475-477.

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

37. Robert D. Silverman, "The multiple polynomial quadratic sieve," *Math. Comp*., 48 (1987), 329-339.

38. Robert D. Silverman, "Parallel implementation of the quadratic sieve," to appear in the *Journal of Supercomputing*.

39. 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.

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

41. S. S. Wagstaff, Jr. and J. W. Smith, "Methods of factoring large integers," in *Number Theory, New York, 1984-85*, D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn and M. B. Nathanson, eds. Springer-Verlag Lecture Notes in Mathematics, v. 1240 (1987), 281-303.

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

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

44. 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.

45. H. C. Williams and Harvey Dubner, "The primality of R1031," *Math. Comp*., 47 (1986), 703-711.

46. H. C. Williams and M. C. Wunderlich, "On the parallel generation of the residues for the continued fraction factoring algorithm," *Math. Comp*. 48 (1987), 405-423.

47. 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.

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

49. Jeff Young and Duncan A. Buell, "The twentieth Fermat number is composite," to appear in *Math. Comp*.