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.

<table>
<thead>
<tr>
<th>Date</th>
<th>Update</th>
<th>Number of New Factorizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 20, 1983</td>
<td>1</td>
<td>244</td>
</tr>
<tr>
<td>August 27, 1984</td>
<td>2</td>
<td>296</td>
</tr>
<tr>
<td>June 30, 1985</td>
<td>3</td>
<td>196</td>
</tr>
<tr>
<td>July 3, 1986</td>
<td>4</td>
<td>1076</td>
</tr>
</tbody>
</table>

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, 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. The Rieles have 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. xliii). 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 factoried 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 \( M_p = 2^p - 1, \ p \leq 257 \), 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 \( k2^n + 1 \) 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.

<table>
<thead>
<tr>
<th>( k )</th>
<th>( n )</th>
<th>( m )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1522849979</td>
<td>27</td>
<td>25</td>
</tr>
<tr>
<td>430816215</td>
<td>29</td>
<td>27</td>
</tr>
<tr>
<td>21626655</td>
<td>54</td>
<td>52</td>
</tr>
<tr>
<td>54985063</td>
<td>66</td>
<td>61</td>
</tr>
<tr>
<td>17853639</td>
<td>67</td>
<td>64</td>
</tr>
<tr>
<td>3447431</td>
<td>77</td>
<td>75</td>
</tr>
<tr>
<td>5234775</td>
<td>124</td>
<td>122</td>
</tr>
<tr>
<td>8152599</td>
<td>145</td>
<td>142</td>
</tr>
<tr>
<td>232905</td>
<td>207</td>
<td>205</td>
</tr>
</tbody>
</table>

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 3  Change "N" to "an odd number \( N \)".
livii 2  Change "by an asterisk." to "by an asterisk, except when \( p = n = 2 \)."
liviii  3  Change "just once." to "just once, if \( m > 2 \)."
lxii 5  Change "probably prime" to "probable prime".

That \( k \) should be 11141971095088142685.

62 "399" Change "(1,7,17,133)" to "(1,17,19,133)".
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


