Update 1 to Factorizations of $a^n \pm 1$, $13 \le a < 100$

Richard P. Brent
Computer Sciences Laboratory
Australian National University
Canberra, ACT 0200, Australia
rpb@cslab.anu.edu.au

Peter L. Montgomery
CWI, Kruislaan 413
1098 SJ Amsterdam
The Netherlands
pmontgom@cwi.nl

and

Herman J. J. te Riele
CWI, Kruislaan 413
1098 SJ Amsterdam
The Netherlands
herman@cwi.nl

with the assistance of

Henk Boender, Thomas Denny, Harvey Dubner,
Marije Huizing, Wilfrid Keller, Arjen Lenstra,
Robert Silverman, Thomas Sosnowski,
and Samuel Wagstaff, Jr.

September 1994

Abstract

In an earlier Report (NM-R9212, June 1992), two of us gave tables of factorizations of $a^n \pm 1$ for $13 \le a < 100$. The exponents n satisfied $a^n < 10^{255}$ if $a < 30$, and $n \le 100$ if $a \ge 30$. The factorizations were complete for $n \le 46$, and the tables contained no composite numbers smaller than 10^{80}. In this Report we update the original tables. The factorizations are now complete for $n \le 58$, and there are no composite numbers smaller than 10^{86}.

1991 Mathematics Subject Classification: Primary 11A25; Secondary 11-04.
Keywords and Phrases: Factor Tables.

Appeared as Report NM-R94??, Centrum voor Wiskunde en Informatica, Amsterdam, September 1994, 46 pp. Only the front matter is given here.
Copyright © 1994, the authors. rpb134u1 typeset using TEX

1. Introduction

For many years there has been an interest in the prime factors of numbers of the form $a^n \pm 1$, where a is a small integer (the *base*) and n is a positive exponent. Such numbers often arise. For example, if a is prime then there is a finite field F with a^n elements, and the multiplicative group of F has $a^n - 1$ elements. Also, for prime a the sum of divisors of a^n is $\sigma(a^n) = (a^{n+1} - 1)/(a - 1)$. Numbers of the form $a^n + 1$ arise as factors of $a^{2n} - 1$ and in other ways.

An extensive table of factors of $a^n \pm 1$ for $a \leq 12$ has been published by Brillhart *et al* [3]. The computation of [3] is referred to as the *Cunningham Project* in recognition of the pioneering computations of Cunningham and Woodall [4]. For a history, see the Introduction in [3].

The tables [3] are limited to $a \leq 12$, but many applications require larger bases. In 1992 two of us published an extension [2] covering the range $13 \leq a < 100$. The exponents n satisfied $a^n < 10^{255}$ if $a < 30$, and $n \leq 100$ if $a \geq 30$.

Since the publication of our tables [2], many new factors have been found. The factorizations are now complete for $n \leq 58$ (formerly $n \leq 46$) and there are no composite numbers with under 87 decimal digits (formerly 81 decimal digits). This report gives all the new (complete or partial) factorizations found from the publication of [2] to the end of August 1994. Altogether, 785 factorizations are listed, some involving several new factors. For example, see the entry for $17^{187} - 1$ (formerly c96.c98, now complete).

2. Availability of Updates

These updates are available by anonymous ftp from `nimbus.anu.edu.au:pub/Brent/rpb134u1.txt.Z` . We shall add new factors to `rpb134u2.txt` as they are found.

A more comprehensive list of over $180,000$ factors, for bases $2 \leq a < 1000$ with various exponent ranges, and complete for exponents $n \leq 30$, is available in machine-readable form from the first author, or by anonymous ftp from `nimbus.anu.edu.au:pub/Brent/rpb117.exe` (a self-extracting IBM PC archive).

3. Factorization Methods

Most (about 700) new factors have been found by variants of the elliptic curve method (ECM) and the multiple-polynomial quadratic sieve (MPQS). References describing these methods are given in [1, 3]. ECM is useful for finding factors up to about 30 decimal digits, or up to about 40 digits if we use a lot of computer time and are lucky. If the number remaining on division by known factors is composite, but not too large, the factorization can be completed by MPQS [9, 10].

The old Pollard $p \pm 1$ methods are still useful: 38 new factors were found by the $p - 1$ method, and 16 by the $p + 1$ method.

The Special Number Field Sieve (SNFS) [6, 7] was not used in the computation of the original tables [2], but SNFS was used to complete 37 difficult factorizations for these updates. For example, see the entries for $18^{158} + 1$ (formerly c96.c98, now complete) and $73^{73} + 1$ (formerly c135, now complete).

4. Format of the Updates

The format of the updates is the same as the format of the tables [2], except that only those entries which have changed are given. For each base a, not a perfect power, in the range $13 \le a < 100$, we give two separate tables –

Table $a-$: factorizations of $a^n - 1$, n odd.
Table $a+$: factorizations of $a^n + 1$.

The exponent ranges are as in the tables [2] –

$13 \le a < 30$, exponents n such that $a^n < 10^{255}$.
$30 \le a < 100$, exponents $n \le 100$.

The entries are similar in format to those of the "short" tables in [3]. All known factors, including algebraic and Aurifeuillian factors, are listed. Factors which are given as decimal numbers are primes. Exponents are indicated by a hat (^), for example "2^3" means 2^3. Multiplication is indicated by a period (.), for example $3^3 + 1 = 2^2 7$ is written as "2^2.7". A period at the end of a line implies that the factorization is continued on the next line.

The largest factor of $a^n \pm 1$ may be found by division by the smaller factors. Thus, such factors are abbreviated. The notation "`pxy`" means a prime factor of `xy` decimal digits. For example, the prime 1238926361552897 might be abbreviated as `p16`. Similarly, the notation "`cxy`" means a composite number of `xy` decimal digits.

An indication of the person and method used to find the new factor(s) is given in square brackets after each entry. We apologise for any errors or omissions in these attributions. Factors found by the authors using ECM and/or MPQS are not usually indicated, except for factors of at least thirty decimal digits which were found using ECM. (Our records of these are probably incomplete.)

5. Probable Primes

Numbers listed as prime in these updates have not in all cases been rigorously proved to be prime; they may merely have passed a probabilistic primality test [5]. There is a positive but extremely small probability (less than 10^{-12}) that a composite number will pass such a test and be mistaken for a prime. In applications where it is essential for primality to be proven rigorously, the reader should apply an algorithm such as Morain's elliptic curve primality test [8], which can easily prove or disprove the primality of numbers of the size considered here.

Acknowledgements

We gratefully acknowledge the assistance of the following people who contributed factors. The number following each name is the number of factors which the person contributed to this update:

Henk Boender (45), Thomas Denny (2), Harvey Dubner (17), Marije Huizing (2), Wilfrid Keller (3), Arjen Lenstra (6), Robert Silverman (8), Thomas Sosnowski (6), and Samuel Wagstaff, Jr. (2).

We thank Mitsuo Morimoto and Hans Riesel, in addition to several of the above, for providing factors outside the range of this update. We thank Walter Lioen for his continuous technical assistance.

The Australian National University Supercomputer Facility provided computer time to run the first author's ECM program on a Fujitsu VP 2200/10 vector processor.

The Dutch National Computing Facilities Foundation, NCF (the former Dutch Working Group on the Use of Supercomputers), provided computer time to run the programs of Boender, Huizing, Montgomery, and te Riele on Cray Y-MP4 and Cray C98/4256 vector computers.

References

1. R. P. Brent, "Parallel algorithms for integer factorisation", *Number Theory and Cryptography* (edited by J. H. Loxton), London Mathematical Society Lecture Note Series 154, Cambridge University Press, 1990, 26-37.
2. R. P. Brent and H. J. J. te Riele, *Factorizations of* $a^n \pm 1$, $13 \le a < 100$, Report NM-R9212, Centrum voor Wiskunde en Informatica, Amsterdam, June 1992, 363+v pp. Available by anonymous ftp from `nimbus.anu.edu.au:pub/Brent/rpb134t.txt.Z, rpb134.dvi.Z .`
3. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1, b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, Contemporary Mathematics, Volume 22, American Mathematical Society, Providence, Rhode Island, second edition, 1988.
4. A. J. C. Cunningham and H. J. Woodall, *Factorisation of* $y^n \mp 1, y = 2, 3, 5, 6, 7, 10, 11, 12$ *Up to High Powers (n)*, Hodgson, London, 1925.
5. D. E. Knuth, *The Art of Computer Programming*, Volume 2, Addison Wesley, second edition, 1981.
6. A. K. Lenstra and H. W. Lenstra, Jr. (editors), *The Development of the Number Field Sieve*, Lecture Notes in Mathematics 1554, Springer-Verlag, New York, 1993.
7. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse and J. M. Pollard, "The number field sieve", *Proc. 22nd Annual ACM Conference on the Theory of Computing*, Baltimore, Maryland, May 1990, 564-572.
8. F. Morain, *Courbes elliptiques et tests de primalité*, thesis, Université de Lyon I, 1990. Available by anonymous ftp from `ftp.inria.fr .`
9. H. J. J. te Riele, W. M. Lioen and D. T. Winter, Factoring with the quadratic sieve on large vector computers, *Belgian J. Comp. Appl. Math.* 27 (1989), 267-278.
10. H. J. J. te Riele, W. M. Lioen and D. T. Winter, Factorization beyond the googol with MPQS on a single computer, *CWI Quarterly* 4 (1991), 69-72.