Factorizations of $\mathbf{a}^n \pm 1$, $13 \leq \mathbf{a} < 100$

Richard P. Brent
Computer Sciences Laboratory, Australian National University
GPO Box 4, Canberra, ACT 2601, Australia
e-mail: rpb@cslab.anu.edu.au

and

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

Abstract

As an extension of the "Cunningham" tables, we present tables of factorizations of $a^n \pm 1$ for $13 \leq a < 100$. The exponents n satisfy $a^n < 10^{255}$ if $a < 30$, and $n \leq 100$ if $a \geq 30$. The factorizations are complete for $n \leq 46$, and the tables contain no composite numbers smaller than 10^{80}.

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

Appeared as Report NM-R9212, Centrum voor Wiskunde en Informatica, Amsterdam, June 1992, 368 pp. Only the front matter is given here.
 rpb134 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 moderately 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 $a \le 12$ has been published by Brillhart *et al* [6]. For historical reasons, the computation of [6] is referred to as the *Cunningham Project* after the pioneering computations of Cunningham and Woodall [9]. For a history, see the Introduction in [6].

In the course of proving [4, 5] that there is no odd perfect number less than 10^{300}, we found the tables of [6] very useful, but needed to extend them to higher bases. For example, we needed many factorizations of $a^n - 1$ for $a = 13, 19, 31, 127$. The majority were computed using Lenstra's *Elliptic Curve Method* (ECM) [13] and in some difficult cases the *Multiple Polynomial Quadratic Sieve* (MPQS) [17, 18, 20]. The factors were kept in a machine-readable file which has been distributed together with a simple factorization program *factor* for IBM PC and compatible computers [3]. The program *factor* should be considered primarily as a means of accessing a file of known factors, rather than as a general-purpose factorization program. For surveys of factorization algorithms and programs, we refer the reader to [1, 2, 7, 8, 10, 13, 14, 16, 17, 18, 19, 20].

Over the past few years we have systematically extended our list of factors, concentrating on numbers $a^n \pm 1$ for $13 \le a < 100$, $n \le 100$, but also considering some larger values of the exponent n for the smaller bases a. The tables are now complete for $n \le 46$ and include no composites with less than 81 decimal digits[1]. Approximately 78% of the numbers $a^n \pm 1$ in the range of the tables have been factorized completely; the remainder have one (or occasionally two) composite factors whose prime factors are unknown. Judging from the size of factors currently being found, most prime factors of less than 20 digits have already been found.

Although a project such as this is never complete, it seemed appropriate to publish some of our factorizations in printed form[2]. Readers are invited to send any new factors to the first author for incorporation in the machine-readable list and possibly in later editions of these tables.

Recently a new algorithm, the *Number Field Sieve* (NFS) [12] has been used successfully in factoring numbers of the form $a^n \pm 1$, for example the ninth Fermat number $F_9 = 2^{2^9} + 1$. None of the factors given in our tables (for $a \ge 13$) have been found using NFS, but future extensions of the tables may well involve the use of NFS.

---

[1] Occasionally such a composite arises when an incomplete factorization is found by ECM, but the factorization can then be completed quickly using MPQS, so any such "small" composites may be regarded as temporary aberrations.

[2] The program *factor* [3] and machine-readable list of factors is still available from the first author.

2. Format of the Tables

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 follows –

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

The border between cases A and B may may change in future extensions of the tables.

The tables are similar in format to the "short" tables of [6]. All known factors, including *algebraic*[3] and *Aurifeuillian*[3] factors, are listed. Factors which are given as decimal numbers are primes. Exponents are indicated by a hat (ˆ), for example "2ˆ3" means 2^3. Multiplication is indicated by a period (.), for example $3^3 + 1 = 2^2 7$ is written as "2ˆ2.7". A period at the end of a line implies that the factorization is continued on the next line.

A factor of more than 72 decimal digits may be written on more than one line. In such a case the underscore character (_) at the end of a line means that the following line is a continuation.

The largest factor of $a^n \pm 1$ may be found by division by the smaller factors. Thus, such factors are often 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. Occasionally two such composite factors are listed; they may be found by removing known prime factors from large algebraic or Aurifeuillian factors. In such cases the smaller composite factor is given explicitly in a comment of the form "`[cxy = ...]`".

3. Probable Primes

Numbers listed as prime in these tables have not in all cases been rigorously proved to be prime; they may merely have passed a probabilistic primality test [11]. 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 [15], which can easily prove or disprove the primality of numbers of the size considered here.

[3] For definitions of these terms, see [6, 19].

Acknowledgements

We gratefully acknowledge the assistance of –

Graeme Cohen, without whom the odd perfect number project [4, 5] would not have been started.

Harvey Dubner, for unpublished factors found by the Pollard "$p-1$" method.

Robert Silverman, for unpublished tables covering the range $a \le 30$, $n \le 100$.

Samuel Wagstaff, for much useful information on the Cunningham project, and the provision of updates to [6]. These are for $a \le 12$, so lie outside the range of the present tables, but are included for the sake of completeness in the machine-readable file [3].

The Australian National University Supercomputer Facility, for the provision of computer time to run the first author's ECM program MVFAC [2] on Fujitsu VP 100 and VP 2200/10 vector processors.

The Dutch National Computing Facilities Foundation, NCF (the former Dutch Working Group on the Use of Supercomputers), for the provision of computer time to run the second author's MPQS program [17, 18] on Cyber 205, NEC SX/2 and Cray Y-MP4 vector processors.

References

1. R. P. Brent, "Some integer factorization algorithms using elliptic curves", *Australian Computer Science Communications* 8 (1986), 149-163.
2. 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.
3. R. P. Brent, *Factor: an integer factorization program for the IBM PC*, Technical Report TR-CS-89-23, Computer Sciences Laboratory, Australian National University, October 1989 (and subsequent revisions).
4. R. P. Brent and G. L. Cohen, "A new lower bound for odd perfect numbers", *Mathematics of Computation* 53 (1989), 431-437. Supplement, *ibid*, S7-S24.
5. R. P. Brent, G. L. Cohen and H. J. J. te Riele, Improved techniques for lower bounds for odd perfect numbers, *Mathematics of Computation* 57 (1991), 857-868.
6. 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*, American Mathematical Society, Providence, Rhode Island, second edition, 1985.
7. D. A. Buell, "Factoring: algorithms, computations, and computers", *J. Supercomputing* 1 (1987), 191-216.
8. T. R. Caron and R. D. Silverman, "Parallel implementation of the quadratic sieve", *J. Supercomputing* 1 (1988), 273-290.
9. 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.
10. R. K. Guy, "How to factor a number", *Congressus Numerantum XVI*, Proc. Fifth Manitoba Conference on Numerical Mathematics, Winnipeg, 1976, 49-89.
11. D. E. Knuth, *The Art of Computer Programming*, Volume 2, Addison Wesley, second edition, 1982.

12. 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.
13. H. W. Lenstra, Jr., "Factoring integers with elliptic curves", *Ann. of Math.* (2) 126 (1987), 649-673.
14. P. L. Montgomery, "Speeding the Pollard and elliptic curve methods of factorization", *Mathematics of Computation* 48 (1987), 243-264.
15. F. Morain, *Courbes elliptiques et tests de primalité*, thesis, Université de Lyon I, 1990. Available by anonymous ftp from `ftp.inria.fr`
16. C. Pomerance, "Analysis and comparison of some integer factoring algorithms", in *Computational Methods in Number Theory* (edited by H. W. Lenstra, Jr. and R. Tijdeman), Math. Centrum Tract 154, Amsterdam, 1982, 89-139.
17. 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.
18. 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.
19. H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.
20. R. D. Silverman, "The multiple polynomial quadratic sieve", *Mathematics of Computation* 48 (1987), 329-339.