Factorizations of $a^n \pm 1$, $13 \le a < 100$: Update 2*

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

Peter L. Montgomery
780 Las Colindas Road
San Rafael, CA 94903–2346
USA
pmontgom@cwi.nl

Herman J. J. te Riele
Centrum voor Wiskunde en Informatica
Kruislaan 413
1098 SJ Amsterdam
The Netherlands
herman@cwi.nl

with the assistance of

Henk Boender, Marije Elkenbracht-Huizing,
Paul Leyland, Andreas Müller, MullFac,
Robert Silverman, and Thomas Sosnowski

23 March 1996

Abstract

This Report updates the tables of factorizations of $a^n \pm 1$ for $13 \le a < 100$, previously published as CWI Report NM-R9212 (June 1992) and updated in CWI Report NM-R9419 (September 1994). A total of 760 new entries in the tables are given here. The factorizations are now complete for $n < 67$, and there are no composite cofactors smaller than 10^{94}.

1991 Mathematics Subject Classification. Primary 11A25; Secondary 11-04
Key words and phrases. Factor tables, ECM, MPQS, SNFS

*To appear as Report NM-R9609, Centrum voor Wiskunde en Informatica, Amsterdam, March 1996.
 Only the front matter is given here. For the tables, see rpb134u2.txt .
rpb134u2 typeset using LaTeX

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* [10]. The computation of these tables is referred to as the *Cunningham Project* in recognition of the pioneering computations of Cunningham and Woodall [12]. For a history, see the Introduction in [10].

The tables [10] are limited to $a \leq 12$, but many applications require larger bases. In June 1992 tables covering the range $13 \leq a < 100$ were published [9]. The exponents n satisfied $a^n < 10^{255}$ if $a < 30$, and $n \leq 100$ if $a \geq 30$. An update [8] containing 780 new factorizations (with the same limits for a and n) was published in September 1994.

Since the first update [8], many new factors have been found. The factorizations are now complete for $n \leq 66$, and there are no composite cofactors with fewer than 95 digits[1]. This report gives all the new (complete or partial) factorizations found from the publication of [8] to 22 March 1996. Altogether, 760 factorizations are listed, involving 882 new factors[2]. Table 1 summarizes progress since the publication of the original tables [9].

Table 1: Statistics regarding the Tables and Updates

Tables	Date	Smallest composite	Complete to exponent	Total entries	Complete entries
Original	June 1992	81 digits	46	13882	10789
Update 1	Sept. 1994	87 digits	58	780	649
Update 2	March 1996	95 digits	66	760	590

Table 2 shows the number of prime factors of different sizes found for Updates 1 and 2 (excluding large factors obtained by division). The median size is 26 digits for Update 1 and 29–30 digits for Update 2.

Table 2: Distribution of Factors

Digits	Update 1	Update 2
14–19	17	24
20–24	333	144
25–29	329	273
30–34	154	197
35–39	72	99
40–45	44	89
45–49	9	39
50–56	1	17
Total	959	882

[1] "digits" always means "decimal digits".

[2] Here and elsewhere we do not count large factors which are obtained by division by other factors.

2 Format of the Updates

The format of Update 2 is the same as that of Update 1. Only those entries which have changed since Update 1 are given. For each base a, not a perfect power, in the range $13 \leq a < 100$, 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 [9] –

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

The entries are similar in format to those of the "short" tables in [10]. All known factors, including algebraic and Aurifeuillian [5] 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. An underscore (_) at the end of a line means that a (large) factor is continued on the next line (see, for example, the entry for $19^{177} - 1$).

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

An indication of the person[3] and method responsible for finding a new factor is given in square brackets (usually on the same line as the factor). Factors found by the authors using ECM or MPQS are not marked unless they have at least 30 digits.

3 Availability of Tables and Updates

These updates are available by anonymous ftp from `ftp://nimbus.anu.edu.au/pub/Brent/rpb134u2.txt.Z` (a compressed text file).

The complete tables incorporating Updates 1 and 2 are available by anonymous ftp from `ftp://nimbus.anu.edu.au/pub/Brent/factors/table*` . For example, the file `table13p` is a table of factorizations of $13^n + 1$ for $n = 1(1)228$, and the file `table99m` is a table of factorizations of $99^n - 1$ for $n = 1(2)127$. (The restriction $n \leq 100$ for bases $a \geq 30$ has been relaxed for these tables; we only require $a^n < 10^{255}$.)

A database of over $207,000$ factors, for bases $2 \leq a < 1000$ with various exponent ranges, is available by anonymous ftp from `ftp://nimbus.anu.edu.au/pub/Brent/rpb117.exe` (a self-extracting IBM PC archive). This includes factors in the range $2 \leq a \leq 12$ from the Cunningham tables [10], factors in the range $100 < a < 1000$ (including some from the tables of Mitsuo Morimoto *et al* [22]), and 15902 factors of Fibonacci and Lucas numbers from the tables of John Brillhart, Wilfrid Keller, Peter Montgomery and Robert Silverman [11, 14]. The database may be accessed using an IBM-compatible PC and programs provided in the above archive (see [4] for details). The database is built into the symbolic algebra package Magma and is used by the integer factorization routines in Magma [3, §19.9].

[3]Except for the three authors. Factors marked simply "ECM" were found by Brent or Montgomery, those marked "MPQS" were found by Brent or te Riele, and those marked "SNFS" were found by Montgomery.

4 Factorization Methods

Since Update 1 we have attempted to factor the remaining composite numbers in the tables by using the *elliptic curve method* (ECM). Sometimes ECM is successful in finding one or more factors. If the factorization can not be completed by ECM, but the remaining composite part is sufficiently small, we use the *multiple polynomial quadratic sieve* (MPQS) method to complete the factorization. In some cases we prefer to use the *special number field sieve* (SNFS) if it is predicted to be faster than MPQS (the choice depends upon the size of the known non-algebraic factors of the number $a^n \pm 1$).

We do not describe ECM, MPQS or SNFS here. The reader should refer to [17, 18, 20] for a general description of ECM, to [24] for MPQS, and to [16] for SNFS.

The particular implementations of ECM by Brent and Montgomery are described in [7, 19]. Computational details regarding the factorizations of various entries in Update 1 and in this Update 2, obtained with an implementation of the "two large primes variation" (PPMPQS) of MPQS on SGI workstations and on a Cray C90 vector computer, are given in [2]. The implementation of SNFS used by Marije Elkenbracht-Huizing and Peter Montgomery is described in [13].

In the following we do not distinguish between different versions of the basic methods (e.g. PMPQS and PPMPQS, ECM and ECM/FFT).

ECM is useful for finding factors of up to about 35 digits, although it occasionally finds larger factors [6, 7]. The largest factor found by ECM in the course of preparation of this update is a 47-digit factor

$$p_{47} = 28207978317787299519881883345010831781124600233$$

of $30^{109} - 1$ (found by Peter Montgomery on 25 February 1996). We knew that

$$\begin{aligned} 30^{109} - 1 &= 29 \cdot 134507 \cdot 111452974016629781 \cdot 1863969251081608763575O3 \cdot \\ &\quad 60663419621805165080404081 \cdot c_{89} \ , \end{aligned}$$

and Montgomery's program split the c_{89} into the product of two prime factors $c_{89} = p_{42} \cdot p_{47}$. ECM did not find the 42-digit factor

$$p_{42} = 731551028948799148140437455525315594459547$$

directly; instead it found p_{47}, and $p_{42} = c_{89}/p_{47}$ was then computed by division[4].

We have used MPQS to factor many numbers of less than 100 digits. Examples and statistics are given in [2]. We mention one example by a collaborator. In January 1996 we knew that

$$24^{97} - 1 = 23 \cdot 4541347 \cdot 69291447660895432806381824641 \cdot c_{98} \ .$$

Paul Leyland helped complete the tables for $a \leq 30$, $n \leq 100$, by finding the factorization

$$c_{98} = 7351880762305548476454345654984875687952 71 \cdot p_{56} \ .$$

We give an example of the use of SNFS. We knew $26^{97} + 1 = 3^3 \cdot 971 \cdot c_{133}$. Using SNFS, Montgomery found

$$c_{133} = 1383158385386706268628631034077604973798814912 5269 \cdot p_{84} \ .$$

Other notable examples completed by SNFS are $29^{94}+1$, whose c_{116} factor was split into $p_{56} \cdot p_{61}$; and $86^{64} + 1 = c_{124} = p_{56} \cdot p_{68}$. (These 56-digit factors are the largest new penultimate factors listed in Update 2.)

[4]For the skeptical reader: details of the "lucky" elliptic curve and group order, proving that ECM found the 47-digit factor, are given in [6]. Although smaller factors are usually found before larger ones, there is no *guarantee* that ECM will find factors in increasing order of size. For another example, see the entry for $29^{83} - 1$ (where a 37-digit factor was found by ECM but a 27-digit factor was missed).

Table 3: Factors Found by Different Methods

	Pollard $p-1$	Pollard $p+1$	ECM (30D+)	MPQS (30D+)	SNFS
Update 1	38	16	69	157	37
Update 2	0	3	151	155	136

Table 3 shows the number of factors found by several methods in the preparation of Updates 1 and 2. For ECM and MPQS these only include penultimate factors of at least 30 digits. An increase in the use of SNFS and decline in the use of Pollard's $p \pm 1$ methods [23] is evident. There is also a marked increase in the number of large (at least 30-digit) factors found by ECM. Most of the new factors found by MPQS and SNFS are large because these methods are only used after ECM has been tried without success.

A summary of new factors found over a recent three-month period (from 19 Dec 1995 to 22 March 1996) is given in Table 4. In the table, "normal range" means the usual limits on base and exponent (as for this Update); "extended range" means the additional numbers $a^n \pm 1$ (with $30 \le a < 100$, $n > 100$, $a^n < 10^{255}$) which are not given in this Update but are available in machine-readable form (see §3). The table suggests that there are few factors with less than 24 digits still to be found in the normal range, and similarly for factors with less than 22 digits in the extended range. A comparison with Table 2 shows progress: factors of less than 25 digits are now found only rarely, and the median size of the factors found is steadily increasing.

Table 4: Recent Factors

	Number of new factors	Number less than 25 digits	Smallest (digits)	Median (digits)	Largest (digits)
Normal range	167	3	24	32	56
Extended range	96	7	22	29	47
Combined range	263	10	22	31	56

5 First Holes

A "first hole" is the first composite number occurring in a table. Thus, each table of factorizations is complete up to, but not including, its first hole. Table 5 lists the exponents of the current first holes for $2 \le a < 100$ (the range $2 \le a \le 12$ is included for the sake of comparison). For example, the first holes in the tables for $a = 17$ occur for exponents 103 and 106. In fact, these holes ($17^{103} - 1 = 2^4 \cdot c_{126}$ and $17^{106} + 1 = 2 \cdot 5 \cdot 29 \cdot 1061 \cdot c_{125}$) are good candidates for factorization by SNFS.

6 Probable Primes

Numbers listed as prime have not in all cases been rigorously proved to be prime; they may merely have passed a probabilistic primality test [15]. There is a positive but extremely small probability 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, one should apply an algorithm such as Morain's elliptic curve primality test [1, 21], which can easily prove or disprove the primality of numbers of the size considered here.

Table 5: Exponents of First Holes for $2 \leq a \leq 99$

a	$-$	$+$	a	$-$	$+$	a	$-$	$+$	a	$-$	$+$
2	559	536	3	331	332	5	233	226	6	199	206
7	187	181	10	167	163	11	151	142	12	137	148
13	119	104	14	125	103	15	103	103	17	103	106
18	107	119	19	127	103	20	103	101	21	101	103
22	103	103	23	101	101	24	101	103	26	107	103
28	103	101	29	101	103	30	103	103	31	97	83
33	73	86	34	91	89	35	73	83	37	89	83
38	73	83	39	67	89	40	83	73	41	85	68
42	67	71	43	67	71	44	79	76	45	73	79
46	71	79	47	71	73	48	71	71	50	89	67
51	73	71	52	73	73	53	89	73	54	77	71
55	71	67	56	83	67	57	83	68	58	73	76
59	71	74	60	67	71	61	67	71	62	71	74
63	67	68	65	71	71	66	73	71	67	83	68
68	77	76	69	73	67	70	73	68	71	73	76
72	71	68	73	67	71	74	73	71	75	77	67
76	71	73	77	73	71	78	77	76	79	67	74
80	73	73	82	71	67	83	67	73	84	67	76
85	67	73	86	71	71	87	67	71	88	79	74
89	83	74	90	73	68	91	83	68	92	67	68
93	67	73	94	67	74	95	67	67	96	71	73
97	67	73	98	73	71	99	67	67			

Acknowledgements

We gratefully acknowledge the assistance of the following people who contributed factors. The number following each name is the number of factors contributed to this update: Henk Boender (56), Marije Elkenbracht-Huizing (1), Paul Leyland (1), Andreas Müller (2), MullFac[5] (1), Robert Silverman (8), and Thomas Sosnowski (55).

Henk Boender, Harvey Dubner, Wilfrid Keller, Samuel Wagstaff, Jr., and Georg Wambach provided factors outside the range of this update (but included in the database [4]).

John Cannon and Allan Steel incorporated our database of factors into the Magma package and incidentally helped to debug our table-generating programs.

Walter Lioen helped us continuously with the solution of implementation problems.

The Australian National University Supercomputer Facility provided computer time to run the first author's ECM programs on a Fujitsu VP 2200/10 vector processor and an SGI Power Challenge. The ANU-Fujitsu CAP Research Project provided time on a Fujitsu AP 1000.

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, Elkenbracht-Huizing, Montgomery, and te Riele on Cray Y-MP4 and Cray C98/4256 vector computers.

The majority of the runs with ECM, MPQS and SNFS were carried out on about 70 SGI workstations at CWI and about 30 SGI workstations at Leiden University. With ECM, different numbers were run on different workstations; the MPQS sieving for each number with 87–94 digits was done in parallel on several workstations at the same time, and similarly for the SNFS

[5]MullFac is the *Isle of Mull Factoring Group* (Richard Edwards, Willie Gough, George Sassoon and Vivian Stephens).

sieving. We are grateful to the workstation "owners" at CWI and Leiden University for letting us use their idle cycles for this project.

References

[1] A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving,* Math. Comp. **61** (1993), 29–68. Programs available from `ftp://ftp.inria.fr/INRIA/ecpp.V3.4.1.tar.Z`.

[2] H. Boender and H. J. J. te Riele, *Factoring integers with large prime variations of the quadratic sieve,* Report NM-R9513, Department of Numerical Mathematics, Centrum voor Wiskunde en Informatica, Amsterdam, July 1995. `ftp://ftp.cwi.nl/pub/CWIreports/NW/NM-R9513.ps.Z` .

[3] W. Bosma and J. Cannon, *Handbook of Magma Functions,* School of Mathematical Sciences, Univ. of Sydney, January 1996. See also the *Magma home page:* `http://www.maths.usyd.edu.au/comp/magma/Overview.html` .

[4] R. P. Brent, *Factor: an integer factorization program for the IBM PC,* Report TR-CS-89-23, Computer Sciences Laboratory, Australian National Univ., Canberra, Oct. 1989, 7 pp. Available from `ftp://nimbus.anu.edu.au/pub/Brent/rpb117.dvi.Z` . The program(s) and database of factors are available from `ftp://nimbus.anu.edu.au/pub/Brent/rpb117.exe` (a self-extracting IBM PC archive).

[5] R. P. Brent, *On computing factors of cyclotomic polynomials,* Math. Comp. **61** (1993), 131–149.

[6] R. P. Brent, *Large factors found by ECM,* Computer Sciences Laboratory, Australian National Univ., Canberra, December 1995 (revised February 1996). `ftp://nimbus.anu.edu.au/pub/Brent/champs.ecm` .

[7] R. P. Brent, *Factorization of the tenth and eleventh Fermat numbers,* Report TR-CS-96-02, Computer Sciences Laboratory, Australian National Univ., Canberra, February 1996, 25 pp. `ftp://nimbus.anu.edu.au/pub/Brent/rpb161tr.dvi.Z` .

[8] R. P. Brent, P. L. Montgomery and H. J. J. te Riele, *Update 1 to: Factorizations of* $a^n \pm 1$, $13 \le a < 100$, Report NM-R9419, Centrum voor Wiskunde en Informatica, Amsterdam, September 1994. `ftp://nimbus.anu.edu.au/pub/Brent/rpb134u1.*.Z` .

[9] R. P. Brent and H. J. J. te Riele, *Factorizations of* $a^n \pm 1$, $13 \le a < 100$, Report NM-R9212, Department of Numerical Mathematics, Centrum voor Wiskunde en Informatica, Amsterdam, June 1992. `ftp://nimbus.anu.edu.au/pub/Brent/rpb134*.*.Z` .

[10] 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*, 2nd ed., Amer. Math. Soc., Providence, RI, 1988. Also updates to page 74, #3866 (Feb. 16, 1996).

[11] J. Brillhart, P. L. Montgomery, and R. D. Silverman, *Tables of Fibonacci and Lucas Factorizations,* Math. Comp. **50** (1988), 251–260. *Supplement, ibid,* S1–S15.

[12] 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.

[13] R. M. Huizing, *An implementation of the number field sieve,* Experimental Mathematics, to appear. Also Report NM-R9511, Department of Numerical Mathematics,

Centrum voor Wiskunde en Informatica, Amsterdam, July 1995. `ftp://ftp.cwi.nl/pub/CWIreports/NW/NM-R9511.ps.Z` .

[14] W. Keller, *Factors of F_n and L_n for* $1000 < n \leq 9750$, machine-readable table, January 1996.

[15] D. E. Knuth, *The art of computer programming, Volume 2: Seminumerical algorithms* (2nd edition), Addison-Wesley, Menlo Park, CA, 1981.

[16] A. K. Lenstra and H. W. Lenstra, Jr. (editors), *The development of the number field sieve,* Lecture Notes in Mathematics **1554**, Springer-Verlag, Berlin, 1993.

[17] H. W. Lenstra, Jr., *Factoring integers with elliptic curves,* Annals of Mathematics (2) **126** (1987), 649–673.

[18] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization,* Math. Comp. **48** (1987), 243–264.

[19] P. L. Montgomery, *An FFT extension of the elliptic curve method of factorization,* Ph. D. dissertation, Mathematics, University of California at Los Angeles, 1992.

[20] P. L. Montgomery, *A survey of modern integer factorization algorithms,* CWI Quarterly **7** (1994), 337–366.

[21] F. Morain, *Courbes elliptiques et tests de primalité,* Ph. D. thesis, Université Claude Bernard – Lyon I, France, 1990. `ftp://ftp.inria.fr/INRIA/publication/Theses/TU-0144.tar.Z` .

[22] M. Morimoto, Y. Kida and M. Kobayashi, *Factorization of cyclotomic numbers,* III, Sophia Kokyuroku No. 35, Dept. of Mathematics, Sophia University, 7-1 Kioi-Cho, Chiyoda-ku, Tokyo 102, Japan, July 1992.

[23] H. Riesel, *Prime numbers and computer methods for factorization,* 2nd edition, Birkhäuser, Boston, 1994.

[24] R. D. Silverman, *The multiple polynomial quadratic sieve,* Math. Comp. **48** (1987), 329–339.