

# FACTORIZATIONS OF $a^n \pm 1$ , $13 \leq a < 100$

RICHARD P. BRENT AND HERMAN J. J. TE RIELE

## ABSTRACT

As an extension of the ‘‘Cunningham’’ tables [4, 5] 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  $10^{80}$ .

## COMMENTS

Only the Abstract is given here. The full report appeared as [2], and an update as [3]. The factors and updates are available in machine-readable form: see [1].

## REFERENCES

- [1] R. P. Brent, *Factor: An Integer Factorization Program for the IBM PC*, Report TR-CS-89-23, October 1989, 7 pp. rpb117.
- [2] R. P. Brent and H. J. J. te Riele, ‘‘Factorizations of  $a^n \pm 1$ ,  $13 \leq a < 100$ ’’ Report NM-R9212, Centrum voor Wiskunde en Informatica, Amsterdam, June 1992, 368 pp. ISSN 0169-0388. rpb134.
- [3] R. P. Brent, P. L. Montgomery and H. J. J. te Riele, ‘‘Update 1 to Factorizations of  $a^n \pm 1$ ,  $13 \leq a < 100$ ’’ Centrum voor Wiskunde en Informatica, Amsterdam, September 1994, 46 pp., to appear.
- [4] 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, 1988.
- [5] 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.

(Brent) COMPUTER SCIENCES LAB, AUSTRALIAN NATIONAL UNIVERSITY, CANBERRA  
*E-mail address:* `rpb@cslab.anu.edu.au`

(te Riele) CWI, KRUISLAAN 413, 1098 SJ AMSTERDAM, THE NETHERLANDS  
*E-mail address:* `herman@cwi.nl`

---

1991 *Mathematics Subject Classification*. Primary 11A25; Secondary 11-04.

*Key words and phrases*. Factor tables, Cunningham tables, Aurifeuillian factors, elliptic curve method, ECM, multiple polynomial quadratic sieve, MPQS.

Copyright © 1992, the authors.

Comments © 1993, R. P. Brent.

rpb134a typeset using  $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{T}\mathcal{E}\mathcal{X}$ .