FACTOR: AN INTEGER FACTORIZATION PROGRAM FOR THE IBM PC

RICHARD P. BRENT

Abstract

Factor is a program which accesses a large database of factors of integers of the form $a^n \pm 1$. As of October 1989 the database contains more than 30,000 factors of size at least 10^4. The program *Factor* implements a simple version of the Elliptic Curve algorithm if it is unable to complete a factorization using trial division and the factor database.

Factor is written in Turbo Pascal and runs on IBM PC or compatible computers. This report describes *Factor* and various related programs. The programs and the factor database are available from the author.

Comments

Only the Abstract is given here. The full report appeared as [1]. The program *Factor* is a convenient way of accessing and updating the factor tables [2]. As of June 1993, the database mentioned in the Abstract has grown to more than 174,000 factors.

References

1. R. P. Brent, "*Factor*: an integer factorization program for the IBM PC", Report TR-CS-89-23, Computer Sciences Laboratory, ANU, October 1989; and Report CMA-R62-89, Centre for Mathematical Analysis, ANU, November 1989, 7 pp. Revision available by anonymous ftp from `dcssoft.anu.edu.au` . rpb117.
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, 368 pp. ISSN 0169-0388. rpb134.

Computer Sciences Laboratory, Australian National University, Canberra
E-mail address: rpb@cslab.anu.edu.au

1991 *Mathematics Subject Classification.* Primary 11-04; Secondary 11A51, 11Y05, 11Y11, 11Y16, 14H52, 68Q22, 68Q25.

Key words and phrases. Factorization, integer factorization, IBM PC, Turbo Pascal, elliptic curve method, ECM.