New Factorization Records on Supercomputers

Herman J.J. te Riele, Walter M. Lioen & Dik T. Winter
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands

Two new factorization records on supercomputers have been recently settled at the Centre for Mathematics and Computer Science (CWI) at Amsterdam. The numbers factorized into their prime factors are the 75-digit composite number:

$$(2^{271} - 2^{136} + 1) \;/\; 10474693 =$$

362232590504406868214617272006414447138055859511851874054762224427178428941 =

104167755499168696693743867494211841 *
347739652033970953169994378027632511310 1

(the product of a 36- and a 40-digit prime number)

and the 72-digit composite number:

$$10^{72} - 10^{36} + 1 =$$

999999999999999999999999999999999990000000000000000000000000000000000001 =

172629000899150450017746330268869 7 *
579276943498154282123686999881829009033

(which is the product of a 34- and a 39-digit prime number).

The factorized numbers were taken from a list of 20 composite numbers whose factorizations are unknown, and 'more wanted', from the book (sometimes called the factor bible): *Factorizations of* $b^n \pm 1$, by JOHN BRILLHART, D.H. LEHMER, J.L. SELFRIDGE, BRYANT TUCKERMAN and S.S. WAGSTAFF, JR. (AMS Contemporary Mathematics Series, vol. 22, 1983).

Interest in factorization and primality testing has increased dramatically since the discovery, in 1978, by RIVEST, SHAMIR and ADLEMAN, that the difficulty of breaking certain cryptographic codes depends on the difficulty of factorization [3].

The method used is the multiple polynomial version of Peter Montgomery of the quadratic sieve method of Carl Pomerance as described in a recent paper by POMERANCE, J.W. SMITH and R. TULER [2]. The computer used is the 1-pipe CDC CYBER 205 of SARA at Amsterdam (SARA is the Academic Computer Centre Amsterdam). The total time used was about 4.3 hours CPU-time for the 72-digit number and 12.2 hours for the 75-digit number. Control Data Benelux has kindly provided part of the computer time for these (and other) factorizations. The method was implemented on the CYBER 205 by a team consisting of Herman J.J. te Riele, Walter M. Lioen and Dik T. Winter from the Department of Numerical Mathematics of the CWI. Advisory help was provided by J. Schlichting of Control Data.

The previous record for supercomputers was held by J.A. Davis and D.B. Holdridge from Sandia Labs (USA) who (in 1984) factorized the number $(10^{71} - 1)/9$ (consisting of 71 1's) on a CRAY X/MP-24 of the Los Alamos Lab (USA) in 9.5 hours CPU-time, using a variant of the quadratic sieve method found by DAVIS [1]. This CRAY X/MP is about twice as fast as the CYBER 205 and has four million words of central memory (the CYBER 205 has one million words). In the heart of the quadratic sieve algorithm, the data to be handled are stored in non-contiguous memory locations. This is a handicap on the CYBER 205. All this illustrates the power of the Montgomery-variant of Pomerance's quadratic sieve.

It should be emphasized that larger difficult numbers have been factorized already by Robert Silverman, who did not use supercomputers, but VAX- and SUN-computers. His record is: a 81-digit composite number using a total of 1260 hours on 8 SUN-3/75 computers running in parallel. He also used the MP-QS method.

A few more details of our algorithm for the initiate:

	c72	c75
multiplier used:	none	5
factor base bound:	130000	160000
# primes in the factor base:	6071	7322
length of sieving interval:	$6(2^{16}-1)$	$6(2^{16}-1)$
# of completely factorized w's:	2672	3376
# of incompletely factorized w's:	24747	26062
# of large prime equalities in the incompletely factorized w's:	3401	3947
bound on the large primes allowed in incomplete w's:	30x130000	20x160000
Gauss elimination time (on a 6073x6072, resp. 7323x7323 linear system):	21 sec.	37 sec.
# of dependencies found:	65	509

REFERENCES

1. J.A. DAVIS, D.B. HOLDRIDGE, G.J. SIMMONS (1985). Status report on factoring (at the Sandia National Laboratories). T. BETH, N. COT, I. INGEMARSSON (eds.). *Advances in Cryptology, Proceedings of EUROCRYPT 84*, 183-215 Springer, Berlin etc.
2. C. POMERANCE, J.W. SMITH, R. TULER (1986). *A Pipe-Line Architecture for Factoring Large Integers with the Quadratic Sieve Algorithm.* Preprint.
3. R. RIVEST, A. SHAMIR, L. ADLEMAN (1978). A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM 21*, 120-126.