CWI Quarterly Volume 10 (2) 1997, pp. 105 – 107

A New World Record for the Special Number Field Sieve Factoring Method

Peter Montgomery
780 Las Colindas Road
San Rafael, CA 94903–2346, USA
e-mail: pmontgom@cwi.nl

Stefania Cavallar and Herman te Riele
Centrum voor Wiskunde en Informatica
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
e-mail: {cavallar, herman}@cwi.nl

On September 3, 1997 a new factoring world record has been established at CWI Amsterdam by the computation of the factors of the 180-digit number $N = (12^{167} + 1)/13$ with the Special Number Field Sieve algorithm[1] (SNFS) [7, 8, 6, 5].

The previous record for SNFS was the 167-digit number $(3^{349} - 1)/2$, completed by NFSNET (Number Field Sieve NETwork) on February 4, 1997. [2]

When factoring an integer N, SNFS requires one to select two polynomials with a common root m modulo N. Usually one polynomial is linear and one has higher degree. For numbers of this size (180 digits), the latter degree should be 5 or 6. Possible choices with these degrees are $f_5(X) = 144X^5 + 1$ with root $m = 12^{33}$ and $f_6(X) = X^6 + 12$ with root $m = 12^{28}$. Another possibility is $2f_5(X/2) = 9X^5 + 2$.

The choice between degrees 5 and 6 was made partially on the quality of the factor base. The siever looks for rational numbers a/b such that the numerators of $f(a/b)$ and of $a/b - m$ are both smooth, meaning that only small prime factors divide these numerators. These are more likely to be smooth when

[1] We assume the reader to be familiar with this factoring method, although no expert knowledge is required to understand the spirit of this announcement.

[2] NFSNET is a collaborative effort to factor numbers by the Number Field Sieve. It relies on volunteers from around the world who contribute the "spare time" of a large number of workstations to perform the sieving. In addition to completing work on other numbers, their 75 workstations sieved $(3^{349} - 1)/2$ during the months of December 1996 and January 1997. The organizers and principal researchers of NFSNET are: Marije Elkenbracht-Huizing, Peter Montgomery, Bob Silverman, Richard Wackerbarth, and Sam Wagstaff, Jr.

1. the polynomial values themselves are small (i.e., when the polynomial coefficients are small and/or a/b is close to a real root of f);
2. the polynomials have many (possibly projective) roots modulo small primes.

The degree-5 polynomials have a real root, but the degree-6 polynomials do not. The degree-5 polynomials have a root modulo every prime below 100 except 31, 41, 61, 71, with five roots modulo 11. The degree-6 polynomials have six roots modulo each of 13, 19, 79, 97, plus one root each modulo 2 and 3. Overall, the degree-5 polynomials rated slightly higher.

Our siever does better if we arrange the sieving region so that $|a/b| > 1$ for most a/b being sieved, since it must re-initialize much data whenever b changes. [It fixes b while it varies a] We chose $f(X) = X^5 - 144$ with $m = -12^{-33} \cong 12^{134}$. This performed slightly better in a simulation than $f(X) = 2X^5 - 9$ with $m = -12^{-33}/2$. The factor base bound was 4.8×10^6 for f and 12×10^6 for the linear polynomial. Both large prime bounds were 150×10^6, with two large primes allowed on each side. We sieved over $|a| \leq 8.4 \times 10^6$ and $0 < b \leq 2.5 \times 10^6$.

Our siever was at least 30 % faster than the version used for the 167-digit record, primarily due to better cache utilization and fewer mispredicted branches. The sieving lasted 10.3 calendar days spanning two weekends, from August 22 to September 2, 1997. During this period, 85 SGI machines (a mixture of O2's, Indy's, R4600's, and one PowerChallenge) at CWI contributed a combined 13027719 relations in 560 machine-days. It took 1.6 more calendar days to process the data. This processing included 16 CPU-hours on a Cray C90 at SARA in Amsterdam to carry out the Block Lanczos iterative algorithm for finding dependencies in a 1969262×1986500 matrix with 57942503 nonzero entries.

The factored number fills a gap in one of the tables of the Cunningham project [2] which has the goal to factor numbers of the form $b^n \pm 1$ for $b \leq 12$.

The factors found are the 75-digit prime

788539152479959923583473870729725158796647538883718863262181413347391236469

and the 105-digit prime

163117845256502920687558543656697020247411364462120385893160945804553250187
472604743326476435522680378897.

Primality of these numbers was proved with help of the Jacobi sum test of Adleman, Pomerance, Rumely, H. Cohen and H.W. Lenstra, Jr. [1, 3], as implemented by H. Cohen and A.K. Lenstra [4] with the help of D.T. Winter at CWI.

Acknowledgements

We thank the Dutch National Computing Facilities Foundation (NCF) for providing access to the Cray C90, our colleague Walter Lioen for technical assistance in this project, and all those CWI workstation owners for allowing us to use their idle evening, night and weekend cycles.

References

1. L. Adleman, C. Pomerance, and R. Rumely (1983). On distinguishing prime numbers from composite numbers. *Ann. of Math.*, **117**, 173–206.
2. J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, and S.S. Wagstaff, Jr. (1988). *Factorizations of* $b^n \pm 1, b = 2,3,5,6,7,10,11,12$ *up to high powers*, volume 22 of *Contemporary Mathematics.* American Mathematical Society, second edition. Updates to this second edition, with new lists of most and more wanted numbers, are distributed regularly by the fifth author. The most recent update is page 76, #4046 (July 30, 1997). The third edition of this book is to appear soon.
3. H. Cohen and H.W. Lenstra, Jr. (1984). Primality testing and Jacobi sums. *Mathematics of Computation*, **42**, 297–330.
4. H. Cohen and A.K. Lenstra (1987). Implementation of a new primality test. *Mathematics of Computation*, **48**, 103–121.
5. A.K. Lenstra and H.W. Lenstra, Jr., editors (1993). *The Development of the Number Field Sieve*, Volume 1554 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin.
6. A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, and J.M. Pollard (1990). The number field sieve. In *Proc. of the 22nd annual ACM Symposium on Theory of Computing*, pages 564–572, ACM, New York.
7. Peter L. Montgomery (1994). A survey of modern integer factorization algorithms. *CWI Quarterly*, **7**(4), 337–366.
8. J.M. Pollard (1993). Factoring with cubic integers. Pages 4–10 in [5].