THE NUMBER FIELD SIEVE: AN ANNOTATED BIBLIOGRAPHY

H. W. LENSTRA, JR.

In the present bibliography I list, in approximately chronological order, all literature that is directly related to the number field sieve.

1. J. M. Pollard, *Factoring with cubic integers*, this volume, pp. 4–10; manuscript, 6 pages, August 1988.

Pollard describes a new method for factoring integers of a special form, and he illustrates it by means of the factorization of the seventh Fermat number $F_7 = 2^{128} + 1$. He uses the ring of integers $\mathbf{Z}[\sqrt[3]{2}]$ of the number field $\mathbf{Q}(\sqrt[3]{2})$. No sieving in the number field takes place, so the name *number field sieve* is less appropriate for this early version of the method than for its descendants.

The manuscript was enclosed with a letter to A. M. Odlyzko, dated 31 August 1988, with copies to R. P. Brent, J. Brillhart, H. W. Lenstra, C. P. Schnorr, and H. Suyama. In this letter, Pollard speculated: "If F_9 is still unfactored, then it might be a candidate for this kind of method eventually?" The answer is in [7].

2. J. M. Pollard, *Factoring with cubic integers* (2), unpublished manuscript, 3 pages, December 1988.

This forms a footnote to the previous paper. It reports on the factorization of $2^{144} - 3$.

3. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard, *The number field sieve*, this volume, pp. 11–42; extended abstract: Proc. 22nd Annual ACM Symp. on Theory of Computing (STOC), Baltimore, May 14–16, 1990, 564–572.

The authors describe the first large-scale implementation of Pollard's new method, with several improvements. The extended abstract contains a rough outline of a heuristic complexity analysis, which indicates that the method is, for the numbers that it applies to, faster than all other known factoring methods. The last section of the extended abstract discusses an idea of Buhler and Pomerance for extending the number field sieve to general integers, and it sketches a solution to a problem that this extension gives rise to. The final version of the paper addresses the same issues in a more detailed manner, and it mentions developments that took place since the extended abstract was written. (*Note:* the

The author thanks Johannes Buchmann, Don Coppersmith, Dan Gordon, and John Pollard for their help. He was supported by NSF under Grant No. DMS–9002939 and by NSA/MSP under Grant No. MDA90–H–4043.

terminology *pf/fp* used in the extended abstract has been switched in all later papers, including the final version.)

4. D. M. Gordon, *Discrete logarithms in $GF(p)$ using the number field sieve*, SIAM J. Discrete Math. **6** (1993), 124–138; prepublication: 15 pages, April 27, 1990.

It is shown that the ideas underlying the number field sieve apply, in theory at least, also to the discrete logarithm problem.

5. L. M. Adleman, *Factoring numbers using singular integers*, Proc. 23rd Annual ACM Symp. on Theory of Computing (STOC), New Orleans, May 6–8, 1991, 64–71; prepublication: TR–20, Department of Computer Science, University of Southern California, 8 pages, September 4, 1990.

Adleman suggests the use of quadratic characters in order to recognize squares in the number field. This provides an alternative solution to the problem that the idea of Buhler and Pomerance gives rise to, and it improves the conjectural run time estimate for the number field sieve as it applies to integers that are not of a special form.

6. D. Coppersmith, *Modifications to the number field sieve*, J. Cryptology, to appear; prepublication: IBM Research Report #RC 16264, Yorktown Heights, New York, 16 pages, November 1990.

The combined use of several number fields leads to an improvement of the conjectural run time estimate of the number field sieve.

7. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), to appear.

The ninth Fermat number $F_9 = 2^{512} + 1$ was factored in 1990 by means of the number field sieve. The paper discusses several aspects of this factorization. It can be read as an introduction to the number field sieve.

8. J. M. Pollard, *The lattice sieve*, this volume, pp. 43–49; manuscript, 7 pages, September 1991.

Pollard advocates the use of a two-dimensional sieve in order to speed up the sieving process. It is not yet clear whether the idea leads to a practical improvement; see also [12].

9. O. Schirokauer, *On pro-finite groups and on discrete logarithms*, Ph. D. thesis, University of California, Berkeley, 68 pages, May 1992.

In the second chapter (46 pp.) of his thesis, Schirokauer considers the application of the number field sieve to the discrete logarithm problem. Through the use of l-adic logarithms he achieves a better conjectural run time than in [4] (see the introduction to [3]). Practical issues are not considered.

10. J. P. Buhler, H. W. Lenstra, Jr., C. Pomerance, *Factoring integers with the number field sieve*, this volume, pp. 50–94.

This paper describes the number field sieve as it applies to integers that are not necessarily of a special form. The description incorporates Adleman's idea [5]. An elaborate complexity analysis is given, and several possible practical improvements are discussed.

11. J.-M. Couveignes, *Computing a square root for the number field sieve*, this volume, pp. 95–102.

One step in Adleman's version of the number field sieve [5; 10] involves a computation with exceedingly large numbers. Couveignes develops a method for avoiding this.

12. D. J. Bernstein, A. K. Lenstra, *A general number field sieve implementation*, this volume, pp. 103–126.

The title explains itself. The implementation applies to "general" integers, but almost all examples given are integers of a special form. It remains to be decided whether the number field sieve will eventually be the method of choice for large integers.

13. D. M. Gordon, *Designing and detecting trapdoors for discrete log cryptosystems*, Advances in cryptology, Crypto '92, to appear.

Gordon discusses the applicability of the number field sieve to the construction of trapdoors in cryptological systems that are based on the discrete logarithm problem.

14. J. Buchmann, J. Loho, J. Zayer, *An implementation of the general number field sieve*, extended abstract, Fachbereich Informatik, Universität des Saarlandes, 7 pages, May 1993.

This report describes the authors' practical experience with their first implementation. They factor three "general" integers of 29, 40, and 49 digits.

Department of Mathematics, University of California, Berkeley, CA 94720, U.S.A.
E-mail address: hwl@math.berkeley.edu