



Springer

1st
edition

1993, VIII, 140 p.

Mathematics : Applications of Mathematics

Lenstra, Arjen K., Lenstra, Hendrik W.Jr. (Eds.)

The Development of the Number Field Sieve

The number field sieve is an algorithm for finding the prime factors of large integers. It depends on algebraic number theory. Proposed by John Pollard in 1988, the method was used in 1990 to factor the ninth Fermat number, a 155-digit integer. The algorithm is most suited to numbers of a special form, but there is a promising variant that applies in general. This volume contains six research papers that describe the operation of the number field sieve, from both theoretical and practical perspectives. Pollard's original manuscript is included. In addition, there is an annotated bibliography of directly related literature.

Order online at [springer.com/booksellers](https://www.springer.com/booksellers)
Springer Nature Customer Service Center LLC

233 Spring Street
New York, NY 10013
USA

T: +1-800-SPRINGER NATURE
(777-4643) or 212-460-1500
customerservice@springernature.com

Printed book

Softcover

Printed book

Softcover

ISBN 978-3-540-57013-4

\$ 49,95

Available

Discount group

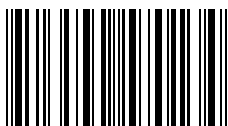
Professional Books (2)

Product category

Proceedings

Series

Lecture Notes in Mathematics



ISBN 978-3-540-57013-4 / BIC: PBW / SPRINGER NATURE: SCM13003

Prices and other details are subject to change without notice. All errors and omissions excepted. Americas: Tax will be added where applicable. Canadian residents please add PST, QST or GST. Please add \$5.00 for shipping one book and \$ 1.00 for each additional book. Outside the US and Canada add \$ 10.00 for first book, \$5.00 for each additional book. If an order cannot be fulfilled within 90 days, payment will be refunded upon request. Prices are payable in US currency or its equivalent.

Part of **SPRINGER NATURE**