🙆 Springer

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

The Development of the Number Field Sieve



1993, VIII, 140 p.

ecture Notes in Mathematics

Printed book

Softcover 34,95 € | £31.99 | \$49.95 ^[1]37,40 € (D) | 38,45 € (A) | CHF 50,55

eBook

28,88 € | £24.99 | \$34.99 ^[2]28,88 € (D) | 28,88 € (A) | CHF 40,00

Available from your library or springer.com/shop

MyCopy^[3]

Printed eBook for just € | \$ 24.99 springer.com/mycopy Arjen K. Lenstra, Hendrik W.Jr. Lenstra (Eds.)

The Development of the Number Field Sieve

Series: Lecture Notes in Mathematics

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 / or for the Americas call (toll free) 1-800-SPRINGER / or email us at: customerservice@springernature.com. / For outside the Americas call +49 (0) 6221-345-4301 / or email us at: customerservice@springernature.com.

The first \in price and the £ and \$ price are net prices, subject to local VAT. Prices indicated with [1] include VAT for books; the \in (D) includes 7% for Germany, the \in (A) includes 10% for Austria. Prices indicated with [2] include VAT for electronic products; 19% for Germany, 20% for Austria. All prices exclusive of carriage charges. Prices and other details are subject to change without notice. All errors and omissions excepted. [3] No discount for MyCopy.

