

# Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications



---

## Authors/ Affiliations

Murray R. Bremner, *University of Saskatchewan, Saskatoon, Canada*

## Features:

- Includes numerous algorithms in structured form (without go to statements) in both pseudocode and Maple
- Presents the essential concepts that should be familiar to all users of lattice algorithms
- Based on fundamental research papers on lattice basis reduction and its applications
- Designed as a complete introduction for non-specialists: the only prerequisites are basic linear algebra and elementary number theory
- Includes two applications to cryptography: knapsack cryptosystems, and Coppersmith's algorithm
- Includes two applications to computer algebra: polynomial factorization, and the Hermite normal form of an integer matrix

---

## About the Book:

First realized in the 1980s by Lenstra, Lenstra, and Lovasz, the LLL algorithm was originally intended to factor polynomials with rational coefficients. It improved upon the existing lattice reduction algorithm in order to solve integer linear programming problems and was later adapted for use in cryptanalysis. This book provides an introduction to the theory and applications of lattice basis reduction and the LLL algorithm. With numerous examples and suggested exercises, the text discusses various applications of lattice basis reduction to polynomial factorization, cryptography, number theory, and matrix canonical forms.

---

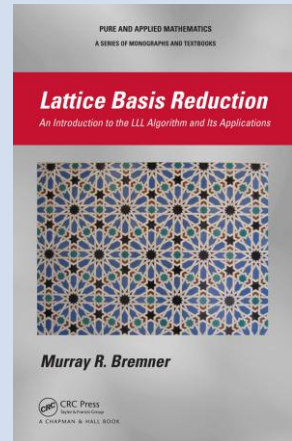
## Select Content:

Introduction to Lattices. Two-Dimensional Lattices. Gram-Schmidt Orthogonalization. The LLL Algorithm. Deep Insertions. Linearly Dependent Vectors. The Knapsack Problem. Coppersmith's Algorithm. Diophantine Approximation. The Fincke-Pohst Algorithm. Kannan's Algorithm. Schnorr's Algorithm. NP-Completeness. The Hermite Normal Form. Polynomial Factorization.

---



**New!**



**Catalog no. K10358**  
**August 2011**  
**Hardback**  
**ISBN: 9781439807026**  
**\$89.95**

---

Order online at:  
[www.crcpress.com](http://www.crcpress.com)  
to get FREE standard shipping.  
**\*Use Promo Code**  
**195CM**  
**to apply discount.**  
*Offer expires 12/31/11.*

---

**SIGN UP ONLINE AND  
RECEIVE INFORMATION  
ABOUT OUR LATEST  
OFFERINGS AND SPECIAL  
DISCOUNTS!**

CRC Press/Taylor & Francis Group  
6000 Broken Sound Parkway, NW Suite 300  
Boca Raton, FL 33487  
Tel: 1-800-272-7737  
Fax: 1-800-374-3401  
e-mail: [orders@taylorandfrancis.com](mailto:orders@taylorandfrancis.com)