89i:11142 11Y16 05A05 11H55 68Q25 90C10

Radziszowski, Stanisław P. (1-RIT); **Kreher, Donald L.** (1-RIT)

Solving subset sum problems with the L^3 algorithm.

J. Combin. Math. Combin. Comput. **3** (1988), 49–63.

This paper presents ideas that speed up the lattice basis reduction algorithm of H. W. Lenstra, Jr., A. K. Lenstra and L. Lovasz [Math. Ann. 261 (1982), no. 4, 515–534; MR 84a:12002] for lattice bases with long integer vectors. A method is proposed to reduce the multiprecision operations on large integers. When given a lattice basis $b_1, \cdots, b_n \in \mathbf{Z}^n$ consisting of large integer vectors the LLL-reduction algorithm is successively applied to the integer part of the vectors $b_1/2^k, \cdots, b_n/2^k$ where k is chosen such that the coordinates of these vectors fit into single word size. After each pass through the reduction the transformation of the reduction is applied to the current full size basis $b_1, \cdots, b_n$. The paper describes these ideas in detail for lattices of the particular form arising from the subset sum (exact knapsack) problem. The authors report extensive computational tests showing that this algorithm performs better than the algorithm of J. C. Lagarias and A. M. Odlyzko [J. Assoc. Comput. Mach. 32 (1985), no. 1, 229–246; MR 87i:11186]. It is faster, and higher density subset sum problems are solved. *Claus-Peter Schnorr* (D-FRNK)