EXTENDED GCD AND HERMITE NORMAL FORM ALGORITHMS VIA LATTICE BASIS REDUCTION

GEORGE HAVAS, BOHDAN S. MAJEWSKI, AND KEITH R. MATTHEWS

Abstract. Extended gcd calculation has a long history and plays an important role in computational number theory and linear algebra. Recent results have shown that finding optimal multipliers in extended gcd calculations is difficult. We present an algorithm which uses lattice basis reduction to produce small integer multipliers $x_1, \ldots, x_m$ for the equation $s = \gcd(s_1, \ldots, s_m) = x_1 s_1 + \cdots + x_m s_m$, where $s_1, \ldots, s_m$ are given integers. The method generalises to produce small unimodular transformation matrices for computing the Hermite normal form of an integer matrix.