

ICM-9403-62 Parallelization of The Sparse Modular GCD Algorithm for Multivariate Polynomials on Shared Memory Multiprocessors, Mohamed Omar Rayes, Paul S. Wang, and Ken Weber.

ABSTRACT Reported are experiences and practical results from parallelizing the modular GCD algorithm for sparse multivariate polynomials. The strategy is to identify key computation steps in the sequential algorithm and implement them in parallel. The two major steps of the sequential algorithm—computing the GCD modulo several primes and applying the Chinese Remainder Algorithm on the integer coefficients—are easily partitioned into independent subtasks. The subtask of computing the GCD modulo one prime can be subdivided further. Several parallel strategies for the multivariate GCD modulo a prime are presented. Actual timings on a Sequent Balance with 26 processors are presented.