

ICM-9201-25 Parallel Univariate p -adic Lifting on Shared-Memory Multiprocessors, Paul S. Wang.

ABSTRACT: Parallelization of univariate p -adic lifting, a procedure important in modern gcd and factorization algorithms, is presented. The strategy is to take the fastest known sequential algorithm and parallelize its key steps: lift basis, residue, correction coefficients, updating factors, detecting true factors, and reformulation for continued lifting. Both linear and quadratic lifting are investigated. A new procedure for reformulating the lifting after finding true factors speeds up the sequential and the parallel lifting. PLIFT, a software package written in C for a 26-processor Sequent Balance, implements the parallel algorithms. Timing results are given in an appendix.