Factoring Integers with Large-Prime Variations of the Quadratic Sieve

Herman J. J. te Riele

Abstract

This article is concerned with the large-prime variations of the multipolynomial quadratic sieve factorization method: the PMPQS (one large prime) and the PPMPQS (two). We present the results of many factorization runs with the PMPQS and PPMPQS on SGI workstations and on a Cray C90 vector computer. Experiments show that for our Cray C90 implementations PPMPQS beats PMPQS for numbers of more than 80 digits, and that this crossover point goes down with the amount of available central memory.

For PMPQS we give a formula to predict the total running time based on a short test run. The accuracy of the prediction is within 10% of the actual running time. For PPMPQS we do not have such a formula. Yet in order to provide measurements to help determining a good choice of the parameters in PPMPQS, we factored *many* numbers. In addition we give an experimental prediction formula for PPMPQS suitable if one wishes to factor many large numbers of about the same size.