Factorization Ambiguity in Algebraic Number Fields: Schönhage-Strassen Algorithm

Vladimir Chernov, Alexander Kalouguine

The multiplication of long numbers using number-theoretical transform (NTT) is considered. It is known that prime numbers with computer-friendly operations modulo p are few and far between (e.g. Mersenne numbers, Fermat numbers etc.). The direct use of NTT modulo nonprime numbers is concerned with some difficulties. These difficulties are caused by existence of zero divisors in corresponding modular rings.

"Bitwise" implementation of arithmetic operations over modular rings generated by Mersenne and Fermat prime numbers has some advantages. In modular rings generated by the integer divisors of Mersenne and Fermat numbers these advantages are not inherited.

The following scheme is proposed for discrete convolution computation.

1. The residue class ring $\mathbf{Z}/m\mathbf{Z}$ modulo composite m is embedded into its algebraic extension **W.**

2. **W** is chosen so that m factorization contains only primes in **W** with the form $p_j = \alpha_j^{k_j} \pm 1$.

3. Convolution computation is carried out using traditional parallel scheme. The set of discrete transforms (NTT analogous) in the system of residue class rings $(\bmod\, p_j)$ is used. Reconstruction of convolution values $(\bmod\, m)$applying the Chinese remainder theorem.

The effectiveness of the proposed scheme results from the effective computations on the data represented in the non-traditional number systems. Among them I.Katai canonical number systems and their generalizations are investigated. In this particular case the NTT analogues are multiplication-free.