Determination of a good indicator for estimated prime factor and its modification in Fermat's Factoring Algorithm

ABSTRACT

Fermat's Factoring Algorithm (FFA) is an integer factorisation methods factoring the modulus N using exhaustive search. The appearance of the Estimated Prime Factor (EPF) method reduces the cost of FFA's loop count. However, the EPF does not work for balanced primes. This paper proposed the modified Fermat's Factoring Algorithm 1-Estimated Prime Factor (mFFA1-EPF) that improves the EPF method. The algorithm works for factoring a modulus with unbalanced and balanced primes, respectively. The main results of mFFA1-EPF focused on three criteria: (i) the approach to select good candidates from a list of convergent continued fraction, (ii) the establishment of new potential initial values based on EPF, and (iii) the application of the above modification upon FFA. The resulting study shows the significant improvement that reduces the loop count of FFA1 via (improved) EPF compared to existing methods. The proposed algorithm can be executed without failure and caters for both the modulus N with unbalanced and balanced primes factor. The algorithm works for factoring a modulus with unbalanced and balanced primes.

Keyword: Estimated prime factor; Integer factorisation problem; Continued fraction; Fermat's Factoring Algorithm