Toom-Cook

Sai Krishna Yedugani.
#991727920

Abstract

In the present scientific computation multiplication of large numbers is vastly used. There are only few algorithms that gain efficiency through this large interger multication. Toom cook and Karatsuba area the well known techniques in multiplying univariate polynomials and long intergers. In this paper we work on the classical Toom-k way of dealing with the multiplication of large integers.

1 Introduction

Dealing with complex multiplications with our mind is completely out of bound. We use calculators or some computer applications to do calculations. With these applications we can work on upto 8 digits and the result we get is about 15 digits, and is accurate. Whereas, for the digits more than this rounding off is done. There comes the issue when one needs to work on large integers i.e more than 8 digits and getting the perfect result. For these complex computations scientist have devised some special routines, and this led to the invention of some algorithms. Few of these popular algorithms are Toom-Cook and Karatsuba Algorithm and Schonhage-Strassen algorithm(SSA).

The Toom-Cook algorithm follows the divide and conquer method for multiplying large integers. Just like Karatsuba it splits the given integer into n limbs of some fixed size. The division is then applied recursively with Toom-3 algorithm. This goes on until we are able to apply another algorithm on it for the last stage of recursion, or until the desired multiplier is reached.

The method works on the principles of polynomial multiplication. The input numbers are divided into limbs of a given size, and each in the form of polynomial, and the limb size is used as radix. Instead of multiplying the obtained polynomials directly, they are evaluated at a set of points, and the values multiplied together at those points. Based on the products obtained at those points the product polynomial is obtained. The final result is then obtained by substituting the radix.

2 History

Toom Cook algorithm is developed by Andrei Toom in 1963 and is later improved and published by Stephen Cook in his Phd thesis. Toom Cook Algorithm is also referred as Toom 3 which is the collective name for all Toom Cook based algorithms. Toom Cook is the faster generalisation of the Karatsuba method. Unllike Karatsuba it deals with 3 parts rather than 2 parts which makes it even more complex.