Arithmetic in large ring and field extension is an important problem in Computer Algebra. It consists essentially of the combination of one multiplication and one division in the underlying ring $R$. Methods are known for replacing one division by two short multiplications in $R$, which can be performed essentially by using convolutions.

The author shows that, using school-book multiplication, modular multiplication may be grouped into $2M(R)$ operations (where $M(R)$ denotes the number of operations involved by one multiplication in $R$), the short multiplication problem is an important obstruction to convolution. It raises the cost in this case to $3M(R)$. This paper contains a very detailed study of this problem and gives a method to replace this cost to roughly $2M(R)$, using also fast convolutions.

Reviewer: Maurice Mignotte (Strasbourg)

MSC:
11Y16 Number-theoretic algorithms; complexity
68W30 Symbolic computation and algebraic computation

Keywords:
convolutions; fast arithmetic; FFT

Software:
NTL; LiDIA

Full Text: DOI

References:


[16] LiDIA: A C++ Library For Computational Number Theory, http://www.informatik.tu-darmstadt.de/TF/LiDIA


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.