

Karatsuba laboratory documentation

Algorithms:

- Regular polynomial multiplication
- Karatsuba algorithm

Parallelization – Java ThreadPool combined with runnable object

Regular multiplication: $O(n^2)$

Distribute every term in each polynomial and combine them by the degree of the exponents.

Karatsuba algorithm: $O(n^{\log 3})$

Divide and conquer approach to multiply 2 numbers.

<https://eprint.iacr.org/2006/224.pdf>

Polynomial degree	Simple sequential	Simple parallelized	Karatsuba sequential	Karatsuba parallelized
10	1 ms	20 ms	1 ms	15 ms
100	5 ms	22 ms	21 ms	18 ms
1000	41 ms	95 ms	78 ms	35 ms
10.000	1223 ms	536 ms	890 ms	300 ms