

Algorithms for Integer Multiplication and their Time Complexities

January 4, 2021 8:06 PM

Let $a, b \in \mathbb{Z}$ be of length n digits.

The classical (gradeschool) algorithm does $O(n^2)$ bit operations.

1960 Karatsuba $O(n^{1.585})$

1963 Cook & Toomb $O(n^{1+\epsilon})$

Toomb 3,2 $T(n) = 3T(n/2) + cn$ $O(n^{1.585})$

Toomb 5,3 $T(n) = 5T(n/3) + cn$ $O(n^{1.465})$

\vdots

1971 Schönhage & Strassen $O(n \log n \log \log n)$

2019 Harvey & van der Hoven $O(n \log n)$

GMP uses Classical, Karatsuba, Toomb 5,3 and Schönhage–Strassen

Can we multiply in $O(n)$? Open.