

Polynomial Multiplication Algorithm Timing Data

Polynomial multiplication in $\mathbb{Z}_p[x]$ for $p = 3 \times 5 \times 2^{27} + 1 = 2013265921$
Run on an Intel Core i7 2600 at 3.4 GHz
Implementation in C compiled with gcc -O3

Timings in CPU seconds for 10,000 multiplications: Jan 29, 2019

Degree	d=50	100	200	400	800	1600	3200	6400	12800	25600
Classical	0.027	0.100	0.378	1.482	5.754	23.01	91.54	365.3	1448.	5796.
Karatsuba	0.044	0.118	0.330	0.960	2.824	8.36	24.82	73.1	219.3	658.4
FFT	0.057	0.121	0.264	0.570	1.220	2.60	5.56	11.7	24.8	52.6

$5796/1448 = 4.003$ and $658.4/219.3 = 3.002$.