# Exercise to prepare for 2023-09-28

## The Toom–Cook Algorithm

Let $\mathbb{A}$ be a ring (for simplicity, it can be assumed to be commutative).

1. Estimate the number of multiplications in $\mathbb{A}$ needed by Karatsuba's algorithm to compute the product $AB$ of any two polynomials $A$ and $B$ of degree at most 3 in $\mathbb{A}[X]$.

2. Let us assume that 2, 3, and 5 are invertible in $\mathbb{A}$ and that the divisions of elements of $\mathbb{A}$ by 2, 3, and 5 are free. Describe an algorithm that multiplies $A$ and $B$ of degree at most 3 using at most 7 multiplications in $\mathbb{A}$.
   *Hint: get inspiration from Karatsuba's algorithm.*

3. Let us assume that 2, 3, and 5 are invertible in $\mathbb{A}$. Describe an algorithm which computes the multiplication of two polynomials of degree at most $n$ in $\mathbb{A}[X]$ using $O(n^{\log_4(7)}) \subset O(n^{1.41})$ operations in $\mathbb{A}$ (additions and multiplications in $\mathbb{A}$).

In what follows, we assume that the ring $\mathbb{A}$ has characteristic zero.

4. Show that, for any integer $\alpha \geq 2$, there exists an algorithm for polynomial multiplication in $\mathbb{A}[X]$ whose arithmetic complexity is $O(n^{\log_\alpha(2\alpha-1)})$.

5. Show that for all $\varepsilon > 0$, there exists an algorithm for polynomial multiplication in $\mathbb{A}[X]$ whose arithmetic complexity is $O(n^{1+\varepsilon})$, where the implied constant in the $O(\cdot)$ depends on $\varepsilon$ but not on $n$.