Exercise 1: Karatsuba / Toom-Cook multiplication (4 points)

For multiplying two integers $a$ and $b$, Karatsuba’s method uses the fact that

\[ a \cdot b = a^{(0)} \cdot b^{(0)} + \left( (a^{(0)} + a^{(1)}) \cdot (b^{(0)} + b^{(1)}) - a^{(0)} \cdot b^{(0)} - a^{(1)} \cdot b^{(1)} \right) \cdot B + a^{(1)} \cdot b^{(1)} \cdot B^2, \]

where $a = a^{(0)} + a^{(1)} \cdot B$ and $b = b^{(0)} + b^{(1)} \cdot B$ with $a^{(i)}, b^{(i)} \in \{0, \ldots, B - 1\}$ for $i = 0, 1$.

(a) In each recursion step of Toom-Cook-$k$ multiplication, a similar relation as in (1) is used. Choose any interpolation points $x_0, \ldots, x_4$ and provide a corresponding relation for Toom-Cook-3.

(b) How do we have to choose the interpolation points $x_0, x_1, x_2$ in Toom-Cook-2 to obtain exactly the same relation as in (1)?

(Hint: You may also choose $x_i = \infty$ for some $i$, where we define $f(\infty) = a_n$ for an arbitrary polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$.)

Exercise 2: Error bound for approximate interval arithmetic (4 points)

Prove Theorem I.3.2.5.

Exercise 3: Box functions and root finding (4 points)

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ be an arbitrary polynomial with integer coefficients. Our goal is to count all real roots of $f$, provided that $f$ has only simple roots.

(a) Show that all real roots of $f$ have absolute value bounded by $M := 1 + \max_{0 \leq i \leq n} \frac{|a_i|}{a_n}$.

(b) Use box functions for $f$ and its derivative $f'$ to derive a method that allows you to decide whether a certain interval $I$ contains no root or exactly one root. Your method may fail (with the output “I don’t know”); however, it should succeed for sufficiently small intervals $I$.

(c) Formulate an algorithm to determine the number of real roots of $f$.

(Hint: By Rolle’s theorem, any interval $I$ which contains more than one root of $f$ also contains a root of its derivative $f'$.)
Exercise 4: Gaussian elimination (4 points + 4 bonus points for ⋆)

Let $A = (a_{ij})_{1 \leq i, j \leq n}$ be an $n \times n$-matrix with integer entries $a_{ij}$ of absolute values bounded by $M$.

(a) Give an upper bound $B$ for the absolute value of the determinant of $A$, such that $\log B$ has polynomial size in $n$ and $\log M$.

(b) We now consider Gaussian elimination with pivoting in order to compute $\det A$.

Let $A^{(0)} := A$ and $A^{(k)}$ be the matrix obtained after $k$ elimination steps. $A^{(k)}$ has rational coefficients $a^{(k)}_{ij}$, and it holds that $a^{(k)}_{ii} \neq 0$ for all $i = 1, \ldots, k$ and $a^{(k)}_{ij} = 0$ for all $i > j$ and $j = 1, \ldots, k$.

The pivoting rule is as follows: Let $r$ be the smallest row index with $r \geq k + 1$ such that $a^{(k)}_{r,k+1} \neq 0$. If no such $r$ exists, then $\det A = 0$ and we finish immediately. Otherwise, we exchange the row $r$ with row $k + 1$. This yields the matrix $A^{(k)} = (\bar{a}^{(k)}_{ij})$. We then define

$$
\bar{a}^{(k+1)}_{ij} := \begin{cases} 
\bar{a}^{(k)}_{ij} & \text{for } i \leq k \\
\frac{\bar{a}^{(k)}_{i,k+1}}{\bar{a}^{(k)}_{k+1,j}} \cdot \bar{a}^{(k)}_{k+1,j} & \text{for } i \geq k + 1.
\end{cases}
$$

⋆ Prove that, for any $k$ and any $a^{(k)}_{ij}$ with $k + 1 \leq i, j \leq n$, it holds that $a^{(k)}_{11} a^{(k)}_{22} \cdots a^{(k)}_{kk}$ as well as $a^{(k)}_{11} a^{(k)}_{22} \cdots a^{(k)}_{kk} \cdot a^{(k)}_{ij}$ can be written as the determinant of a submatrix of $A$, up to some unit factor ($\pm 1$).

• Conclude that all intermediate values created by the Gaussian elimination algorithm can be represented with a number of digits that is polynomial in $\log M$ and $n$.

• Show that, when using fixed point arithmetic, a precision $\rho$ that is polynomial in $\log M$ and $n$ is sufficient to compute $\det A$.

• Show that computing the inverse $A^{-1}$ has a bit complexity that is polynomial in $\log M$ and $n$. 

2 / 2