Exercise 1 (+): Approximate Polynomial Evaluation (4 bonus points)

Let $x_1, x_2, \ldots, x_{d+1}$ be pairwise distinct real values and $f \in \mathbb{R}[x]$ a polynomial of degree $d$. We assume the existence of an oracle that provides arbitrary good fixed point approximations of the values $x_i$ as well as of the coefficients of $f$. Give an algorithm to compute an $i$ with $f(x_i) \neq 0$ and to compute the sign of $f(x_i)$. Can you estimate the running time of the algorithm with respect to $d$, the size of the coefficients of $f$ and $\max_i |f(x_i)|$?

Hint: Use the fact that $\max_i |f(x_i)| \neq 0$ as $f$ has at most $d$ distinct roots. Then, use fixed point arithmetic to evaluate $f$ at the points $x_i$ with increasing precision.

Exercise 2: Discrete Fourier transform (4 points)

Let $F = \mathbb{Z}/29\mathbb{Z}$.

1. Find a primitive 4-th root of unity $\omega \in F$ and compute its inverse $\omega^{-1} \in F$.

2. Consider the $4 \times 4$ - Vandermonde matrices $V_\omega = \text{Vand}(1, \omega, \omega^2, \omega^3)$ and $V_{\omega^{-1}} = \omega^3$, and check that their product is $4I_4$, where $I_4$ denotes the identity matrix in $F^{4 \times 4}$.

Exercise 3: Fast Fourier Transform (4 points)

Use the Fast Fourier Transform to compute $\text{DFT}_\omega(f)$ for a general polynomial $f = a_3x^3 + a_2x^2 + a_1x + a_0$ and $\omega = i$ a primitive 4-th root of unity.

Exercise 4: Fast polynomial multiplication (4 points)

The complex number $\omega = e^{2\pi i/8} = \cos(\pi/4) + i \cdot \sin(\pi/4) \in \mathbb{C}$ is a primitive 8-th root of unity. Let $f = 5x^3 + 3x^2 - 4x + 3$ and $g = 2x^3 - 5x^2 + 7x - 2 \in \mathbb{C}[x]$, and run the Fast Convolution algorithm to compute the coefficients of the product $f \cdot g$. You may use a numerical approximation of $\omega$ and carry out the computations with a pocket calculator. You do not need to estimate the occurring errors.

Exercise 5: Existence of primitive roots in prime fields (4 points)

Denote by $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the finite field with $p$ elements for some prime $p$, and let $n \in \{1, \ldots, p-1\}$. Show that $\mathbb{F}_p$ contains a primitive $n$-th root of unity if and only if $n$ divides $p-1$, and conclude that the multiplicative group $\mathbb{F}_p^\times$ of $\mathbb{F}_p$ is cyclic.
Hints: 1. Use (without proof) Fermat’s little theorem: If \( p \in \mathbb{N} \) is prime and \( a \in \mathbb{Z} \) arbitrary, then
\[
a^p \equiv a \mod p.
\]
In particular, if \( a \in \{1, \ldots, p-1\} \), then
\[
a^{p-1} \equiv 1 \mod p.
\]

2. Let \( q \in \mathbb{N} \) be a divisor of \( p-1 \) and \( q = q_1^{e_1} \cdots q_r^{e_r} \) its prime factorization. For \( a \in \mathbb{F}_p^\times \), we denote by \( \text{ord}(a) := \min\{i \in \mathbb{N}_{>0} : a^i = 1\} \) the order of \( a \) in \( \mathbb{F}_p^\times \).
Prove the following facts:

- \( \text{ord}(a) = q \) if and only if \( a^q = 1 \) and \( a^{q/q_i} \neq 1 \) for \( i = 1, \ldots, r \).
- For each \( i \), \( \mathbb{F}_p^\times \) contains an element \( a_i \) with \( q_i^{e_i} | \text{ord}(a_i) \). Conclude that there is an element \( b_i \) with \( \text{ord}(b_i) = q_i^{e_i} \).
- If \( a, b \in \mathbb{F}_p^\times \) are elements of coprime orders, then \( \text{ord}(ab) = \text{ord}(a) \text{ord}(b) \).
- \( \mathbb{F}_p^\times \) contains an element of order \( q \).

3. Keep on going if you cannot prove one of the hints. Depending on your background in algebra, you may also want to try out other ways to solve this exercise.