Aufgabe 9.1 (4 Punkte)

Beweise, dass der Algorithmus FFT (Skript vom 14.12., Seite 8) eine Laufzeit von $O(n \log n)$ hat.

Aufgabe 9.2 (4 Punkte)

Zeige, dass die Determinante der Vandermonde Matrix

$$\det V(x_0, \ldots, x_{n-1}) = \det \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} \end{pmatrix} = \Pi_{0 \leq j < k \leq n-1}(x_k - x_j)\,.$$

Damit ist $\det V(x_0, \ldots, x_{n-1}) \neq 0$ für paarweise verschiedene x_i und damit invertierbar.

Aufgabe 9.3 (4 Punkte)

Berechne effizient $DFT(a, \omega)$ für den Koeffizientenvektor $a = (1, 6, 2, 2, 0, 3, 4, 1)$.

Wir betrachten im Folgenden eine Version von DFT für Polynome mit ganzzahlige Koeffizenten. Sei dazu $m = m_n = 2^{\frac{tn}{2}} + 1$ für ein beliebiges $t \in \mathbb{N}$. Wir betrachten nun Polynome $A(x), B(x) \in \mathbb{Z}_m[x]$ mit Koeffizientenvektoren, $a = (a_0, \ldots, a_n)$, $b = (b_0, \ldots, b_n)$ mit $a_i, b_i \in \mathbb{Z}_m$ für alle $i = 1, \ldots, n$.

Aufgabe 9.4 (4 Punkte)

Wir nutzen nun $\omega = 2^t \in \mathbb{Z}_m^*$ anstatt ω_n als "n-te Einheitswurzel".

a) Zeige, dass $(\langle \omega \rangle, \cdot)$ eine multiplikative, zyklische Untergruppe der Ordnung n von $\mathbb{Z}_m^*$ ist.
b) Zeige: Je zwei ω^k, $\omega^{k'}$ für $k, k' \in \{0, \ldots, n-1\}$ haben dasselbe Quadrat.

Bonusaufgabe 9.5 (4 Punkte)

Formuliere die Algorithmen DFT und DFT^{-1} für Polynome über $\mathbb{Z}_m^*$, die die Umrechnung von Koeffizienten in Punkt-Werte-Form (bzw. zurück) in Laufzeit $O(n \log n)$ durchführen. Beweise, dass diese Algorithmen korrekt sind, und begründe die Laufzeitschranke.

Frohe Weihnachten und einen Guten Rutsch!

Präsenzaufgabe 9.6

Berechne die Determinante der Vandermonde Matrix

$$V(1,2,3,4) = \begin{pmatrix} 1 & 1 & 1^2 & 1^3 \\ 1 & 2 & 2^2 & 2^3 \\ 1 & 3 & 3^2 & 3^3 \\ 1 & 4 & 4^2 & 4^3 \end{pmatrix}$$

Präsenzaufgabe 9.7

Berechne effizient $DFT(a, \omega)$ für den Koeffizientenvektor $a = (1, 2, 3, 4)$.

Präsenzaufgabe 9.8

Ist $g(x) = x^3 + x^2 + 4 \in \mathbb{Z}_5[x]$ ein Teiler von $f(x) = 3x^5 + 3x^3 - x^2 + 3 \in \mathbb{Z}_5[x]$?