In diesem Übungsblatt geht es Divide-and-Conquer Algorithmen bei Polynomen. Die Polynome haben "Zahlen" als Koeffizienten, die Elemente eines Körpers sind und mit denen man die üblichen Rechenoperationen $(+, -, \cdot, /, \text{mod})$ in jeweils konstanter Zeit durchführen kann. Die Polynome sind als Folge ihrer Koeffizienten dargestellt, z.B. das Polynom

$$A(x) = a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n$$

durch die Folge $\langle a_0, a_1, a_2, \ldots, a_n \rangle$.

Sie können annehmen, dass für Polynome $A(x)$ und $B(x)$ vom Grad n das Produktpolynom $A(x) \cdot B(x)$ in $O(n \log n)$ Zeit berechnet werden kann. Die Summe $A(x) + B(x)$ kann natürlich in $O(n)$ Zeit gefunden werden, die Differenz auch.

Für Polynom P vom Grad n und Zahlenmenge S der Kardinalität n bedeutet *Simultanevaluation von P auf S* die Berechnung der Menge $\{(s, P(s)) | s \in S\}$. Sie können annehmen, dass das Problem der Simultanevaluation in Zeit $O(n \log^2 n)$ gelöst werden kann.

1. (20 Punkte)
   Es sei S eine Menge von n Zahlen. Definiere das Polynom $F_S(x)$ als jenes monische Polynom (monisch bedeutet, der Koeffizient des höchstgradigen Monoms ist 1), dessen Nullstelln genau die Zahlen in S sind. Offensichtlich gilt
   $$F_S(x) = \prod_{s \in S} (x - s)\,.$$
   Zeigen Sie, dass dieses Polynom, genauer gesagt seine Koeffizietendarstellung, in $O(n \log^2 n)$ Zeit berechnet werden kann.

2. (30 Punkte)
   Das Problem der Polynominterpolation ist folgendes: Gegeben ist eine Menge $U = \{(s_i, v_i) | 1 \leq i \leq n\}$ von n Zahlenpaaren, sodass keine zwei Paare in der ersten Komponente übereinstimmen, also $s_i \neq s_j$ für $i \neq j$. Gesucht ist ein Polynom F_U vom Grad $n-1$, sodass für jedes $(s, v) \in U$ gilt $F_U(s) = v$.

   Entwickeln Sie einen Divide-and-Conquer Algorithmus, der das Polynominterpolationsproblem in $O(n \log^3 n)$ Zeit löst.

   Hinweis: Es sei U' die Menge, die man aus U bekommt, wenn man $v_1, \ldots, v_{n/2}$ alle durch 0 ersetzt, und es sei U'' die Menge, die man aus U erhält, wenn man $v_{n/2+1}, \ldots, v_n$ durch 0 ersetzt. (Bei ungeradem n verfahren Sie entsprechend.)

   Es gilt dann offensichtlich $F_U = F_{U'} + F_{U''}$. Es bleibt dann nur die Frage, wie man die beiden Polynome $F_{U'}$ und $F_{U''}$ berechnet. Versuchen Sie, jedes dieser beiden Polynome als Produkt zweier Polynome darzustellen, sodass eines so wie in Frage 1 berechnet werden kann, das andere aber, leicht manipuliert, als rekursives Unterproblem.

Zusatzaufgaben

In den folgenden Aufgaben geht es um multiple Evaluation und um Interpolation von Polynomen für besondere Wertemengen, nämlich n-te Einheitswurzeln, das Zahlen ϕ, für die gilt $\phi^n = 1$, also Wurzeln des Polynoms $x^n - 1$. Damit das interessant ist, bewegen wir uns im Körper der komplexen Zahlen. Wir nehmen ein Rechenmodell an, das mit komplexen Zahlen hantieren kann, insbesondere die 4 Grundrechenoperationen in konstanter Zeit durchführen kann. Weiters nehmen wir an, dass die primitive n-te Einheitswurzel $\omega = e^{2\pi i/n}$ in konstanter Zeit berechnet werden kann. Jede n-te Einheitswurzel ist dann als ω^j darstellbar, $1 \leq j \leq n$. Insbesondere gilt $\omega^{n/2} = -1$ und $\omega^n = 1$. Wir nehmen hier an, dass n gerade ist, ja, wir nehmen im Weiteren sogar an, dass n eine Zweierpotenz ist, also $n = 2^k$.

Beachten Sie folgende algebraischen Indentitäten:

$$x^{2m} - a^{2\ell} = (x^m - a^\ell)(x^m + a^\ell)\,, \qquad \text{insbesondere}$$

$$x^{2m} - \omega^{2\ell} = (x^m - \omega^\ell)(x^m + \omega^\ell) = (x^m - \omega^\ell)(x^m - \omega^{n/2}\omega^\ell) = (x^m - \omega^\ell)(x^m - \omega^{\ell+n/2})\,.$$

3. (2 Punkte) Sei $P(x)$ ein Polynom vom Grad m und $B(x) = x^\ell - a$ ein Binom. Zeigen Sie, dass sich $P(x) \cdot B(x)$, $P(x)$ mod $B(x)$ in $O(m)$ Zeit berechnen lassen.

4. (20 Punkte) Es sei $P(x)$ ein Polynom vom Grad $m < n = 2^k$, und es sei S_n die Menge der n-ten Einheitswurzeln, also die Wurzeln von $x^n - 1$.

   Zeigen Sie, dass die multiple Evaluation von $P()$ für die Elemente aus S_n in $O(n \log n)$ Zeit berechnet werden kann.

   Verwenden Sie den Ansatz aus der Vorlesung unter Berücksichtigung der besonderen Struktur von S_n und der obigen algebraischen Identitäten. Die Lösung sollte sich auf keine zusätzlichen Annahmen verlassen (z.B. dass zwei Polynome vom Grad höchstens n in Zeit $O(n \log n)$ multipliziert werden können).

5. (20 Punkte) Es sei $S_n = \{\omega^j | 1 \leq j \leq n\}$ die Menge der n-ten Einheitswurzeln, also die Wurzeln von $x^n - 1$. Es soll das Interpolationsproblem für die Paaremenge $U = \{(\omega^j, v_j) | 1 \leq j \leq n\}$ gelöst werden. Adaptieren Sie dafür den Ansatz aus Problem 2. Welche Laufzeit können Sie erreichen?

6. (5 Punkte) Zeigen Sie, wie man mit Lösungen von Aufgaben 4 und 5 zwei Polynome effizient multiplizieren kann?