# Computeralgebra

SS 2000
Prof. Dr. K. Madlener
Übungsblatt 4

**Aufgabe 4.1**
Untersuchen Sie, ob die polynomialen Restefolgen aus der Vorlesung tatsächlich zur ggT-Berechnung verwendet werden können. Zeigen Sie dazu:

Sind $a(x)$ und $b(x)$ primitive Polynome über einem ZPE-Ring $D$ und ist $f_1(x) = a(x), f_2(x) = b(x), f_3(x), \ldots, f_{k-1}(x), f_k(x)$ eine polynomiale Restefolge für $a(x)$ und $b(x)$, wobei $f_k(x) = 0$ sei, so gilt:

$$\mathrm{GGT}(a(x), b(x)) = \mathrm{pp}(f_{k-1}(x)).$$

**Aufgabe 4.2**
Sei $D$ ein euklidischer Ring mit Bewertungsfunktion $\nu$. Entwerfen Sie einen Algorithmus, der der folgenden Spezifikation genügt:

**Eingabe:** Eine positive ganze Zahl $n$ sowie $a, d_1, \ldots, d_n \in D \setminus \{0\}$ mit $\mathrm{GGT}(d_i, d_j) = 1$ für $i \neq j$.

**Ausgabe:** $a_0, a_1, \ldots, a_n \in D$, so dass

$$\frac{a}{d_1 \cdots d_n} = a_0 + \sum_{i=1}^{n} \frac{a_i}{d_i}$$

und entweder $a_i = 0$ oder $\nu(a_i) < \nu(d_i)$ für $i \geq 1$.

Begründen Sie auch, weshalb Ihr Algorithmus korrekt ist. Ist Ihnen dieser Algorithmus schon einmal begegnet?

**Aufgabe 4.3**
Nehmen Sie an, Alice und Bob hätten jeweils eine Nachricht von $n$ Bit, $M_A$ und $M_B$. Sie würden gerne verifizieren, dass ihre Nachrichten identisch sind, und zwar einerseits mit einer großen Wahrscheinlichkeit und andererseits mit wenig Kommunikationsaufwand. Insbesondere sei $n$ so groß, dass ein Nachrichtenaustausch ausscheide.

Alice und Bob wählen $k$ Primzahlen $p_1, \ldots, p_k$ uniform aus der Menge der ersten $2n$ Primzahlen und prüfen dann, ob $M_A \equiv M_B \pmod{p_i}$ für $1 \leq i \leq k$. Zeigen Sie, dass, wenn $M_A = M_B$, so ist $M_A \equiv M_B \pmod{p_i}$ für alle $i$, während, wenn $M_A \neq M_B$, so ist $M_A \not\equiv M_B \pmod{p_i}$ für ein $i$ mit Wahrscheinlichkeit mindestens $1 - 2^{-k}$.

**Aufgabe 4.4**
a) Machen Sie sich klar, dass der Multiplikationsalgorithmus nach Karatsuba und Ofman (in der Vorlesung für Langzahlarithmetik eingeführt) auch für univariate Polynome funktioniert. Formulieren Sie eine entsprechende rekursive Prozedur.

b) Zeigen Sie, dass dieser Algorithmus eine Multiplikation zweier Polynome vom Grade höchstens $n$ (wobei $n$ eine Zweierpotenz sei) mit höchstens $9n^{\log_2 3} + O(n)$ Ringoperationen durchführt.

Zeigen Sie dazu folgendes Lemma:

Seien $b, d \in \mathbb{N}$ mit $b > 0$, und seien $S, T : \mathbb{N} \to \mathbb{N}$ Funktionen mit $S(2n) \geq 2S(n)$ sowie $S(n) \geq n$ für alle $n \in \mathbb{N}$. Es gelte $T(1) = d$ und $T(n) \leq bT(n/2) + S(n)$ für $n = 2^i$ und $i \in \mathbb{N}^+$. Dann gilt für $i \in \mathbb{N}$ und $n = 2^i$:

$$T(n) \leq \begin{cases} (2 - 2/n)S(n) + d \in O(S(n)) & \text{falls } b = 1, \\ S(n)\log_2 n + dn \in O(S(n)\log_2 n) & \text{falls } b = 2, \\ \frac{2}{b-2}(n^{\log_2 b - 1} - 1)S(n) + dn^{\log_2 b} \in O(S(n)n^{\log_2 b - 1}) & \text{falls } b \geq 3. \end{cases}$$

c) Überzeugen Sie sich, dass der Algorithmus nach Karatsuba und Ofman für „kleine“ Eingaben langsamer ist als der klassische Multiplikationsalgorithmus für Polynome.

Untersuchen Sie nun einen hybriden Algorithmus, der rekursiv die Karatsuba/Ofman-Idee anwendet, bis die Grade kleiner als eine Grenze $2^d \in \mathbb{N}$ werden, und dann die klassische Multiplikation verwendet.

Zeigen Sie, dass dieser hybride Algorithmus höchstens $\gamma(d)n^{\log_2 3} + O(n)$ Ringoperationen durchführt, wobei $\gamma(d)$ nur von $d$ abhängt. Finden Sie $d$, so dass $\gamma(d)$ minimal ist. (Dazu brauchen Sie eine recht genaue Abschätzung für die Anzahl der Ringoperationen im klassischen Multiplikationsalgorithmus.)

Abgabe am 8.5.2000 bis 10.30 Uhr, Übungskasten in Bau 34, zweites OG.

Informationen zur Vorlesung:
http://www-madlener.informatik.uni-kl.de/ag-madlener/lectures/compalg/ss2000/compalg.html