Computeralgebra

SS 2000
Prof. Dr. K. Madlener
Übungsblatt 5

Aufgabe 5.1
Nehmen Sie an, dass ungerade und teilerfremde Moduli m_j gegeben seien. Außerdem sei $u = (u_1, \dots, u_r)$ als Restevektor bezüglich der m_j dargestellt. Wie kann man (unter der Annahme, dass u ein Vielfaches von 2 ist) $u/2$ modular berechnen?

Aufgabe 5.2

a) Sei F ein Körper, $f(x)$ ein univariates Polynom über F und $u \in F$. Geben Sie eine Methode zur Berechnung von $f(u)$ an, die mit möglichst wenigen Operationen in F auskommt.

b) Verallgemeinern Sie diese Methode auf Polynome aus $F[x, y]$ und geben Sie auch hier Abschätzungen für die Anzahl der Körperoperationen an.

Aufgabe 5.3

a) Geben Sie für $n = 4$ und $n = 8$ jeweils primitive Einheitswurzeln in $\mathbb{C}$ an und berechnen Sie die Fouriertransformierten von $(0, 1, 2, 3)$ und $(1, 2, 0, 2, 0, 0, 0, 1)$.

b) Seien $a(x) = -x^3 + 3x + 1$ und $b(x) = 2x^4 - 3x^3 - 2x^2 + x + 1$ Polynome aus $\mathbb{Z}_{17}[x]$. Bestimmen Sie das Produkt dieser Polynome mit Hilfe der schnellen Fourier-Transformation.

Aufgabe 5.4
Sei $a(x)$ ein Polynom vom Grade $3^n - 1$ mit $n \geq 0$.

a) Zeigen Sie, dass $a(x)$ als

$$a(x) = b(x^3) + x \cdot c(x^3) + x^2 \cdot d(x^3)$$

geschrieben werden kann; dabei sind $b(x)$, $c(x)$ und $d(x)$ Polynome vom Grade kleiner oder gleich $3^{n-1} - 1$.

b) Finden Sie Symmetriebedingungen ähnlich zu denen aus der Vorlesung, die es erlauben, $a(x)$ an 3^n Stellen auszuwerten, indem man drei geeignete Polynome jeweils an 3^{n-1} geeigneten Stellen auswertet.

c) Zeigen Sie, dass für eine primitive 3^n-te Einheitswurzel ω eines Körpers die Elemente $1, \omega, \dots, \omega^{3^n - 1}$ die Symmetriebedingungen aus b) erfüllen.

d) Welches sind die Kosten der Auswertung von $a(x)$ an den 3^n in c) genannten Stellen?

e) Verwenden Sie a) bis d), um einen 3-FFT-Algorithmus zu entwickeln und eine Abschätzung der Anzahl der Multiplikationen im Koeffizientenkörper anzugeben.

Abgabe am 15.5.2000 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