

Klausur Computer-Algebra SS 2009

Iwanowski 20.08.2009

Hinweise:

Bearbeitungszeit: 90 Minuten

Erlaubte Hilfsmittel: Taschenrechner

Bitte notieren Sie Ihre Antworten ausschließlich auf dem Aufgabenblatt! Bei Bedarf benutzen Sie die Rückseite! Für Skizzen und Entwürfe steht ebenfalls die Rückseite zur Verfügung. Entwürfe, die nicht gewertet werden sollen, sind durchzustreichen.

Insgesamt gibt es 39 Bewertungseinheiten (BE) zu erzielen. Zum Bestehen benötigen Sie mindestens 19,5 BE.

Viel Erfolg!

Aufgabe 1: Thema: Arbeiten mit einem Computer-Algebra-System

(2 BE)

Vergleichen Sie die unterschiedliche Qualität der Lösungen zwischen einem Computer-Algebra-System wie Maxima und einer herkömmlichen algorithmischen Programmiersprache wie Pascal oder Java am folgenden Beispiel:

Lösung von $x^2 + 3x + 6 = 0$

Sie brauchen das Ergebnis nicht konkret auszurechnen. Skizzieren Sie stattdessen in Worten, welcher Art das Ergebnis im jeweiligen System ist und begründen Sie, welchen Vorteil ein Computer-Algebra-System für die Aufgabe hat.

Aufgabe 2: Thema: Ganzzahlarithmetik

(6 BE)

- a) Mit welchem Algorithmus verbessert man das asymptotische Laufzeitverhalten der Multiplikation von langen Zahlen im Vergleich zum Schulalgorithmus? Geben Sie das Laufzeitverhalten dieses Algorithmus an. (2 BE)
- b) Skizzieren Sie die wesentliche Idee, wie der schnellere Algorithmus die verbesserte Laufzeit erreicht: Geben Sie dafür an, welches algorithmische Grundprinzip er benutzt und welchen Trick er zur Beschleunigung verwendet im Vergleich zur offensichtlichen Verwendung des gewählten Grundprinzips.
(Die rechnerischen Details müssen nicht genannt werden, dürfen aber, falls Sie das einfacher empfinden) (4 BE)

Aufgabe 3: Modulare Arithmetik

(5 BE)

- a) Für welche der 4 Grundrechenarten ist in \mathbb{Z}_n für allgemeine n kein effizienter Algorithmus bekannt? (1 BE)
- b) Geben Sie an, unter welchen Bedingungen die in a) genannte Grundrechenart doch effizient implementiert werden kann und welchen Algorithmus man dafür als Modul benutzen muss. Geben Sie an, was dieser Algorithmus genau berechnet: Was ist die Eingabe und was die Ausgabe?
(Anmerkung: Wie der Algorithmus genau verwendet wird, um die Grundrechenart effizient zu implementieren, muss im Detail nicht gezeigt werden) (4 BE)

Aufgabe 4: Modulare Arithmetik

(6 BE)

Berechnen Sie die folgenden Aufgaben in \mathbb{Z}_5 . Geben Sie an, wenn es keine Lösung gibt und geben Sie bei Mehrdeutigkeit alle Lösungen an. Begründen Sie in jedem Fall Ihre Antwort.

a) $\sqrt{3}$

b) $\log_3 2$

c) $\sqrt[5]{4}$

Betrachten Sie die Multiplikation von zwei Polynomen mittels Fouriertransformation:

- a) Beschreiben Sie die 3 wesentlichen Schritte der Multiplikation und benennen Sie die Schritte, in denen die Fouriertransformierte angewendet wird. Geben Sie auch die asymptotische Laufzeit der einzelnen Schritte an, wenn die schnelle Fouriertransformierte verwendet wird! (5 BE)
- b) Geben Sie an, an welchen Stellen das Polynom x^3+3x^2+x+5 in der schnellen Fouriertransformation ausgewertet wird. (1 BE)

Aufgabe 6: Polynomiale Gleichungssysteme

(9 BE)

- a) Was ist eine Resultante? Geben Sie an, wovon die Resultante als Eingabe abhängt und was sie als Ausgabe liefert. (3 BE)
- b) Schildern Sie für ein polynomiales Gleichungssystem mit 3 Gleichungen p_1, p_2, p_3 und 3 Variablen x, y, z die Schritte in Worten, wie man dieses Gleichungssystem mit Hilfe von Resultanten löst. Erwähnen Sie insbesondere, an welcher Stelle man einen Faktorisierungsalgorithmus dafür braucht. (6 BE)

Aufgabe 7: Polynomfaktorisierung

(5 BE)

- a) Auf welches Problem kann man den Berlekampalgorithmus anwenden? (1 BE)
- b) Was ist der entscheidende Unterschied zwischen dem Berlekampalgorithmus und dem Algorithmus von Kronecker sowohl in der Problemstellung als auch in der Laufzeit?(2 BE)
- c) Mit Hilfe von welcher numerischen Schranke kann man den Berlekampalgorithmus auf dieselbe Problemstellung wie den Algorithmus von Kronecker anwenden? Wofür wird eine Schranke angegeben (genauer Wert nicht erforderlich)? Was für eine Auswirkung hat diese Anwendung auf die Gesamtlaufzeit? (2 BE)