Fachhochschule Wedel
Prof. Dr. Sebastian Iwanowski

04.02.2013

Aufgaben zur Klausur in *Computer-Algebra* (WS 2012/2013)

Zeit: 90 Minuten

erlaubte Hilfsmittel: Taschenrechner

Bitte tragen Sie Ihre Antworten und fertigen Lösungen auf gesonderten karierten Blättern ein. Markieren Sie klar, welche Lösung zu welcher Aufgabe gehört und als solche gewertet werden soll. Nicht zu wertende Passagen sind durchzustreichen.

Notizen auf diesem Aufgabenblatt werden grundsätzlich nicht gewertet!
Vergessen Sie nicht, das Deckblatt zu unterschreiben.

Für die Prüfung werden insgesamt Bewertungseinheiten 36 (BE) vergeben. Zum Bestehen benötigen Sie mindestens 18 BE.

Viel Erfolg !

Aufgabe 1: Arbeiten mit einem Computer-Algebra-System (4 BE)

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

a) Berechnung von 123456789101112131415 * 98765432110090807060504030201

b) Lösung von $x^2 + 5x + 5 = 0$

Sie brauchen die Ergebnisse 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 jeweilige Aufgabe hat.

Aufgabe 2: Ganzzahlarithmetik (5 BE)

Betrachten Sie die Aufgabe 1040 * 4010 und beschreiben Sie, in welche rekursive Teilaufgaben der Algorithmus von Karatsuba diese Aufgabe zerlegt und stellen Sie eine Gleichung auf, wie aus den zerlegten Teilaufgaben die gesamte Aufgabe berechnet wird.
Kennzeichnen Sie konkret die Operationen, in denen ein rekursiver Aufruf erfolgt. Die rekursiven Teilaufgaben müssen Sie nicht weiter analysieren und auch nicht ausrechnen.
Hinweis: Hier werden als Kurzzahlen ausschließlich die Ziffern von 0 bis 9 betrachtet

Aufgabe 3: Modulare Arithmetik (5 BE)

a) Für welche der 4 Grundrechenarten ist in $\mathbb{Z}_n$ für allgemeine n kein effizienter Algorithmus bekannt?

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)

Aufgabe 4: Modulare Arithmetik (6 BE)

a) Geben Sie ein n an, für das $\mathbb{Z}_n$ nicht den kleinen Satz von Fermat erfüllt. Demonstrieren Sie das an einem Beispiel.
(Tipp: Sie werden fündig beim kleinsten theoretisch möglichen Gegenbeispiel)

b) Für welche Zahlen n erfüllt $\mathbb{Z}_n$ immer den kleinen Satz von Fermat?

c) Für welchen Test würde man den kleinen Satz von Fermat gerne benutzen, wie würde dieser Test aussehen, und warum funktioniert dieser Test nicht?

Aufgabe 5: Modulare Arithmetik (2 BE)

Es gibt bekanntlich keinen effizienten Algorithmus, um eine Zahl in ihre Primfaktoren zu zerlegen. Ist es notwendig, diese Aufgabe zu lösen, um zu bestimmen, ob eine Zahl eine Primzahl ist? Begründen Sie Ihre Antwort!

Aufgabe 6: Polynomarithmetik (6 BE)

Betrachten Sie die Multiplikation von zwei Polynomen mittels Fouriertransformation:

a) Beschreiben Sie die 3 wesentlichen Schritte der Multiplikation, von denen die Fouriertransformierte nur ein Modul ist. Geben Sie auch die asymptotische Laufzeit der Schritte an! (3 BE)

b) Was löst die Fouriertransformierte genau? Spezifizieren Sie die Eingabe und die Ausgabe der Fouriertransformierten im Allgemeinen. (2 BE)

c) Geben Sie an, an welchen Stellen das Polynom x^3+2x^2-7 in der Fouriertransformation ausgewertet wird. (1 BE)

Aufgabe 7: Polynomiale Gleichungssysteme (4 BE)

Lösen Sie folgendes Gleichungssystem mit dem Resultantenverfahren:

$x + y^2 = 0$

$x^2 + y = 0$

Hierfür reicht es nicht aus, dass Sie eine gültige Lösung angeben: Sie sollen auch die Zwischenschritte beschreiben, die das Resultantenverfahren nimmt. Beschreiben Sie dafür auch explizit die Zwischenschritte, die sich aus Matrizenumformungen ergeben.
Errechnen Sie zwei gültige Lösungen!

Aufgabe 8: Polynomfaktorisierung (4 BE)

Schildern Sie die Grundidee der Polynomfaktorisierung nach Kronecker: Auf welche Sorte von Polynomen wird es überhaupt angewandt, was ist das grundlegende Prinzip und welche Laufzeit ist zu erwarten?