Fachhochschule Wedel
Prof. Dr. Sebastian Iwanowski

26.08.2013

Aufgaben zur Klausur in *Computer-Algebra* (SS 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 32 (BE) vergeben. Zum Bestehen benötigen Sie mindestens 16 BE.

Viel Erfolg !

Aufgabe 1: Ganzzahlarithmetik (4 BE)

Erklären Sie den Unterschied zwischen Kurzzahl- und Langzahlarithmetik anhand folgender Fragestellungen:

a) Wie groß dürfen die Operanden sein (qualitative Aussage erwünscht, muss also nicht genau quantifiziert werden) und wie werden diese dargestellt?

b) Gehen Sie darauf ein, in welcher der beiden Arithmetiken mit softwaretechnisch realisierten Algorithmen gearbeitet wird und erklären Sie das Kostenmaß zur Laufzeitbestimmung dieser Algorithmen.

c) Wie werden die Operationen in der anderen Arithmetik anstelle dieser Algorithmen realisiert?

Aufgabe 2: Ganzzahlarithmetik (4 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.

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)

Aufgabe 3: Modulare Arithmetik (5 BE)

a) Zu welcher Rechenoperation ist in $\mathbb{Z}_n$ für gar kein n ein effizienter Algorithmus bekannt?

b) Im Diffie-Hellman-Verfahren wird die in a) genannte Tatsache verwendet: Skizzieren Sie die generelle Aufgabe dieses Verfahrens und die Vorgehensweise!

Aufgabe 4: Polynomarithmetik (8 BE)

Betrachten Sie die Multiplikation von zwei Polynomen p(x), q(x) der Größe n mittels Fouriertransformation:

a) Nach welchem Grundprinzip arbeitet diese Multiplikation? Spezifizieren Sie die 3 Teilschritte, welche dafür notwendig sind!
Hinweis: Der Einsatz der schnellen Fouriertransformierten muss hier noch nicht zwingend angewendet werden. Sie muss daher hier noch nicht näher spezifiziert werden.

b) Demonstrieren Sie das Verfahren von a) im Detail an der Aufgabe
$m(x) = (x^2+1) \bullet (x^2-3)$ und den Stützstellen -2, -1, 0, 1, 2.
Hinweis: Hier wird die schnelle Fouriertransformierte tatsächlich noch nicht eingesetzt.

c) Was macht man mit Hilfe der schnellen Fouriertransformierten anders als in b)?

d) Warum ist es ein Vorteil, c) statt b) anzuwenden?

Aufgabe 5: Polynomiale Gleichungssysteme (7 BE)

a) Was ist eine Resultante? Geben Sie an, wovon die Resultante als Eingabe abhängt und was sie als Ausgabe liefert.

b) Schildern Sie für ein polynomiales Gleichungssystem mit 3 Gleichungen p1, p2, p3 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.

Aufgabe 6: Polynomfaktorisierung (4 BE)

a) Was versteht man unter quadratfreier Faktorisierung? Nennen Sie die Eigenschaften von Eingabe und Ausgabe!

b) Was ist der Vorteil der quadratfreien Faktorisierung im Vergleich zur Methode von Kronecker?