Fachhochschule Wedel
Prof. Dr. Sebastian Iwanowski

17.02.2014

Aufgaben zur Klausur in *Computer-Algebra* (WS 2013/2014)

Zeit: 90 Minuten
erlaubte Hilfsmittel: keine

Bitte tragen Sie Ihre Antworten 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. Für die Prüfung werden insgesamt 40 Bewertungseinheiten (BE) vergeben. Zum Bestehen benötigen Sie mindestens 20 BE. Viel Erfolg !

Aufgabe 1: Ganzzahlarithmetik (3 BE)

Geben Sie das asymptotische Laufzeitverhalten (O-Notation) für alle 4 Grundrechenarten bei Verwendung der Schulalgorithmen an.

Geben Sie ferner an, welche dieser Laufzeiten optimal sind, d.h. es ist bewiesen, dass es keinen asymptotisch besseren Algorithmus geben kann oder zumindest ist keiner bekannt.

Aufgabe 2: Ganzzahlarithmetik (5 BE)

Demonstrieren Sie den 1. Schritt der rekursiven Aufteilung des Algorithmus von Karatsuba am folgenden Beispiel: 1413 * 2712

a) Zerlegen Sie dafür die Aufgabe erst einmal mit normaler Bisektionierung und geben Sie dann die Verbesserung von Karatsuba an. (3 BE)

b) Geben Sie alle verschiedenen Langzahlmultiplikationen an, die im 1. Rekursionsschritt aufgerufen werden. (1 BE)

c) Geben Sie die asymptotische Laufzeit des Algorithmus an. (1 BE)

Hinweis: Sie müssen für keine der Teilaufgaben das konkrete Ergebnis ausrechnen.

Aufgabe 3: Ganzzahlarithmetik (5 BE)

Erläutern Sie den Euklidischen Algorithmus:

a) Was rechnet der normale Algorithmus zu gegebenen Eingaben x und y aus? (1 BE)

b) Für welche Operation bei den Grundrechenarten wird der Euklidische Algorithmus als Nachfolgeoperation gebraucht? Welche Aufgabe erfüllt er da? (1 BE)

c) Was rechnet der erweiterte Algorithmus zusätzlich aus? Geben Sie eine Gleichung an! (1 BE)

d) Für welche Operation in der modularen Arithmetik kann man die zusätzlich ausgerechneten Koeffizienten verwenden? (genaue Herleitung nicht erforderlich) Welche Konsequenz hat das für die Kryptographie? (2 BE)

Aufgabe 4: Modulare Arithmetik (3 BE)

Betrachten Sie die modularen Operationen Multiplizieren, Potenzieren, Radizieren und Logarithmieren:

a) Welche dieser Operationen kann man effizient berechnen und welche nicht?

b) Welche dieser Operationen ist die sicherste für die Kryptographie, d.h. es ist für keinen Fall bekannt, wie man sie anders ausrechnet, als alle Möglichkeiten durchzuprobieren?

c) Nennen Sie ein kryptographisches Verfahren, in dem die Operation aus b) eingesetzt wird und sagen Sie, welches Problem mit diesem Verfahren gelöst wird. Das Verfahren selbst müssen Sie nicht beschreiben.

Aufgabe 5: Modulare Arithmetik (7 BE)

Betrachten Sie das Fiat-Shamir-Protokoll:

a) Für welche Problemstellung wird es eingesetzt? Beschreiben Sie die Problemstellung mit mehr als einem Wort, sondern dem gesamten Sachverhalt, der zu berücksichtigen ist. (1 BE)

b) Geben Sie im Detail an, wie das Verfahren funktioniert. (5 BE)

c) Aufgrund welcher algorithmischen Schwierigkeit kann ein Angreifer das Verfahren nicht unterminieren? (1 BE)

Aufgabe 6: Polynomarithmetik (6 BE)

a) Beschreiben Sie die wesentlichen Schritte, wie man das Produkt von 2 Polynomen ermittelt, welche der Multiplikation mit Hilfe der schnellen Fouriertransformation zugrundeliegt. (3 BE)

b) Geben Sie an, welches die Laufzeit der einzelnen Schritte ist, wenn man sie mit Matrizen anstelle der schnellen Fouriertransformation löst. (1 BE)

c) Welcher Unterschied in der Gesamtlaufzeit besteht zwischen b) und der Schulmethode, 2 Polynome zu multiplizieren (mit dem Cauchy-Produkt). (1 BE)

d) An welcher Stelle in a) verbessert sich die Laufzeit auf welchen Wert, wenn die schnelle Fouriertransformation eingesetzt wird? (1 BE)

Aufgabe 7: Polynomiale Gleichungssysteme (8 BE)

Finden Sie eine gemeinsame Nullstelle aller 3 Polynome mit Hilfe des Resultantenverfahrens:

$p_1(x,y,z) = x^2 - 1$

$p_2(x,y,z) = xy - z$

$p_3(x,y,z) = z^2 - x$

Hinweis: Es reicht nicht aus, einfach nur die Lösung anzugeben. Sie sollen das Resultantenverfahren mit den wesentlichen Zwischenschritten angeben. Stellen Sie dafür alle benötigten Matrizen auf und berechnen Sie die Determinanten. Es reicht aus, nur eine Lösung auszurechnen, auch wenn es mehrere gibt.
Tipp: Bilden Sie erst die Resultanten bezüglich x und dann bezüglich y.

Aufgabe 8: Polynomfaktorisierung (3 BE)

Betrachten Sie das Polynom $p(x) = x^6+x^5-7x^4-5x^3+14x^2+4x-8$, welches die einfachen Nullstellen -1 und 2 sowie die doppelten Nullstellen 1 und -2 hat:

a) Was ist bei einer vollständigen Faktorisierung als Ergebnis zu erwarten?

b) Wenn das Polynom wie oben eingegeben wird, was ist bei einer quadratfreien Faktorisierung als Ergebnis zu erwarten?

c) Warum lohnt es sich, zunächst eine quadratfreie Faktorisierung durchzuführen, wenn man an einer vollständigen Faktorisierung interessiert ist?