Fachhochschule Wedel
Prof. Dr. Sebastian Iwanowski

10.02.2012

Aufgaben zur Klausur in *Computer-Algebra* (WS 2011/2012)

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 36 Bewertungseinheiten (BE) vergeben. Zum Bestehen benötigen Sie mindestens 18 BE.

Viel Erfolg !

Aufgabe 1: Ganzzahlarithmetik (7 BE)

a) Was berechnet der erweiterte Euklidische Algorithmus für zwei ganze Zahlen m und n? (1 BE)

b) Führen Sie diesen Algorithmus am Beispiel m = 100 und n = 49 vor! Sie müssen nicht die effizienteste Implementierungsvariante vorführen, sondern dürfen zunächst den einfachen Euklid verwenden und die vom erweiterten Euklid zu berechnenden zusätzlichen Größen durch nachträgliche Rücksubstition errechnen. (4 BE)

c) Welche Laufzeit (asymptotische Größenordnung) hat der erweiterte Euklidische Algorithmus und was für eine Auswirkung hat das bezüglich der Verschlüsselung mit modularer Arithmetik? (Sie müssen diese Auswirkung nur nennen, aber nicht beweisen). (2 BE)

Aufgabe 2: Modulare Arithmetik (8 BE)

a) Geben Sie an, wie man eine Authentifizierung durch das Fiat-Shamir-Protokoll vortäuschen kann, wenn sie ausschließlich einen Test macht, der auf der Schwierigkeit des Wurzelziehens beruht: Skizzieren Sie diesen Test und erklären Sie, wie man ihn bestehen kann, ohne die für die Authentifizierung benötigte Zahl zu kennen. (5 BE)

b) Wie macht man das Fiat-Shamir-Protokoll sicher gegen solche Angriffsversuche? Erklären Sie, wie man eine beliebig große Sicherheit nahe 100 % erreichen kann, dass nur derjenige den Test besteht, der die Authentifizierungszahl wirklich kennt! (3 BE)

Aufgabe 3: Modulare Arithmetik (5 BE)

a) Geben Sie ein Kriterium an, das eine Zahl erfüllen muss, wenn sie keinen Fermatschen Zeugen besitzt und dennoch keine Primzahl ist (Nennung eines Namens reicht nicht aus!) (2 BE)

b) Geben Sie eine Wahrscheinlichkeit an, mit der das Verfahren von Rabin-Miller eine korrekte Antwort gibt und geben an, wie dieses Verfahren mit den Zahlen von a) umgeht. (2 BE)

c) Geben Sie an, für welche Zahlen Rabin-Miller mit 100 % Sicherheit das richtige Testergebnis liefert. (1 BE)

Aufgabe 4: Polynomarithmetik (7 BE)

Gegeben seien die Polynome $2x^2-x+1$ und $2x-1$.

a) An wie vielen Stützstellen müssen diese Polynome mindestens ausgewertet werden, damit das Produkt richtig berechnet werden kann? (1 BE)

b) Führen Sie die Stützstellentransformation an geeigneten ganzzahligen Argumenten vor, bis Sie den Stützstellenvektor des Produktpolynoms erhalten. Überprüfen Sie den Stützstellenvektor, indem Sie das Produkt auf herkömmliche Weise berechnen. (3 BE)

c) Beschreiben Sie exakt die Aufgabenstellung, die jetzt noch gelöst werden muss, um das gewünschte Ergebnis zu erhalten (die Lösung selbst müssen Sie nicht vorführen).(2 BE)

d) Mit welchen Stützstellen würde die Fouriertransformation arbeiten? Geben Sie diese Stützstellen konkret in Normaldarstellung für komplexe Zahlen an! (1 BE)

Aufgabe 5: Polynomiale Gleichungssysteme (5 BE)

a) Erklären Sie, wie zu den Polynomen x^3-2y+1 und $2xy-6y$ die Resultante bezüglich x definiert wird. Geben Sie die dazugehörige Matrix konkret an und benennen Sie die Operation, die Sie auf dieser Matrix ausführen müssen! Die Operation selbst brauchen Sie nicht auszurechnen. (3 BE)

b) Geben Sie den algebraischen Grund an, warum diese Resultante für die Ermittlung einer gemeinsamen Lösung dieser Polynome auf Null gesetzt werden muss. Handelt es sich dabei um eine notwendige oder um eine hinreichende Bedingung? (2 BE)

Aufgabe 6: Polynomfaktorisierung (4 BE)

a) Was versteht man unter einer quadratfreien Faktorisierung? Erläutern Sie das in Worten und geben Sie ein Beispiel für eine quadratfreie Faktorisierung des Polynoms $x^4-6x^3+8x^2+6x-9$ an, die nicht mehr Faktoren aufweist als nötig.
Hinweise: Die Nullstellen sind -1, 1 und 3 (doppelt). (2 BE)

b) Wofür ist eine quadratfreie Faktorisierung nützlich? Geben Sie die Vorteile sowohl in Verbindung mit dem Kroneckeralgorithmus als auch mit dem Berlekampalgorithmus an!(2 BE)