

---

## Aufgaben zur Klausur in *Computer-Algebra* (SS 2010)

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 32 Bewertungseinheiten (BE) vergeben. Zum Bestehen benötigen Sie mindestens 16 BE.

Viel Erfolg !

### 1. Aufgabe (3 BE):

Erklären Sie den Unterschied zwischen Kurzzahl- und Langzahlarithmetik:

- a) Was ist die Definition von Kurzzahl und Langzahl? (2 BE)
- b) Wenn die Langzahlarithmetik mit einer herkömmlichen algorithmischen Programmiersprache implementiert wird, mit welcher Datenstruktur sollte man eine Langzahl in der Programmiersprache repräsentieren? (1 BE)

### 2. Aufgabe (4 BE)

Betrachten Sie den Schulalgorithmus zum Teilen von zwei Langzahlen mit Rest:

- a) Welches Teilproblem wird in der Schule durch Raten gelöst? Wie kann man dieses Problem in einem Algorithmus lösen? Schildern Sie die Lösung in Worten für das Beispiel, dass die Kurzzahlen genau die dezimalen Ziffern sind. (2 BE)
- b) Was löst das Verfahren von Pope-Stein besser als der Schulalgorithmus? Welche asymptotische Laufzeitverbesserung (im Sinne der O-Notation) ergibt sich? (2 BE)

### 3. Aufgabe (5 BE)

- a) Zu welcher Rechenoperation ist in  $\mathbb{Z}_n$  für kein  $n$  ein effizienter Algorithmus bekannt? (1 BE)
- b) In welchem kryptographischen Verfahren wird die in a) genannte Tatsache verwendet? Skizzieren Sie die generelle Aufgabe dieses Verfahrens und die Vorgehensweise! (4 BE)

### 4. Aufgabe (3 BE)

- a) Geben Sie den kleinen Satz des Fermat an und begründen Sie, warum man mit Hilfe dieses Satzes die Zerlegbarkeit einer Zahl beweisen kann. (2 BE)
- b) Warum reicht die in a) beschriebene Methode nicht aus, um festzustellen, ob eine Zahl  $p$  eine Primzahl ist oder nicht? (1 BE)

## 5. Aufgabe (6 BE)

Betrachten Sie die Multiplikation von zwei Polynomen mittels Fouriertransformation:

- Was löst die Fouriertransformierte genau? Spezifizieren Sie die Eingabe und die Ausgabe der Fouriertransformierten im Allgemeinen. (2 BE)
- Die schnelle Fouriertransformierte arbeitet nach dem Divide-and-conquer-Verfahren. Beschreiben Sie in Worten, was dieser Teilungsschritt macht und demonstrieren sie den Schritt am Polynom  $x^3+2x^2-x+7$ . Welche Laufzeit kostet dieser Teilungsschritt in Abhängigkeit von  $n$ ? (4 BE)

## 6. Aufgabe (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?

## 7. Aufgabe (7 BE)

- Was versteht man unter quadratfreier Faktorisierung? Nennen Sie die Eigenschaften von Eingabe und Ausgabe! (2 BE)
- Auf welchem Prinzip aus der Analysis beruht die quadratfreie Faktorisierung in Körpern mit Charakteristik 0? (1 BE)
- Was bedeutet die Charakteristik eines Körpers? (2 BE)
- Geben Sie für den Körper  $\mathbb{Z}_3$  ein Beispiel an, an dem das Prinzip aus b) nicht funktioniert. Welche Charakteristik hat dieser Körper? (2 BE)