Sommersemester 2005

Hasso- Plattner- Institut, Universität Potsdam

Übung zur Vorlesung

Fachgebiet Internet- Technologien und - Systeme

Meinel / Kutzner

Aufgabenblatt 6
(Nur für ULI-Studenten)

(URL: http://www3.hpi.uni- potsdam.de/index.php?id=411)

Abgabe: Mo, 30.05.2005, bis 12 Uhr MEZ (per E-Mail an mathias.kutzner@hpi.uni- potsdam.de)

Thema: Zahlentheoretische Referenzprobleme

Erreichbare Punkte: 17

Aufgabe 1: **4 Punkte**

Überprüfen Sie mit Hilfe des Fermat- Tests, ob 1103, 1109, 1111 und 2701 Primzahlen sind. Um die Wahrscheinlichkeit von Pseudo- Primzahlen zu verringern, wählen Sie zusätzlich noch bis zu drei weitere $a \in Z$, falls Sie kein Indiz haben, dass n zusammengesetzt ist. Dokumentieren Sie Ihren Lösungsweg.

Aufgabe 2: **4 Punkte**

Implementieren Sie den Primzahlentest von Fermat in einer Programmiersprache Ihrer Wahl und ermitteln Sie die kleinste Pseudoprimzahl zur Basis 2. Aus welchen Primzahlen setzt sich diese Pseudoprimzahl zusammen? Geben Sie Ihre Ergebnisse an.

Hinweis: Um echte und Pseudoprimzahlen zu unterscheiden, testen Sie diese mit drei weiteren Basen, solange die Zahl nicht als zusammengesetzt erkannt wird.

Aufgabe 3: **4 Punkte**

Beweisen Sie mit dem Miller- Rabin- Primzahlentest, dass die Pseudoprimzahl aus Aufgabe 2 zusammengesetzt ist. Welche Bedingungen müssen für zusammengesetzte Zahl n und die Basis a erfüllt sein?

Aufgabe 4: **5 Punkte**

Bestimmen Sie alle $a \in \{2,3,\ldots,120\}$ die Falschzeuge sind, wenn mit Hilfe des Miller- Rabin- Primzahlentests die Zusammengesetztheit der Zahl 121 gezeigt werden soll. Implementieren Sie dazu diesen Primzahlentest in einer Programmiersprache Ihrer Wahl. Geben Sie als Lösung Ihre Ergebnisse an. Formulieren Sie außerdem alle Bedingungen, die für diese Falschzeugen gelten müssen.
