Aufgaben zur Vorlesung
Algorithmen für Zahlen und Primzahlen
Wintersemester 2006/07

Die Lösungen sind in logisch und grammatisch einwandfreien Sätzen zu formulieren. Neben dem unmittelbaren Ergebnis muss auch der Lösungsweg erkennbar sein, also insbesondere die mit dem Computer ausgeführten Rechnungen. Umfangreiche Zwischen- oder Endergebnisse können abgekürzt oder verbal dargestellt werden.

Serie 7 — Abgabetermin: 12.12.

18. Führen Sie die folgenden Rechnungen für $k = 8$, $k = 12$ und $k = 20$ aus. (6 Pkt.)

    a) Bestimmen Sie die Anzahl der zusammengesetzten Zahlen m im Intervall $10^k < m < 10^k + 10^4$, die durch keinen Primteiler kleiner als 10^3 teilbar sind.

    b) Bestimmen Sie für jede dieser Zahlen m den kleinsten Rabin-Miller-Zeugen $W(m)$, der belegt, dass m im Rabin-Miller-Test als zusammengesetzt erkannt wird.

19. a) Prüfen Sie, dass $m = \frac{4^p+1}{5}$ für Primzahlen $5 < p < 100$ eine zusammengesetzte ganze Zahl, aber $a = 2$ kein Rabin-Miller-Zeuge für m ist. (2 Pkt.)

    b) Beweisen Sie die Aussagen (a) für Primzahlen $p > 5$. (5 Pkt.)

20. Zeigen Sie, dass $a = 2$ kein Fermatzeuge für zusammengesetzte Fermatzahlen $F_k = 2^{2^k} + 1$, $k > 0$ ist. (4 Pkt.)