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 3 — Abgabetermin: 14.11.

8. Untersuchen Sie, wie groß die Wahrscheinlichkeit ist, dass bei der Multiplikation zweier DIGITs im Zahlsystem zur Basis β kein Übertrag auftritt. Zeigen Sie, dass dieser Wert die Ordnung $O\left(\frac{\log(\beta)}{\beta}\right)$ hat. (4 Pkt.)

9. Zur schriftlichen Division `divmod(a,b)` mit Ziffernraten: Zeigen Sie, dass es stets einen Skalierungsfaktor k gibt, der sich allein aus Kenntnis der ersten Ziffer von b berechnen lässt, so dass $k\,b$ mit einer Ziffer $\geq \left[\frac{\beta}{2}\right]$ beginnt. (5 Pkt.)

10. Untersuchen Sie, für welche natürlichen Zahlen $m > 1$ die Eulersche ϕ-Funktion $\phi(m)$ einen ungeraden Wert hat. (2 Pkt.)

11. Es gilt folgender Satz:

    Ist p eine Primzahl, so ist die Gruppe der primen Restklassen $\mathbb{Z}_p^*$ zyklisch.

    Überprüfen Sie diese Aussage für die ersten 20 Primzahlen, indem Sie jeweils eine Restklasse angeben, die $\mathbb{Z}_p^*$ erzeugt. Weisen Sie jeweils nach, dass die von Ihnen angegebene Restklasse diese Eigenschaft hat. (5 Pkt.)