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 8 — Abgabetermin: 19.12.

21. Zeigen Sie, dass für eine quadratfreie ungerade Zahl $m = p_1 \cdot \ldots \cdot p_k$ die Restklasse $a \in \mathbb{Z}_m^*$ genau dann ein quadratischer Rest ist, wenn für alle $i = 1, \ldots, k$ stets $\left(\frac{a}{p_i}\right) = +1$ gilt. (Hinweis: Chinesischer Restklassensatz) (4 Pkt.)

22. Seien $\{p_1, \ldots, p_k\}$ die (verschiedenen) Primfaktoren von $m - 1$. Zeigen Sie folgenden Zusammenhang:

$$\exists\, a \in \mathbb{Z}_m^*\ \forall i\ a^{\frac{m-1}{p_i}} \not\equiv 1 \pmod{m}$$

genau dann, wenn

$$\forall i\ \exists\, a_i \in \mathbb{Z}_m^*\ a_i^{\frac{m-1}{p_i}} \not\equiv 1 \pmod{m},$$

d.h. es gibt eine gemeinsame Basis für alle Primteiler von $m - 1$, wenn es für jeden Primteiler einzeln eine passende Basis gibt. (6 Pkt.)

23. Bestimmen Sie für die zusammengesetzten Zahlen $2 < n < 1000$ jeweils die kleinste Zahl $k > 0$, für welche $\binom{n}{k} \not\equiv 0 \pmod{n}$ gilt. Stellen Sie ein Vermutung über den Zusammenhang zwischen n und k auf. (3 Pkt.)

Zeigen Sie allgemein: Ist $n \in \mathbb{N}$ zusammengesetzt, so existiert stets ein $k \in \mathbb{N}, 0 < k < n$, mit $\binom{n}{k} \not\equiv 0 \pmod{n}$. (4 Pkt.)