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 10 — Abgabetermin: 23.1.

26. Die Laufzeit der Pollardschen Rho-Methode hat viel mit dem „Geburtstagsparadoxon“ zu tun: Bereits auf einer kleinen Party ist die Chance, dass zwei Leute am selben Tag Geburtstag haben, groß.

    Wieviele Leute müssen auf der Party wenigstens anwesend sein, damit die Chance, dass zwei von ihnen am selben Tag Geburtstag haben, mindestens 50 % beträgt? (3 Pkt.)

27. Analysieren Sie, in welche Pollardsequenzen bzgl. f die Restklassen $\mathbb{Z}_m$ zerfallen und stellen Sie Ihr Ergebnis graphisch dar, indem sie die Restklassen geeignet anordnen und jeweils Pfeile $x \mapsto f(x)$ eintragen. Wie viele verschiedene Pollardzyklen existieren jeweils? (4 Pkt.)

    a) Für $m = 17$ und $f(x) = x^2 + 1$.

    b) Für $m = 37$ und $f(x) = x^2 + x + 11$.

28. Gegeben seien eine Funktion $f : \mathbb{Z}_m \to \mathbb{Z}_m$, eine Pollardsequenz $\{x_n\}$ mit Startwert x_0 und $x_n = f(x_{n-1})$ für $n > 0$ und eine Zahl $r \mid m$.

    Beweisen, widerlegen oder präzisieren Sie folgende Aussage: Die Periodenlänge der Pollardsequenz $\pmod r$ ist ein Teiler der Periodenlänge $\pmod m$. (6 Pkt.)