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 5 — Abgabetermin: 28.11.

14. Zeigen Sie:

    (a) Das Gruppenelement $x = (x_1, \ldots, x_n) \in \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^*$ hat die Ordnung $ord(x) = \mathrm{lcm}(ord(x_1), \ldots, ord(x_n))$. (2 Pkt.)

    (b) In einer abelschen Gruppe G gibt es zu vorgegebenen $a, b \in G$ stets ein $c \in G$, so dass $ord(c) = \mathrm{lcm}(ord(a), ord(b))$ gilt. (6 Pkt.)
    (Beachten Sie, dass die „einfache“ Lösung $c = a \cdot b$ z.B. für $b = a^{-1}$ nicht funktioniert.)

    (c) Folgern Sie daraus, dass für alle $a \in G$ deren Ordnung $ord(a)$ ein Teiler der Exponente $exp(G)$ der Gruppe G ist, d.h. dass

    $$exp(G) = \max\{ord(a) \,|\, a \in G\} = \mathrm{lcm}\,\{ord(a) \;:\; a \in G\}$$

    gilt. (2 Pkt.)

15. Untersuchen Sie die Wirksamkeit von `smallPrimesTest`. Bestimmen Sie dazu die Wahrscheinlichkeit, dass der Test für eine Zahl fehlschlägt, wenn die Testliste der Primzahlen $[2, 3, 5, 7]$ verwendet wird.

    Bestimmen Sie analog die Wahrscheinlichkeiten, wenn

    1. die Liste aller Primzahlen < 100,
    2. die Liste aller Primzahlen < 1000

    verwendet wird. (5 Pkt.)