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 9 — Abgabetermin: 16.1.

24. **a)** Zeigen Sie, dass die folgende Implementierung (MuPAD-Notation)

```
myisqrt:=proc(n) local a,b;
begin
  a:=n; b:=(n+1) div 2;
  while (b<a) do a:=b; b:=(a^2+n) div (2*a) end_while;
  a;
end_proc;
```

für $n \in N$ die Funktion $c = \lfloor\sqrt{n}\rfloor$, also die größte ganze Zahl mit $c^2 \leq n$, berechnet. (6 Pkt.)

b) Leiten Sie eine (möglichst gute) Abschätzung für die Laufzeit dieser Implementierung in Abhängigkeit von der Bitlänge $l(n)$ der Zahl n her. (4 Pkt.)

25. Vergleichen Sie die Laufzeiten von `trialFactor`, `FermatFactor` und `LehmanFactor` für die Zahlen $m = 10^n + 1,\ 10 \leq n \leq 30$. Geben Sie für jede dieser Zahlen die Faktorisierung an. Welche dieser Zahlen werden bereits durch `smallPrimeFactors` vollständig faktorisiert? (6 Pkt.)

Informieren Sie sich dazu, wie im CAS Ihrer Wahl Rechnungen mit Zeitbeschränkung ausgeführt werden können und brechen Sie damit Rechnungen nach 20 s. ab.