UNIVERSITÄT DES SAARLANDES
Fachbereich 14 – Informatik

Prof. J. Buchmann
Stefan Neis

9. November 1995

4. Übung zu
"Algebra für Informatiker"

1. Es ist $\varphi(n) := |\{x \in \mathbb{N} | x < n \text{ und } \mathrm{ggT}(x,n) = 1\}|$. Zeige: Ist $n = \prod_{i=1}^{k} p_i^{e_i}$, $p_1, \ldots, p_k$ paarweise verschiedene Primzahlen, $e_1, \ldots, e_k \in \mathbb{N}$, so ist
$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}.$$
Hinweis: Zeige die Behauptung mittels vollständiger Induktion nach k. "Zähle" dazu jeweils die Elemente $y \in \mathbb{N}$, $y < n$ mit $\mathrm{ggT}(y,n) > 1$.
2. Programmiere einen Algorithmus, der n einliest und $\varphi(n)$ ausgibt.
Hinweis: Mit der in LiDIA enthaltenen Klasse "rational_factorization" ist es "leicht" möglich, n zu faktorisieren und auf die Basen p_i und die Exponenten e_i zuzugreifen. (Das Manual steht auf den Cips in /home/stud/neis/LiDIA/doc/dvi/lidiaman.dvi)
3. Zum Rechnen in $\mathbb{Z}/m\mathbb{Z}$ ist in LiDIA die Klasse "bigmod" enthalten. Programmiere den in der Vorlesung vorgestellten Baby-Step – Giant-Step – Algorithmus für bigmods. Zur Speicherung der Paare (g^{-r}, r) benutze folgende Strategie (Hashing): Lege ein Array der Größe $2\sqrt{m}$ an, wobei in jeder Zelle des Arrays eine Liste abgelegt wird. Das Paar (g^{-r}, r) wird dann an die Liste in der Zelle $g^{-r} \bmod (2\sqrt{m})$ angehängt (Im Mittel enthält also jede solche Liste $\leq \frac{1}{2}$ Element). Um zu testen, ob ein Element (g^y, r) für ein Element g^y gespeichert ist, genügt es dann, die Liste in Zelle $g^y \bmod (2\sqrt{m})$ zu durchsuchen.
4. Benutze die Baby-Step – Giant-Step – Idee zur Lösung des diskreten Logarithmus – Problems in einer endlichen abelschen Gruppe G, d.h. gib einen Algorithmus an, der für zwei Elemente $g_1, g_2 \in G$ mit $g_2 \in \langle g_1 \rangle$ den kleinsten Exponenten $j \in \mathbb{N}_0$ bestimmt, so daß $g_1^j = g_2$ ist.

Abgabe:

Donnerstag, 16. 11. 1995