UNIVERSITÄT DES SAARLANDES
Fachbereich 14 – Informatik

Prof. J. Buchmann
Stefan Neis

15. November 1995

5. Übung zu
"Algebra für Informatiker"

1. Zeige: Die Gruppe $\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} ; a,b,c,d \in \mathbb{Z},\ a \cdot d - b \cdot c = 1 \right\}$ wird von den Matrizen
$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{und} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
erzeugt.
Hinweis: Berechne $D = B^{-1}AB$ und betrachte für eine beliebige Matrix $L^{(0)} \in \mathrm{SL}(2,\mathbb{Z})$ die Folge
$$L^{(2i+1)} = L^{(2i)} \cdot A^{\lambda_{2i+1}} \qquad \text{und} \qquad L^{(2i+2)} = L^{(2i+1)} \cdot D^{\lambda_{2i+2}},$$
wobei $\lambda_i \in \mathbb{Z}$ so gewählt wird, daß der Eintrag oben rechts höchstens noch halb so groß ist, wie der Eintrag oben links bzw. umgekehrt. Zeige, daß man durch eine solche Iteration Matrizen in Dreiecksform erhalten kann und wie man diese durch A und B erzeugen kann. Folgere schließlich daraus die Aussage der Aufgabe.
2. In der Vorlesung haben wir eine Idee gesehen, wie man eine Permutation als Produkt elementfremder nicht trivialer Zyklen schreiben kann. Gib einen Algorithmus an, der diese Idee realisiert, und analysiere den Zeit– und Platzbedarf des Algorithmus.
3. Programmiere den Pohlig – Hellmann – Shanks – Algorithmus zur Bestimmung diskreter Logarithmen in $(\mathbb{Z}/m\mathbb{Z})^*$.
Vergleiche Deinen Algorithmus mit der in LiDIA enthaltenen Implementierung.

Abgabe:

Donnerstag, 23. 11. 1995