UNIVERSITÄT DES SAARLANDES
Fachbereich 14 – Informatik

Prof. J. Buchmann
Stefan Neis

22. November 1995

6. Übung zu
"Algebra für Informatiker"

1. In der Vorlesung haben wir gesehen:
   Wenn $|G| = p_1^{e_1} \cdots p_k^{e_k}$ eine Faktorisierung der Ordnung von G in ein Produkt von Primzahlpotenzen ist ($p_1, \ldots, p_k$ paarweise verschiedene Primzahlen), dann ist die Ordnung eines Elementes $g \in G$ das Produkt der Ordnungen der Elemente $g^{|G|/p_i^{e_i}}$, $1 \leq i \leq k$.
   Programmiere ausgehend von dieser Idee einen Algorithmus in LiDIA, der die Ordnung eines Elementes in $(\mathbb{Z}/m\mathbb{Z})^*$ berechnet. Bestimme dazu zunächst mit dem Algorithmus des vorletzten Übungsblattes die Gruppenordnung $\varphi(m)$ und faktorisiere diese (mit Hilfe von "rational_factorization").
   Vergleiche die Laufzeit dieses neuen Algorithmus mit der Laufzeit des Babystep – Giantstep – Algorithmus vom vorletzten Übungsblatt.
2. Für $n \in \mathbb{N}, n \geq 3$ wird die Symmetriegruppe des regelmäßigen n–Ecks (D_n) von den Permutationen
   $$a = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix}, \; b = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$$
   erzeugt. Zeige: D_n ist eine Gruppe mit $2n$ Elementen und es gilt:
   (a) $a^n = b^2 = e$, $a^k \neq e$ für $0 < k < n$ (e neutrales Element).
   (b) $b \cdot a = a^{-1} \cdot b$.

   Zeige: Jede Gruppe G, die von Elementen $a, b \in G$ erzeugt wird, die (a) und (b) für ein $n \geq 3$ erfüllen, ist isomorph zu D_n.
   Hinweis: Betrachte die Abbildung $\varphi : D_n \longrightarrow G, a^i b^j \longmapsto a^i b^j$. Zeige, daß diese Abbildung ein Homomorphismus ist, der surjektiv und injektiv ist.
3. Zeige $Q[\frac{1+\sqrt{5}}{2}]$ ist ein Körper.
4. Zeige: In $\mathbb{Z}/m\mathbb{Z}$ sind alle Ideale Hauptideale. Gib einen Algorithmus an, der aus einem Erzeugendensystem für ein Ideal einen Erzeuger berechnet.

Abgabe:

Donnerstag, 30. 11. 1995