Prof. C. P. Schnorr Sommersemester 2006

Diskrete Mathematik

Blatt 3, 05.05.2006, Abgabe 12.05.2006

Aufgabe 1. 6 Punkte. Betrachte $\mathbf{Z}_m = [0, m[$.

1. Zeige: $\mathbf{Z}_m^* = \{b \in [0, m[: \ \mathrm{ggT}(b, m) = 1\}$,

2. Berechne die b^{-1} für alle $b \in \mathbf{Z}_{15}^*$ mit Erläuterung

3. Zeige: $\mathbf{Z}_m$ ist Körper gdw m prim ist.

Aufgabe 2. 5 Punkte. Zeige, dass der Ring $\mathbf{Z}[i]$ der ganzen Gauss'schen Zahlen mit der Abbildung $g(a+ib) = \|a+ib\|^2 = a^2+b^2$ Euklidisch ist.

Hinweis: Zu jedem $z \in \mathbf{C}$ gibt es ein $y \in \mathbf{Z}[i]$ mit $\|z-y\|^2 \le 1/2$.

Aufgabe 3. 6 Punkte. Sei $\alpha \in \mathbf{R}^*$, $\begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{bmatrix} = \begin{bmatrix} 2^n\alpha & , & 1 \\ 2^n & , & 0 \end{bmatrix}$ und $\begin{bmatrix} \mathbf{b}'_1 \\ \mathbf{b}'_2 \end{bmatrix} = \begin{bmatrix} q_1, & -p_1 \\ q_2, & -p_2 \end{bmatrix} \begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{bmatrix}$ reduzierte Basis von $L(\mathbf{b}_1, \mathbf{b}_2)$ mit $p_i, q_i \in \mathbf{Z}$.

Zeige: **1.** $|\alpha - \frac{p_1}{q_1}| \le (\frac{4}{3})^{1/2} q_1^{-2}$, **2.** $(\frac{4}{3})^{-1/2} 2^n \le q_1^2 \le (\frac{4}{3})^{1/2} 2^n$.

Hinweise: $\|\mathbf{b}'_1\|^2 \le (\frac{4}{3})^{1/2} \det L(b_1, b_2) = (\frac{4}{3})^{1/2} 2^n$ und $|\alpha - \frac{p_1}{q_1}| \le (\frac{4}{3})^{1/4} \frac{1}{q_1 2^{n/2}}$.

Aufgabe 4. 4 Punkte. Löse folgendes Kongruenzensystem:

$$x = 18 \bmod 11, \quad x = 3 \bmod 18, \quad x = 7 \bmod 25.$$