Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

Algorithmisches Lernen
Wintersemester 2000/01
Köbler/Lindner

Aufgabenblatt 11

Aufgabe 1

Der Euklidsche Algorithmus zur Berechnung des ggT zweier Zahlen r_0 und r_1 mit $r_0 > r_1$ berechnet schrittweise natürliche Zahlen $r_1 > r_2 > r_3 > \cdots > r_m > 0$ und $q_1 \ldots q_m$,

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\vdots \\ r_{m-2} &= q_{m-1} r_{m-1} + r_m \\ r_{m-1} &= q_m r_m \end{aligned}$$

Zeigen Sie

a) $ggT(r_0, r_1) = ggT(r_1, r_2) = \cdots = ggT(r_{m-1}, r_m) = r_m$

b) $r_i \geq f_{m+1-i}$ für $0 \geq i \geq m$, wobei f_j die j-te Fibonacci-Zahl mit $f_0 = 0$, $f_1 = 1$ und $f_j = f_{j-1} + f_{j-2}$ für $j \geq 2$ bezeichnet.

c) $f_{i+2} \geq b^i$ für $b = \frac{1+\sqrt{5}}{2}$

Aufgabe 2

Der erweiterte Euklidsche Algorithmus berechnet zusätzlich die Zahlen

$$\begin{aligned} t_0 &= 0 \\ t_1 &= 1 \\ t_j &= t_{j-2} - q_{j-1} t_{j-1} \bmod r_0, \quad j \geq 2 \end{aligned}$$

Zeigen Sie $r_j \equiv t_j r_1 (\bmod r_0)$ für $0 \leq j \leq m$ (mittels Induktion)

Aufgabe 3

Zeigen Sie, daß $ggT(a, b) = 1$ genau dann gilt, wenn $\exists x : ax \equiv 1 \pmod b$. (*Hinweis:* Benutzen Sie Aufgabe 2)

Aufgabe 4

Für alle $m \geq 1$ bezeichnet $\mathbb{Z}_m^*$ die Menge $\{a \mid 1 \leq a \leq m-1, ggT(a, m) = 1\}$, und $\phi(m) = \|\mathbb{Z}_m^*\|$. Zeigen Sie, daß $a^{\phi(m)} \equiv 1 \pmod m$ für alle $a \in \mathbb{Z}_m^*$ gilt. (*Hinweis:* Beachten Sie, daß $a \cdot u \not\equiv a \cdot v \pmod m$ für alle $u, v \in \mathbb{Z}_m^*$ mit $u \neq v$, und betrachten Sie das Produkt aller Elemente der Form $a \cdot u$ in $\mathbb{Z}_m^*$)