5. Aufgabe: *GGT*

a) Zu Satz 2.13: Sei F_i für $i \in \mathbb{N}$ die i-te Fibonacci-Zahl (also $F_0 = 0$, $F_1 = 1$ und $F_i = F_{i-1} + F_{i-2}$ für $i \geq 2$). Zeigen Sie, dass $\lfloor F_{i+2}/F_{i+1} \rfloor = 1$ und $F_{i-1} = F_{i+1} \bmod F_i$ für alle $i \geq 2$.

b) Sei $F[x]$ der euklidische univariate Polynomring über einem Körper F. Seien weiter $a, b \in F[x] \setminus \{0\}$ und $g = \mathrm{ggT}(a, b) \in F[x]$. Zeigen Sie, dass es dann für jedes Polynom $c \in F[x]$ mit $g \mid c$ eindeutige Polynome $\sigma, \tau \in F[x]$ gibt, so dass $\sigma a + \tau b = c$ und $\deg(\sigma) < \deg(b) - \deg(g)$ gilt; wenn zudem noch $\deg(c) < \deg(a) + \deg(b) - \deg(g)$ ist, so gilt $\deg(\tau) < \deg(a) - \deg(g)$.

c) Seien $a, b \in \mathbb{N}^+$ und $a > b$. Wir wollen entscheiden, ob es $i, j \in \mathbb{N}^+$ gibt, so dass $a^i = b^j$ ist. Betrachten Sie dazu folgendes Entscheidungsverfahren für dieses Problem:

Teste zuerst, ob $b \mid a$. Wenn nicht, so antworte „nein“. Ansonsten ersetze (a, b) durch $(a/b, b)$, wenn $a \geq b^2$, bzw. durch $(b, a/b)$, wenn $a < b^2$. Wenn durch Iterieren schließlich ein Paar $(a', 1)$ erreicht wird, antworte „ja“.

Zeigen Sie, dass dieses Verfahren das Problem für jede Eingabe korrekt löst (und terminiert) und im schlechtesten Fall $O(\lambda(a)^2)$ Bitoperationen benötigt.

6. Aufgabe: *Division in* $\mathbb{Z}$

a) Wir betrachten noch einmal den Algorithmus zur Division mit Rest nicht negativer ganzer Zahlen zur Basis $b \geq 2$. Es seien $u = (u_0 \cdots u_n)_b$ sowie $v = (v_1 \cdots v_n)_b$ mit $\lfloor u/v \rfloor < b$. Es sei wie in der Vorlesung $\hat{q} = \min\left(\left\lfloor \frac{u_0 b + u_1}{v_1} \right\rfloor, b - 1\right)$ die Schätzung für $q = \lfloor u/v \rfloor$ mit $u = qv + r$ und $0 \leq r < v$.

Zeigen Sie, dass $\hat{q} \geq q$ und für $v_1 \geq \lfloor b/2 \rfloor$ auch $\hat{q} - 2 \leq q$.

b) Finden Sie ein Beispiel für u und v bei Basis 10, so dass die Notwendigkeit der bedingten Anweisung

if $(u_j \cdots u_{j+n})_b < \hat{q} \cdot (v_1 \cdots v_n)_b$ **then** $\hat{q} := \hat{q} - 1$

im Algorithmus aus der Vorlesung klar wird.