Jun.Prof. Dr. C. Diem
diem@math.uni-leipzig.de
http://www.math.uni-leipzig.de/∼diem/la

LINEARE ALGEBRA FÜR INFORMATIKER
ÜBUNGSBLATT NR. 7

Aufgaben für die Übungsgruppen

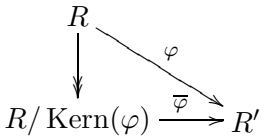
Aufgabe Ü1

a) Bestimmen Sie den ggT von 561 und 221!

b) Bestimmen Sie $x, y \in \mathbb{Z}$ mit $x \cdot 1001 + y \cdot 123 = 1$!

c) Bestimmen Sie das multiplikative Inverse von $[3]_{1009} \in \mathbb{F}_{1009}$!

Aufgabe Ü2 Seien R, R' Ringe und $\varphi : R \longrightarrow R'$ ein Ringhomomorphismus. Zeigen Sie: φ induziert eine eindeutig bestimmte Abbildung $\overline{\varphi} : R/\operatorname{Kern}(\varphi) \longrightarrow R'$ so das das Diagramm



kommutiert. (Hier ist $R \longrightarrow R/\operatorname{Kern}(\varphi)$ der kanonische Homomorphismus $r \mapsto [r]_{\operatorname{Kern}(\varphi)}$.) Die Abbildung $\overline{\varphi}$ ist ein injektiver Ringhomomorphismus.

Aufgabe Ü3 Seien $a_1, \ldots, a_k \in \mathbb{N}$ paarweise teilerfremd (d.h. für alle i, j mit $i \neq j$ ist $\operatorname{ggT}(a_i, a_j) = 1$). Zeigen Sie:

a) Der Kern des Homomorphismus $\mathbb{Z} \longrightarrow \mathbb{Z}/(a_1) \times \cdots \times \mathbb{Z}/(a_k)$ ist das Ideal $(a_1 \cdots a_k)$.

b) Man erhält einen Isomorphismus von Ringen $\mathbb{Z}/(a_1 \cdots a_k) \longrightarrow \mathbb{Z}/(a_1) \times \cdots \times \mathbb{Z}/(a_k)$.

Hinweis. Sie dürfen die eindeutige Primfaktorzerlegung voraussetzen!

Aufgabe Ü4

a) Seien $a_1, \ldots, a_k \in \mathbb{Z}$ paarweise teilerfremd, und seien $c_1, \ldots, c_k \in \mathbb{Z}$. Zeigen Sie: Es gibt ein $x \in \mathbb{Z}$ mit

$$x \equiv c_1 \mod a_1 \,, \quad x \equiv c_2 \mod a_2 \quad, \ \ldots \ , \quad x \equiv c_k \mod a_k \,,$$

und x ist eindeutig bestimmt "modulo $a_1 \cdots a_k$".

b) Geben Sie einen (effizienten) Algorithmus an, mit dem man für alle i ein $x \in \mathbb{Z}$ mit

$$x \equiv 1 \mod a_i, \quad x \equiv 0 \mod a_j \ \text{ für alle } j \neq i$$

finden kann!

c) Verallgemeinern Sie diesen Algorithmus, um beliebige Systeme wie in a) zu lösen!

d) Lösen Sie das System $x \equiv 2 \mod 3$, $x \equiv 1 \mod 4$, $x \equiv 2 \mod 5$!

Schriftliche Hausaufgaben

Abgabe. Bis Freitag, 5.12., 10:00.

Jede der folgenden Aufgaben hat 4 Punkte.

Aufgabe H1

a) Bestimmen Sie $x, y \in \mathbb{Z}$ mit $x \cdot 1009 + y \cdot 123 = 1$!

b) Bestimmen Sie das multiplikative Inverse von $[5]_{1013} \in \mathbb{F}_{1013}$!

c) Lösen Sie das folgende System von Kongruenzen!

$$x \equiv 4 \mod 5 \quad , \quad x \equiv 2 \mod 6 \quad , \quad x \equiv 5 \mod 11$$

Aufgabe H2 Mit der "Schulbuchmethode" kann man zwei natürliche Zahlen n, m mit Bit-Länge $\leq k$ mit $O(k^2)$ Bit-Operationen multiplizieren. Zeigen Sie, dass man zwei solche natürliche Zahlen auch mit $O(k^{\log_2(3)})$ Bit-Operationen multiplizieren kann!
Gehen Sie dabei wie folgt vor:
Nehmen wir an, dass k gerade ist. Dann können wir schreiben: $n = n_0 + n_1 2^{k/2}, m = m_0 + m_1 2^{k/2}$, wobei n_0, n_1, m_0, m_1 höchstens eine Bit-Länge von $k/2$ haben. Nun haben wir die Formel

$$\begin{aligned} nm = & \ (n_0 + n_1 2^{k/2}) \cdot (m_0 + m_1 2^{k/2}) \\ = & \ n_0 m_0 + \big((n_0 + n_1)(m_0 + m_1) - n_0 m_0 - n_1 m_1\big) 2^{k/2} + n_1 m_1 2^k \ . \end{aligned}$$

Geben Sie einen Algorithmus an, in dem diese Formel rekursiv angewendet wird!
Leiten Sie eine rekursive Formel (Ungleichung) für die Komplexität der Multiplikation von zwei Zahlen mit Bit-Länge $k = 2^a$ mittels dieses Algorithmus her, und zeigen Sie dann die Behauptung für beliebige k!

Definition Die *Fibonacci Zahlen* sind wie folgt definiert:
$F_0 := 0, F_1 := 1, F_{n+2} := F_{n+1} + F_n$ für $n \geq 0$.

Aufgabe H3 Sei für natürliche Zahlen a, b $E(a, b)$ die Anzahl der Schritte, die man benötigt, um mittels des Euklidischen Algorithmus den ggT von a und b zu berechnen. D.h. es ist $E(a, b) = 1$ falls $b|a$ und $E(a, b) = E(b, \mathrm{mod}(a, b)) + 1$ falls $b \nmid a$.
Zeigen Sie, dass für $n \in \mathbb{N}$ gilt:

a) $E(F_{n+2}, F_{n+1}) = n$.

b) Seien $a, b \in \mathbb{N}$ mit $a > b$ und $E(a, b) = n$. Dann ist $a \geq F_{n+2}$ und $b \geq F_{n+1}$.

c) Sei $b \in \mathbb{N}$ mit $b \leq F_{n+1}$. Dann gilt für alle $a \in \mathbb{N}$: $E(a, b) \leq n$.