Algebra für Informatiker/Innen
12. Übungsblatt für den 19. und 20. Juni 2008

88. Für das RSA-Verfahren wählen wir $p = 5$, $q = 11$ und $e = 13$. Chiffrieren Sie $(01, 22, 03, 08)$ und deffrichieren Sie das Ergebnis.

89. Frau Huber sendet Herrn Müller mit dem RSA-Verfahren die Nachricht PMOXY. Herr Müller weiß, dass Frau Huber das RSA-Verfahren mit ($n = 35$, $e = 5$) verwendet hat (A= 0, Z= 25). Entschlüsseln Sie die Nachricht.

90. Zeigen Sie, dass es in einem Körper für jedes Element x höchstens ein Element y mit $x \cdot y = 1$ gibt.

91. Zeigen Sie, dass das Produkt zweier Elemente in einem Körper nur dann 0 ist, wenn einer der Faktoren gleich 0 ist.

92. Definieren Sie geeignete Operationen a, b, c, d, sodass $\langle (\mathbb{Z}_7)^3, a, b, c, d \rangle$ ein Vektoraum über $\mathbb{Z}_7$ ist. Beweisen Sie auch Ihre Behauptung.

93. Bestimmen Sie eine Basis des folgenden Unterraums des Vektorraums $(\mathbb{Z}_7)^3$:
$$\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in (\mathbb{Z}_7)^3 | x + 2y + z = 0 \}$$

94. Zeigen Sie, dass $\langle \mathbb{R}^{\mathbb{R}}, +, -, 0, \cdot \rangle$ ein Vektorraum über $\mathbb{R}$ ist. $\mathbb{R}^{\mathbb{R}}$ bezeichnet die Menge aller Funktionen (Abbildungen) von $\mathbb{R}$ nach $\mathbb{R}$. Weiters sei für alle $f, g \in \mathbb{R}^{\mathbb{R}}$ und $\lambda \in \mathbb{R}$
$$\begin{aligned} f + g: &\quad \mathbb{R} \to \mathbb{R}, \quad x \mapsto f(x) + g(x) \\ -f: &\quad \mathbb{R} \to \mathbb{R}, \quad x \mapsto -f(x) \\ 0: &\quad \mathbb{R} \to \mathbb{R}, \quad x \mapsto 0 \\ \lambda \cdot f &\quad \mathbb{R} \to \mathbb{R}, \quad x \mapsto \lambda \cdot f(x). \end{aligned}$$

95. Zeigen Sie, dass die Polynommultiplikation assoziativ ist.