Algebra für Informatiker/innen
12. Übungsblatt für den 18. und 19. Juni 2009

(Für „Nebenrechnungen“ dürfen Sie wie gewohnt Mathematica verwenden).

1. Berechnen Sie jeweils den ggT **mit Kofaktoren** für folgende Polynome:
   (a) $2x^4 + x^2 + x, \quad x^2 + x$ über $\mathbb{Z}_3$
   (b) $x^5 + x^4 + x^2 + x, \quad x^4 + 1$ über $\mathbb{Z}_2$

2. Bestimmen Sie jeweils die Anzahl der Elemente folgender Faktorringe.
   Welche davon sind Körper?
   (a) $\mathbb{Z}_7[x] \,/\, (x^3 + 3x + 2)$
   (b) $\mathbb{Z}_2[x] \,/\, (x^2 + x + 1)$
   (c) $\mathbb{Z}_4[x] \,/\, (x^3 + 3)$
   (d) $\mathbb{Z}_3[x] \,/\, (x^2 + 2)$

3. Sei $p = x^2 + 1$ und sei $K = \mathbb{Z}_3[x] \,/\, (p)$. Berechnen Sie in diesem Körper:
   (a) $[x^2 + x + 1]_p + [x^3 + 2x]_p$
   (b) $[2x^2 + x + 2]_p \cdot [x^2 + 2x + 1]_p$
   (c) ${[x^2 + 2x]_p}^{-1}$
   (d) Finden Sie ein $q \in K$ mit $[x^2 + 1]_p \cdot q = [2x + 1]_p$

4. Lösen Sie folgendes lineare Gleichungssystem über $\mathbb{Z}_3[x] \,/\, (x^2 + 1)$.

$$\begin{pmatrix} \boldsymbol{x+1} & \boldsymbol{2x+1} \\ \boldsymbol{2x} & \boldsymbol{x+2} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{u} \\ \boldsymbol{v} \end{pmatrix} = \begin{pmatrix} \boldsymbol{x+1} \\ \boldsymbol{2} \end{pmatrix}$$

5. Zeigen oder widerlegen Sie: Ein Polynom vom Grad 2 oder 3 ist irreduzibel genau dann, wenn es keine Nullstellen hat.

6. (a) Finden Sie, falls möglich, ein reduzibles Polynom vom Grad 4 über $\mathbb{Z}_2$, das aber keine Nullstellen hat.
   (b) Finden Sie, falls möglich, ein irreduzibles Polynom vom Grad 4 über $\mathbb{Z}_2$.

7. Ist $a = 2$ nach dem Test von Miller-Rabin ein Zeuge gegen die Primalität von 561?

8. Seien $B = ((1,1,1), (1,0,1), ((-1,1,1))$ bzw. $C = ((1,0), (0,1))$ Basen des $\mathbb{R}^3$ bzw. $\mathbb{R}^2$
   und sei $h(x, y, z) = (x + 3y - z, 2y + 3z)$.
   Bestimmen Sie $S_{h(B,C)}$.