Feruzan Ay (ayferuzan@yahoo.de)
Marco Kunze (makunze@cs.tu-berlin.de)
Sebastian Nowozin (nowozin@cs.tu-berlin.de)

SS 2003
28. 6. 2003

Lösungen zum 6. Übungsblatt
Diskrete und strukturelle Mathematik für Informatiker

Lösung zu Aufgabe 1:

a) Da $|\{x^{p-1}|x \in \mathbb{Z}_p \setminus \{0\}\}|$ laut Satz 3.4 im Skript immer Eins ist, bleibt zu zeigen:

$$|\{x^{p-2}|x \in \mathbb{Z}_p \setminus \{0\}\}| = p - 2$$

Weiter gilt nach Satz 3.3 im Skript, dass $\mathbb{Z}_p$ ein Körper ist, da p prim ist. Wir beweisen die obige Formel.

Dazu sei $x \in \mathbb{Z}_p \setminus \{0\}$ und $e \in \mathbb{Z}_p$ das Einserelement. Wir definieren $b \in \mathbb{Z}_p$ als:

$$b := x^{p-2}$$

Dann gilt:

$$\begin{array}{rcl} & b & = x^{p-2} \\ \Leftrightarrow & b \cdot x \cdot x & = x^{p-2} \cdot x \cdot x \\ \Leftrightarrow & b \cdot x \cdot x & = x^{p} \\ \Leftrightarrow & b \cdot x \cdot x & = x \\ \Leftrightarrow & b \cdot x \cdot x & = e \cdot x \\ \Leftrightarrow & b \cdot x & = e \\ \Leftrightarrow & b & = x^{-1} \end{array}$$

Da $\mathbb{Z}_p$ ein Körper ist, gibt es zu jedem $x \in \mathbb{Z}_p \setminus \{0\}$ genau ein eindeutiges und verschiedenes Inverses x^{-1}, d.h. es gilt:

$$|\{x^{p-2}|x \in \mathbb{Z}_p \setminus \{0\}\}| = |\{x^{-1}|x, x^{-1} \in \mathbb{Z}_p, x \cdot x^{-1} = e\}| = p - 1$$

Dann ist

$$|\{x \in \mathbb{Z}_p\}| = p - 1 + 1 = p$$

was zu zeigen war.

b) Zunächst, der Beweis, dass das zu Zeigende nicht gilt:

$$\sum_{x \in \mathbb{Z}_2} x = 1$$

Allerdings gilt die Gleichung für alle $p > 2$. Was nun zu zeigen wäre.

$$\begin{aligned} \sum_{x \in Z_p} x &= \sum_{x=1}^{p-1} x \\ &= \frac{p \cdot (p+1)}{2} \end{aligned}$$

Zu zeigen:

$$\frac{p \cdot (p-1)}{2} \equiv 0 \bmod p$$

Da $p > 2$, und jedes $p > 2$ ungerade, folgt, dass $p-1$ gerade. Folglich ist $\frac{p-1}{2}$ eine ganze Zahl und sei hier k genannt. Also ist zu zeigen

$$p \cdot k \equiv 0 \bmod p$$

was leicht ersichtlich ist. Damit ist die Formel bewiesen, q.e.d. $\square$

Lösung zu Aufgabe 2:

- in $\mathbb{R}[x]$:

$$\begin{aligned}
x^5 + 4x^4 + 4x^3 - 2x^2 - 8x - 3 &= (x+1) \cdot (x^4 + 3x^3 - 2x - 6) + (x^3 + 3) \\
x^4 + 3x^3 - 2x - 6 &= (x+3) \cdot (x^3 + 3) + (-5x - 15) \\
x^3 + 3 &= (-\frac{1}{5}x^2 + \frac{3}{5}x - \frac{9}{5}) \cdot (-5x - 15) + (-24) \\
-5x + 15 &= (\frac{5}{24}x + \frac{15}{24}) \cdot (-24) + 0
\end{aligned}$$

  Folglich ist -24 der gesuchte ggT.

- in $\mathbb{Z}_5[x]$:

$$\begin{aligned}
x^5 + 4x^4 + 4x^3 - 2x^2 - 3x - 3 &= (x+1) \cdot (x^4 + 3x^3 - 2x - 1) + (x^3 - 2) \\
x^4 + 3x^3 - 2x - 1 &= (x+3) \cdot (x^3 - 2) + 0
\end{aligned}$$

  Folglich ist $(x^3 - 2)$ der gesuchte ggT.

Lösung zu Aufgabe 3:

- Wir zeigen: $x^4 + 1$ ist reduzibel über $\mathbb{Z}_2$, da

$$x^4 + 1 = (x^2 + 1)(x^2 + 1)$$

- Wir zeigen: $x^4 + 1$ ist irreduzibel über $\mathbb{Q}$.

  Nehmen wir dazu an, $x^4 + 1$ sei reduzibel. Nach Skript (2) ist

$$x^4 + 1 = (x^j + b_{j-1}x^{j-1} + \ldots + b_0)(x^k + c_{k-1}x^{k-1} + \ldots + c_0)$$

  mit $0 < j < 4, 0 < k < 4$ und $b_0, \ldots, b_{j-1}, c_0, \ldots, c_{k-1} \in \mathbb{Q}$.

  Wir machen eine Fallunterscheidung bezüglich j:

  - Sei $j = 3$. Dann folgt $k = 1$ und es gilt:

$$\begin{aligned}
x^4 + 1 &= (x^3 + b_2x^2 + b_1x + b_0)(x + c_0) \\
&= x^4 + b_2x^3 + b_1x^2 + b_0x + c_0x^3 + c_0b_2x^2 + c_0b_1x + c_0b_0 \\
&= x^4 + (b_2 + c_0)x^3 + (c_0b_2 + b_1)x^2 + (c_0b_1 + b_0)x + c_0b_0
\end{aligned}$$

Daraus folgt ein Gleichungssystem

$$
\begin{aligned}
& b_2 + c_0 = 0 && (1)\\
\wedge \quad & c_0 b_2 + b_1 = 0 && (2)\\
\wedge \quad & c_0 b_1 + b_0 = 0 && (3)\\
\wedge \quad & c_0 b_0 = 1 && (4)
\end{aligned}
$$

Aus der Gleichung (4) ergibt sich, dass $c_0 = \frac{1}{b_0}$. Mit (3) folgt, dass $b_1 = -b_0 b_0$ ist. Jetzt folgt mit (2) das $b_2 = b_0 b_0 b_0 = b_0^3$ ist. Mit (1) folgt aus $b_0^3 + c_0 = 0$ das $c_0 = -b_0^3$ ist. Mit der am Anfang aus (4) gefolgten Bedingung ergibt sich:

$$-b_0^3 = \frac{1}{b_0} \Leftrightarrow -b_0^4 = 1$$

Diese Gleichung hat offensichtlich in $\mathbb{Q}$ keine Lösung.

– Sei $j = 2$. Dann folgt $k = 2$ und es gilt:

$$
\begin{aligned}
x^4 + 1 &= (x^2 + b_1 x + b_0)(x^2 + c_1 x + c_0)\\
&= x^4 + b_1 x^3 + b_0 x^2 + c_1 x^3 + c_1 b_1 x^2 + c_1 b_0 x + c_0 x^2 + c_0 b_1 x + c_0 b_0\\
&= x^4 + (c_1 + b_1)x^3 + (c_0 + c_1 b_1 + b_0)x^2 + (c_0 b_1 + c_1 b_0)x + c_0 b_0
\end{aligned}
$$

Daraus folgt wiederum ein Gleichungssystem:

$$
\begin{aligned}
& c_1 + b_1 = 0 && (5)\\
\wedge \quad & c_0 + c_1 b_1 + b_0 = 0 && (6)\\
\wedge \quad & c_0 b_1 + c_1 b_0 = 0 && (7)\\
\wedge \quad & c_0 b_0 = 1 && (8)
\end{aligned}
$$

Aus (5) folgt $c_1 = -b_1$. Mit (7) gilt: $c_0 b_1 - b_1 b_0 = 0 \Leftrightarrow b_1(c_0 - b_0) = 0$. Also ist $b_1 = 0$ oder $c_0 = b_0$. Fallunterscheidung:

∗ Sei $b_1 = 0$, dann ist wegen (5) auch $c_1 = 0$. Dann ist wegen (6) auch $c_0 = -b_0$ und (8) jetzt nicht mehr erfüllbar.

∗ Sei $c_0 = b_0$, dann ist wegen (8): $c_0 = b_0 = 1$ oder $c_0 = b_0 = -1$. Dann ist wegen (7) auch $c_1 = -b_1$. Wegen (6) muss $c_0 + (-b_1)b_1 + c_0 = 0 \Leftrightarrow b_1^2 = 2c_0$ sein. Das heißt es ist zu lösen: $b_1^2 = \pm 2$, d.h. es gibt in $\mathbb{Q}$ keine Lösung.

Damit ist $x^4 + 1$ in $\mathbb{Q}$ irreduzibel.

Lösung zu Aufgabe 4:

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	x^3	x^2+x	x^3+x^2	x^3+x^2+x
$x+1$	0	$x+1$	x^2+x	x^2+1	x^3+x^2	x^3+x^2+x+1	x^3+x	x^3+1
x^2	0	x^2	x^3	x^3+x^2	x^4	x^4+x^2	x^4+x^3	$x^4+x^3+x^2$
x^2+1	0	x^2+1	x^2+x	x^3+x^2+x+1	x^4+x^2	x^4+1	$x^4+x^3+x^2+x$	x^4+x^3+x+1
x^2+x	0	x^2+x	x^3+x^2	x^3+x	x^4+x^3	$x^4+x^3+x^2+x$	x^4+x^2	x^4+x
x^2+x+1	0	x^2+x+1	x^3+x^2+x	x^3+1	$x^4+x^3+x^2$	x^4+x^3+x+1	x^4+x	x^4+x^2+1