ETH Zürich, D-INFK
HS 2016, 17. November 2016

Prof. Ueli Maurer
Daniel Tschudi

Diskrete Mathematik

Lösung 10

10.1 Eigenschaften kommutativer Ringe

Sei $\langle R; +, -, 0, \cdot, 1\rangle$ ein kommutativer Ring und $a, b, c \in R$.

a) Aus $a|b$ folgt $\exists d\ b = ad$ und damit $bc = (ad)c = a(dc)$. Somit gilt $a|bc$.

b) Aus $a|b$ folgt $\exists d\ b = ad$ und aus $a|c$ folgt $\exists e\ c = ae$. Nun gilt $b+c = ad+ae = a(d+e)$ und daher auch $a|(b+c)$.

10.2 Nullteiler und Integritätsbereiche

a) Sei $a(x) = \sum_{i=0}^{d} a_i x^i$ mit Grad d und $a_d = 1$. Wir müssen zeigen, dass kein Polynom $b(x) \in R[x] - \{0\}$ existiert mit $a(x)b(x) = 0$ oder $b(x)a(x) = 0$. *(1 Punkt)*

Sei also $b(x) = \sum_{i=0}^{d'} b_i x^i \in R[x] - \{0\}$ mit Grad d' beliebig, wobei $b_{d'} \neq 0$ der höchste Koeffizient ist. Daraus folgt aber für $a(x)b(x)$, dass der höchste Koeffizient $a_d b_{d'} = b_{d'} \neq 0$ ist. *(1 Punkt)*

Somit gilt $a(x)b(x) \neq 0$. Analog gilt $b(x)a(x) \neq 0$, da auch $b_{d'}a_d = b_{d'} \neq 0$ ist. Das Polynom $a(x)$ ist daher kein Nullteiler. *(1 Punkt)*

b) Sei D ein endlicher Integritätsbereich, d.h. D ist ein nichttrivialer, kommutativer Ring ohne Nullteiler. Ein Körper ist ein nichttrivialer, kommutativer Ring, in dem jedes Element ausser 0 eine Einheit ist. Wir müssen also zeigen, dass jedes $d \in D - \{0\}$ ein multiplikatives Inverses besitzt. *(1 Punkt)*

Wir führen einen Beweis durch Widerspruch und nehmen an, es existiert ein $d \in D - \{0\}$, das keine Einheit ist. *(1 Punkt)*

Sei $(d) := \{d \cdot a \mid a \in D\}$, dann gilt $1 \notin (d)$ und somit, da D endlich ist, auch $|(d)| < |D|$. Nach dem Schubfachprinzip existieren daher $a, b \in D$ mit $a \neq b$ und $d \cdot a = d \cdot b$. *(1 Punkt)*

Daraus folgt[1] $d \cdot (a - b) = 0$. *(1 Punkt)*

Da sowohl d als auch $a - b$ ungleich 0 sind, widerspricht dies der Nullteilerfreiheit von D. Daher ist d eine Einheit und D ein Körper. *(1 Punkt)*

10.3 Lineares Gleichungssystem

Wir verwenden eine Art Gausssche Eliminationsverfahren (über $\mathbb{Z}_{11}$). Dabei ist es praktisch zu jeder Einheit in $\mathbb{Z}_{11}$ die Inversen zu kennen. Wir berechen daher folgende Tabelle.

[1] Nach der Lösung der Aufgabe 9.6 b) gilt $-(d \cdot b) = d \cdot (-b)$.

Element	1	2	3	4	5	6	7	8	9	10
mult. Inverses	1	6	4	3	9	2	8	7	5	10
addt. Inverses	10	9	8	7	6	5	4	3	2	1

Wir können das Gleichungssystem als Matrix darstellen.

$$\begin{bmatrix} 10 & 2 & 5 & 1 \\ 7 & 4 & 6 & 2 \\ 3 & 6 & 9 & 4 \end{bmatrix}$$

Nun beginnen wir mit der Vorwärtselimination. Wir multiplizieren die erste Zeile mit 10, da $10 \odot 10 = 1$.

$$\begin{bmatrix} 1 & 9 & 6 & 10 \\ 7 & 4 & 6 & 2 \\ 3 & 6 & 9 & 4 \end{bmatrix}$$

Nun eliminieren wir die Variable x in den unteren zwei Zeilen. Da $\ominus 7 = 4$ addieren wir die erste Zeile viermal zur zweiten Zeile.

$$\big[7 \oplus (4 \odot 1),\ 4 \oplus (4 \odot 9),\ 6 \oplus (4 \odot 6),\ 2 \oplus (4 \odot 10)\big] = \big[0,\ 7,\ 8,\ 9\big]$$

Analog addieren wir achtmal die erste Zeile zur dritten (da $\ominus 3 = 8$).

$$\big[3 \oplus (8 \odot 1),\ 6 \oplus (8 \odot 9),\ 9 \oplus (8 \odot 6),\ 4 \oplus (8 \odot 10)\big] = \big[0,\ 1,\ 2,\ 7\big]$$

Wir vertauschen die dritte Zeile mit der zweiten Zeile und erhalten folgende Matrix.

$$\begin{bmatrix} 1 & 9 & 6 & 10 \\ 0 & 1 & 2 & 7 \\ 0 & 7 & 8 & 9 \end{bmatrix}$$

Danach addieren wir viermal die zweite Zeile zur dritten Zeile ($\ominus 7 = 4$).

$$\big[0 \oplus (4 \odot 0),\ 7 \oplus (4 \odot 1),\ 8 \oplus (4 \odot 2),\ 9 \oplus (4 \odot 7)\big] = \big[0,\ 0,\ 5,\ 4\big]$$

Wir multiplizieren die letzte Zeile mit neun ($5 \odot 9 = 1$) und erhalten.

$$\begin{bmatrix} 1 & 9 & 6 & 10 \\ 0 & 1 & 2 & 7 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

Nun können wir die Rückwärtselimination beginnen. Dazu addieren wir die letzte Zeile neunmal zur zweiten Zeile ($\ominus 2 = 9$) und fünfmal zur ersten Zeile ($\ominus 6 = 5$).

$$\begin{bmatrix} 1 & 9 & 0 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

Zum Schluss addieren wir die zweite Zeile zweimal zur ersten Zeile ($\ominus 9 = 2$).

$$\begin{bmatrix} 1 & 0 & 0 & 5 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

Wir erhalten $x = 5$, $y = 1$ und $z = 3$.

10.4 Rechnen mit Polynomen

a) In $\mathbb{Z}_7$ ist 3 das multiplikative Inverse von 5, da $3 \cdot 5 \equiv_7 1$. Daher ist der erste Koeffizient des Resultats $5^{-1} = 3$ (in $\mathbb{Z}_7$). Die restlichen Berechnungen verlaufen analog.

$$
\begin{array}{rrrrrrl}
(x^5 & & & +\,6x^2 & & +5) & : \ (5x^2+2x+1) \ = \ 3x^3+3x^2+x+3 \\
-(x^5 & +\,6x^4 & +\,3x^3 & & &) & \\
\hline
 & x^4 & +\,4x^3 & +\,6x^2 & + & +5 & \\
 & -(\ x^4 & +\,6x^3 & +\,3x^2 & &) & \\
\hline
 & & 5x^3 & +\,3x^2 & + & +5 & \\
 & & -(5x^3 & +\,2x^2 & +\,x &) & \\
\hline
 & & & + \ x^2 & +6x & +5 & \\
 & & & -(\ x^2 & +6x & +3) & \\
\hline
 & & & \text{Rest:} & & 2 &
\end{array}
$$

b) Die gesuchten Polynome sind $x^4 + x^3 + 1$, $x^4 + x + 1$ und $x^4 + x^3 + x^2 + x + 1$.

Wir möchten dies zeigen, indem wir alle *reduziblen* Polynome von Grad vier ausschliessen. Obige sind dann die einzigen, welche noch auftreten. Ein Polynom $p(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ von Grad vier ist sicher dann reduzibel, wenn $a_0 = 0$, denn nach Lemma 5.29 gilt genau dann $x \mid p(x)$. Angenommen, $a_0 = 1$. Es gilt nach Lemma 5.29 genau dann $(x + 1) \mid p(x)$, wenn $-1 = 1$ eine Nullstelle von $p(x)$ ist. Dies ist aber genau dann der Fall, wenn $a_3 + a_2 + a_1 = 0$ ist, was wir also auch ausschliessen.

Wir haben jetzt bereits alle Polynome mit linearen Faktoren ausgeschlossen; es bleiben also lediglich solche mit mindestens quadratischen Faktoren. Davon gibt es aber nur eines, nämlich $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, denn alle Polynome von Grad zwei ausser $x^2 + x + 1$ sind reduzibel, und haben damit einen linearen Faktor.

Übrig bleiben die Polynome x^4+x^3+1, x^4+x+1 und $x^4+x^3+x^2+x+1$ welche somit weder einen linearen noch einen quadratischen Faktor haben, und damit irreduzibel sind.

c) Da 2 eine doppelte Nullstelle ist, muss $a(x) = (x - 2)^2 b(x)$ sein, wobei $b(x)$ ein Polynom von Grad zwei ist.

Wir wissen, dass $a(3) = 2 = (3 - 2)^2\, b(3)$, $a(4) = (4 - 2)^2\, b(4) = 3$ und $a(6) = (6 - 2)^2\, b(6) = 5$. Wir folgern für das Polynom $b(x)$, dass $b(3) = 2$, $b(4) = 3 \cdot 4^{-1} = 6$ und $b(6) = 5 \cdot 2^{-1} = 6$. Wir verwenden Lagranges Interpolationsformel, um $b(x)$ zu bestimmen:

$$
\begin{aligned}
b(x) &= 2\frac{(x-4)(x-6)}{(3-4)(3-6)} + 6\frac{(x-3)(x-6)}{(4-3)(4-6)} + 6\frac{(x-3)(x-4)}{(6-3)(6-4)} \\
&= 3(x+3)(x+1) + 4(x+4)(x+1) + (x+4)(x+3) \\
&= x^2 + 4x + 2
\end{aligned}
$$

Daraus folgt $a(x) = (x - 2)^2(x^2 + 4x + 2) = x^4 + 4x^2 + x + 1$ und $a(0) = 1$.

10.5 Absicherung von Nuklearwaffen

a) Das Polynom $a(x)$ von Grad $t - 1$ ist durch die Werte an t verschiedenen Stützstellen

eindeutig bestimmt. Ein Share $s_i = a(\alpha_i)$ entspricht dem Wert von $a(x)$ an der Stützstelle α_i. Die Generäle können also mit ihren t Shares (und den α_i) das Polynom mit der Lagrange-Interpolation rekonstruieren. Der Schlüssel entspricht dann dem Wert $s = a(0)$.

b) Seien dem General die Shares $s_1, \ldots, s_{t-1}$ bekannt. Wir zeigen, dass jeder Schlüssel zu diesen $t-1$ Shares passt kann. Dazu beweisen wir, dass für jedes $s' \in \mathrm{GF}(q)$ ein Polynom $a'(x) \in GF(q)[x]$ mit Grad $t-1$ existiert, so dass $a'(0) = s'$ und $a'(\alpha_i) = s_i$ für $1 \leq i < t$. Da $\forall i\ \alpha_i \neq 0$ gilt, ist der Wert von $a'(x)$ an genau t Stützstellen festgelegt. Das Lemma 5.32 besagt nun, dass (genau) ein solches $a'(x)$ existiert. Für den General bedeutet dies, dass seine $t-1$ Shares (allein) wertlos sind. Er könnte genau so gut versuchen den Schlüssel ohne Shares zu erraten. Alternativ kann er aber auch versuchen einen weiteren Share zu bekommen (vgl. a)).