Abgabe Algebra 1, Blatt 07

Studierende(r): Weerts, Steffen, steffen.weerts@uni-oldenburg.de

Aufgabe 7.1

(a) Bestimmen Sie all Lösungen $x \in \mathbb{Z}$ der folgenden simultanen Kongruenzen:

(i) $2X \equiv 1 \mod 3,\ 3X \equiv 2 \mod 5,\ X \equiv 1 \mod 11,\ X \equiv -11 \mod 14.$
Es gilt:

$$2X \equiv 1 \mod 3 \iff 2X \equiv 4 \mod 3 \iff X \equiv 2 \mod 3,$$

$$3X \equiv 2 \mod 5 \iff 3X \equiv -3 \mod 5 \iff X \equiv 4 \mod 5,$$

$$X \equiv 1 \mod 11,$$

$$X \equiv -11 \mod 14 \iff X \equiv 3 \mod 14.$$

Seien $m_1 = 3, m_2 = 5, m_3 = 11, m_4 = 14; m = 3 \cdot 5 \cdot 11 \cdot 14 = 2310.$
Außerdem seien:

$$N_1 = \frac{m}{m_1} = 770, \qquad N_2 = \frac{m}{m_2} = 462,$$
$$N_3 = \frac{m}{m_3} = 210, \qquad N_4 = \frac{m}{m_4} = 165.$$

Bestimme nun Inverse zu $[N_i]_{m_i}\ \forall 1 \leq i \leq 4.$
Es gilt:

$$\begin{aligned}
[N_1]_{m_1} = [770]_3 = [2]_3 &\implies [N_1]_{m_1} \cdot [y_1]_{m_1} = [2]_3 \cdot [2]_3 = [1]_3,\\
[N_2]_{m_2} = [462]_5 = [2]_5 &\implies [N_2]_{m_2} \cdot [y_2]_{m_2} = [2]_5 \cdot [3]_5 = [1]_5,\\
[N_3]_{m_3} = [210]_{11} = [1]_{11} &\implies [N_3]_{m_3} \cdot [y_3]_{m_3} = [1]_{11} \cdot [1]_{11} = [1]_{11},\\
[N_4]_{m_4} = [165]_{14} = [11]_{14} &\implies [N_4]_{m_4} \cdot [y_4]_{m_4} = [11]_{14} \cdot [9]_{14} = [1]_{14}.
\end{aligned}$$

Nach Bemerkung 4.7.12 gilt:

$$b = 2 \cdot 770 \cdot 2 + 4 \cdot 462 \cdot 3 + 1 \cdot 210 \cdot 1 + 3 \cdot 165 \cdot 9 = 3080 + 5544 + 210 + 4455 = 13269.$$

$= 13289.\ \ -0,5$ P

Die Lösung der simultanen Kongruenzen ist nach Satz 4.7.5 eindeutig modulo m. Die Lösungsmenge ist also

$$\{13269 + 2310z \mid z \in \mathbb{Z}\} = \{1719 + 2310z \mid z \in \mathbb{Z}\}.$$

$\square$

(ii) Es gilt $X \equiv 2 \mod 3,\ X \equiv 1 \mod 5,\ X \equiv 5 \mod 84$.
Da $3 \mid 84$ gilt:

$$X \equiv 5 \mod 84 \implies X \equiv 5 \mod 3 \implies X \equiv 2 \mod 3.$$

Demnach ist die Kongruenz $X \equiv 2 \mod 3$ in der Kongruenz $X \equiv 5 \mod 84$ enthalten, weshalb sie weggelassen werden kann.

Betrachte also die Kongruenzen $X \equiv 1 \mod 5,\ X \equiv 5 \mod 84$.
Sei $m = 5 \cdot 84 = 420$. Seien außerdem

$$N_1 = \frac{m}{m_1} = 84, \qquad N_2 = \frac{m}{m_2} = 5.$$

Es gilt:

$$\begin{aligned}
&[N_1]_{m_1} = [84]_5 = [4]_5 &&\implies [N_1]_{m_1} \cdot [y_1]_{m_1} = [4]_5 \cdot [4]_5 = [1]_5,\\
&[N_2]_{m_2} = [5]_{84} &&\implies [N_2]_{m_2} \cdot [y_2]_{m_2} = [5]_{84} \cdot [17]_{84} = [85]_{84} = [1]_5.
\end{aligned}$$

Nach Bemerkung 4.7.12 gilt:

$$b = 1 \cdot 84 \cdot 4 + 5 \cdot 5 \cdot 17 = 336 + 425 = 761.$$

Die Lösung b der simultanen Kongruenzen ist nach Satz 4.7.5 eindeutig modulo m. Die Lösungsmenge ist also

$$\{761 + 420z \mid z \in \mathbb{Z}\} = \{341 + 420z \mid z \in \mathbb{Z}\}.$$

Probe: Es gilt: $3 \mid 420z,\ 5 \mid 420z,\ 84 \mid 420z\ \forall z \in \mathbb{Z}$, daher muss nur gezeigt werden, dass die Kongruenzen für 341 gelten.

$$\begin{aligned}
341 &= 113 * 3 + 2 \equiv 2 \mod 3.\\
341 &= 68 * 5 + 1 \equiv 1 \mod 5.\\
341 &= 4 * 84 + 5 \equiv 5 \mod 84.
\end{aligned}$$

□

Punkte Teil a): $3,5/4$

(b) Sei $R[t] = \mathbb{Z}_3[t]$. Es gilt $X \equiv 1 \mod (t+1),\ X \equiv t+2 \mod (t^2+1), X \equiv t^2 + t \mod (t^3 + t^2 + 2)$. Sei

$$\begin{aligned}
N =& m_1 \cdot m_2 \cdot m_3\\
=& (t+1) \cdot (t^2+1) \cdot (t^3 + t^2 + 2)\\
=& t^6 + t^5 + 2t^3 + t^4 + t^3 + 2t + t^5 + t^4 + 2t^2 + t^3 + t^2 + 2\\
=& t^6 + 2t^5 + 2t^4 + t^3 + 2t + 2.
\end{aligned}$$

Seien

$$\begin{aligned}
N_1 &= (t^2+1)\cdot(t^3+t^2+2) &&= t^5+t^4+2t^2+t^3+t^2+2 &&= t^5+t^4+t^3+2,\\
N_2 &= (t+1)\cdot(t^3+t^2+2) &&= t^4+t^3+2t+t^3+t^2+2 &&= t^4+2t^3+t^2+2t+2,\\
N_3 &= (t+1)\cdot(t^2+1) &&= t^3+t+t^2+1 &&= t^3+t^2+t+1.
\end{aligned}$$

Es gilt:

$$\begin{aligned}
&[N_1]_{m_1} = [t^5+t^4+t^3+2]_{t+1} = [1]_{t+1}\\
&\qquad \implies [N_1]_{m_1}\cdot[y_1]_{m_1} = [1]_{t+1}\cdot[1]_{t+1} = [1]_{t+1}\\
&[N_2]_{m_2} = [t^4+2t^3+t^2+2t+2]_{t^2+1} = [2]_{t^2+1}\\
&\qquad \implies [N_1]_{m_2}\cdot[y_1]_{m_2} = [2]_{t^2+1}\cdot[2]_{t^2+1} = [1]_{t^2+1}\\
&[N_3]_{m_3} = [t^3+t^2+t+1]_{t^3+t^2+2} = [t-1]_{t^3+t^2+2}\\
&\qquad \implies [N_1]_{m_3}\cdot[y_1]_{m_3} = [t-1]_{t^3+t^2+2}\cdot[2t^2+t+1]_{t^3+t^2+2} = [1]_{t^3+t^2+2}.
\end{aligned}$$

Definiere $b_1+b_2+b_3=b$ so, dass sie Summe aus Bemerkung 4.7.12 sind:

$$\begin{aligned}
b_1 &:= 1\cdot(t^5+t^4+t^3+2)\cdot 1\\
&= t^5+t^4+t^3+2,\\
b_2 &:= (t+2)\cdot(t^4+2t^3+t^2+2t+2)\cdot 2\\
&= (t\cdot(t^4+2t^3+t^2+2t+2)+2\cdot(t^4+2t^3+t^2+2t+2))\cdot 2\\
&= (t^5+2t^4+t^3+2t^2+2t+2t^4+t^3+2t^2+t+1)\cdot 2\\
&= (t^5+t^4+2t^3+t^2+1)\cdot 2\\
&= 2t^5+2t^4+t^3+2t^2+2,\\
b_3 &:= (t^2+t)\cdot(t^3+t^2+t+1)\cdot(2t^2+t+1)\\
&= ((t^5+t^4+t^3+t^2)+(t^4+t^3+t^2+t))\cdot(2t^2+t+1)\\
&= (t^5+2t^4+2t^3+2t^2+t)\cdot(2t^2+t+1)\\
&= (2t^7+t^6+t^5+t^4+2t^3)+(t^6+2t^5+2t^4+2t^3+t^2)+(t^5+2t^4+2t^3+2t^2+t)\\
&= 2t^7+2t^6+t^5+2t^4+t.
\end{aligned}$$

Nach Bemerkung 4.7.12 gilt:

$$\begin{aligned}
b &= b_1+b_2+b_3\\
&= t^5+t^4+t^3+2+2t^5+2t^4+t^3+2t^2+2+2t^7+2t^6+t^5+2t^4+t\\
&= 2t^7+2t^6+t^5+2t^4+2t^3+2t^2+t+1.
\end{aligned}$$

Die Lösung b der simultanen Kongruenzen ist nach Satz 4.7.5 eindeutig modulo N. Mit $f := 2t^7+2t^6+t^5+2t^4+2t^3+2t^2+t+1, g := t^6+2t^5+2t^4+t^3+2t+2 \in \mathbb{Z}_3[t]$ ist die Lösungsmenge ist also

$$\{b+Nz \mid z\in\mathbb{Z}\} = \{f+gz \mid z\in\mathbb{Z}\}\,.$$

$\square$

Punkte Teil b): 3/3

(c) Sei $R = \mathbb{Z}[i], m_1 := 11 \in R, m_2 := 3 + 2i \in R, m_3 := 13 \in R$.
Es gilt:

$$X \equiv 1 \mod 11, X \equiv 2 \mod (3+2i), X \equiv 2 \mod 13.$$

Da $m_2 = (3+2i) \mid (3+2i) \cdot (3-2i) = 13 = m_3$ gilt, ist $X \equiv 2 \mod 13$ eine stärkere Einschränkung als $X \equiv 2 \mod (3+2i)$. Betrachte daher nur

$$X \equiv 1 \mod 11, X \equiv 2 \mod 13.$$

Definiere:

$$\begin{aligned} N &:= m_1 \cdot m_2 = 11 \cdot 13 = 143, \\ N_1 &:= m_3 = 13, \\ N_2 &:= m_1 = 11. \end{aligned}$$

Es gilt:

$$\begin{aligned} [N_1]_{m_1} &= [13]_{11} = [2]_{11} &&\implies [N_1]_{m_1} \cdot [y_1]_{m_1} = [2]_{11} \cdot [6]_{11} = [1]_{11}, \\ [N_2]_{m_2} &= [11]_{13} &&\implies [N_2]_{m_2} \cdot [y_2]_{m_2} = [11]_{13} \cdot [6]_{13} = [1]_{13}. \end{aligned}$$

Nach Bemerkung 4.7.12 gilt:

$$\begin{aligned} b &= 1 \cdot N_1 \cdot y_1 + 2 \cdot N_2 \cdot y_2 \\ &= 13 \cdot 6 + 2 \cdot 11 \cdot 6 \\ &= 78 + 132 \\ &= 210. \end{aligned}$$

Die Lösung b der simultanen Kongruenzen ist nach Satz 4.7.5 eindeutig modulo N. Die Lösungsmenge ist also

$$\{210 + 143z \mid z \in \mathbb{Z}\} = \{67 + 143z \mid z \in \mathbb{Z}\}.$$

$\square$

Punkte Teil c): 2/2

$6,5/7$ P $+2$ P

Aufgabe 7.2

(a) Sei $f := t^4 - 2t^3 - 7t^2 + \frac{11}{3}t - \frac{4}{3} \in \mathbb{Q}$.
Zu zeigen: Das Polynom f besitzt eine rationale Nullstelle.
Sei $\alpha = 4 \in \mathbb{Q}$. Es gilt:

$$\begin{aligned} E_\alpha(f) =& 4^4 - 2 \cdot 4^3 - 7 \cdot 4^2 - \frac{11}{3} \cdot 4 - \frac{4}{3} \\ =& 256 - 128 - 112 - \frac{44}{3} - \frac{4}{3} \\ =& 128 - 112 - 16 \\ =& 0. \end{aligned}$$

$\implies$ α ist rationale Nullstelle von f.
Wie bist Du auf die 4 gekommen?
Ferner ist zu zeigen, dass $f = (t-4) \cdot \left(t^3 + 2t^2 + t + \frac{1}{3}\right)$ die Faktorisierung von f in irreduzible Polynome ist.
Es gilt:

$$\begin{aligned} f &= t^4 - 2t^3 - 7t^2 + \frac{11}{3}t - \frac{4}{3} \\ &= (t-4) \cdot \left(t^3 + 2t^2 + t + \frac{1}{3}\right) \\ &= \frac{1}{3} \cdot (t-4) \cdot \left(3t^3 + 6t^2 + 3t + 1\right) \end{aligned}$$

(i) Zu zeigen $g := \left(t^3 + 2t^2 + t + \frac{1}{3}\right)$ irreduzibel.
Sei $\mathbb{Q} \ni \alpha = \frac{A}{B}$ rationale Nullstelle von g mit $A, B \in \mathbb{Z}$ teilerfremd.
Es gilt:

$$t^3 + 2t^2 + t + \frac{1}{3} = 0$$

Das gilt nicht. Polynome sind genau dann 0, wenn alle Koeffizienten 0 sind.

$$\begin{aligned} &\overset{5.2.2}{\implies} B \mid 1 \text{ und } A \mid \frac{1}{3} \\ &\implies B \in \{-1, 1\}, A \in \{-1, 1\} \\ &\implies \alpha \in \{-1, 1\}. \end{aligned}$$

Satz 5.2.2 lässt sich nur auf Polynome aus $R[t]$ anwenden, hier also $\mathbb{Z}[t]$. Ansonsten ergäbe die Teilbarkeitsbedingung wenig Sinn, da in einem Körper alle Elemente außer der 0 assoziiert zueinander sind. -1 P.

Damit ergibt sich für die Nullstellen:

$$\begin{aligned}
E_{-1}(g) &= (-1)^3 + 2 \cdot (-1)^2 + (-1) + \frac{1}{3} \\
&= -1 + 2 - 1 + \frac{1}{3} \\
&= \frac{1}{3} \neq 0, \\
E_1(g) &= 1^3 + 2 \cdot 1^2 + 1 + \frac{1}{3} \\
&= 1 + 2 + 1 + \frac{1}{3} \\
&= \frac{13}{3} \neq 0.
\end{aligned}$$

Alle möglichen Funktionswerte von $g(\alpha)$ sind ungleich 0. Dies steht im Widerspruch zu α rationale Nullstelle von g. Daraus folgt, dass g keine rationale Nullstelle besitzt.
Nach Satz 5.1.6 ist $g \in \mathbb{Q}[t]$ irreduzibel.

(ii) Zu zeigen: $h := t - 4$ irreduzibel in $\mathbb{Q}[t]$.
Es gilt:

$$\mathbb{Q} \text{ Körper},\ \deg(t-4) = 1 \overset{5.1.2}{\Longrightarrow} t - 4 \in \mathbb{Q}[t] \text{ irreduzibel.}$$

Daraus folgt, dass $f = (t-4) \cdot \left(t^3 + 2t^2 + t + \frac{1}{3}\right)$ eine Faktorisierung von f in irreduzible Polynome in $\mathbb{Q}[t]$ ist.

$\square$

Punkte Teil a): 1/2

(b) Seien R Integritätsring, $f \in R[t]$ und $\varphi : R[t] \to R[t]$ ein Ringisomorphismus.
Zu zeigen: f ist irreduzibel $\iff$ $\varphi(f)$ ist irreduzibel.

"$\Longrightarrow$": Sei f irreduzibel. Es gilt:

$$\begin{aligned}
& \forall a, b \in R[t], f = a \cdot b : a \in R[t]^* \text{ oder } b \in R[t]^* \quad -0,5 \text{ P} \\
\Longrightarrow\ & \forall a, b \in R[t], f = a \cdot b : \varphi(f) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \\
\overset{2.3.3b)}{\Longrightarrow}\ & \varphi(a) \in R[t]^* \text{ oder } \varphi(b) \in R[t]^* \\
\Longrightarrow\ & \varphi(f) \text{ ist irreduzibel.}
\end{aligned}$$

Es ist noch zu zeigen, dass jede Zerlegung von $\varphi(f)$ die Form $\varphi(f) = \varphi(g) \cdot \varphi(h)$ hat mit $f = g \cdot h$. Nur für diesen Fall wurde Irreduzibilität gezeigt. $-0,5$ P.

"$\Longleftarrow$": Sei $\varphi(f)$ irreduzibel. Sei φ^{-1} der inverse Ringisomorphismus zu φ. Es gilt:

$$
\begin{aligned}
&\forall a,b \in R[t], \varphi(f) = a \cdot b : a \in R[t]^* \text{ oder } b \in R[t]^* \\
\overset{f=\varphi^{-1}(\varphi(f))}{\Longrightarrow} &\forall a,b \in R[t], \varphi(f) = a \cdot b : f = \varphi^{-1}(\varphi(f)) = \varphi^{-1}(a \cdot b) = \varphi^{-1}(a) \cdot \varphi^{-1}(b) \\
\overset{2.3.3}{\Longrightarrow} &\varphi^{-1}(a) \in R[t]^* \text{ oder } \varphi^{-1}(b) \in R[t]^* \\
\Longrightarrow &f \text{ irreduzibel.}
\end{aligned}
$$

S.o.

$\square$

Punkte Teil b): 1/2

(c) Fehlt.

2/6 P

Aufgabe 7.3

(a) Sei $R[t] = \mathbb{Z}_5[t], f = t^3 + t^2 + 2 \in \mathbb{Z}_5[t]$.
Zu zeigen: f ist irreduzibel über in $\mathbb{Z}_5[t]$.
Es gilt:

$$
\begin{aligned}
&R = \mathbb{Z}_5 \text{ ist nullteilerfreier Ring und } \mathrm{LC}(f) = 1 \in R^* \\
\overset{\deg(f)=3}{\Longrightarrow} &(f \text{ irreduzibel } \Longleftrightarrow f \text{ besitzt Nullstelle in } R)
\end{aligned}
$$

Es gilt:

$$
\begin{aligned}
&\forall z \in \mathbb{Z}_5 : z \in \{0, \cdots, 4\} \\
\Longrightarrow &\forall z \in \mathbb{Z}_5 : z \geq 0 \\
\Longrightarrow &\forall z \in \mathbb{Z}_5 : z^3 + z^2 \geq 0 \\
\Longrightarrow &\forall z \in \mathbb{Z}_5 : z^3 + z^2 + 2 \geq 2 \\
\Longrightarrow &f \text{ besitzt keine Nullstelle in } \mathbb{Z}_5 \\
\Longrightarrow &f \text{ irreduzibel über } \mathbb{Z}_5.
\end{aligned}
$$

$\square$

Es gibt in $\mathbb{Z}_5$ kein $>, <$. Wenn man die Elemente als Elemente in $\mathbb{Z}$ auffasst, ist das möglich, doch dann führt > 0 nicht zu $\neq 0$, da $5 > 0$ in $\mathbb{Z}$, jedoch $5 = 0$ in $\mathbb{Z}_5$. Es wurde also nicht gezeigt, dass f keine Nullstellen hat. $-1,5$ P
$0,5/2$ P

(b) Sei $R[t] = \mathbb{Q}[t], f = 5t^{10} - 3t^6 + 18t^2 + 9t - 6 \in \mathbb{Z}[t]$.
Zu zeigen: f irreduzibel in $\mathbb{Q}[t]$.
Es gilt:

$$\begin{aligned}
\mathrm{ggT}(5,-3,18,9,-6) &= \mathrm{ggT}(5,3,18,9,6) \\
&= \mathrm{ggT}(5,\mathrm{ggT}(3,\mathrm{ggT}(18,\mathrm{ggT}(9,6)))) \\
&= \mathrm{ggT}(5,\mathrm{ggT}(3,\mathrm{ggT}(18,3))) \\
&= \mathrm{ggT}(5,\mathrm{ggT}(3,3)) \\
&= \mathrm{ggT}(5,3) \\
&= 1 \\
\implies & f \text{ primitiv.}
\end{aligned}$$

Sei $p = 3, n := \deg(f) = 10$. Es gilt:

(i)

$$p = 3 \nmid 5 = a_n.$$

(ii)

$$\forall 0 \leq i < n : p \mid a_i,$$
$$\text{denn } a_i \in \{0, -3, 18, 9, -6\} \text{ und } 3 \mid 0, 3 \mid -3, 3 \mid 18, 3 \mid 9, 3 \mid -6.$$

(iii)

$$p^2 = 9 \nmid -6 = a_0.$$

Nach dem Kriterium von Eisenstein ist f irreduzibel in $\mathbb{Q}[t]$.

$\square$

Punkte Teil b): 2/2

(c) Fehlt.

(d) Fehlt.

$2,5/7$ P

Insgesamt $12,5/20$ Punkten.

korrigiert von Tom Engels am 11.06.2020