WS 05/06
Priv.-Doz. Dr. S. Wewers

Algebra I

6. Übungsblatt

Aufgabe 1: (1+2=3 P) Sei $n \in \mathbb{N}$ und $n = n_1 \cdot \ldots \cdot n_r$ eine Zerlegung von n in paarweise teilerfremde Faktoren. Setze $m_i := n/n_i$.

(a) Zeigen Sie: Für jedes i gibt es eine natürliche Zahl $y_i \in \{1, \ldots, n-1\}$ mit $y_i m_i \equiv 1 \pmod{n_i}$. Weiterhin gilt: sind $x_1, \ldots, x_r \in \mathbb{Z}$ beliebige ganze Zahlen, so ist

$$x := \sum_{i=1}^{r} x_i y_i m_i$$

eine Lösung der simultanen Kongruenzen $x \equiv x_i \pmod{n_i}$, $i = 1, \ldots, r$.

(b) Bestimmen Sie die eindeutige ganze Zahl $x \in \{0, \ldots, 104\}$ mit

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

Verwenden Sie dazu Teil (a).

Lösung:

(a) Wir setzen $n \geq 2$ voraus.

- Im Falle $n_i = 1$ setze man $y_i := 1$. Es sei nun $n_i \geq 2$ vorausgesetzt. Nach Voraussetzung sind die Zahlen n_i und $m_i = n_1 \cdot \ldots \cdot n_{i-1} \cdot n_{i+1} \cdot \ldots \cdot n_r$ teilerfremd. Also gibt es nach dem Euklidischen Algorithmus Zahlen $a, b \in \mathbb{Z}$ derart, daß $1 = an_i + bm_i$. Es sei $y_i \equiv b \mod n_i$ so gewählt, daß $y_i \in \{0, \ldots, n-1\}$. Es folgt

  $$y_i m_i \equiv bm_i = 1 - an_i \equiv 1 \mod n_i .$$

  Insbesondere ist $y_i \neq 0$. Damit ist der erste Teil der Behauptung gezeigt.
- Betrachtet man x modulo n_j, so ergibt sich wegen $m_i \equiv 0 \mod n_j$ für $j \neq i$ und aufgrund der Wahl der y_j demnach

  $$x \equiv x_j y_j m_j \equiv x_j \mod n_j$$

  für $j = 1, \ldots, r$.
- Wir wollen zusatzlich noch beweisen, daß obige Lösung eindeutig modulo n ist, d.h. daß jede weitere Lösung x' der simultanen Kongruenzen $x' \equiv x_i \mod n_i$, $i = 1, \ldots, r$, notwendigerweise $x' \equiv x \mod n$ erfüllen muß. Dazu beachte man, daß $y := x - x'$ erfüllt

  $$y \equiv 0 \mod n_i$$

  für $i = 1, \ldots, r$. Also sind $n_1, \ldots, n_r$ jeweils Teiler von y. Da die Zahlen $n_1, \ldots, n_r$ paarweise teilerfremd sind, folgt daraus, daß auch deren Produkt $n := n_1 \cdot \ldots \cdot n_r$ ein Teiler von $y = x - x'$ ist. Daraus folgt definitionsgemäß $x' \equiv x \mod n$.

(b) Der Euklidische Algorithmus liefert

$$1 \;=\; 12 \cdot 3 - 1 \cdot 35 \;=\; -4 \cdot 5 + 1 \cdot 21 \;=\; -2 \cdot 7 + 1 \cdot 15\,.$$

Also haben wir

$$\begin{array}{rcccc} 2 \cdot 35 & \equiv & 1 & \mod & 3 \\ 1 \cdot 21 & \equiv & 1 & \mod & 5 \\ 1 \cdot 15 & \equiv & 1 & \mod & 7\,. \end{array}$$

Nach Teil (a) ist die eindeutige Lösung modulo 105 gegeben durch

$$1 \cdot 2 \cdot 35 + 2 \cdot 1 \cdot 21 + 3 \cdot 1 \cdot 15 \;=\; 157 \;\equiv\; 52 \mod 105\,.$$

Aufgabe 2: (3 P) Sei G eine endliche zyklische Gruppe der Ordnung n und g ein Erzeuger von G. Sei $h \in G$ ein beliebiges Element. Der *diskrete Logarithmus* von h zur Basis g ist die (eindeutige) Zahl $x = \log_g(h) \in \{0, \ldots, n-1\}$ mit $h = g^x$.

Sei $n = n_1 \cdot \ldots \cdot n_r$ eine Zerlegung von n in teilerfremde Faktoren. Setze $m_i := n/n_i$, $g_i := g^{m_i}$ und $h_i := h^{m_i}$. Zeigen Sie:

(a) Das Element $g_i \in G$ hat die Ordnung n_i.

(b) Die Ordnung von h_i ist ein Teiler von n_i.

(c) Es gibt eindeutige Zahlen $x_i \in \{0, \ldots, n_i - 1\}$ mit $h_i = g_i^{x_i}$, $i = 1, \ldots, r$.

(d) Sei $x \in \{0, \ldots, n-1\}$ die eindeutige Lösung der simultanen Kongruenzen $x \equiv x_i \pmod{n_i}$. Dann gilt $h = g^x$, d.h. $x = \log_g(h)$.

Lösung:

(a) Für $x \in \mathbb{Z}$ gilt $g_i^x = g^{xn/n_i}$, und wegen $\operatorname{ord} g = n$ folgt

$$1 = g_i^x \iff xn/n_i \equiv 0 \mod n \iff n_i | x\,.$$

Daher ist $\operatorname{ord} g_i = n_i$.

(b) Es gilt

$$h_i^{n_i} \;=\; h^{m_i n_i} \;=\; h^n \;=\; 1\,,$$

denn $n = |G|$. Daher ist die Ordnung von h_i ein Teiler von n_i.

(c) Es sei $y := \log_g(h)$, d.h. es gelte $h = g^y$. Es sei $x_i \in \{0, \ldots, n_i - 1\}$ derart, daß $x_i \equiv y \mod n_i$. Dann gilt wegen $\operatorname{ord} g_i = n_i$ folglich

$$g_i^{x_i} \;=\; g_i^y \;=\; g^{m_i y} \;=\; h^{m_i} \;=\; h_i\,.$$

Wegen $\operatorname{ord} g_i = n_i$ ist dieses x_i auch eindeutig bestimmt.

(d) Nach dem Beweis zu Teil (c) war $x_i \equiv y \mod n_i$, wobei $y = \log_g(h)$. Nach der Wahl von x gilt also $x \equiv y \mod n_i$ für $i = i, \ldots, r$. Aufgrund der Eindeutigkeit von x folgt daraus $x = y$.

Aufgabe 3: (1+2=3 P)

(a) Zeigen Sie, dass 3 eine Primitivwurzel modulo 31 ist.

(b) Bestimmen Sie den diskreten Logarithmus von 2 modulo 31 zur Basis 3, d.h. die eindeutige Zahl $x \in \{0, \dots, 29\}$ mit

$$3^x \equiv 2 \pmod{31}.$$

Benutzen Sie dazu das in Aufgabe 2 angegebene Verfahren (mit $G := (\mathbb{Z}/\mathbb{Z} \cdot 31)^\times$, $g := 3$ und $h := 2$).

Lösung:

(a) Die Ordnung von $\overline{3}$ in $(\mathbb{Z}/31\mathbb{Z})^\times$ ist ein Teiler von $\varphi(31) = 30$, d.h. sie ist eine der Zahlen $1, 2, 3, 5, 6, 10, 15, 30$. Wir müssen also lediglich nachprüfen, daß $3^n \not\equiv 1 \mod 31$ gilt für $n = 2, 3, 5, 6, 10, 15$. Wir berechnen

$$\begin{array}{rclclclcrcc}
3^2 & & & & & & & \equiv & 9 & \text{mod} & 31 \\
3^3 & \equiv & 3 \cdot 3^2 & & & & & \equiv & -4 & \text{mod} & 31 \\
3^5 & \equiv & 3^2 \cdot 3^3 & \equiv & 9 \cdot (-4) & \equiv & -36 & \equiv & -5 & \text{mod} & 31 \\
3^6 & \equiv & (3^3)^2 & \equiv & (-4)^2 & & & \equiv & 16 & \text{mod} & 31 \\
3^{10} & \equiv & (3^5)^2 & \equiv & (-5)^2 & & & \equiv & -6 & \text{mod} & 31 \\
3^{15} & \equiv & 3^5 \cdot 3^{10} & \equiv & (-5) \cdot (-6) & & & \equiv & -1 & \text{mod} & 31\,.
\end{array}$$

Daher gilt $\operatorname{ord} \overline{31} = 30$ in $(\mathbb{Z}/31\mathbb{Z})^\times$.

(b) Wir berechnen zunächst

$$\begin{array}{rclclcc}
2^5 & & & \equiv & 1 & \text{mod} & 31 \\
2^6 & & & \equiv & 2 & \text{mod} & 31 \\
2^{10} & \equiv & 1^2 & \equiv & 1 & \text{mod} & 31 \\
2^{15} & \equiv & 1^3 & \equiv & 1 & \text{mod} & 31
\end{array}$$

Also ergibt sich folgendes Tableau.

i	n_i	m_i	g_i	h_i	x_i
1	2	15	$\overline{3}^{15} = \overline{-1}$	$\overline{2}^{15} = \overline{1}$	0
2	3	10	$\overline{3}^{10} = \overline{-6}$	$\overline{2}^{10} = \overline{1}$	0
3	5	6	$\overline{3}^{6} = \overline{16}$	$\overline{2}^{6} = \overline{2}$	x_3

Um x_3 zu berechnen, brauchen wir folgende Nebenrechnungen

$$\begin{array}{lclclclclcl}
g_3^2 & = & \overline{3}^{12} & = & \overline{3}^2 \cdot \overline{3}^{10} & = & \overline{9} \cdot \overline{-6} & = & \overline{-54} & = & \overline{8} \\
g_3^3 & = & \overline{3}^{18} & = & \overline{3}^15 \cdot \overline{3}^3 & = & \overline{-1} \cdot \overline{-4} & & & = & \overline{4} \\
g_3^4 & = & \overline{3}^{24} & = & (\overline{3}^{12})^2 & = & \overline{8}^2 & = & \overline{64} & = & \overline{2}\,.
\end{array}$$

Demnach ergibt sich $x_1 = x_2 = 0$ und $x_3 = 4$. Die gesuchte Zahl x ist also Lösung der simultanen Kongruenzen

$$\begin{array}{lcc}
x \equiv 0 & \text{mod} & 2 \\
x \equiv 0 & \text{mod} & 3 \\
x \equiv 4 & \text{mod} & 5\,.
\end{array}$$

Dieses hat die Lösung $x = 24$. (Bemerkung: Wir hatten in obiger Rechnung bereits $\overline{3}^{24} = \overline{2}$ herausgefunden und wären damit fertig gewesen. Das war aber nur ein glücklicher Zufall.)

Aufgabe 4: (3 P) Sei $r \geq 2$ eine ganze Zahl. Zeigen Sie:

(a) Es gilt die Kongruenz
$$5^{2^{r-2}} \equiv 1 \pmod{2^r}$$
und, falls $r \geq 3$,
$$5^{2^{r-3}} \not\equiv 1 \pmod{2^r}.$$
Hinweis: Schreibe $5 = 1 + 4$ und benutze die Binomialentwicklung und Induktion nach r.

(b) Sind $x, y \in \mathbb{Z}$ ganze Zahlen mit
$$(-1)^x \cdot 5^y \equiv 1 \pmod{2^r},$$
so gilt $x \equiv 0 \pmod 2$ und $y \equiv 0 \pmod{2^{r-2}}$.

(c) Die Abbildung $(x, y) \mapsto (-1)^x \cdot 5^y$ definiert einen Isomorphismus
$$\mathbb{Z}/\mathbb{Z} \cdot 2 \times \mathbb{Z}/\mathbb{Z} \cdot 2^{r-2} \cong (\mathbb{Z}/\mathbb{Z} \cdot 2^r)^\times.$$

Lösung:

(a) Wir wollen durch Induktion nach $r \geq 2$ folgende Aussage beweisen.
$$5^{2^{r-2}} \;\equiv\; 1 + 2^r \mod 2^{r+1} .$$
Für $r = 2$ stimmt die Aussage offenbar. Im Induktionsschritt nehmen wir an, die Aussage stimme für ein $r \geq 2$. Also gibt es ein $k \in \mathbb{Z}$ derart, daß $5^{2^{r-2}} = 1 + 2^r + k \cdot 2^{r+1}$. Es folgt
$$\begin{aligned} 5^{2^{r-1}} &= \left(5^{2^{r-2}}\right)^2 = (1 + (1+2k)2^r)^2 \\ &= 1 + (1+2k)2^{r+1} + (1+2k)^2 2^{2r} \\ &= 1 + 2^{r+1} + (k + (1+2k)^2 2^{r-2})2^{r+2} \\ &\equiv 1 + 2^{r+1} \mod 2^{r+2} . \end{aligned}$$
Also ist obige Behauptung bewiesen. Insbesondere folgt daraus
$$5^{2^{r-2}} \;\equiv\; 1 + 2^r \;\equiv\; 1 \mod 2^r ,$$
da eine Kongruenz $\mod 2^{r+1}$ stets auch eine Kongruenz $\mod 2^r$ nach sich zieht. Im Falle $r \geq 3$ gilt
$$5^{2^{r-3}} \;\equiv\; 1 + 2^{r-1} \;\not\equiv\; 1 \mod 2^r ,$$
da $2^{r-1} \not\equiv 0 \mod 2^r$ gilt.

Zusatz: Aus dem hier Bewiesenen folgt
$$\operatorname{ord} \overline{5} \;=\; 2^{r-2} \text{ in } (\mathbb{Z}/2^r\mathbb{Z})^\times .$$
Denn wegen $\overline{5}^{2^{r-2}} = \overline{1}$ ist die Ordnung $t := \operatorname{ord} \overline{5}$ ein Teiler von 2^{r-2}, d.h. es gilt $t = 2^s$ für ein $s \in \{0, \ldots, r-2\}$. Es kann aber nicht $s \leq r-3$ gelten, da sonst $\overline{5}^{2^{r-3}} = \left(\overline{5}^{2^s}\right)^{2^{r-3-s}} = \overline{1}$ wäre, im Widerspruch zur zweiten Aussage der Aufgabestellung.

(b) Wir nehmen $x, y \geq 0$ an. Es gilt $5^y = (1+4)^y \equiv 1 \mod 4$. Andererseits gilt nach Voraussetzung

$$(-1)^x 5^y \equiv 1 \mod 4 \, ,$$

da 4 ein Teiler von 2^r ist. Daraus folgt $x \equiv 0 \mod 2$, denn es gilt $-1 \not\equiv 1 \mod 4$. Die Voraussetzung besagt also

$$5^y \equiv 1 \mod 2^r \, ,$$

d.h.

$$\overline{5}^{\,y} = \overline{1}$$

in $(\mathbb{Z}/2^r\mathbb{Z})^\times$. Nach Teil (a) ist die Ordnung von $\overline{5}$ in $(\mathbb{Z}/2^r\mathbb{Z})^\times$ gleich 2^{r-2}. Daraus folgt, daß 2^{r-2} ein Teiler von y ist, d.h. es gilt $y \equiv 0 \mod 2^{r-2}$.

(c) Wir betrachten die Abbildung

$$\begin{aligned} \varphi : (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{r-2}\mathbb{Z}) &\rightarrow (\mathbb{Z}/2^r\mathbb{Z})^\times \, , \\ (\overline{x}, \overline{y}) &\mapsto \overline{-1}^{\,x} \cdot \overline{5}^{\,y} \, . \end{aligned}$$

Wegen $\operatorname{ord} \overline{-1} = 2$ und $\operatorname{ord} \overline{5} = 2^{r-2}$ in $(\mathbb{Z}/2^r\mathbb{Z})^\times$ ist die Abbildung wohldefiniert. Man rechnet leicht nach, daß sie ein Gruppenhomomorphismus ist. Nach Teil (b) ist sie injektiv. Ferner haben beide Gruppen je 2^{r-1} Elemente. Also ist φ ein Gruppenisomorphismus.