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).

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. $x = \log_g(h)$.

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 $x \in \{0, \ldots, 29\}$ 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 $h := 2$).

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

$$\mathbb{Z}/\mathbb{Z} \cdot 2 \times \mathbb{Z}/\mathbb{Z} \cdot 2^{r-2} \cong (\mathbb{Z}/\mathbb{Z} \cdot 2^r)^\times.$$

Abgabe: am Donnerstag, den 8.12. (in der Vorlesung, oder bei Herrn Martin).