Humboldt-Universität zu Berlin
Institut für Mathematik

Mathematik für Informatiker I (Lineare Algebra)
Wintersemester 2017/18

Dr. B. Gerlach, Dr. B. Güneysu, Dr. F. Schmäschke
http://www.math.hu-berlin.de/∼linalginf

Übungsblatt 4

Gleichungen in Restklassen

Aufgabe 1 (6 Punkte).

(a) Sei $m \in \mathbb{N}$ beliebig. Zeigen Sie, dass, wenn $n \in \mathbb{Z}_m \setminus \{0\}$ ein multiplikatives Inverses besitzt, dann ist dieses eindeutig bestimmt.

(b) Sei nun $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie, dass jedes Element in $\mathbb{Z}_p \setminus \{0\}$ ein multiplikatives Inverses besitzt.

Hinweis: Wie aus Satz 2.20 der Vorlesung bekannt ist, besitzt $n \in \mathbb{Z}_m \setminus \{0\}$ genau dann ein multiplikatives Inverses in $\mathbb{Z}_m \setminus \{0\}$, wenn die Bedingung $\mathrm{ggT}(n, m) = 1$ erfüllt ist.

Aufgabe 2 (6 Punkte). Bestimmen Sie alle Lösungen $(x_1, x_2, x_3, x_4) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ des Gleichungssystems

$$\begin{aligned} x_1 + 2x_2 \quad\quad + \quad x_4 &= 2 \\ 2x_1 + \quad x_2 + x_3 + 2x_4 &= 0 \\ 2x_2 + x_3 + \quad x_4 &= 0 \\ 2x_1 + 2x_2 \quad\quad + \quad x_4 &= 0 \end{aligned}$$

Beachten Sie, dass die Gleichungen in $\mathbb{Z}_3$ zu verstehen sind, d. h. als Kongruenzen modulo 3.

Aufgabe 3.

(a) Bestimmen Sie welche Elemente in $\mathbb{Z}_{12}$ ein multiplikatives Inverses besitzen. Geben Sie die multiplikativen Inversen von 7 und 11 an.

(b) Bestimmen Sie alle Lösungen. Geben Sie auch eine Begründung an, dass nicht mehr Lösungen existieren können, als Sie angegeben haben.

(i) Bestimmen Sie alle $x \in \mathbb{Z}_{33}$ mit $17x \equiv 25 \mod 33$.

(ii) Bestimmen Sie alle $x \in \mathbb{Z}_{91}$ mit $52x \equiv 15 \mod 91$.

Präsenzaufgabe 1. Nach dem Lemma von Bezout (auch Erweiterter Euklidischer Algorithmus) gilt: Für alle $n, m \in \mathbb{Z}$ mit $d = \mathrm{ggT}(n, m)$ gibt es $x, y \in \mathbb{Z}$, so dass $nx + my = d$. Folgern Sie daraus ohne Verwendung von Satz 2.20 aus der Vorlesung, dass, wenn $\mathrm{ggT}(m, n) = 1$, dann gibt es ein multiplikatives Inverses zu n in $\mathbb{Z}_m \setminus \{0\}$.

Abgabe:
Dienstag, 14.11.2017 vor der Vorlesung. *Die ersten drei Aufgaben sind auf getrennten Blättern zu bearbeiten und mit Namen, Matrikelnummer und* ***Übungsgruppe*** *zu versehen. Die Nummer n der Übungsgruppe soll wie unter http://www.mathematik.hu-berlin.de/∼linalginf angegeben werden (d. h.* $n \in \{1, 2, 3, 4\}$*). Die Abgabe erfolgt in Dreier- oder mindestens Zweiergruppen.*