Innermathematische Beziehungen
Übungsveranstaltung

Fabian Grünig
gruenig@ph-heidelberg.de

Wintersemester 2017/18
Mittwoch, 10:00 Uhr, A206

In Aufgabe 23 haben wir das sogenannte *Lemma von Bezout* kennengelernt. Dieses besagt, dass sich der größte gemeinsame Teiler zweier ganzer Zahlen $x, m \in \mathbb{Z}$ als ganzzahlige Linearkombination dieser Zahlen x und m schreiben lässt. Es gibt also zwei ganze Zahlen $\alpha, \beta \in \mathbb{Z}$ mit

$$\text{ggT}(x, m) = \alpha \cdot x + \beta \cdot m.$$

Die Zahlen α, β findet man mit Hilfe des erweiterten Euklidischen Algorithmus. Das *Lemma von Bezout* hat weitreichende theoretische und praktische Konsequenzen.

Aufgabe 24 *(Exkurs: Teilerfremde Zahlen)*
Es gilt auch die Umkehrung des *Lemma von Bezout*. Wir nennen zwei Zahlen $x, m \in \mathbb{Z}$ *teilerfremd*, falls $\text{ggT}(x, m) = 1$. Zeige: Gibt es für zwei Zahlen $x, m \in \mathbb{Z}$ zwei weitere Zahlen $\alpha, \beta \in \mathbb{Z}$, sodass

$$\alpha \cdot x + \beta \cdot m = 1,$$

dann sind x und m bereits teilerfremd bzw. es gilt gilt $\text{ggT}(x, m) = 1$.
Hinweis: Verwende ein Widerspruchsargument. Was wäre, wenn x und m einen echten gemeinsamen Teilen hätten?

Aufgabe 25 *(Hinreichendes Kriterium für Einheiten in $\mathbb{Z}_m$)*
Wir betrachten die Restklassen bzgl. einer Zahl $m \in \mathbb{Z}$ und kehren zu der Frage zurück, wann eine Restklasse $\overline{x} \in \mathbb{Z}_m$ ein multiplikatives Inverses besitzt.
Zeige: Sind x und m teilerfrend, so besitzt $\overline{x}$ in $\mathbb{Z}_m$ ein multiplikatives Inverses.
Hinweis: Verwende das Lemma von Bezout und gehe zu einer Betrachtung in den Restklassen über.

Aufgabe 26 *(Konstruktion von Einheiten in $\mathbb{Z}_m$)*
Finde mit Hilfe des Erweiterten Euklidischen Algorithmus (bzw. Lemma von Bezout) die multiplikativen Inversen der folgenden Elemente jeweils in $\mathbb{Z}_m$.

(i) $\overline{5}, \overline{14}$ und $\overline{15}$ in $\mathbb{Z}_{22}$.
(ii) $\overline{15}$ in $\mathbb{Z}_{19}$, $\overline{1028}$ in $\mathbb{Z}_{1055}$.
(iii) $\overline{2}, \overline{3}, \overline{4}, \overline{5}$ und $\overline{6}$ in $\mathbb{Z}_7$.

Aufgabe 27 *(Notwendiges Kriterium für Einheiten in $\mathbb{Z}_m$)*
Das ist Aufgabe 25 entwickelte hinreichende Kriterium für Einheiten in $\mathbb{Z}_m$ ist auch ein notwendiges Kriterium. Argumentiere mit Hilfe von Aufgabe 20 (iii) und Aufgabe 24: Ist $\overline{x}$ eine Einheit in $\mathbb{Z}_m$, so sind x und m teilerfremd.

Aufgabe 28 *(Einheiten und nicht-Einheiten in $\mathbb{Z}_m$)*
Finde mit Hilfe des obigen Kriteriums die Restklassen in $\mathbb{Z}_m$, die Einheiten sind und diejenigen, welche keine Einheiten sind.

(i) Finde alle Einheiten in $\mathbb{Z}_6$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{14}$.
(ii) Finde alle Einheiten in $\mathbb{Z}_{60}$, $\mathbb{Z}_{30}$, $\mathbb{Z}_{15}$ und $\mathbb{Z}_5$.
(iii) Finde alle Einheiten in $\mathbb{Z}_7$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$, $\mathbb{Z}_{19}$ und $\mathbb{Z}_{691}$.