Innermathematische Beziehungen
Übungsveranstaltung

Fabian Grünig
gruenig@ph-heidelberg.de

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

Die Restklassen bezüglich einer Zahl $m \in \mathbb{Z}$ haben wir bisher mit $[x]_m$ bezeichnet. In Zukunft werden wir, sofern aus dem Kontext erkennbar ist, bezüglich welcher Zahl m wir die Restklassen betrachten, in die Schreibweise $\overline{x} = [x]_m$ wechseln.

Aufgabe 20 *(Einheiten in $\mathbb{Z}_m$)*
Es sei $m \in \mathbb{Z}$. In Aufgabe 16 haben wir die Einheitengruppe $\mathbb{Z}_m^\times$ definiert. Die Restklassen $\overline{x}$ in $\mathbb{Z}_m^\times$ zeichnen sich durch die Existenz von Inversen Elementen bzgl. der Multiplikation aus:

$$\text{Es existiert ein } \overline{y} \in \mathbb{Z}_m, \text{ sodass } \overline{x} \cdot \overline{y} = \overline{1}.$$

Die Elemente in $\mathbb{Z}_m^\times$ bezeichnen wir auch als die *Einheiten* von $\mathbb{Z}_m$.

(i) Zeige, dass $\overline{5}$ eine Einheit in $\mathbb{Z}_{22}$ ist.

(ii) Zeige, dass $\overline{4}$ *keine* Einheit in $\mathbb{Z}_{22}$ ist.

(iii) Es sei $\overline{x}$ eine Einheit in $\mathbb{Z}_m$. Zeige, dass es dann zwei Zahlen $\alpha, \beta \in \mathbb{Z}$ gibt, sodass

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

Aufgabe 21 *(Exkurs: Der größte gemeinsame Teiler)*
Es seien $x, m \in \mathbb{Z}$ zwei ganze Zahlen. Wir definieren den *größten gemeinsamen Teiler* $\mathrm{ggT}(x, m)$ von x und m als die Zahl natürliche Zahl, die folgende Eigenschaften erfüllt:

- $\mathrm{ggT}(x, m)$ teilt x und $\mathrm{ggT}(x, m)$ teilt m.
- Wenn t ein weiterer Teiler von x und m ist, dann teilt t auch $\mathrm{ggT}(x, m)$.

(i) Bestimme: $\mathrm{ggT}(4, 6)$, $\mathrm{ggT}(30, 36)$, $\mathrm{ggT}(13, 31)$, $\mathrm{ggT}(4, 16)$.

(ii) Zeige: Für $x, m \in \mathbb{Z}$ gilt: $\mathrm{ggT}(x, m) = \mathrm{ggT}(m, x)$

(iii) Zeige: Für $x, m \in \mathbb{Z}$ gilt: $\mathrm{ggT}(x, m) = \mathrm{ggT}(x - m, m)$

(iv) Zeige: Für $x, m, q \in \mathbb{Z}$ gilt: $\mathrm{ggT}(x, m) = \mathrm{ggT}(x - q \cdot m, m)$

Aufgabe 22 *(Exkurs: Der Euklidische Algorithmus)*
Zur Berechnung von $\mathrm{ggT}(x, m)$ kann man den modernen Euklidischen Algorithmus verwenden, der auf der Division mit Rest basiert. Man beginnt mit den „Eingabezahlen“ $x_1 := x$ und $m_1 := m$.

(1) Erhalte aus den Divsion mit Rest $x_1 = q_1 \cdot m_1 + r_1$ die Zahlen q_1 und r_1.
  (1a) Falls $r_1 = 0$, breche ab. Es ist $\mathrm{ggT}(x, m) = m_1$
  (1b) Falls $r_1 \neq 0$, führe fort. Setze $x_2 := m_1$ und $m_2 := r_1$.

(2) Erhalte aus den Divsion mit Rest $x_2 = q_2 \cdot m_2 + r_2$ die Zahlen q_2 und r_2.
  (2a) Falls $r_2 = 0$, breche ab. Es ist $\mathrm{ggT}(x, m) = m_2$
  (2b) Falls $r_2 \neq 0$, führe fort. Setze $x_3 := m_2$ und $m_3 := r_2$.

$\vdots$

(i) Erhalte aus den Divsion mit Rest $x_i = q_i \cdot m_i + r_i$ die Zahlen q_i und r_i.
  (ix) Falls $r_i = 0$, breche ab. Es ist $\mathrm{ggT}(x, m) = m_i$
  (ib) Falls $r_i \neq 0$, führe fort. Setze $x_{i+1} := m_i$ und $m_{i+1} := r_i$.

($i+1$) ...

Berechne $\mathrm{ggT}(x, m)$ für die folgenden Zahlen.

(i) $x = 19$ und $m = 15$.
(ii) $x = 225$ und $m = 60$.
(iii) $x = 1843$ und $m = 855$.
(iv) $x = 1055$ und $m = 1028$.

Aufgabe 23 *(Exkurs: Lemma von Bezout)*
Eine Erweiterung des Euklidischen Algorithmus liefert das folgende Resultat: Es seien $x, m \in \mathbb{Z}$ und $\mathrm{ggT}(x, m)$ der größte gemeinsame Teiler von x und m. Dann existieren zwei Zahlen $\alpha, \beta \in \mathbb{Z}$, sodass

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

Wende den Erweiterten Euklidischen Algorithmus auf die Zahlenpaare aus Aufgabe 22 an.
Hinweis: Zur Erklärung des Erweiterten Euklidischen Algorithmus, siehe am Minute 9:
`https://tinyurl.com/EEAvideo`.