Übung zu Modul: Innermathematische Beziehungen
Zahlentheorie

Fabian Grünig
gruenig@ph-heidelberg.de

Sommersemester 2017
Mittwoch, 12:00 Uhr, A233

Aufgabe 35 *(Kongruenzklassen und Diophantische Gleichungen)*
Wir betrachten eine lineare Diophantische Gleichung $G\colon a \cdot x + m \cdot y = c$ mit Koeffizienten $a, m, c \in \mathbb{Z}$. Aus der bisherigen Theorie ist bekannt, dass

$$G \text{ ist lösbar} \qquad \text{gdw.} \qquad \operatorname{ggT}(a, m) \mid c.$$

Für den Spezialfall $\operatorname{ggT}(a, m) = 1$ ist die Gleichung G also unabhängig von c immer lösbar.

(i) Zeige die Äquivalenz der folgenden Aussagen für diesen Spezialfall.
   (a) Es ist $\operatorname{ggT}(a, m) = 1$.
   (b) Es ist die Gleichung G für alle $c \in \mathbb{Z}$ lösbar.
   (c) Es ist $[a]_m$ eine Einheit in $\mathbb{Z}_m$.

(ii) Zeige die Äquivalenz der folgenden Aussagen für fixiertes $c \in \mathbb{Z}$.
   (a) Es gilt $\operatorname{ggT}(a, m) \mid c$.
   (b) Die Gleichung G ist lösbar.
   (c) Es ist $[a]_m$ ein Teiler[1] von $[c]_m$ in $\mathbb{Z}_m$.

Aufgabe 36 *(Auswirkungen der Vertreterwahl von Kongruenzklassen)*
Bestimme, ob die lineare Diophantische Gleichung $96 \cdot x + 21 \cdot y = 15$ lösbar ist. Löse dann die folgenden Aufgaben mit möglichst wenig Rechenaufwand.

(i) Sind die folgenden linearen Diophantischen Gleichungen lösbar?

$$117 \cdot x + 21 \cdot y = 15; \qquad 54 \cdot x + 21 \cdot y = 15;$$
$$(-30) \cdot x + 21 \cdot y = 15; \qquad (-72) \cdot x + 21 \cdot y = 15$$

(ii) Sind die folgenden linearen Diophantischen Gleichungen lösbar?

$$75 \cdot x + 21 \cdot y = 14; \qquad 128 \cdot x + 21 \cdot y = 14;$$
$$(-93) \cdot x + 21 \cdot y = 16; \qquad 12 \cdot x + 21 \cdot y = 16$$

(iii) Sind die folgenden linearen Diophantischen Gleichungen lösbar?

$$96 \cdot x + (-75) \cdot y = 15; \qquad 96 \cdot x + 117 \cdot y = 15;$$

(iv) Sind die folgenden linearen Diophantischen Gleichungen lösbar?

$$96 \cdot x + 213 \cdot y = 16; \qquad 96 \cdot x + (-171) \cdot y = 16$$

---

[1] Die Teilbarkeit in $\mathbb{Z}_m$ wird analog zur Teilbarkeit in $\mathbb{Z}$ definiert: Wir nennen $[x]_m$ einen Teiler von $[y]_m$, falls es ein $[z]_m \in \mathbb{Z}_m$ gibt, sodass $[z]_m \cdot [x]_m = [y]_m$.

AUFGABE 37 *(Vorzeichen in linearen Diophantischen Gleichungen)*
Zur Erinnerung: Eine spezielle Lösung für die lineare Diophantische Gleichung

$$440 \cdot x + 198 \cdot y = 22$$

liefert das folgende mehrschrittige Verfahren. Vervollständige das Verfahren um eine spezielle Lösung zu finden. Gebe die allgemeinen Lösungen der Gleichung an.

(1) Anwendung des Euklidischen Algorithmus:

a	b	a div b	Rest (a mod b)	x'	y'
440	198	2	44		
198	44	...	...		
...	...				

Wir erhalten $\text{ggT}(a,b)$ und prüfen $\text{ggT}(a,b) \mid c$.

(2) Anwendung des Erweiterten Euklidischen Algorithmus:

a	b	a div b	Rest (a mod b)	x'	y'
440	198	2	44	...	
198	44	4	22	1	$0 - 4 \cdot 1$
44	22	2	0	0	1

Wir erhalten x', y' mit $x' \cdot a + y' \cdot b = \text{ggT}(a,b)$ und daraus eine Lösung der Gleichung.

$$440 \cdot \underbrace{\left(x' \cdot \frac{c}{\text{ggT}}\right)}_{=x} + 198 \cdot \underbrace{\left(y' \cdot \frac{c}{\text{ggT}}\right)}_{=y} = 44$$

Wir verändern obige Gleichung durch ein Vorzeichenwechsel in

$$440 \cdot x - 198 \cdot y = 44.$$

Untersuche mit folgenden Aufgaben die Auswirkung auf die spezielle Lösungen und die allgemeinen Lösungen.

(i) *Interpretation als Vorzeichen des Koeffizienten*
Wir schreiben die Gleichung um, in

$$440 \cdot x + (-198) \cdot y = 44.$$

Löse die Gleichung mit obigem Verfahren.

a	b	a div b	Rest (a mod b)	x'	y'
440	-198	...	...		

(ii) *Interpretation als Vorzeichen der Variable (Variablensubstitution)*
Wir schreiben die Gleichung um und ersetzen $z := (-y)$, in

$$440 \cdot x + 198 \cdot (-y) = 440 \cdot x + 198 \cdot z = 44.$$

Löse die Gleichung mit obigem Verfahren und bestimme anschließend y (speziell und allgemein).

a	b	a div b	Rest (a mod b)	x'	z'
440	198	...	...		