Innermathematische Beziehungen
Zahlentheorie (Übung)

Prof. Dr. Markus Vogel
Fabian Grünig

Sommersemester 2018
Mittwoch, 14:00 Uhr, H009

Aufgabe 31 *(Kongruenzgleichungen und Diophantische Gleichungen)*
Betrachten wir die Kongruenzgleichung $7 \cdot x \equiv 4 \pmod{14}$. Man kann diese Kongruenzgleichung auch äquivalent durche eine Diophantische Gleichung ausdrücken.

(i) Erkläre den Zusammenhang obiger Kongruenzgleichung und der Diophantischen Gleichung $4 = 7 \cdot x + 14 \cdot y$.

(ii) Gebe die zur Kongruenzgleichung $3 \cdot x \equiv 5 \pmod{20}$ äquivalente Diophantische Gleichung an und löse sie. Wie erbigt sich daraus die Lösung der Kongruenzleichung?

(iii) Gebe für den allgemeinen Fall einer Kongruenzgleichung der Form $a \cdot x \equiv b \pmod{m}$ die äquivalente Diophantische Gleichung an.

(iv) Entwickle ein Kriterium, wann diese allgemeine Kongruenzleichung lösbar ist.

Aufgabe 32 *(Kongruenzklassen und Diophantische Gleichungen)*
Wir betrachten eine lineare Diophantische Gleichung $a \cdot X + m \cdot Y = c$ mit Koeffizienten $a, m, c \in \mathbb{Z}$. Aus der bisherigen Theorie ist bekannt, dass

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

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 LDG 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 LDG ist lösbar.
   (c) Es ist $[a]_m$ ein Teiler[1] von $[c]_m$ in $\mathbb{Z}_m$.

---

[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 $[z]_m \cdot [x]_m = [y]_m$.

ZUSATZAUFGABE 8 *(Vorzeichen in linearen Diophantischen Gleichungen)*
Zur Erinnerung: Eine spezielle Lösung für die lineare Diophantische Gleichung

$$440 \cdot x + 198 \cdot y = 44$$

liefert der erweiterte Euklidische Algorithmus.

(i) Vervollständige das Verfahren um eine spezielle Lösung zu finden. Gebe die allgemeinen Lösungen der Gleichung an.

a	b	q	r	x'	y'
440	198	2	44		
198	44	...	...		
...	...				

(ii) Wir variieren die Gleichung durch Änderung eines Vorzeichens, etwa:

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

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

(a) *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	q	r	x'	y'
440	-198	...	...		
-198	...	...	...		
...	...				

(b) *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	q	r	x'	z'
440	198	...	...		
198	...	...	...		
...	...				