Übung zu Modul: Innermathematische Beziehungen
Zahlentheorie

Fabian Grünig
gruenig@ph-heidelberg.de

Sommersemester 2017
Mittwoch, 12:00 Uhr, A233

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 *(Ein erstes System von Kongruenzleichungen)*
Es seien die folgenden Kongruenzgleichungen gegeben.

$$x \equiv 2 \pmod{5}$$
$$x \equiv 3 \pmod{7}$$

Welche Zahlen x lösen beide Gleichungen?
Tipp: Bei der Überführung in lineare Diophantische Gleichungen entstehen zwei neue Variablen.

Aufgabe 33 *(Verknüpfungstafeln von Kongruenzklassen)*

(i) Erstelle für $\mathbb{Z}_4$ die Verknüpfungstafel der Addition. Trage jeweils den kleinsten positiver Vertreter einer Restklasse ein.

(ii) Erstelle für $\mathbb{Z}_6$ und für $\mathbb{Z}_7$ die Verknüpfungstafeln der Multiplikation. Trage jeweils den kleinsten positiver Vertreter einer Restklasse ein.

(iii) Bestimme jeweils in $\mathbb{Z}_6$ und in $\mathbb{Z}_7$ die *Einheiten*, also diejenigen Restklassen x, für die eine weitere Restklasse y existiert, sodass $x \cdot y = [1]$.
(Vergleiche Aufgabe 29 oder Kapitel 5, Seite 31.)

(iv) Bestimme jeweils in $\mathbb{Z}_6$ und in $\mathbb{Z}_7$ die *Nullteiler*, also diejenigen von Null verschiedenen Restklassen x, für die es eine weitere Restklasse von Null verschiedene Restklasse y gibt, sodass $x \cdot y = [0]$.
(Vergleiche Kapitel 5, Seite 31.)

AUFGABE 34 *(Einheiten und Nullteiler)*
Es sei R ein Ring mit Einselement 1_R. Zur Erinnerung: Wir nennen $x \in R$ eine *Einheit*, falls es ein $y \in R$ gibt, mit $x \cdot y = 1_R$; wir nennen $x \in R$ einen *Nullteiler*, falls es ein $0 \neq y \in R$ gibt, mit $x \cdot y = 0_R$.

(i) Zeige: Sind $a, b \in R$ beides Einheiten, dann ist auch $a \cdot b$ eine Einheit.

(ii) Zeige: Sind $a, b \in R$ beides Nullteiler, dann ist auch $a \cdot b$ ein Nullteiler.

(iii) Zeige: Ein Element $a \in R$ kann nicht gleichzeitig Einheit und Nullteiler sein.
Tipp: Führe einen Widerpsruchsbeweis.

(iv) Es sei $a \in R$ ein Element, das *kein* Nullteiler ist. Wir betrachten die folgende Abbildung.

$$\begin{aligned} f\colon R &\longrightarrow R \\ x &\longmapsto a \cdot x \end{aligned}$$

Zeige, dass f eine injektive Abbildung ist, also dass aus $f(x) = f(y)$ bereits $x = y$ für beliebige $x, y \in R$ folgt.

(v) Folgere aus (iv), dass es in *endlichen* Ringen[1] nur Nullteiler und Einheiten gibt.

[1] Dies sind insbesondere die Ringe $\mathbb{Z}_m$ der Kongruenzklassen modulo $m \in \mathbb{Z}$.