Innermathematische Beziehungen
Zahlentheorie (Übung)

Prof. Dr. Markus Vogel
Fabian Grünig

Sommersemester 2018
Mittwoch, 14:00 Uhr, H009

Zusatzaufgabe 9 *(Primzahlen)*
Wiederhole im Skript oder diskutiere in Kleingruppen.

(i) Was ist eine Primzahl? Welche Charakterisierungen oder Definitionen kennst Du?

(ii) Was ist eine Primfaktorzerlegung?

(iii) Hättest Du Lust, in der Modulprüfung die Primfaktorzerlegung von 2013 auszurechnen? Begründe Deine Antwort.

Zusatzaufgabe 10 *(Teilerfremde Zahlen)*
Es seien $a, m \in \mathbb{Z}$ teilerfremd[1]. Finde möglichst viele Aussagen aus der Vorlesungen und den Übungen, die unter dieser Voraussetzung gelten.
Tipp: Was weißt Du über die Primfaktorzerlegung dieser Zahlen? Welche Teilbarkeitsaussagen kannst Du schließen? Welche Eigenschaften haben lineare Diophantische Gleichungen mit diesen Koeffizienten? Welche Eigenschaften haben Restklassen bezüglich dieser Zahlen? Welche Rechenregeln gelten für Kongruenzgleichungen? etc.

Zusatzaufgabe 11 *(Teiler und Vielfache)*

(i) Wiederhole die Definition der Mengen $M(z)$ und $T(z)$ für eine ganze Zahle $z \in \mathbb{Z}$.

(ii) Gebe *jeweils* beispielhaft einige Zahlen an, die in den folgenden Mengen enthalten sind: $M(1), T(1), M(2), T(2), M(6), T(6), T(-6), M(-9), T(9)$.

(iii) Wie ist für zwei ganze Zahlen $x, y \in \mathbb{Z}$ auf Basis obiger Mengen $\mathrm{ggT}(x, y)$ und $\mathrm{kgV}(x, y)$ definiert?

(iv) Was ist $\mathrm{ggT}(6, 9)$? Was ist $\mathrm{kgV}(6, 9)$?

Zusatzaufgabe 12 *(Primfaktorzerlegung)*
Es seien $x, y \in \mathbb{Z}$ ganze Zahlen und $x = \prod_p p^{k_p(x)}$ sowie $y = \prod_p p^{k_p(y)}$ die Primfaktorzerlegungen von x, y.

(i) Formuliere die Aussage $x = y$ mit Hilfe der Exponenten der Primfaktorzerlegungen.

(ii) Formuliere die Aussage $x \mid y$ mit Hilfe der Exponenten der Primfaktorzerlegungen.

(iii) Definiere $\mathrm{ggT}(x, y)$ mit Hilfe der Primfaktorzerlegungen von x, y.

(iv) Definiere $\mathrm{kgV}(x, y)$ mit Hilfe der Primfaktorzerlegungen von x, y.

(v) Beweise: Es gilt $\mathrm{ggT}(x, y) \cdot \mathrm{kgV}(x, y) = x \cdot y$.

---

[1] Zur Erinnerung: Wir nennen zwei Zahlen $a, m \in \mathbb{Z}$ *teilerfremd*, falls $\mathrm{ggT}(a, m) = 1$.

ZUSATZAUFGABE 13 *(Lösungsmengen linearer Diophantischer Gleichungen)*
Es sei die Gleichung $a \cdot X + b \cdot Y = c$ für ganze Zahlen $a, b, c \in \mathbb{Z}$ mit $c \neq 0$ gegeben. Es sei (x_0, y_0) eine (spezielle) Lösung dieser Gleichung.

(i) Wie lauten die allgemeinen Lösungen dieser Gleichung?

(ii) Wie lauten die allgemeinen Lösungen dieser Gleichung, falls $\mathrm{ggT}(a, b) = 1$? Wie im Falle $\mathrm{ggT}(a, b) = a$?

(iii) Die Gleichung laute nun $20 \cdot X + 56 \cdot Y = 32$. Eine spezielle Lösung ist $x_0 = -8; y_0 = 24$ und es gilt $\mathrm{ggT}(20, 56) = 4$. Wie lauten die allgemeinen Lösungen dieser Gleichung? Gebe drei weitere spezielle Lösungen an.

ZUSATZAUFGABE 14 *(Euklischer und Erweiterter Euklidischer Algorithmus)*
Führe für die unten gegebenen Zahlen $a, b \in \mathbb{Z}$ den Euklidischen und den Erweiterten Euklidischen Algorithmus zur Berechnung von $\mathrm{ggT}(a, b)$ sowie von $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = a \cdot x + b \cdot y$ durch.

(i) Für $a = 20$ und $b = 56$.

(ii) Für $a = 56$ und $b = 20$.

(iii) Für $a = -20$ und $b = 56$.

(iv) Für $a = 20$ und $b = -56$.

(v) Für $a = -20$ und $b = -56$.

ZUSATZAUFGABE 15 *(Kongruenzen, Kongruenzklassen und Vertreter)*
Es sei $0 \neq m \in \mathbb{Z}$. Für zwei weitere Zahlen $a, b \in \mathbb{Z}$ ist die Kongruenz $(a \equiv b \mod m)$ definiert über die Bedingung $m \mid (a - b)$.

(i) Prüfe für $m = 5$ mit obigem Kriterium nach, ob Kongruenzen $(a \equiv b \mod 5)$ für die folgenden Zahlen erfüllt sind oder nicht.

$$\begin{array}{lll}
a = 12, b = 7; & a = 13, b = 8; & a = 24, b = 12; \\
a = 12, b = 17; & a = 13, b = 20; & a = 24, b = 34; \\
a = 2, b = -18; & a = 2, b = -3; & a = 2, b = -2; \\
a = -8, b = 2; & a = -9, b = 11; & a = -7, b = 13; \\
a = -8, b = -3; & a = -12, b = -4; & a = -4, b = -4;
\end{array}$$

(ii) Zeige: $(a \equiv 0 \mod m)$ gdw. $(m \mid a)$

(iii) Zeige: $(0 \equiv b \mod m)$ gdw. $(m \mid b)$

(iv) Zeige: $(a \equiv b \mod m)$, falls (a und b lassen beim Teilen durch m den gleichen Rest.)

ZUSATZAUFGABE 16 *(Rechenregeln für Kongruenzklassen)*
Es seien alle folgenden Variablen ganze Zahlen, insbesondere $m, d \neq 0$, und $n \in \mathbb{N}$. Mache Dir bewusst, warum die folgenden Rechenregeln in $\mathbb{Z}_m$ gelten und realisiere sie an einem Beispiel Deiner Wahl. Überführe die Regeln (wo noch nicht geschehen) in die Schreibweise für Kongruenzklassen.

(i) $a \equiv a \mod m$ bzw. $[a]_m = [a]_m$

(ii) $(a \equiv b \mod m)$ und $(b \equiv c \mod m) \Rightarrow (a \equiv c \mod m)$

(iii) $(a_1 \equiv a_2 \mod m)$ und $(b_1 \equiv b_2 \mod m) \Rightarrow (a_1 + b_1 \equiv a_2 + b_2 \mod m)$

(iv) $(a_1 \equiv a_2 \mod m)$ und $(b_1 \equiv b_2 \mod m) \Rightarrow (a_1 - b_1 \equiv a_2 - b_2 \mod m)$

(v) $(a \equiv b \mod m) \Rightarrow (a \pm c \equiv b \pm c \mod m)$

(vi) $(a \equiv b \mod m) \Rightarrow (a^2 \equiv b^2 \mod m)$

(vii) $(a \equiv k \cdot m + r \mod m) \Rightarrow (a \equiv r \mod m)$

(viii) $(a \equiv b \mod m)$ und $(\mathrm{ggT}(d, m) = 1)$ und $(d \mid a, b) \Rightarrow (\frac{a}{d} \equiv \frac{b}{d} \mod m)$

Zusatzaufgabe 17 *(Einheiten und Nullteiler)*

(i) Wie sind Einheiten und Nullteiler in $\mathbb{Z}_m$ definiert?

(ii) Welches Kriteraum muss erfüllt sein, damit a eine Einheit in $\mathbb{Z}_m$ ist?

(iii) Welches Kriteraum muss erfüllt sein, damit a ein Nullteiler in $\mathbb{Z}_m$ ist?

(iv) Es gelte $\mathrm{ggT}(a, m) = 1$. Ist dann m eine Einheit in $\mathbb{Z}_a$?

(v) Bestimme alle Einheiten und Nullteiler in $\mathbb{Z}_8$.

(vi) Bestimme alle Einheiten und Nullteiler in $\mathbb{Z}_{12}$.

(vii) Bestimme alle Einheiten und Nullteiler in $\mathbb{Z}_{13}$.

Zusatzaufgabe 18 *(Einheiten und multiplikative Inverse)*

(i) Zeige, dass $\overline{11}$ keine Einheit in $\mathbb{Z}_{1353}$ ist. Ist 11 (multiplikativ) invertierbar in $\mathbb{Z}_{1353}$?

(ii) Zeige, dass $\overline{11}$ eine Einheit in $\mathbb{Z}_{23}$ ist und bestimme die Restklasse $\overline{x} \in \mathbb{Z}_{23}$ mit $\overline{11} \cdot \overline{x} = \overline{1}$.