ALTA
Institute for Algebra, Geometry, Topology and their Applications

Dr. Tim Haga

Universität Bremen

Mathematische Grundlagen I
WS 2018/19

Übungsblatt 7

Präsenzübungen

P24. Wenden Sie den euklidischen Algorithmus an um den ggT von 96 und 60 zu berechnen.

P25. Nutzen Sie den *erweiterten* euklidischen Algorithmus, um Zahlen $a, b \in \mathbb{Z}$ zu finden, welche die Gleichung $13a + 34b = 1$ lösen.

P26. Lösen Sie das folgende System von Kongruenzen

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 8 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

P27. Warum hat das folgende System von Kongruenzen keine Lösung?

$$\begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 6 \end{aligned}$$

P28. Betrachten Sie die Kongruenzgleichung $ax \equiv b \pmod m$. Geben Sie je zwei Beispiele für a, b, m, sodass die Kongruenz

a) keine Lösung,

b) eine eindeutige Lösung $\pmod m$

besitzt.

Bitte wenden!

Verständnisfragen (Diese Aufgaben dienen ihrer Selbstkontrolle)

1. Warum ist die Relation $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ definiert durch
$$(m, n) \sim (m', n') :\Leftrightarrow m + n' = m' + n$$
eine Äquivalenzrelation?
2. Warum erfüllen die ganzen Zahlen $\mathbb{Z}$ die Peano-Axiome nicht?
3. Warum ist Teilbarkeitsrelation auf den ganzen Zahlen keine Halbordnung, auf den natürlichen Zahlen aber schon?
4. Wie kann man die natürlichen Zahlen in die ganzen Zahlen einbetten?
5. Warum ist die Division mit Rest eindeutig?
6. Wann heißen zwei Zahlen kongruent (modolo m) zueinander?
7. Was für eine Relation ist diese Kongruenzrelation?
8. Was ist $n\mathbb{Z}$? Was ist $\mathbb{Z}_n$?
9. Warum ist für festes $m \in \mathbb{Z}$ die Relation $aRb :\Leftrightarrow m \mid (a - b)$ eine Äquivalenzrelation? Welches sind die Äquivalenzklassen?
10. Warum gilt für $a = qb + r$, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$ ist?
11. Ist ggT auch assoziativ; d.h. gilt: $\mathrm{ggT}(a, \mathrm{ggT}(b, c)) = \mathrm{ggT}(\mathrm{ggT}(a, b), c)$?
12. Gegeben $m \in \mathbb{Z}$. Für welche Zahlen $a \in \mathbb{Z}$ ist $\mathrm{ggT}(a, m) = m$ und für welche ist $\mathrm{ggT}(a, m) = 1$.
13. Wie kann man den ggT berechnen?
14. Warum mach es (fast) keinen Unterschied, ob man den euklidischen Algorithmus mit `euklid(a,b)` *oder* `euklid(b,a)` aufruft?
15. Für welche Zahlenpaare benotigt der euklidische Algorithmus wenig Schritte, für welche benötigt er viele?
16. Worin besteht die Erweiterung in dem erweiterten euklidischen Algorithmus?
17. Warum ist die Primfaktorzerlegung einer natürlichen Zahl eindeutig (bis auf Reihenfolge der Faktoren)?
18. Kann man den chinesischen Restesatz auch benutzen, wenn die Moduln nicht teilerfremd sind? Wie ist das Verfahren anzupassen?
19. Warum erkennt die Prüfziffer der ISBN-13 stets, ob eine einzelne Ziffer falsch eingegeben wurde?
20. Warum werden nicht alle Vertauschungen benachbarter Ziffern von der Prüfziffer der ISBN-13 erkannt? Welche werden nicht erkannt?
21. Welche Eingabefehler erkennt die Prüfziffer der ISBN-13, wenn genau zwei Zahlen falsch eingegeben wurden?

Weitere Aufgaben zum Selbststudium

1. Beweisen Sie die folgenden Aussagen aus der Vorlesung: Seien $k, l, m, n \in \mathbb{Z}$ und $k \neq 0$. Dann gelten:
   a) Wenn $k \mid l$ und $k \mid m$ gelten, dann auch $k \mid (l + m)$.
   b) Wenn $k \mid l$ und $k \mid m$ gelten, dann auch $k \mid (l - m)$.
   c) Wenn $k \mid l$ gilt, dann gilt auch $k \mid ln$.
   d) Sei $m \neq 0$. Dann gilt: Aus $k \mid l$ und $m \mid n$ folgt $km \mid ln$.

2. Der Fundamentalsatz der elementaren Zahlentheorie besagt, dass sich jede natürliche Zahl $n > 1$ als Produkt von Primzahlen ausdrücken lässt, z.B. $90 = 2 \cdot 3^2 \cdot 5$.
   a) Geben Sie 42 als Produkt von Primpotenzen an.
   b) Sei A die Menge der Teiler von 90 und B die Menge der Teiler von 42. Geben Sie A und B explizit an. Bestimmen Sie $A \cap B$.

3. Zeigen Sie:
   a) Seien $z, q, r \in \mathbb{N}$ sodass $q \leq r$ und $z = q \cdot r$. Dann gilt $q \leq \sqrt{z}$.
   b) Es gibt unendlich viele Primzahlen.

4. Lösen Sie die folgenden Systeme von Kongruenzen:
   a)
   $$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$
   b)
   $$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 2 \pmod 5 \end{aligned}$$

5. Bestimmen Sie die Lösungsmenge der folgenden Kongruenzen:
   a) $x \equiv 18 \pmod{21}$
   b) $x \equiv 1 \pmod{20}$
   c) $15x \equiv 1 \pmod{32}$
   d) $11x \equiv 1 \pmod{27}$