Algebra für Informatik (2016S)

10. Übungsblatt, mit Lösungen

für den 6. Juni 2016

1. Berechnen Sie das kleinste gemeinsame Vielfache von

   (a) 62 und 93

   (b) 55 und 89

   (c) 120 und 126

   Lösung:
   Nach Satz 6.12 gilt $\mathrm{kgV}(a,b) = \frac{a}{\mathrm{ggT}(a,b)} \cdot b$. Daher ist (a) $\mathrm{kgV}(62,93) = 2 \cdot 93 = 186$, (b) $\mathrm{kgV}(55,89) = 55 \cdot 89 = 4895$ und (c) $\mathrm{kgV}(120,126) = 20 \cdot 126 = 2520$. □

2. Es seien $a, b, c, d \in \mathbb{N}$ sodass $a \mid c$ und $b \mid d$. Zeigen Sie, dass dann gilt:

$$ab \mid \mathrm{kgV}(c,d)\,\mathrm{ggT}(a,b).$$

   Lösung:
   Nach Satz 6.12 gilt $ab = \mathrm{kgV}(a,b)\,\mathrm{ggT}(a,b)$. Es ist also zu zeigen, dass $\mathrm{kgV}(a,b)\,\mathrm{ggT}(a,b) \mid \mathrm{kgV}(c,d)\,\mathrm{ggT}(a,b)$. Da $\mathrm{ggT}(a,b) \neq 0$, ist das äquivalent zu $\mathrm{kgV}(a,b) \mid \mathrm{kgV}(c,d)$.

   Da $a \mid c$ und $c \mid \mathrm{kgV}(c,d)$, gilt $a \mid \mathrm{kgV}(c,d)$.
   Und ebenso, $b \mid \mathrm{kgV}(c,d)$. Mit Satz 6.11 folgt daher die Behauptung. □

3. Sei $(p_1, p_2, p_3, \dots) = (2, 3, 5, \dots)$ die Folge der Primzahlen. Für $a, b \in \mathbb{N}$ seien $(\alpha_i)_{i\in\mathbb{N}}$ und $(\beta_i)_{i\in\mathbb{N}}$ sodass $a = \prod_{i\in\mathbb{N}} p_i^{\alpha_i}$ und $b = \prod_{i\in\mathbb{N}} p_i^{\beta_i}$ die Primzahlzerlegungen von a und b sind. Dann lassen sich ggT und kgV auf folgende Weise ausdrücken:

$$\mathrm{ggT}(a,b) = \prod_{i\in\mathbb{N}} p_i^{\min(\alpha_i,\beta_i)} \quad \text{und} \quad \mathrm{kgV}(a,b) = \prod_{i\in\mathbb{N}} p_i^{\max(\alpha_i,\beta_i)}.$$

   Verwenden Sie diese Formeln um die Distributivgesetze für ggT und kgV zu beweisen, siehe Satz 6.13 (3–4) im Skriptum. Zeigen Sie also, dass für $a, b, c \in \mathbb{N}$ folgende Identitäten gelten:

   (a) $\mathrm{ggT}(\mathrm{kgV}(a,b),c) = \mathrm{kgV}(\mathrm{ggT}(a,c),\mathrm{ggT}(b,c))$

   (b) $\mathrm{kgV}(\mathrm{ggT}(a,b),c) = \mathrm{ggT}(\mathrm{kgV}(a,c),\mathrm{kgV}(b,c))$

   Lösung:
   Wir zeigen zunächst, dass min und max die Distributivgesetze erfüllen:

   (a) $\min(\max(a,b),c) = \max(\min(a,c),\min(b,c))$

   (b) $\max(\min(a,b),c) = \min(\max(a,c),\max(b,c))$

   Eine Möglichkeit dazu ist, die verschiedenen Fälle zu unterscheiden.

   $a \leq b$**:** Dann ist $\max(a,b) = b$, $\min(a,b) = a$. Es sind somit nur noch zu zeigen:

   (a) $\min(b,c) = \max(\min(a,c),\min(b,c))$

   (b) $\max(a,c) = \min(\max(a,c),\max(b,c))$

   $b \leq c$**:** Dann vereinfachen sich die Bedingungen zu

(a) $b = \max(a, b)$
(b) $c = \min(c, c)$
welche unter diesen Voraussetzungen gelten.

$c \leq a$**:** Dann vereinfachen sich die Bedingungen zu
(a) $c = \max(c, c)$
(b) $a = \min(a, b)$
welche ebenfalls gelten.

$a \leq c \leq b$**:** Dann vereinfachen sich die Bedingungen zu
(a) $c = \max(a, c)$
(b) $c = \min(c, b)$
welche ebenfalls gelten.

$b \leq a$**:** analog.

□

4. Geben Sie zu jeder der folgenden Kongruenzen eine Teilmenge T von $\mathbb{N}$ an, sodass die Kongruenz *genau dann* lösbar ist, wenn $c \in \mathbb{N}$ von keinem Element von T geteilt wird.

   (a) $42x \equiv 22 \pmod{c}$
   (b) $20x \equiv 29 \pmod{c}$
   (c) $36x \equiv 10 \pmod{c}$

   Lösung:
   Nach Satz 6.15 gilt (a) $T = \{3, 7\}$, (b) $T = \{2, 5\}$ und (c) $T = \{3, 4\}$. Zu beachten ist insbesondere, dass bei (b) $2 \in T$ gilt während bei (c) $2 \notin T$ gelten muss. □

5. Bestimmen Sie das kleinste $x \in \mathbb{N}$ sodass

$$7x \equiv 22 \pmod{100}.$$

   Lösung:
   Mittels erweitertem Euklidischen Algorithmus berechnet man $43{\cdot}7 - 3{\cdot}100 = 1 = \text{ggT}(7, 100)$. Daher ist $22 = 22{\cdot}43{\cdot}7 - 22{\cdot}3{\cdot}100 = 946{\cdot}7 - 66{\cdot}100 = (946 - 100k){\cdot}7 - (66 - 7k){\cdot}100$. Mit $k = 9$ erhält man $x = 46$ als kleinste Lösung. □

6. Seien $a, b, c \in \mathbb{Z}$ mit $c \neq 0$ sodass die Kongruenz $ax \equiv b \pmod{c}$ in $\mathbb{Z}$ lösbar ist. Zeigen Sie, dass dann genau eine Lösung $x_0 \in \mathbb{Z}$ mit $0 \leq x_0 < \frac{|c|}{\text{ggT}(a,c)}$ existiert.

   Lösung:
   Sei x eine Lösung der Kongruenz. Dann gilt $\text{ggT}(a, c) \mid b$. Weiters gibt es ein $q \in \mathbb{Z}$ und $x_0 \in \mathbb{Z}$, sodass $x = q\frac{c}{\text{ggT}(a,c)} + x_0$ und $0 \leq x_0 < \frac{|c|}{\text{ggT}(a,c)}$. Es gilt dann

$$ax_0 \equiv a(x - q\frac{c}{\text{ggT}(a, c)}) \equiv ax - \frac{a}{\text{ggT}(a, c)}qc \equiv ax \equiv b \pmod{m}.$$

   Sei umgekehrt x_1 eine weitere Lösung mit dieser Eigenschaft. Dann gilt

$$a(x_1 - x_0) \equiv 0 \pmod{c}$$

   Es gibt also ein $y \in \mathbb{Z}$, sodass

$$a(x_1 - x_0) + cy = 0.$$

   Und damit auch

$$\frac{a}{\text{ggT}(a, c)}(x_1 - x_0) + \frac{c}{\text{ggT}(a, c)}y = 0.$$

   Somit

$$\frac{a}{\text{ggT}(a, c)}(x_1 - x_0) \equiv 0 \pmod{\frac{c}{\text{ggT}(a, c)}}.$$

Sei z ein Inverses von $\frac{a}{\mathrm{ggT}(a,c)}$ modulo $\frac{c}{\mathrm{ggT}(a,c)}$. Dann gilt

$$x_1 - x_0 \equiv 0 \pmod{\frac{c}{\mathrm{ggT}(a,c)}}.$$

Da aber $|x_1 - x_0| < \frac{|c|}{\mathrm{ggT}(a,c)}$, muss $x_1 - x_0 = 0$ sein. □

7. Bestimmen Sie alle ganzzahligen Lösungen der Gleichung

$$26x + 16y = 42.$$

Lösung:
Die Gleichung ist lösbar da 42 durch $\mathrm{ggT}(26, 16) = 2$ teilbar ist. Offensichtlich ist $(x_0, y_0) = (1, 1)$ eine Lösung, alternativ erhält man $(x_0, y_0) = (-63, 105)$ aus dem erweiterten Euklidischen Algorithmus. Die gesamte Lösungsmenge ist dann gegeben durch $\{(x_0 + 8k, y_0 - 13k) \mid k \in \mathbb{Z}\}$. □

8. Berechnen Sie die Lösungen $x \in \mathbb{Z}$ der folgenden Kongruenzen.

   (a) $44x \equiv 74 \pmod{14}$

   (b) $44x \equiv 74 \pmod{15}$

   (c) $44x \equiv 74 \pmod{16}$

Lösung:
Unter Verwendung der Sätze 6.15 und 6.16 erhält man

(a) $\{x_0 + 7k \mid k \in \mathbb{Z}\}$ mit $x_0 = 1 \cdot \frac{74}{2} = 37$ oder $x_0 = 2$

(b) $\{x_0 + 15k \mid k \in \mathbb{Z}\}$ mit $x_0 = -1 \cdot 74 = -74$ oder $x_0 = 1$

(c) Es existiert keine Lösung da 74 nicht durch $\mathrm{ggT}(44, 16) = 4$ teilbar ist

□