Übungsblatt 1

Aufgabe 1. (a) Bestimmen Sie mit Hilfe des euklidischen Algorithmus ggT(3611730, 47469).

(b) Bestimmen Sie die dazugehörenden Bézout-Koeffizienten, d.h. $\lambda_1, \lambda_2 \in \mathbb{Z}$ so, dass

$$\mathrm{ggT}(3611730, 4746) = \lambda_1 \cdot 3611730 + \lambda_2 \cdot 4746$$

gilt.

(a) Es gilt

$$\begin{aligned} 3611730 &= 761 \cdot 4746 + 24 \\ 4746 &= 197 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0. \end{aligned}$$

Demnach ist ggT(3611730, 47469) = 6.

(b) Das Rückrechnen des obigen Verfahrens liefert

$$\begin{aligned} 6 &= 24 + (-1) \cdot 18 \\ &= 24 + (-1) \cdot (4746 - 197 \cdot 24) = 198 \cdot 24 + (-1) \cdot 4746 \\ &= 198 \cdot (3611730 - 761 \cdot 7476) - 4746 = 198 \cdot 3611730 - 150679 \cdot 4746. \end{aligned}$$

Man erhält also $\lambda_1 = 198$, $\lambda_2 = -150679$.

Aufgabe 2. Die Notation sei wie in der Vorlesung. Zeigen Sie

(a) $a_n =$ggT(a_1, a_2).

(b) Es existieren $\lambda_1, \lambda_2 \in \mathbb{Z}$ mit $a_n = \lambda_1 a_1 + \lambda_2 a_2$.

Beweis. (a) Es reicht die folgende Eigenschaft zu beweisen. Seien $\lambda, r \in \mathbb{Z}$ mit $a_2 = \lambda a_1 + r$, so gilt ggT$(a_1, a_2) =$ggT(a_1, r). Wir müssen zeigen, dass

$$\mathrm{ggT}(a_1, r) \mid a_1, a_2 \text{ und } \mathrm{ggT}(a_1, a_2) \mid \mathrm{ggT}(a_1, r).$$

Aus der Definition des ggT's folgt dann ggT$(a_1, a_2) =$ggT(a_1, r).
Nach Definition gilt ggT$(a_1, r) \mid a_1$. Außerdem gilt wegen ggT$(a_1, r) \mid r$ auch ggT$(a_1, r) \mid \lambda a_1 + r = a_2$.
Sei $t \in \mathbb{Z}$ mit $t \mid a_1, a_2$, so gilt $t \mid a_2 - \lambda a_1 = r$ und somit $t \mid$ggT(a_1, r). Insbesondere gilt für $t =$ggT(a_1, a_2) auch ggT$(a_1, a_2) \mid$ggT(a_1, r). Insgesamt gilt also ggT$(a_1, a_2) =$ggT(a_1, r).
Somit erhalten wir induktiv mit $a_{n+1} = 0$ (siehe Vorlesung)

$$\mathrm{ggT}(a_1, a_2) = \mathrm{ggT}(a_n, a_{n+1}) = \mathrm{ggT}(a_n, 0) = a_n.$$

(b) Nach dem ersten Teil ist $a_n =$ggT(a_1, a_2). Wie in Aufgabe 1b) kann man den euklidischen Algorithmus benutzen, um konkret Bézout-Koeffizienten zu errechnen. Im Folgenden führen wir einen anderen Existenzbeweis. Betrachte anstelle von a_1, a_2 die ganzen Zahlen $a_1' := \frac{a_1}{\mathrm{ggT}(a_1, a_2)}$, $a_2' := \frac{a_2}{\mathrm{ggT}(a_1, a_2)}$ und somit gilt ggT$(a_1', a_2') = 1$. Da der ggT bis auf Vorzeichen eindeutig definiert ist, können wir annehmen, dass a_1', a_2' nicht negativ sind. Betrachte die endliche Folge

$$a_1', 2a_1', 3a_1', \ldots, (a_2' - 1)a_1', a_2' a_1'.$$

Je zwei Zahlen aus obiger Folge haben verschiedenen Rest bei der Division durch a_2', denn angenommen es existieren $1 \le k < k' \le a_2'$, $\lambda, \lambda' \in \mathbb{Z}$, $r \in \mathbb{Z}$ mit

$$ka_1' = \lambda a_2' + r \text{ und } k' a_1' = \lambda' a_2' + r,$$

so gilt $(k' - k) a_1' = (\lambda - \lambda') a_2'$. Da a_1' und a_2' teilerfremd sind, gilt $a_2' \mid k' - k$. Dies ist aber nicht möglich, denn $0 < k' - k < a_2'$.
Da es bei der Division durch a_2' nur a_2'–verschiedene Rest geben kann, muss jeder Rest ($\le a_2'$) in der Folge genau einmal auftreten. Also gibt es ein $1 \le k \le a_2$ und $\lambda \in \mathbb{Z}$ mit

$$ka_1' = \lambda a_2' + 1,$$

was äquivalent zu $1 = ka_1' - \lambda a_2'$ ist. Offensichtlich gilt nun

$$\operatorname{ggT}(a_1, a_2) = \operatorname{ggT}(a_1, a_2)(ka_1' - \lambda a_2') = ka_1 - \lambda a_2.$$

Setze also $\lambda_1 = k$ und $\lambda_2 = -\lambda$.

□

Aufgabe 3. Bestimmen Sie ganzzahlige Lösungen der folgenden diophantischen Gleichungen:

(a) $15x + 35y = 5$.

(b) $15x + 35y + 21z = 1$.

(a) Zunächst dividieren wir die Gleichung mit $\operatorname{ggT}(15, 35) = 5$ und erhalten eine Gleichung deren Lösungsmenge mit der Lösungsmenge der ursprünglichen Gleichung übereinstimmt. Betrachte also die neue Gleichung $3x + 7y = 5$. Da der Koeffizient vor der Variable x betragsmäßig der kleinste ist, lösen wir die Gleichung nach x auf und führen eine komponentenweise Division mit Rest durch. Wir erhalten somit

$$x = \frac{1 - 7y}{3} = -2y + \frac{1 - y}{3} = -2y + a,$$

wobei $a := \frac{1-y}{3}$ eine ganze Zahl sein muss. Also gilt $y = 1 - 3a$ und somit $x = 7a - 2$. Die Lösungsmenge $\mathbb{L}$ lautet

$$\mathbb{L} = \{(7a - 2, 1 - 3a) \mid a \in \mathbb{Z}\}.$$

(b) Hier gehen wir analog vor. Wir lösen die Gleichung nach x auf und führen eine komponentenweise Division durch. Wir erhalten also

$$x = \frac{1 - 35y - 21z}{15} = -2y - z + \frac{1 - 5y - 6z}{15} = -2y - z + a,$$

wobei $a := \frac{1-5y-6z}{15}$ eine ganze Zahl ist. Letzteres impliziert

$$y = \frac{1 - 6z - 15a}{5} = -z - 3a + \frac{1 - z}{5} = -z - 3a + b,$$

wobei $b = \frac{1-z}{5}$ eine ganze Zahl ist. Wir erhalten also $z = 1 - 5b$ und somit

$$y = -z - 3a + b = -(1 - 5b) - 3a + b = -3a + 6b - 1$$

und

$$x = -2y - z + a = -2(-3a + 6b - 1) - (1 - 5b) + a = 1 + 7a - 7b.$$

Die Lösungsmenge $\mathbb{L}$ lautet also

$$\mathbb{L} = \{(1 + 7(a - b), -3a + 6b - 1, 1 - 5b) \mid a, b \in \mathbb{Z}\}.$$

Aufgabe 4. Sei $n \in \mathbb{N}$ beliebig. Zeigen Sie: 3 und 5 teilen $n^5 - n$.

Beweis. Sei $a \in \{3,5\}$. Nehme zunächst an, dass $a \mid n$, so folgt aus $n^5 - n = n(n^4-1)$ direkt $a \mid n^5 - n$. Also sei $a \nmid n$. Es gilt $n = a \cdot k + l$ mit $k \in \mathbb{N}_0$ und $1 \leq l \leq a-1$. Wir erhalten somit

$$n^4 - 1 = \left(\sum_{q=0}^{4} \binom{4}{q} (ak)^{4-q} l^q\right) - 1 = (ak)^4 + 4(ak)^3 l + 6(ak)^2 l^2 + 4(ak) l^3 + l^4 - 1.$$

Im Folgenden zeigen wir, dass $a \mid l^4 - 1$, woraus direkt die Behauptung folgt.

$$\begin{aligned} l = 1,\ a \in \{3,5\} &: a \mid l^4 - 1 = 0 \\ l = 2,\ a \in \{3,5\} &: a \mid l^4 - 1 = 15 \\ l = 3,\ a \in \{5\} &: a \mid l^4 - 1 = 80 \\ l = 4,\ a \in \{5\} &: a \mid l^4 - 1 = 250 \end{aligned}$$

Also existiert ein $b \in \mathbb{N}_0$ mit $l^4 - 1 = a \cdot b$ und wir erhalten insgesamt

$$n^5 - n = n(n^4 - 1) = n \cdot a(a^3 k + 4a^2 k^3 l + 6a(kl)^2 + 4kl^3 + b),$$

d.h. $a \mid n^5 - n$. $\square$