# vhb - Kurs: Grundlagen der elementaren Zahlentheorie

## III.2. Lineare diophantische Gleichungen - Beispiel einer Diophantischen Gleichung

Zu Lösen sei die Gleichung

$$(1) \qquad 106X - 333Y = 1.$$

Mit dem euklidischen Algorithmus berechnen wir den größten gemeinsamen Teiler von 333 und 106 wie folgt:

$$\begin{aligned} \mathbf{333} &= 3 \cdot \mathbf{106} + 15, \\ 106 &= 7 \cdot 15 + \mathbf{1}, \end{aligned}$$

Also ist $\mathrm{ggT}(333, 106) = \mathbf{1}$ und nach unseren vorangegangenen Überlegungen ist unsere Ausgangsgleichung (1) somit lösbar. Um eine *explizite* Lösung zu finden, bemühen wir wiederum den euklidischen Algorithmus, diesmal jedoch, in dem wir ihn *von unten nach oben* lesen: Es gilt

$$\begin{aligned} \mathbf{1} &= 1 \cdot 106 - 7 \cdot \mathbf{15} = 1 \cdot 106 - 7 \cdot (\mathbf{333} - 3 \cdot \mathbf{106}) \\ &= 22 \cdot \mathbf{106} - 7 \cdot \mathbf{333}. \qquad \hookleftarrow \end{aligned}$$

Also ist $x = 22$ und $y = 7$ eine spezielle Lösung der Gleichung. Aber existieren weitere Lösungen? Diese Frage ist zu bejahen; tatsächlich existieren mit dieser einen Lösung *unendlich viele* weitere Lösungen in ganzen Zahlen, denn für beliebiges $m \in \mathbb{Z}$ ist

$$\begin{aligned} &106(22 + 333m) - 333(7 + 106m) \\ = \ &\underbrace{106 \cdot 22 - 333 \cdot 7}_{=1} + m \underbrace{(106 \cdot 333 - 333 \cdot 106)}_{=0} = 1. \end{aligned}$$

Hier haben wir also zur speziellen Lösung $(x, y) = (22, 7)$ Lösungen der leicht variierten, so genannten **homogenen Gleichung**

$$106X - 333Y = 0$$

hinzuaddiert; letztere sind leicht zu berechnen und offensichtlich sämtliche von der Form $x = 333m, y = 106m$ für $m \in \mathbb{Z}$. Diese Idee wird später auch noch in der *Linearen Algebra* beim Lösen von Gleichungssystemen eine wichtige Rolle spielen! Die vollständige ganzzahlige Lösungsmenge von (1) ist also

$$(x, y) = (22, 7) + m(333, 106) \qquad \text{für} \quad m \in \mathbb{Z}.$$

Mit dieser (aus der Schulgeometrie bekannten) Schreibweise ist $x = 22 + 333m$ und $y = 7 + 106m$ gemeint (also eine Addition von 'Vektoren').