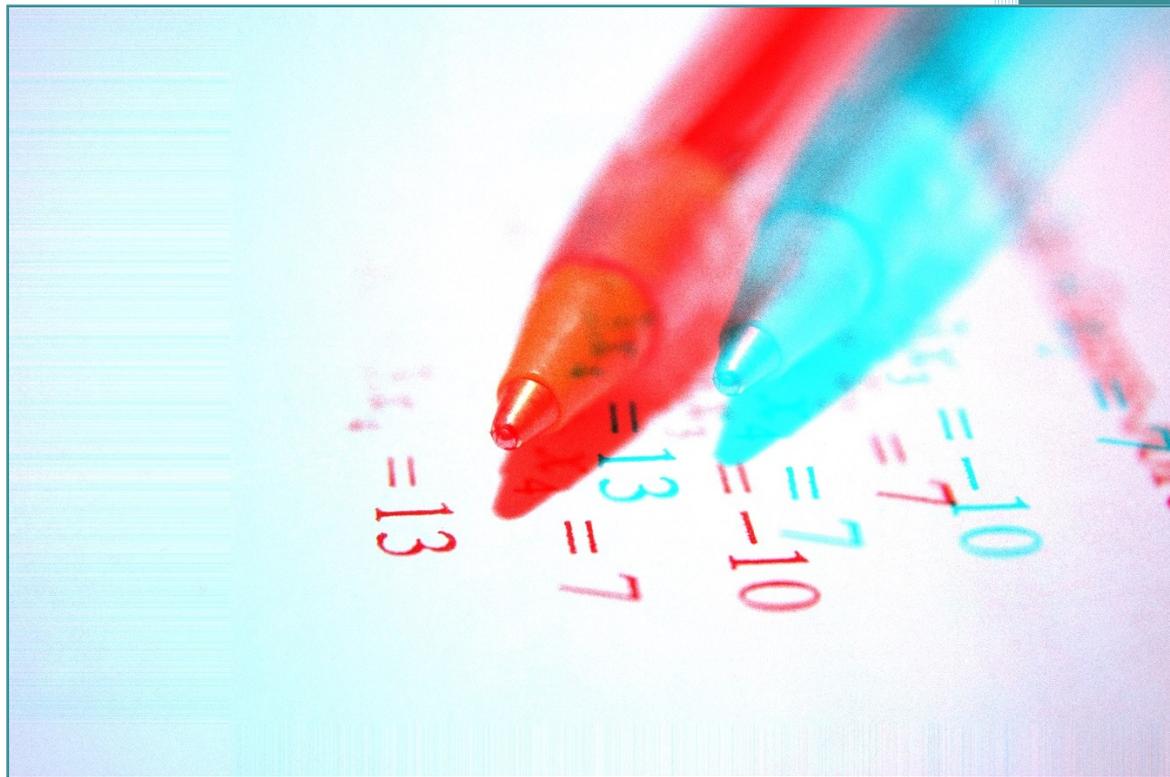


# Zahlentheorie – Teil 2

## Lineare diophantische Gleichungen



# ZAHLENTHEORIE – TEIL 3

## LINEARE DIOPHANTISCHE GLEICHUNGEN

### INHALT

Grundlagen.....	1
Lineare diophantische Gleichungen (in 2 Variablen).....	2
Homogene und inhomogene lineare diophantische Gleichung.....	3
Die Lösungen der homogenen linearen diophantischen Gleichung.....	4
Die Lösungen der inhomogenen linearen diophantischen Gleichung.....	4
Aufgaben.....	5

### GRUNDLAGEN

Die Zahlentheorie ist ein Teilgebiet der Mathematik, das sich mit den Eigenschaften der **ganzen Zahlen** beschäftigt.

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}, \mathbb{N}^{+\mathbb{Z}} = \{1, 2, 3, \dots\}^{\mathbb{Z}}$$

$$\mathbb{Z}^{+\mathbb{Z}} = \mathbb{N}^{+\mathbb{Z}} = \{1, 2, 3, \dots\}^{\mathbb{Z}}, \text{ analog } \mathbb{Z}^{-\mathbb{Z}}$$

$$\mathbb{Z}_0^{+\mathbb{Z}} = \mathbb{N} = \{0, 1, 2, 3, \dots\}^{\mathbb{Z}}, \text{ analog } \mathbb{Z}_0^{-\mathbb{Z}}$$

$\mathbb{Z}$  und  $(\mathbb{N}, \cdot)$  sind nur kommutative Halbgruppen.

$\mathbb{Z}$  ist eine kommutative Gruppe

$(\mathbb{Z}, \cdot)$  ist eine kommutative Halbgruppe

$(\mathbb{Z}, +, \cdot)$  ist ein kommutativer Ring mit Einselement. Das Einzige, was fehlt: es gibt im Allgemeinen keine multiplikativen Inversen (d.h. die Division funktioniert nicht uneingeschränkt).

## LINEARE DIOPHANTISCHE GLEICHUNGEN (IN 2 VARIABLEN)

### Definition: Eine Gleichung der Form

$a \cdot x + b \cdot y = c$  mit  $a, b, c \in \mathbb{Z}$ ,  $a, b \neq 0$ , bei der man nur an **ganzzahligen Lösungen** interessiert ist

(d.h.  $x, y \in \mathbb{Z}$ ), heißt lineare diophantische Gleichung in 2 Variablen.

*Diophantos von Alexandria war ein antiker griechischer Mathematiker. Er gilt als der bedeutendste Algebraiker der Antike. (Wikipedia)*

**Bemerkung:** Unter „Lösungen“ sind in weiterer Folge immer **ganzzahlige** Lösungen gemeint.

Beispiele:

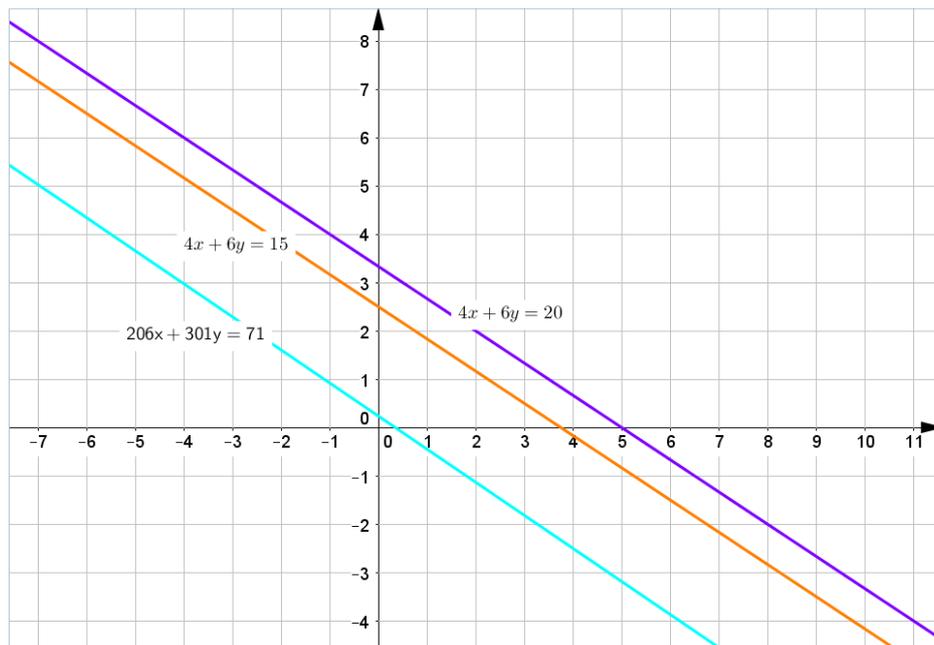
a)  $4x + 6y = 20$

b)  $4x + 6y = 15$

c)  $206x + 301y = 71$

In der graphische Darstellung sind für a) folgende Lösungen ersichtlich:

...  $(-7, 8)$   $(-4, 6)$   $(-1, 4)$   $(2, 2)$   $(5, 0)$   $(8, -2)$   $(11, -4)$  ...



Für die Gleichungen  $4x + 6y = 15$  bzw.  $206x + 301y = 71$  ist dies schwieriger! Gibt es überhaupt zu jeder diophantischen Gleichung Lösungen? Wann gibt es sie, wann nicht?

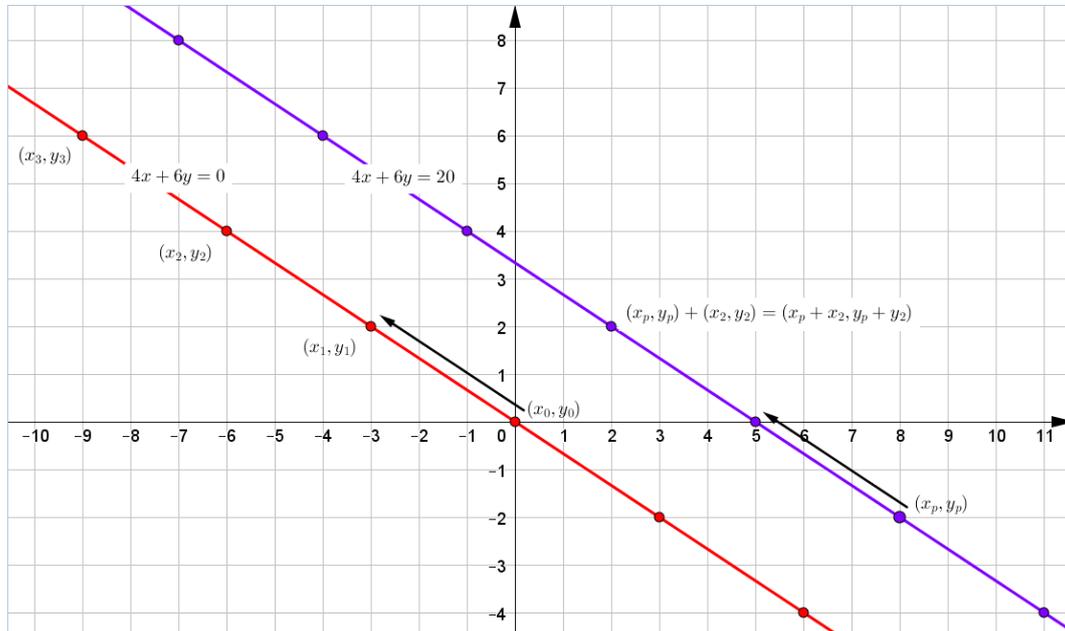
**Satz:** Eine lineare diophantische Gleichung  $a \cdot x + b \cdot y = c$  ist genau dann ganzzahlig lösbar, wenn  $c$  ein ganzzahlig Vielfaches des  $\text{ggT}(a, b)$  ist.

*Beweisskizze:* Dies ist bei  $4x + 6y = 15$  nicht der Fall. Hier kann es keine Lösungen geben, was einleuchtend ist. Der  $\text{ggT}(4, 6) = 2$ . Beide Koeffizienten sind Vielfache von 2. Für eine mögliche Lösung  $(x_0, y_0)$  ist  $4 \cdot x_0 + 6 \cdot y_0$  ein Vielfaches des  $\text{ggT}$ , also von 2. Dies stimmt mit der rechten Seite nicht überein! Damit es Lösungen gibt, muss auch  $c$  ein Vielfaches des  $\text{ggT}(a, b)$  sein. Dass es in diesem Fall aber auch garantiert mindestens eine Lösung gibt, wird später gezeigt.

## HOMOGENE UND INHOMOGENE LINEARE DIOPHANTISCHE GLEICHUNG

**Definition:** Eine lineare diophantische Gleichung  $ax+by=c$  heißt homogen, falls  $c=0$ . Sie heißt inhomogen, wenn  $c \neq 0$ .

Wie aus der Grafik ersichtlich, liegen die Lösungen der inhomogenen diophantischen Gleichung nur parallelverschoben zur homogenen.



Kennt man alle Lösungen der homogenen Gleichung, so kann man auch alle Lösungen der inhomogenen Gleichung finden, sobald man eine einzige (**partikuläre**) Lösung  $(x_p, y_p)$  der inhomogenen Gleichung kennt.

**Satz:** Sind  $(x_h, y_h)$  die Lösungen der homogenen Gleichung  $ax+by=0$ , so ergeben sich alle Lösungen der inhomogenen Gleichung  $ax+by=c$  durch  $(x_i, y_i) = (x_p, y_p) + (x_h, y_h)$ .

*Beweis:*

Gegeben sei eine der Lösungen  $(x_h, y_h)$  der homogenen und eine partikuläre Lösung  $(x_p, y_p)$  der inhomogenen Gleichung. Dann gilt:

$$ax_h + by_h = 0 \vee [ax_p + by_p = c] \quad ax_h + by_h + ax_p + by_p = ca \cdot (x_p + x_h) + b \cdot (y_p + y_h) = c$$

Somit sind alle  $(x_p, y_p) + (x_h, y_h)$  ganzzahlige Lösungen der inhomogenen Gleichung  $ax+by=c$

---

## DIE LÖSUNGEN DER HOMOGENEN LINEAREN DIOPHANTISCHEN GLEICHUNG

Die homogene lineare diophantische Gleichung hat unendlich viele (ganzzahlige) Lösungen.

$ax + by = 0 \Leftrightarrow y = -\frac{a}{b}x \vee$  Kürzen durch  $ggT(a, b)$   $y = -\frac{\alpha}{\beta}x$  Dann sind alle

$(x_h, y_h) = (n\beta, -n\alpha) = n \cdot (\beta, -\alpha)$  mit  $\alpha = \frac{a}{ggT(a, b)}$  und  $\beta = \frac{b}{ggT(a, b)}$  und  $n \in \mathbb{Z}$  Lösungen der homogenen linearen diophantischen Gleichung.

*Beispiel:*

$$18x + 15y = 0 \Leftrightarrow y = -\frac{18}{15}x = -\frac{6}{5}x$$

Falls  $x = n \cdot 5$  mit  $n \in \mathbb{Z}$ , folgt  $y = -\frac{6}{5} \cdot n \cdot 5 = n \cdot (-6)$ .

Lösungsmenge  $L_0 = \{(x_h, y_h) = (n \cdot 5, n \cdot (-6)), n \in \mathbb{Z}\} = \{\dots, (-10, 12), (-5, 6), (0, 0), (6, -6), \dots\}$

---

## DIE LÖSUNGEN DER INHOMOGENEN LINEAREN DIOPHANTISCHEN GLEICHUNG

Die Lösung der Gleichung  $ax + by = c$  mit ganzzahligen Koeffizienten und Lösungen erfolgt in mehreren Stufen. Wir zeigen das Verfahren exemplarisch an der Gleichung

$$4x + 6y = 20$$

- 1) Es kann nur Lösungen geben, wenn  $ggT(a, b) \mid c$ . Der  $ggT(4, 6) \mid 20$ , es kann also Lösungen geben.
- 2) Wir benötigen alle Lösungen der homogenen Gleichung  $ax + by = 0$ .
- 3) Wir benötigen eine partikuläre Lösung der inhomogenen Gleichung  $ax + by = c$ .
- 4) Alle Lösungen der inhomogenen Gleichung ergeben sich aus der Addition der einen partikulären Lösung mit allen Lösungen der homogenen Gleichung.

ad 2)

$4x + 6y = 0$  Kürzen durch den  $ggT(a, b)$   $y = -\frac{4}{6}x = -\frac{2}{3}x$  Ganzzahlige Lösungen gibt es für

$$x = n \cdot 3, y = -\frac{2}{3} \cdot n \cdot 3 = n \cdot (-2) \text{ also}$$

$$n \cdot (3, -2)$$

$$L_h = \{\dots; (-6, 4); (-3, 2); (0, 0); (3, -2); (6, -4); (12, -6); \dots\}$$

ad 3) Für die partikuläre Lösung der Gleichung

$ax + by = c$  wird zuerst die Gleichung

$ax + by = ggT(a, b)$  gelöst. Dafür gibt es ein konstruktives Verfahren, den bekannten **erweiterten Euklidischen Algorithmus**.

$$4x + 6y = 2 = ggT(4, 6)$$

$ggT(4, 6) \rightarrow$  Tabelle für den Euklidischen Algorithmus

$a$	$(n)b$	$a-(n)b$
6	1·4	2 = ggT
4	2·2	0

ausführlich von unten nach oben aufgelöst ergibt sich

$$2 = \text{ggT}(4,6) = 1 \cdot 6 - 1 \cdot 4 = 4 \cdot (-1) + 6 \cdot 1 \quad (x^i, y^i) = (-1, 1)$$

Wir haben also eine Lösung für  $a \cdot x^i + b \cdot y^i = \text{ggT}(a, b)$

$$4 x^i + 6 y^i = 2$$

$$(x^i, y^i) = (-1, 1)$$

Da  $\text{ggT}(a, b) \vee c$  gibt es ein  $q \in \mathbb{Z}$ , sodass  $c = q \cdot \text{ggT}(a, b)$ . Durch die Multiplikation der Gleichung mit  $q$  erhalten wir die partikuläre Lösung.

$$a \cdot x^i + b \cdot y^i = \text{ggT}(a, b) \vee \cdot q$$

$$4 x^i + 6 y^i = 2 \vee \cdot 10$$

$$4 \cdot (10 x^i) + 6 \cdot (10 y^i) = 20$$

Somit bilden  $x_p = 10 x^i = -10$  und  $y_p = 10 y^i = 10$  die gesuchte partikuläre Lösung von  $4x + 6y = 20$

ad 4)

$$L = (-10, 10) + L_h = \{ \dots; (-16, 14); (-13, 12); (-10, 10); (-7, 8); (-4, 6); (2, 4); \dots \}$$

## AUFGABEN

Suche die Menge der ganzzahligen Lösungen folgender linearer diophantischer Gleichungen

- $45x + 42y = 117$
- $30x + 63y = 91$
- $6x - 4y = 14$