Lineare diophantische Gleichungen

NaG: Diophant (ca. 250 n. Chr. in Alexandria)

Definition 2

Eine Gleichung $ax + by = c$ mit $a, b \in \mathbb{N}, c \in \mathbb{Z}$ heißt lineare diophantische Gleichung mit zwei Variablen, falls man als Lösungen nur Elemente aus $\mathbb{Z} \times \mathbb{Z}$ (Paare ganzer Zahlen) zulässt.

Umformulierung von Satz 10:

Satz 12

Die lin. diophantische Gleichung $ax + by = c$ ist genau dann lösbar, wenn gilt $ggT(a,b) \mid c$.

Beispiel: Ist es möglich, für 1000 € Werbegeschenke zu kaufen, wenn jedes Stück von Sorte A 13 € kostet, während jedes Stück von Sorte B 19 € kostet?

$$13 \cdot x + 19y = 1000$$

Da $ggT(13,19) = 1$, ist es lösbar (nach Satz 12).

Satz 12

Die lineare diophantische Gleichung $ax+by=c$ ist genau dann lösbar, wenn gilt $ggT(a,b) \mid c$.

[Folgerung aus Satz 10.]

Beispiele:

Ist $3x+4y=2$ „lösbar"? Ja. [$ggT(3,4)=1 \mid 2$].

Ist $3x+6y=2$ „lösbar"? Nein. [$ggT(3,6)=3 \nmid 2$].

Bemerkung: lösbare !

Man kann jede diophant. Gleichung durch äquiv. Umformungen zu einer diophant. Gleichung machen, in der $ggT(a,b)=1$ gilt.

[Bsp. $210x+704y=2$ $\quad ggT(210,704)=2 \mid 2$

$105x+352y=1$ $\quad ggT(105,352)=1$]

Der folgende Satz kann daher für $a,b \in \mathbb{N}$ mit $ggT(a,b)=1$ formuliert werden, gilt aber entsprechend für alle $a,b \in \mathbb{N}$.

Satz 13

Sei (x_0, y_0) eine Lösung der (lösb.) diophl. Gleichung $ax + by = c$ wobei a und b teilerfremd sind.

Dann besteht die zugehörige Lösungsmenge $\mathbb{L}$ genau aus den Paaren $(x_0 + t \cdot b, y_0 - t \cdot a)$ mit $t \in \mathbb{Z}$.

Bew.:

1. z.z. $(x_0 + tb, y_0 - ta) \in \mathbb{L}$.

Sei (x_0, y_0) Lösung von $ax + by = c$. Dann gilt

$$a(x_0 + tb) + b(y_0 - ta) = ax_0 + tab + by_0 - tab = c$$

(da (x_0, y_0) Lsg.)

$\Rightarrow (x_0 + tb ; y_0 - ta) \in \mathbb{L}$ für alle $t \in \mathbb{Z}$.

2. z.z. Jedes Lösungspaar kann wie oben angegeben werden.

Seien $(x_0, y_0), (x_1, y_1) \in \mathbb{L}$.

Dann gilt $ax_0 + by_0 = c$

und $ax_1 + by_1 = c \quad | -$

$$a(x_0 - x_1) + b(y_0 - y_1) = 0 \quad | -a(x_0 - x_1)$$

$$b(y_0 - y_1) = -a(x_0 - x_1) = a(x_1 - x_0)$$

$\overset{\text{ggT}(a,b)=1}{\Rightarrow}$ $a \mid y_0 - y_1 \Rightarrow \exists t \in \mathbb{Z}: ta = y_0 - y_1$, also $y_1 = y_0 - ta$

Mit diesem t gilt auch: $a(x_1 - x_0) = b \cdot ta \quad | : a \ (a \neq 0)$

$\Leftrightarrow x_1 - x_0 = bt \Leftrightarrow x_1 = x_0 + tb$

$\overset{1) \text{ und } 2)}{\Rightarrow}$ Beh.

Beispiel (vgl. Bsp. S. 121)

(*) $13x + 19y = 1000$ $\quad ggT(13,19) = 1 \mid 1000$
$\Rightarrow$ lösbar in $\mathbb{Z}$

Betrachte: $13x + 19y = 1$ mit Hilfe des erweiterten Euklid. Algorithmus erhält man $(3, -2)$ als Lösung, also $(3000, -2000)$ als Lsg von (*).

ABER: Für eine Aufgabenlösung zum Bsp. auf S. 121 ist nur eine Lösung aus $\mathbb{N}_0 \times \mathbb{N}_0$ sinnvoll.

Frage: Ex. solche Lösungen in $\mathcal{L}$?

$$\mathcal{L} := \{(x,y) \mid x = 3000 + t \cdot 19 \wedge y = -2000 - t \cdot 13, t \in \mathbb{Z}\}$$

Gesucht: $t \in \mathbb{Z}$, so dass gilt $x = 3000 + t \cdot 19 \geq 0$
und $y = -2000 - t \cdot 13 \geq 0$.

$$x = 3000 + 19 \cdot t \geq 0 \quad \mid -3000 \mid : 19$$
$$t \geq -\frac{3000}{19} \approx -157{,}9$$

$$y = -2000 - 13 \cdot t \geq 0 \quad \mid +2000 \mid : (-13)$$
$$t \leq -\frac{2000}{13} \approx -153{,}8$$

$\Rightarrow \quad -157{,}9 \leq t \leq -153{,}8 \quad \Rightarrow \quad t \in \{-157, -156, -155, -154\}$

$\Rightarrow$ Lösungen:
$(17, 41)$
$(36, 28)$
$(55, 15)$
$(74, 2)$
} sinnvolle Lösungen für die Aufgabe von S. 121.

7. Kleinstes gemeinsames Vielfaches (kgV) und Vielfachenmengen

Def. 3

Die Menge $V(a) = \{x \in \mathbb{N} \mid a \mid x\}$ nennen wir die Vielfachenmenge von $a \in \mathbb{N}$.

Beispiele:

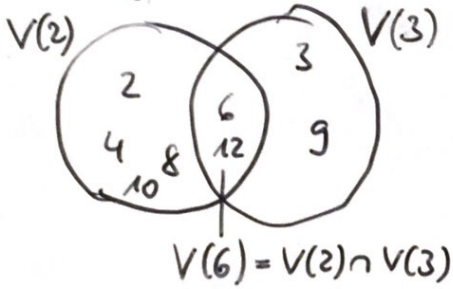
$V(1) = \{1, 2, 3, \dots\} = \mathbb{N}$

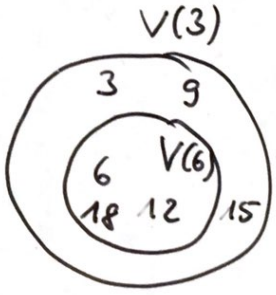
$V(2) = \{2, 4, 6, \dots\}$

$V(3) = \{3, 6, 9, 12, \dots\}$

$V(6) = \{6, 12, 18, \dots\} = V(2) \cap V(3)$

Venndiagramme:





$V(6) \subset V(3)$, also

$V(6) \cap V(3) = V(6)$

Frage:

Gibt es Vielfachenmengen $V(a)$ und $V(b)$, die sich nicht „überschneiden"?

Nein, denn $a \cdot b \in V(a) \cap V(b)$ für alle $a, b \in \mathbb{N}$.

Def. 4

Seien $V(a)$, $V(b)$ mit $a, b \in \mathbb{N}$ gegeben.
Die Elemente von $V(a) \cap V(b) = \{x \in \mathbb{N} \mid a|x \wedge b|x\}$ heißen gemeinsame Vielfache von a und b.
Das kleinste Element von $V(a) \cap V(b)$ heißt kleinstes gemeinsames Vielfaches von a und b ($kgV(a,b)$)

Satz 14

$$\forall a,b \in \mathbb{N}: V(a) \cap V(b) = V(kgV(a,b))$$

Bew. „$\supseteq$"

Sei $v \in V(kgV(a,b))$. [zz. $v \in V(a) \cap V(b)$]
Dann gilt $kgV(a,b) \mid v$. $a \mid kgV(a,b) \wedge b \mid kgV(a,b)$
$\Rightarrow a \mid v \wedge b \mid v \Rightarrow v \in V(a) \cap V(b)$.
(Transitivität von „|")

„$\subseteq$"

Seien $k = kgV(a,b)$ und $v \in V(a) \cap V(b)$. [z.z. $v \in V(kgV(a,b))$]
Dann gilt $v = q \cdot k + r$ mit $q, r \in \mathbb{N}_0$ und $0 \leq r < k$.
(nach Satz 3, Satz von der eindeut. Division mit Rest).
zz. $r = 0$ (woraus dann $k \mid v$ folgt). (Satz 3, kap. Teilb.)
Wegen $v \in V(a) \cap V(b)$ gilt: $a \mid v \wedge b \mid v$
wegen $k = kgV(a,b)$ gilt: $a \mid k \wedge b \mid k$
$\Rightarrow a \mid v - q \cdot k \Rightarrow a \mid r$
$\Rightarrow b \mid \underbrace{v - q \cdot k}_{=r} \Rightarrow b \mid r$
$\Rightarrow r \in V(a) \cap V(b)$ mit $0 \leq r < k$. Nach Vor. gilt $k = kgV(a,b)$,
also gilt $r = 0$ und damit $v = q \cdot k$ und somit $k \mid v \Rightarrow$ Beh. □

Charakterisierung des kgV(a,b)

Seien $a, b \in \mathbb{N}$. Dann ist das kgV(a,b) die Zahl $v \in \mathbb{N}$ mit: $a \mid v$ und $b \mid v$

und $(a \mid w$ und $b \mid w \Rightarrow v \mid w)$

Bemerkung:

Sei $a \in \mathbb{N}$.

Die Vielfachenmenge V(a) besitzt unendlich viele Elemente, während die Teilermenge T(a) immer nur endlich viele Elemente besitzt.

kgV und PFZ

Beispiel:

$$126 = 2 \cdot 3^2 \cdot 7$$

$$280 = 2^3 \cdot 5 \cdot 7$$

$$\text{kgV}(126, 280) = 2^3 \cdot 3^2 \cdot 5 \cdot 7$$

$$= 2520$$

Satz 15

Für alle $a = \prod_{i=1}^{\infty} p_i^{m_i}$, $b = \prod_{i=1}^{\infty} p_i^{n_i}$ $(p_i \in \mathbb{P}, n_i, m_i \in \mathbb{N}_0)$

gilt

$$ggV(a,b) = \prod_{i=1}^{\infty} p_i^{Max(m_i,n_i)}$$

($Max(m_i,n_i)$ bedeutet Maximum von m_i und n_i)

Bew.

Definiere: $v := \prod_{i=1}^{\infty} p_i^{Max(m_i,n_i)}$

z.z. $v = ggV(a,b)$.

Also 1. zz. $v \in V(a) \cap V(b)$

2. zz. v ist $ggV(a,b)$

zu 1: $v \in V(a)$, da $Max(m_i,n_i) \geq m_i$
$v \in V(b)$, " " $\geq n_i$ f.a. $i \in \mathbb{N}$.

$\Rightarrow v \in V(a) \cap V(b)$

zu 2: Sei $w \in V(a) \cap V(b)$ mit $w = \prod_{i=1}^{\infty} p_i^{\ell_i}$.

Also gilt: $a \mid w$ und $b \mid w$.

und nach Satz 3 (Kap. Primzahlen („Teilbarkeitskriterium"))

$m_i \leq \ell_i$ und $n_i \leq \ell_i$ f.a. $i \in \mathbb{N}$

und damit auch $Max(m_i,n_i) \leq \ell_i$ f.a. $i \in \mathbb{N}$

Es folgt: $v \mid w$

Nach der Charakterisierung von $ggV(a,b)$ folgt

$v = ggV(a,b)$.

□

Es folgt unmittelbar:

Satz 16:

1) $\forall_{a,b,n \in \mathbb{N}}$: $kgV(n \cdot a, n \cdot b) = n \cdot kgV(a,b)$

2) $\forall_{\substack{a,b \in \mathbb{N} \\ \text{m.T. } ggT(a,b)=1}}$: $kgV(a,b) = a \cdot b$.

Beispiel:

$$kgV(480, 560) \overset{(16.1)}{=} 80 \cdot kgV(6,7) = 80 \cdot 42 = 3360$$

Bemerkung:

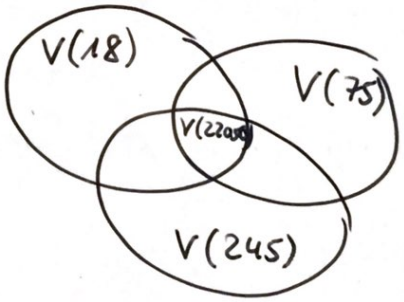
Mit der PFZ können gemeinsame Vielfache und auch das kgV von drei (oder auch mehr) natürlichen Zahlen bestimmt werden.

Beispiel:

$18 = 2 \cdot 3^2$

$75 = \quad 3 \cdot 5^2$

$245 = \quad 5 \cdot 7^2$



$kgV(18,75,245) = 2 \cdot 3^2 \cdot 5^2 \cdot 7^2 = 22050$

$= 18 \cdot 1225$

$= 75 \cdot 294$

$= 245 \cdot 90$

Zusammenhang von $ggT(a,b)$ und $kgV(a,b)$

Betrachte: 3 und 15

$3 \mid 15$, also $ggT(3,15) = 3$ und $kgV(3,15) = 15$.

Es gilt: $ggT(3,15) \cdot kgV(3,15) = 3 \cdot 15$

Allgemein:

Vor. $a, b \in \mathbb{N}$ mit $a \mid b$.

Dann gilt: $\underbrace{ggT(a,b)}_{\overset{\text{Satz 2}}{=} a} \cdot \underbrace{kgV(a,b)}_{\overset{\text{Satz 15}}{=} b} = a \cdot b$

Betrachte: 3 und 5

$ggT(3,5) = 1$, $kgV(3,5) = 3 \cdot 5$

$\Rightarrow ggT(3,5) \cdot kgV(3,5) = 3 \cdot 5$

Allgemein:

Vor. $a, b \in \mathbb{N}$ mit $ggT(a,b) = 1$.

Dann gilt: $\underbrace{ggT(a,b)}_{\overset{\text{n. Vor.}}{=} 1} \cdot \underbrace{kgV(a,b)}_{\overset{\text{Satz 16}}{=} a \cdot b} = a \cdot b$

Satz 17

$$\forall_{a,b\in\mathbb{N}} : ggT(a,b)\cdot kgV(a,b) = a\cdot b$$

Bew.

Seien $a = \prod_{i=1}^{\infty} p_i^{m_i}$, $b = \prod_{i=1}^{\infty} p_i^{n_i}$

$\overset{\text{Satz 2, Satz 15}}{\Rightarrow}$ $ggT(a,b) = \prod_{i=1}^{\infty} p_i^{Min(m_i,n_i)}$

$$kgV(a,b) = \prod_{i=1}^{\infty} p_i^{Max(m_i,n_i)}$$

$$\Rightarrow ggT(a,b)\cdot kgV(a,b) = \prod_{i=1}^{\infty} p_i^{Min(m_i,n_i)} \cdot \prod_{i=1}^{\infty} p_i^{Max(m_i,n_i)}$$

$$= \prod_{i=1}^{\infty} p_i^{Min(m_i,n_i)} \cdot p_i^{Max(m_i,n_i)} = \prod_{i=1}^{\infty} p_i^{m_i+n_i} = \prod_{i=1}^{\infty} p_i^{m_i}\cdot p_i^{n_i}$$

$$= \prod_{i=1}^{\infty} p_i^{m_i} \cdot \prod_{i=1}^{\infty} p_i^{n_i} = a\cdot b.$$

□

Bemerkung:

Es gilt f.a. $a,b\in\mathbb{N}$: $ggT(a,b)\cdot kgV(a,b) = ab \quad | : ggT(a,b)$

$$kgV(a,b) = \frac{a\cdot b}{ggT(a,b)} \qquad \left(\neq 0 \text{ f.a. } a,b\in\mathbb{N}\right)$$

Also lässt sich $kgV(a,b)$ mit Hilfe des Euklidischen Algorithmus bestimmen.

Betrachte: $a = 2$, $b = 3$, $c = 6$

$ggT(2,3,6) = 1$ $\qquad$ $kgV(2,3,6) = 6$

$ggT(2,3,6) \cdot kgV(2,3,6) = 1 \cdot 6 \neq 2 \cdot 3 \cdot 6$

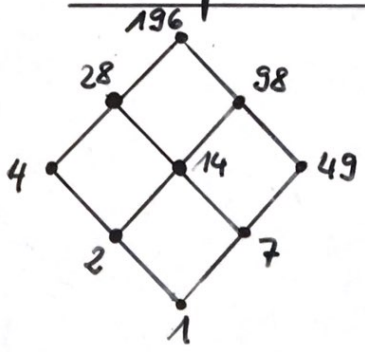
$\Rightarrow$ Satz 17 lässt sich also nicht für drei natürliche Zahlen verallgemeinern.
Es gilt also i. A. <u>nicht</u>

$$ggT(a,b,c) \cdot kgV(a,b,c) = a \cdot b \cdot c \quad , a,b,c \in \mathbb{N}.$$

Veranschaulichung durch Hassediagramme

Wdh. $ggT(a,b)$ — 1. Beispiel: $T(196)$ — $ggV(a,b)$

z.B. ist ablesbar:



$ggT(28,98) = 14$

$ggT(4,14,49) = 1$

$ggT(28,98,49) = 7$

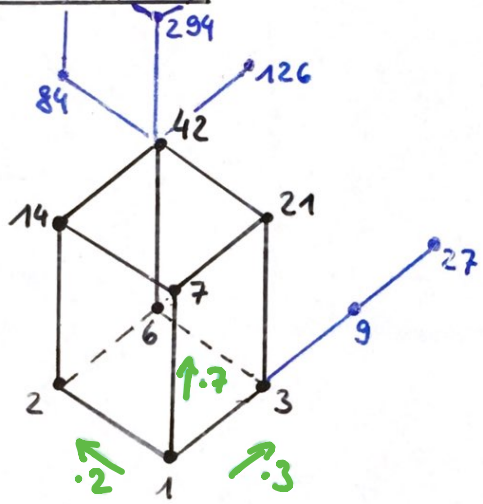
$T(28) \cap T(98) \cap T(49) = \{1,7\}$

$ggV(14,49) = 98$

$ggV(4,7,14) = 28$

$ggV(2,7,49) = 98$

2. Beispiel: $T(42)$



$ggT(42,27) = ggT(21,27) = 3$

$ggT(126,14,6) = 2$

$ggV(2,21) = 42$

$2 \cdot 42 = 84$

$3 \cdot 42 = 126$

$4 \cdot 42 = 168$

$5 \cdot 42 = 210$

$6 \cdot 42 = 252$

$7 \cdot 42 = 294$

Einige gemeinsame Vielfache von 2 und 21 sind im nebenstehenden Diagramm enthalten – aber nicht alle.