Lineare diophantische Gleichungen
Arbeitsmaterial für Klasse 8

Hans-Gert Gräbe, Leipzig

Dieser Text baut auf den Texten „Rechnen mit Kongruenzen“ (graebe-04-4) und „Rechnen mit Kongruenzen – Teil 2“ (graebe-04-7) auf.

Lineare diophantische Gleichungen

Als *lineare diophantische Gleichung* bezeichnet man folgende Problemstellung:

Zur linearen Gleichung

$$a \cdot x + b \cdot y = c \tag{1}$$

mit gegebenen Zahlen $a, b, c \in \mathbb{Z}$ sind alle ganzzahligen Lösungen $(x; y) \in \mathbb{Z}^2$ zu bestimmen.

Beispiel: Bestimme alle ganzzahligen Lösungspaare $(x; y)$ der Gleichung

$$3\,x - 7\,y = 5 \tag{1a}$$

Lineare diophantische Gleichungen und lineare Kongruenzen

Es besteht ein enger Zusammenhang zwischen linearen diophantischen Gleichungen und linearen Kongruenzen, die im Arbeitsblatt „Rechnen mit Kongruenzen – Teil 2“ besprochen sind. Offensichtlich liefert eine Lösung von (1a) auch eine Lösung der linearen Kongruenz

$$3\,x \equiv 5 \pmod 7. \tag{2a}$$

Ist umgekehrt x_0 eine Lösung der linearen Kongruenz (2a), so ist $3\,x_0 - 5$ durch 7 teilbar und die ganze Zahl $y_0 = \frac{3\,x_0 - 5}{7}$ die einzige Zahl, die x_0 zu einem Lösungspaar $(x_0; y_0)$ von (1a) ergänzt.
Die (eindeutige) Lösung $x_0 \equiv 4 \pmod 7$ von (2a) finden wir etwa durch vollständiges Probieren. Damit sind genau die ganzen Zahlen der Form $x_0 = 4 + 7\,t,\ t \in \mathbb{Z}$, Lösung von (2a) und nach dem eben beschriebenen Verfahren bekommen wir für jeden solchen Wert x_0 einen eindeutig bestimmten zugehörigen Wert y_0

$$y_0 = \frac{3\,x_0 - 5}{7} = \frac{3\,(4 + 7\,t) - 5}{7} = \frac{7 + 21\,t}{7} = 1 + 3\,t\,,$$

so dass $(x_0; y_0)$ eine Lösung von (1a) ist. Die Lösungsmenge von (1a) lässt sich also anschreiben als

$$L = \{(x; y)\,|\,x = 4 + 7\,t,\ y = 1 + 3\,t,\ t \in \mathbb{Z}\} = \{\ldots, (-3; -2), (4; 1), (11; 4), \ldots\}\,.$$

Die Probe zeigt, dass jedes der Paare auch wirklich Lösung ist:

$$3\,x - 7\,y = 3(4 + 7\,t) - 7(1 + 3\,t) = (12 + 21\,t) - (7 + 21\,t) = 5$$

This material belongs to the Public Domain KoSemNet data base. It can be freely used, distributed and modified, if properly attributed. Details are regulated by the *Creative Commons Attribution License*, see `http://creativecommons.org/licenses/by/2.0`.
For the KoSemNet project see `http://lsgm.uni-leipzig.de/KoSemNet`.

unabhängig von der Wahl von $t \in \mathbb{Z}$.

Allgemein lässt sich zur linearen diophantischen Gleichung (1) sowohl die lineare Kongruenz $a\,x \equiv c \pmod{b}$ als auch $b\,y \equiv c \pmod{a}$ betrachten.

Lösungsverfahren für lineare diophantische Gleichungen

Im Arbeitsblatt „Rechnen mit Kongruenzen – Teil 2“ hatten wir festgestellt, dass manche lineare Kongruenz überhaupt keine Lösung besitzt. Dies gilt auch für diophantische Gleichungen (1): Haben a und b einen gemeinsamen Teiler d, so muss für die Existenz einer Lösung auch $c \mid b$ gelten. $\gcd(a,b) \mid c$ ist also eine *notwendige* Bedingung für die Existenz einer Lösung. Ist diese notwendige Bedingung erfüllt und $d := \gcd(a,b)$, so gilt $a = d \cdot a',\ b = d \cdot b',\ c = d \cdot c'$. Wir können dann (1) durch die äquivalente Gleichung

$$a'x + b'y = c' \tag{1'}$$

ersetzen, in der a' und b' teilerfremd sind. Eine solche Gleichung bezeichnet man als *reduzierte diophantische Gleichung* oder *Gleichung in Normalform*. Es stellt sich heraus, dass jede solche Gleichung lösbar ist, wobei sich die Lösungsmenge sogar genau beschreiben lässt.

Ein gutes Verfahren zur Bestimmung der Lösungen einer reduzierten diophantischen Gleichung ist das *Eulersche Reduktionsverfahren*, das dauernd zwischen diophantischer Gleichung (d.G.), zugehöriger linearer Kongruenz (l.K.) und Reduktion auf kleinste positive Reste „pendelt“. Es soll hier nur am Beispiel der Gleichung $179\,x + 234\,y = 251$ beschrieben werden:

Ausgangsgleichung	$179\,x + 234\,y$	$=$	251
Verwandlung in l.K.	$234\,y$	$\equiv$	$251 \pmod{179}$
Kleinste positive Reste	$55\,y$	$\equiv$	$72 \pmod{179}$
Verwandlung in d.G.	$55\,y + 179\,u$	$=$	72
Verwandlung in l.K.	$179\,u$	$\equiv$	$72 \pmod{55}$
Kleinste positive Reste	$14\,u$	$\equiv$	$17 \pmod{55}$
Verwandlung in d.G.	$14\,u + 55\,v$	$=$	17
Verwandlung in l.K.	$55\,v$	$\equiv$	$17 \pmod{14}$
Kleinste positive Reste	$13\,v$	$\equiv$	$3 \pmod{14}$
Verwandlung in d.G.	$13\,v + 14\,w$	$=$	3
Verwandlung in l.K.	$14\,w$	$\equiv$	$3 \pmod{13}$
Kleinste positive Reste	w	$\equiv$	$3 \pmod{13}$

Die Lösung der letzten linearen Kongruenz können wir ablesen: $w = 3 + 13\,k,\ k \in \mathbb{Z}$. Daraus ergeben sich rückwärts nacheinander

$$\begin{aligned}
v &= \frac{3 - 14\,w}{13} &&= -14\,k - 3\\
u &= \frac{17 - 55\,v}{14} &&= 55\,k + 13\\
y &= \frac{72 - 179\,u}{55} &&= -179\,k - 41\\
x &= \frac{251 - 234\,y}{179} &&= 234\,k + 55
\end{aligned}$$

Die Lösungsmenge der diophantischen Gleichung (3) ergibt sich also zu

$$\begin{aligned}
L &= \{(x;y) \mid x = 234\,k + 55,\ y = -179\,k - 41,\ t \in \mathbb{Z}\}\\
&= \{\ldots, (-413;317), (-179;138), (55;-41), (289;-220), (523;-399), \ldots\}
\end{aligned}$$

Die speziellen Werte ergeben sich, wenn du $k \in \{-2,-1,0,1,2\}$ einsetzt.

Bemerkung: Die Ähnlichkeit zum Euklidschen Algorithmus, mit dem sich der größte gemeinsame Teiler bestimmen lässt, ist nicht zufällig, wird aber hier nicht weiter erörtert.

$$\begin{aligned} 234 &= 1 \cdot 179 + 55 \\ 179 &= 3 \cdot 55 + 14 \\ 55 &= 3 \cdot 14 + 13 \\ 14 &= 1 \cdot 13 + 1 \end{aligned}$$

Mehr zum Euklidschen Algorithmus findest du im Arbeitsblatt „Berechnung des größten gemeinsamen Teilers mit dem Euklidschen Algorithmus“ für Klasse 7 (graebe-04-2).

Das Lösbarkeitskriterium für lineare diophantische Gleichungen

Als letztes wollen wir noch einen Beweis für das Lösbarkeitskriterium anschauen.

Satz 1 (Hauptsatz über diophantische Gleichungen)

1. *Die diophantische Gleichung (1) hat genau dann Lösungen, wenn* $\gcd(a,b) \mid c$ *gilt.*
2. *Ist* $(x_0; y_0)$ *eine Lösung der reduzierten diophantischen Gleichung (1'), so ist*

$$L = \{(x;y) \mid x = x_0 - b'\,t,\ y = y_0 + a'\,t,\ t \in \mathbb{Z}\}$$

die Lösungsmenge von (1') und damit auch von (1).

Beweis: Nach unseren vorbereitenden Überlegungen sind nur noch die folgenden beiden Aussagen zu beweisen:

1. Jede **reduzierte** diophantische Gleichung hat Lösungen.
2. L ist genau die Lösungsmenge.

Wir beginnen mit der **zweiten Aussage**: Ist neben $(x_0; y_0)$ auch $(x_1; y_1)$ eine Lösung von (1'), so gilt

$$a'x_0 + b'y_0 = a'x_1 + b'y_1 = c,$$

also auch

$$a'(x_0 - x_1) = b'(y_1 - y_0). \tag{4}$$

Nun sind aber a' und b' teilerfremd, so dass $a' \mid (y_1 - y_0)$ gilt. Folglich existiert ein $t \in \mathbb{Z}$ mit $y_1 = y_0 + a'\,t$ und aus (4) ergibt sich dann sofort $x_1 = x_0 - b'\,t$. $(x_1; y_1)$ gehört also zu L.
Umgekehrt überzeugt man sich leicht, dass jedes Paar aus L eine Lösung ist.

Zum **Beweis der Existenz einer Lösung** führen wir einen **indirekten Beweis**. Wir nehmen dazu für einen Moment an, dass es reduzierte Gleichungen (1') gibt, die keine Lösungen haben und führen dies auf einen Widerspruch.
Vorüberlegung: Wir folgen der Idee des Eulerschen Reduktionsverfahrens, dass aus einer Gleichung immer „kleinere“ Gleichungen gewonnen werden können. Starten wir mit einer Gleichung ohne Lösung, so dürften diese „kleineren“ Gleichungen auch alle keine Lösung haben. Denn sonst könnte man ja aus einer solchen Lösung eine der Ausgangsgleichung „bauen“. Andererseits gibt es „ganz kleine“ Gleichungen wie etwa $2x + y = 3$ oder so, die offensichtlich Lösungen besitzen. Wenn wir nur lange genug „absteigen“, dann kommen wir irgendwann auf eine solche Gleichung und haben einen Widerspruch gefunden: Die Gleichung hat dann Lösungen, darf aber eigentlich keine haben.
Wie behandeln wir das beweistechnisch, dass es auch überzeugt? Die Idee ist, das *kleinste* Gegenbeispiel zu nehmen und von diesem aus abzusteigen zum „noch kleineren“ Gegenbeispiel, das es

nach Lage der Dinge aber nicht geben kann. Dieses Herangehen bezeichnet man auch als **unendlichen Abstieg**.

Ausführung: Nehmen wir an, dass es reduzierte Gleichungen (1') ohne Lösungen gibt. Sei $a'x+b'y = c'$ eine solche Gleichung, für die $|a'|+|b'|$ kleinstmöglich ist[1]. Sei weiter $|a'| \geq |b'|$ und $a' = q \cdot b' + r$ das Ergebnis der Division mit Rest (so dass $0 \leq r < |b'|$ ist). Sicher ist $b' \neq \pm 1$, denn für eine solche Gleichung (1') lässt sich leicht eine Lösung angeben. Wegen $\gcd(a', b') = \gcd(b', r)$ sind auch b' und r teilerfremd und insbesondere $r \neq 0$ (denn sonst wäre $\gcd(b', r) = |b'| > 1$).

Setzen wir das in (1') ein, so erhalten wir

$$a'x + b'y = (q \cdot b' + r)x + b'y = r\,x + b'(y + q\,x) = c$$

Die diophantische Gleichung $r\,x + b'z = c$ ist aber eine „kleinere" Gleichung, denn es gilt $|r|+|b'| < 2|b'| \leq |a'| + |b'|$. Da $|a'| + |b'|$ so ausgewählt war, dass jede „kleinere" Gleichung Lösungen hat, muss die diophantische Gleichung $r\,x + b'z = c$ Lösungen haben. Aus jeder solchen Lösung (x_0, z_0) kann aber leicht eine Lösung $(x_0, y_0 = z_0 - q\,x_0)$ der Gleichung (1') berechnet werden, was der Annahme widerspricht, dass diese Gleichung keine Lösungen hat.

Also ist was faul in unserer Argumentationskette – und da sie in sich logisch ist, muss der Anfang faul sein: Die Annahme, dass es reduzierte Gleichungen ohne Lösungen gibt, kann nicht zutreffen. Folglich hat jede reduzierte Gleichung wenigstens eine Lösung. □

Bemerkung: Damit können wir die Lösungsmenge einer reduzierten Gleichung sofort hinschreiben, wenn wir nur eine einzige Lösung (x_0, y_0) kennen. In vielen Fällen lässt sich die (mehr oder weniger einfach) erraten.

Attribution Section

graebe (2006-01-04):
Begleitmaterial für den LSGM-Korrespondenzzirkel in der Klasse 8

[1] Für ganz Pingelige: Da $|a'| + |b'|$ eine natürliche Zahl ist und jede nicht leere Menge natürlicher Zahlen eine kleinste enthält, gibt es kleinstmögliche solche $|a'| + |b'|$.