GYMNASIUM KLEINE BURG

FACHARBEIT

im Leistungskurs: **Mathematik**

Thema: **Lineare diophantische Gleichungen**

Verfasser: Jan Stellet

Themenausgabe: 08.02.2006 Abgabetermin: 22.03.2006

Inhaltsverzeichnis

1 Einleitung

Seit mehr als 2.500 Jahren befassen sich Mathematiker mit dem Problem des Findens von Lösungen zu einer Gleichung, welche nur aus einer bestimmten Zahlenmenge stammen. Diese Facharbeit soll einen Teil hiervon, die linearen diophantischen Gleichungen, behandeln und zugehörige Aspekte beleuchten. Dies soll mit dem Ziel geschehen, Auflösungsstrategien nicht nur vorzustellen, sondern ihre Herkunft zu ergründen. Aus diesem Grund liegt der Fokus des ersten der beiden Hauptkapitel auf theoretischen Grundlagen der Teilbarkeitslehre, im zweiten auf ihrer Anwendung. Zunächst soll jedoch kurz auf die für das Thema prägenden Namen Diophant und Euklid eingegangen werden. Persönlicher Reiz der Themenstellung ist das niedrige Einstiegsniveau durch die einfache Struktur der Gleichungen verbunden mit der beliebig steigerbaren Komplexität der Vertiefungen. Die Grenze soll hierbei nach dem Auffinden einzelner Lösungen zu Gleichungen mit beliebig vielen Unbekannten gezogen werden, die Beschreibung der Gesamtheit aller Lösungen in den ganzen oder natürlichen Zahlen entfällt.

2 Historische Gesichtspunkte

Diophantos von Alexandria ist einer der bedeutendsten Mathematiker der Antike. Zwar ist nur wenig über das Leben des griechischen Mathematikers bekannt und die Schätzung seiner Lebensdaten von ca. 200-280 v. Chr. basiert auf der Erwähnung älterer Mathematiker in seinen Arbeiten und nachfolgenden Zitaten dieser, doch prägen seine Erkenntnisse die Geschichte der Mathematik in hohem Maße. Diophant lebte im ägyptischen Alexandria, jahrhundertelang das wissenschaftliche Zentrum der Antike.[1]

Die „Arithmetik“ (griech.: Ἀριδητικά) ist sein Hauptwerk und markiert eine bedeutende Entwicklung der Algebra, jenem Teilgebiet der Mathematik, unter welchem man die formale Auflösung algebraischer Gleichungen versteht. Diophant schlug dort ein neues Kapitel in der griechischen Mathematik auf, indem er sich darauf konzentrierte bestimmte und unbestimmte Gleichungen mit bis zu sechs Unbekannten ohne Rückgriff auf geometrische

1 Informationen entnommen aus: Bundschuh, Peter: Einführung in die Zahlentheorie S. 28.

Überlegungen zu lösen. Statt geometrischer Algebra wird dies auch als echte Algebra bezeichnet. Die von ihm benutzte algebraische Bezeichnungsweise wird als synkopiert (verkürzt) bezeichnet und gilt als Zwischenschritt von einer rein verbalen zu einer vollständig symbolischen Algebra. Die „Arithmetik“ ist der einzige bekannte umfassende Text zur Algebra und Arithmetik aus der griechischen Antike und stellt gleichzeitig das erste große, ausschließlich zahlentheoretischen Problemen gewidmete Werk dar. Von den dreizehn Büchern der in griechischer Sprache verfassten „Arithmetik“ waren bis vor einigen Jahrzehnten nur sechs[2] bekannt, in den 70er Jahren fand man vier[3] weitere, in arabische Sprache übersetzte Bände.[4]

Euklid von Alexandria (ca. 365-300 v. Chr.) war ebenfalls ein bedeutender griechischer Mathematiker, welcher auch heute die Sprache der modernen Mathematik prägt (Bsp.: euklidische Ringe, euklidische Räume u. v. m.). In seinem berühmten Hauptwerk „Elemente“ (griech.: Ετσχετα) fasste er mathematisches Wissen seiner Zeit zusammen, damit es als Lehrwerk an der Akademie des Platon verwendet werden konnte. Auch dienten die „Elemente“ Euklid als Fundament für tiefer gehende mathematische Untersuchungen. Mindestens drei vorherige Verfasser ähnlicher Werke sind bekannt, diese sind jedoch nicht erhalten. Euklid wird nachgesagt sie als Grundlage genommen und erweitert sowie verbessert zu haben. Insgesamt setzen sich die „Elemente“ aus dreizehn Büchern zusammen. In den ersten sechs Bänden werden Erkenntnisse aus dem Bereich der Geometrie, in den Büchern sieben bis neun der Zahlentheorie und in Kapitel elf bis dreizehn der Stereometrie behandelt.[5]

Euklid führte Eigenschaften von ganzen Zahlen und geometrischen Objekten auf eine Menge von Elementaraussagen (Axiome) zurück, was der Axiomatisierung in der modernen Mathematik ähnelt.

---

2 Übersetzung und Kommentierung: Czwalina, A.:Arithmetik des Diophant aus Alexandria. Göttingen: Vandenhoeck-Ruprecht 1952.

3 Sesiano, J.: Books IV to VII of Diophantus' Arithmetica: In the Arabic Translation Attributed to Qusta Ibn Luqa. New York: Springer 1982.

4 Informationen entnommen aus: Mankiewicz, Richard: Zeitreise der Mathematik S. 46.

5 Informationen entnommen aus: Schreiber, Peter: Euklid S. 5; 32-37.

3 Der euklidische Algorithmus

Der euklidische Algorithmus ist ein Verfahren zur Bestimmung des größten gemeinsamen Teilers (ggT) zweier Zahlen. Er wird von Euklid von Alexandria im Buch VII seines Hauptwerks „Elemente“ vollkommen allgemein beschrieben. Der französische Mathematiker Bachet de Mézinac (1581-1638) führte das Verfahren erstmals in Europa ein.[6] Auf seine bedeutende Folgerung hinsichtlich des euklidischen Algorithmus, das Lemma von Bachet, wird in Kapitel 3.3 eingegangen. Da der euklidische Algorithmus eine wiederholte Division mit Rest darstellt, soll zunächst diese erläutert werden.

3.1 Division mit Rest

Geht die Division zweier ganzer Zahlen a, b mit $b>0$ nicht mit Rest 0 auf (man schreibt auch $a \nmid b$ im Gegensatz zu $a|b$ für aufgehende Division), lautet sie in der Schreibweise[7] des Divisionsalgorithmus wie folgt:

$a=qb+r;\ \ q,r\in\mathbb{Z},\ \ 0<r<b$. **Beispiel:** $15:4$ entspricht $15=3\cdot 4+3$.

Hierbei ist q ein ganzer Quotient von a und r der auftretende Rest.[8] Es sollen nun Existenz und Eindeutigkeit dieser Darstellung bewiesen werden.

Beweis der Existenz:[9]

Der Rest von $a:b$ ist die kleinstmögliche natürliche Zahl $r=a-qb\geq 0;\ \ q\in\mathbb{Z}$. Für $a\geq 0$ und $q=0$ ist die Forderung $a-qb\geq 0$ erfüllt.

Ist hingegen $a<0$, so kann man ein $m>0$ mit $m\cdot b\geq|a|$ bestimmen, damit für $q=-m$ gilt: $(-q)\cdot b\geq|a|=-a$, woraus $a-qb\geq 0$ folgt.

Die Menge aller Reste $R=\{z|z=a-qb\geq 0;\ \ q\in\mathbb{Z}\}$ ist damit nicht leer und es existiert ein kleinstes Element r aus dieser Menge. Um zu zeigen, dass $r<b$ gilt, formt man $r-b$ durch Einsetzen von $r=a-qb$ um zu $a-qb-b$ und damit $a-b(q+1)$. Da $b>0$ ist, muss $a-b(q+1)<a-qb$ sein, denn für $b>0$ ist $b(q+1)>qb$.

---

6 Informationen entnommen aus: Bundschuh, Peter: Einführung in die Zahlentheorie S. 23.
7 Dies entspricht in der aus der Schule bekannten Notation: „a geteilt durch b = q Rest r“.
8 Vgl. für diesen Abschnitt: Rose, H. E.: A Course in Number Theory S. 2.
9 Vgl.: Schreiber, A.: Einführung in die Mathematik, Kapitel 4 „Teilbarkeit“ S. 1-4.

Weil r jedoch das durch ein bestimmtes ganzzahliges q mittels $r=a-qb$ definierte kleinstes positives Element aus der Menge ist, kann nicht gelten, dass $a-b(q+1)\geq 0$. Denn andernfalls würde ein kleineres Element aus R als r existieren. Somit resultiert, dass $r-b<0$ ist und damit $r<b$.

Beweis der Eindeutigkeit:[10]

Um die Eindeutigkeit zu beweisen, wählt man je zwei verschiedene q und r: $a=q_1 b+r_1$ und $a=q_2 b+r_2$ mit $0\leq r_{1,2}<b$.

Es soll gezeigt werden, dass $q_1=q_2$ und $r_1=r_2$ gilt, wobei man annimmt, dass $r_1\geq r_2$ ist. Denn dann gäbe es für dasselbe Zahlenpaar a, b nur eine Möglichkeit der Darstellung und die Eindeutigkeit wäre bewiesen.

Man subtrahiert beide Gleichungen voneinander und erhält:

$a-a=q_1 b-q_2 b+r_1-r_2$

$0=b(q_1-q_2)+r_1-r_2$

$b(q_2-q_1)=r_1-r_2$.

Es folgt damit, dass die Differenz r_1-r_2 ein Vielfaches von b ist. Aufgrund der Voraussetzung $0\leq r_1-r_2<b$ schließt man weiterhin, dass $r_1-r_2=0$ sein muss und erhält wegen $b>0$ zudem, dass $q_2-q_1=0$ ist. Im Folgenden wird die Verwendung der auch als Divisionsalgorithmus bezeichneten Darstellung anhand des euklidischen Algorithmus demonstriert.

3.2 Der euklidische Algorithmus

Der euklidische Algorithmus ist ein Verfahren der Wechselwegnahme und gehört zu den ältesten und wichtigsten Algorithmen der Mathematik. Er dient der Bestimmung des gemeinsamen Maß zweier Größen, d. h. einer Größe d,[11] welche in beiden Größen aufgeht.

Prinzipiell handelt es sich um eine sukzessiv wiederholte Division mit Rest, bei der als Divisor der jeweils aktuelle Rest und als Dividend der vorherige Rest gewählt werden.[12]

Die k-te Zeile entspricht dann der Form $r_k=q_{k+1} r_{k+1}+r_{k+2};\ \ k=0,1,2,\ldots n$.

10 Vgl.: Schreiber, A.: Einführung in die Mathematik, Kapitel 4 „Teilbarkeit“ S. 1-4.
11 Eine weitere gängige Schreibweise für d=ggT(a,b) ist: (a,b).
12 Schreiber, A.: Einführung in die Mathematik, Kapitel 4 „Teilbarkeit“ S. 5.

Das Erreichen des Restes $r_{n+1}=0$ in der $(n-1)$-ten Gleichung ist die Abbruchbedingung des Algorithmus, der vorhergegangene Rest r_n der gesuchte größte gemeinsame Teiler.

Die Bestimmung des ggT mithilfe des euklidischen Algorithmus soll nun im allgemeinen Fall für zwei natürliche Zahlen a, b $(a>b)$ [13] und für das Beispiel 123, 90 gezeigt werden.

$r_0=a=q_1 b+r_2$	$123=1\cdot 90+33$
$r_1=b=q_2 r_2+r_3$	$90=2\cdot 33+24$
$r_2=q_3 r_3+r_4$	$33=1\cdot 24+9$
$\vdots$	$24=2\cdot 9+6$
$r_{n-2}=q_{n-1} r_{n-1}+r_n$	$9=1\cdot 6+3$
$r_{n-1}=q_n r_n$	$6=2\cdot 3$

Hierbei entspricht der letzte nicht verschwindende Rest r_n bzw. 3 dem größten gemeinsamen Teiler beider Zahlen.

Beweis:[14]

Der Beweis gliedert sich in drei Abschnitte, in denen die Aspekte der Monotonie von der Folge der Reste, die gemeinsamen Teiler zweier aufeinander folgender Paare von Resten wie z. B. r_2, r_3 und r_3, r_4 sowie die Frage, ob der letzte nicht verschwindende Rest r_n der $ggT(a,b)$ ist, getrennt behandelt werden.

a) **Monotonie der Folge von Resten:** Die auftretenden Folge der Reste $r_0, r_1, r_2, ..., r_n$ ist streng monoton fallend, da der Divisor r_{k+1} in der k-ten Zeile des Verfahrens kleiner ist als der Dividend r_k. Für $k=0$ ist das die vorausgesetzte Ungleichung $b<a$. Ist $k>0$, ergibt sich dies direkt aus der Division mit Rest: $a=qb+r;\ b>r\geq 0$. Das heißt, dass der entstehende Rest immer kleiner ist als der Divisor. Damit besitzt die streng monoton fallende Folge natürlicher Zahlen nur endlich viele von 0 verschiedene Glieder:
$r_0>r_1>r_2>...>r_n>r_{n+1}=0$.

13 Da ggT(a,b)=ggT(|a|,|b|) und ggT(a,a)=a ist, genügt die Betrachtung von a>b>0.
14 Vgl.: Schreiber, A.: Einführung in die Mathematik, Kapitel 4 „Teilbarkeit“ S. 5-6.

b) **Gemeinsame Teiler von Restepaaren:** Bei Betrachtung der k-ten Zeile $r_k = q_{k+1} r_{k+1} + r_{k+2}$ stellt man fest, dass offensichtlich für eine beliebige Zahl $t \in \mathbb{Z}$ $t | r_k \wedge t | r_{k+1}$ nur dann gilt, wenn $t | r_{k+1} \wedge t | r_{k+2}$. Dies bedeutet, dass ein gemeinsamer Teiler t von r_k, r_{k+1} nur dann existiert, wenn er auch gemeinsamer Teiler von r_{k+1}, r_k ist. Ausgehend von $k = 0$ bis $k = n+1$ kann somit gefolgert werden, dass a, b und r_n, r_{n+1} dieselben gemeinsamen Teiler besitzen. Da nach a) jedoch $r_{n+1} = 0$ ist, sind alle Teiler von r_n die gemeinsamen Teiler von a, b.

c) **Größter gemeinsamer Teiler:** Sei t irgendein gemeinsamer Teiler von a, b, so ist t auch Teiler von r_n. Daraus folgt, dass $r_n \geq t$ ist und somit r_n der größte aller gemeinsamen Teiler von a, b ist.

Die Bestimmung des ggT mithilfe des euklidischen Algorithmus ist insbesondere bei großen Zahlen ein deutlich schnelleres Verfahren als die Methode der Primfaktorzerlegung. Die Anzahl l der dabei durchzuführenden Divisionsgleichungen ist gegeben durch: $l \leq \log_\lambda a, \quad \lambda = \frac{1+\sqrt{5}}{2} \approx 1{,}61$.[15]

3.3 Das Lemma von Bachet

Der französische Mathematiker Bachet de Mézinac folgerte 1624 in der 2. Ausgabe seines Werkes „Problèmes plaisants et délectables“ über den ggT:

> *Der größte gemeinsame Teiler d zweier natürlicher Zahlen a und b ist als Vielfachensumme (Linearkombination) von a und b darstellbar, d. h. es gibt ganze Zahlen x, y für die gilt: $d = ax + by$.*[16]

Beweis:[17] Um Bachets Satz zu beweisen, betrachtet man zunächst alle für beliebige $x, y \in \mathbb{Z}$ möglichen Linearkombinationen. Diese Menge $\{ax + by\}$ enthält sowohl positive als auch negative ganzzahlige Werte. Nun sei das kleinste positive Element k der Menge bestimmt durch: $k = ax_0 + by_0$. Zu zeigen ist nun, dass k sowohl a als auch b teilt. Für ersteres wird dies durch einen indirekten Beweis (d. h.: man nimmt an, dass $k \nmid a$ gilt und ein Widerspruch ergibt sich) erledigt, der zweite Fall kann analog dazu erfolgen.

15 Vgl.: Wiesenbauer, Johann: AKDIS Zahlentheorie und Anwendung S. 4 Satz 1.8.
16 Aus: Schreiber, A.: Einführung in die Mathematik, Kapitel 4 „Teilbarkeit“ S. 6.
17 Vgl.: Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 6 Satz 1.3.

Nach der Annahme geht k in a nicht auf, weshalb man die Darstellung der Division mit Rest anwenden kann: $a=qk+r\,;\;\; q,r\in\mathbb{Z},\;\; 0<r<k$.

$r=a-qk$. Setzt man ax_0+by_0 für k ein, so erhält man:

$r=a-q(ax_0+by_0)$

$r=a-qax_0-qby_0$

$r=a\underbrace{(1-qx_0)}_{x_1}+b\underbrace{(-qy_0)}_{y_1}$.

Nun ist erkennbar, dass der Rest r Element der Menge $\{ax+by\}$ ist, gebildet mit den gekennzeichneten x_1, y_1. Da der Rest r jedoch kleiner als der Divisor k ist, ergibt sich ein Widerspruch, denn k ist per Voraussetzung das kleinste Element der Menge. Des Weiteren können, sofern d der größte gemeinsame Teiler von a und b ist, diese mit $A, B\in\mathbb{Z}$ in der Form $a=Ad$ und $b=Bd$ geschrieben werden, womit für k folgt: $k=ax_0+by_0=Adx_0+Bdy_0=d(Ax_0+By_0)$.

Man erkennt sofort, dass $d|k$ gelten muss, da der Inhalt der Klammer in jedem Fall einen ganzzahligen Wert annimmt. Aus der Division zweier natürlicher Zahlen geht weiterhin hervor, dass der Divisor immer kleiner oder gleich dem Dividenden ist. Überträgt man dies auf $k:d$, so folgt: $k\geq d$. Weil d aber der *größte* gemeinsame Teiler ist, ist der Fall $k>d$ unmöglich und es gilt: $k=d=ax_0+by_0$.

3.4 Die Darstellung des ggT als Linearkombination

Der ggT als letzter positiver Rest im euklidischen Algorithmus soll nun entsprechend dem Lemma von Bachet als Linearkombination geschrieben werden. Hierzu eliminiert man die Reste $r_2, r_3, .., r_{n-2}, r_{n-1}$ aus der Gleichungskette des Algorithmus. Für $r_0=a$ und $r_1=b$ ist sofort ersichtlich:

$r_0=1\cdot a+0\cdot b$

$r_1=0\cdot a+1\cdot b$

Die weiteren Reste können nun folgendermaßen geschrieben werden:

$r_2=a+b(-q_1)$, denn $a=r_0=q_1b+r_2$;

$r_3=a(-q_2)+b(1+q_1q_2)$, da $r_3=r_1-q_2r_2$ sowie $r_2=a-q_1b$ und $r_1=b$.

Dieses Vorgehen kann sukzessive für die folgenden $r_4, r_5, ..., r_{n-1}, r_n$ fort-

gesetzt werden, so dass man letztendlich erhält:

$r_n = d = a(...) + b(...)$

Der Inhalt der Klammern stellt hierbei eine Lösung der Gleichung $d = ax + by$ dar und erlaubt somit eine Darstellung von $d = ggT(a, b)$ als Linearkombination von a und b.[18]

Im Folgenden soll eine weitere Möglichkeit, der erweiterte euklidische Algorithmus (auch Berlekamp-Algorithmus genannt), gezeigt werden, um die Linearkombination effektiv zu bestimmen. Aus dem Verlauf des euklidischen Algorithmus stammen hierbei die auftretenden q_i, sowie der Index n des letzten positiven Rests r_n. Gesucht werden nun die $\alpha_{n-1}, \beta_{n-1}$, welche als Koeffizienten von a und b die Linearkombination bilden. Diese α_i, β_i werden dabei durch zwei rekursiv definierte Folgen gebildet: $\alpha_0 = 0,\ \alpha_{i+1} = \beta_i,\ \beta_0 = 1,\ \beta_{i+1} = \alpha_i - q_{n-1-i}\beta_i;\ i = 0,1,2,...,n-2,n-1$. Eingesetzt wird nach der Formel $\alpha_i \cdot r_{n-1-i} + \beta_i \cdot r_{n-i} = r_n$, was im Folgenden für die ersten Werte für i getan wird.

$i = 0$: $\alpha_0 \cdot r_{n-1} + \beta_0 \cdot r_n = r_n$

$0 \cdot r_{n-1} + 1 \cdot r_n = r_n$

$i = 1$: $\alpha_1 \cdot r_{n-2} + \beta_1 \cdot r_{n-1} = r_n$

$\beta_0 \cdot r_{n-2} + (\alpha_0 - q_{n-1}\beta_0) \cdot r_{n-1} = r_n$

$1 \cdot r_{n-2} - q_{n-1} \cdot r_{n-1} = r_n$

$i = 2$: $\alpha_2 \cdot r_{n-3} + \beta_2 \cdot r_{n-2} = r_n$

$\beta_1 \cdot r_{n-3} + (\alpha_1 - q_{n-2}\beta_1) \cdot r_{n-2} = r_n$

$(\alpha_0 - q_{n-1}\beta_0) \cdot r_{n-3} + (\beta_0 - q_{n-2}\beta_1) \cdot r_{n-2} = r_n$

$-q_{n-1} \cdot r_{n-3} + (1 - q_{n-2}\beta_1) \cdot r_{n-2} = r_n$

Die Richtigkeit der ersten beiden Fälle ist sofort offensichtlich. Man kann so bis $i = n-1$ weiter fortfahren und erhält dann die Linearkombination mit $\alpha_{n-1} \cdot r_0 + \beta_{n-1} \cdot r_1 = \alpha_{n-1} \cdot a + \beta_{n-1} \cdot b = r_n = d$.[19]

18 Vgl.: Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 11-12 Satz 1.11.

19 Vgl. für diesen Abschnitt: Bundschuh, Peter: Einführung in die Zahlentheorie S. 31-32;
6. Wiesenbauer, Johann: AKDIS Zahlentheorie und Anwendung S. 3-4

Diese Methode findet vor allem in Computer-Programmen[20] z. B. für die Kryptographie[21] Anwendung, wo sie zur Verschlüsselung von Daten dient. Ein weiterer Aspekt, welcher beim Umformen der Gleichungskette des euklidischen Algorithmus auftritt und ebenfalls die Bildung der Linearkombination ermöglicht, sind endliche Kettenbrüche. Sie entstehen, wenn man die erste Gleichung im euklidischen Algorithmus nach $\frac{a}{b}$ umformt und die Brüche der Form $\frac{r_{k-1}}{r_k}$, welche im Nenner des Ausdrucks $\frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}}$ vorliegen, jeweils durch die entsprechend umgeformte folgende Gleichung im euklidischen Algorithmus ersetzt. Aufgrund der Komplexität dieses Themas sei hier anstatt einer genaueren Betrachtung nur der Verweis auf [22] gegeben.

20 Siehe für eine Umsetzung in der Programmiersprache C: http://www.lexiwise.de/info_skripte/quellcodes/erweiterter_euklid.c.

21 Siehe auch zur Verwendung in der Kryptographie: http://www.wiwi.uni-bielefeld.de/StatCompSci/lehre/material_spezifisch/statalg00/rsa/rsa.html.

22 Gelfond, A. O.: Die Auflösung von Gleichungen in ganzen Zahlen S. 11-17.

4 Lineare diophantische Gleichungen

Unter diophantischen Gleichungen versteht man algebraische Gleichungen, von denen ausschließlich Lösungen in einer bestimmten Zahlenmenge wie z. B. den ganzen Zahlen $\mathbb{Z}$ gesucht werden.[23] Viele bedeutende Mathematiker wie Euklid, Pythagoras, oder Pierre de Fermat befassten sich mit diesem Thema der Zahlentheorie . Benannt werden sie zu Ehren des griechischen Mathematikers Diophant von Alexandria, welcher sich um 250 v. Chr. in seinem Werk „Arithmetika“ mit ihnen befasste. Vollständig geklärt ist das Problem nur für Gleichungen bis zum zweiten Grad und somit fehlen allgemeine Methoden.[24] Abgesehen von theoretischen Interessen kommen solche Gleichungen bisweilen auch in physikalischen und chemischen Zusammenhängen vor.[25] Hier sollen nun lineare diophantische Gleichungen mit ganzzahligen Koeffizienten ungleich Null behandelt werden. Da eine solche Gleichung in jedem Fall unendlich viele Lösungen in den rationalen Zahlen $\mathbb{Q}$ hat, werden nur Lösungen in den Mengen der ganzen Zahlen $\mathbb{Z}$ und der natürlichen Zahlen $\mathbb{N}$ betrachtet. Die allgemeine Form einer solchen Gleichung lautet: $a_1 x_1 + a_2 x_2 + ... + a_{k-1} x_{k-1} + a_k x_k = c\,; \quad a_i, c \in \mathbb{Z}$.

4.1 Gleichungen mit einer Unbekannten

Jede lineare Gleichung mit nur einer Variablen und ganzzahligem Koeffizienten lässt sich durch Äquivalenzumformung in die Form $a_1 x_1 = c\,; \; c \in \mathbb{Z}$ bringen. Stellt man dies nach x_1 um, so erhält man $x_1 = \frac{c}{a_1}$. Es ist sofort ersichtlich, dass nur dann eine ganzzahlige Lösung für x_1 existieren kann, wenn a_1 in c restlos aufgeht. Ist das der Fall, so hat man die einzige Lösung der Gleichung bereits durch den entsprechenden Quotienten gefunden. Auch die Bedingung für die Existenz einer Lösung in den natürlichen Zahlen ist offensichtlich: Sowohl c als auch a_1 müssen entweder positive oder negative ganze Zahlen sein, nur dann ist ihr Quotient größer als Null.[26]

---

23 Informationen entnommen aus: Rose, H. E.: A Course in Number Theory S. 4.

24 Hilberts zehntes Problem - Wie kann man entscheiden, ob eine beliebige diophantische Gleichung lösbar ist? 1970 zeigte Juri W. Matijassewitsch, dass dies nicht möglich ist.

25 Informationen aus: Gelfond, A. O.: Die Auflösung von Gleichungen in ganzen Zahlen S. 5-6.

26 Vgl. für diesen Abschnitt: Gelfond, A. O.: Die Auflösung von Gleichungen in ganzen Zahlen S. 7.

4.2 Gleichungen mit zwei Unbekannten

Hierbei handelt es sich um den wichtigsten Fall, denn das Lösen aller weiteren Gleichungen mit mehr als zwei Variablen basiert auf der Zurückführung auf eine Gleichung mit zwei Unbestimmten.

4.2.1 Kriterium für die Existenz ganzzahliger Lösungen

Gegeben sei die lineare diophantische Gleichung

$a_1 x_1 + a_2 x_2 = c;\ \ a_1, a_2, c \in \mathbb{Z}$ (1),

für welche ermittelt werden soll, ob ganzzahlige Lösungen existieren. Der größte gemeinsame Teiler $d = ggT(a_1, a_2)$ teilt naturgemäß beide Koeffizienten a_1, a_2. Dividiert man die gesamte Gleichung durch d, so können ganzzahlige Werte für x_1, x_2 nur dann existieren, wenn $c|d$ gilt. Die Anzahl aller möglichen Lösungen in $\mathbb{Z}$ ist dann unendlich groß. Angemerkt sei, dass $c:d$ bei $c=0$ immer Null ergibt und entsprechend jede Gleichung der Form $a_1 x_1 + a_2 x_2 = 0$ in ganzen Zahlen lösbar ist.[27]

4.2.2 Auffinden einzelner Lösungen

Für das Finden von Zahlenpaaren $x_0, y_0 \in \mathbb{Z}$, welche die Gleichung (1) auflösen, bieten sich verschiedene Möglichkeiten an. Der triviale Fall liegt für $c=0$ vor: Man erkennt sofort, dass $x_0 = 0,\ y_0 = 0$ eine Lösung ist. Ist jedoch $c \neq 0$, eröffnen sich verschiedene Möglichkeiten:

Zum einen das systematische Einsetzen verschiedener ganzzahliger Zahlenpaare, um so durch Ausprobieren bzw. „Ablesen“ eine Lösung zu finden.

Beispiel: Bei der Gleichung $11x_1 - 2x_2 = 1$ ist $x_0 = 1, y_0 = 5$ offensichtlich.

Eine andere und insbesondere bei großen Zahlenwerten deutlich effektivere Methode, die in jedem Fall eine ganzzahlige Lösung der Gleichung liefert, soll nun gezeigt werden. Nach dem Lemma von Bachet gibt es zur Darstellung des $ggT(a_1, a_2)$ die Linearkombination $a_1 x + a_2 y = d;\ \ x, y \in \mathbb{Z}$.

Die Ähnlichkeit zur Gleichung (1) springt sofort ins Auge und nach Multiplikation mit $\frac{c}{d}$ erhält man: $a_1 \frac{c}{d} x + a_2 \frac{c}{d} y = c$. So ist $x_0 = \frac{c}{d} x,\ y_0 = \frac{c}{d} y$ eine Lösung der Gleichung (1).[28]

27 Vgl. für diesen Abschnitt: Bundschuh, Peter: Einführung in die Zahlentheorie S. 30.
28 Vgl. für diesen Abschnitt: Bundschuh, Peter: Einführung in die Zahlentheorie S. 30.

Es handelt sich aber nur um eine partikuläre (einzelne) Lösung. Die Gesamtheit der unendlich vielen möglichen Lösungen beschreibt man mit einem Parameter.

4.2.3 Bestimmung aller Lösungen

Voraussetzung für die Darstellung aller Lösungen ist zunächst die Kenntnis einer einzelnen Lösung. Im weiteren Verlauf sei r, s eine beliebige und x_0, y_0 eine bekannte Lösung zu (1). Es resultiert somit die Gleichung:

$a_1 r + a_2 s = c = a_1 x_0 + a_2 y_0 \quad | -a_1 x_0 \; -a_2 s$

$a_1 r - a_1 x_0 = -a_2 s + a_2 y_0$

$a_1 (r - x_0) = -a_2 (s - y_0) \quad | \; : d = ggT(a, b)$

$\frac{a_1}{d}(r - x_0) = -\frac{a_2}{d}(s - y_0)$ (2).

Da $\frac{a_1}{d}$ sowie $\frac{a_2}{d}$ teilerfremd[29] sind und $s - y_0$ einen ganzzahligen Wert annimmt (denn per Voraussetzung sind $s, y_0 \in \mathbb{Z}$), ist $r - x_0$ ein Vielfaches von $\frac{a_2}{d}$ und $s - y_0$ ein solches von $\frac{a_1}{d}$. Das führt zu der Darstellung $r - x_0 = \frac{a_2}{d} t; \; t \in \mathbb{Z}$ sowie $s - y_0 = \frac{a_1}{d} u; \; u \in \mathbb{Z}$. Setzt man dies in (2) ein, ergibt sich $u = -t$ und man erhält damit $r = x_0 + \frac{a_2}{d} t$ sowie $s = y_0 - \frac{a_1}{d} t$.[30]
Nun bleibt noch zu zeigen, dass jedes so mit einem beliebigen $t_0 \in \mathbb{Z}$ erhaltene Zahlenpaar r_0, s_0 auch eine Lösung der diophantischen Gleichung ist.

Beweis:[31]

Man setzt diese Lösung $r_0 = x_0 + \frac{a_2}{d} t_0, \; s_0 = y_0 - \frac{a_1}{d} t_0$ in (1) ein:

$a_1 r_0 + a_2 s_0 = c$

$a_1 (x_0 + \frac{a_2}{d} t_0) + a_2 (y_0 - \frac{a_1}{d} t_0) = c$

$a_1 x_0 + \frac{a_1 a_2}{d} t_0 + a_2 y_0 - \frac{a_1 a_2}{d} t_0 = c$

$a_1 x_0 + a_2 y_0 = c$.

Da x_0, y_0 eine bekannte Lösung ist, wird die Gleichung gelöst. Damit ist die Gesamtheit aller ganzzahligen Lösungen r, s der linearen diophanti-

29 Vgl.: Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 8 Satz 1.7.
30 Vgl. für diesen Abschnitt: Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 134.
31 Vgl.: Gelfond, A. O.: Die Auflösung von Gleichungen in ganzen Zahlen S. 10.

schen Gleichung (1) mit dem als Lösung bekannten Zahlenpaar x_0, y_0 und dem Parameter $t \in \mathbb{Z}$ in der Form $r = x_0 + \frac{a_2}{d} t$, $s = y_0 - \frac{a_1}{d} t$ gegeben. Für den Fall $c = 0$ folgt analog hierzu, dass alle Lösungen r, s durch $r = \frac{a_2}{d} t$, $s = -\frac{a_1}{d} t$ gebildet werden, da $x_0 = 0$, $y_0 = 0$ bekanntermaßen eine Lösung einer Gleichung der Form $a_1 x_1 + a_2 x_2 = 0$ ist.

4.2.4 Lösungen in den natürlichen Zahlen

Neben den ganzzahligen Lösungen in $\mathbb{Z}$ können auch die Lösungen in den natürlichen Zahlen $\mathbb{N}$ bestimmt werden.[32] Vorausgesetzt wird für die zu betrachtende Gleichung (1), dass $a_1, a_2, c \in \mathbb{N}$ sind. Um nur positive Werte für die allgemeine ganzzahlige Lösung r, s zu erhalten, beschränkt man t.

$$r = x_0 + \frac{a_2}{d} t > 0 \qquad s = y_0 - \frac{a_1}{d} t > 0$$

$$\frac{a_2}{d} t > -x_0 \qquad y_0 > \frac{a_1}{d} t$$

$$t > -\frac{d}{a_2} x_0 \qquad \frac{d}{a_1} y_0 > t$$

Da die Ungleichung $-\frac{d}{a_2} x_0 < t < \frac{d}{a_1} y_0$ auch für ein $t \notin \mathbb{Z}$ erfüllt wird, verwendet man die Gaußsche Klammerfunktion,[33] um einen Wert für das größt- und kleinstmögliche ganzzahlige t zu finden. Diese Funktion $f(x) = [x]$ gibt für ein $x \in \mathbb{R}$ die nächste ganze Zahl kleiner oder gleich x an. Zur Bestimmung von t_{min} muss der Wert dementsprechend zuvor um eins erhöht werden und es resultiert: $t_{min} = [-\frac{d}{a_2} x_0 + 1]$, $t_{max} = [\frac{d}{a_1} y_0] = -[-\frac{d}{a_1} y_0 + 1]$.
Die Tatsache, dass sowohl eine obere als auch eine untere Grenze für t besteht, legt nahe, dass es im Gegensatz zu den unendlich vielen Lösungen in $\mathbb{Z}$ nur eine endliche Zahl hiervon in $\mathbb{N}$ gibt. Um diese Anzahl n zu bestimmen, bildet man die Differenz von t_{max} und t_{min} und erhöht um eins:

$$n = t_{max} - t_{min} + 1 = -[-\frac{d}{a_1} y_0 + 1] - [-\frac{d}{a_2} x_0 + 1] + 1 = -([-\frac{d}{a_1} y_0] + [-\frac{d}{a_2} x_0] + 1)$$

Die letzte Umformung beruht auf der Tatsache,[34] dass für $x \in \mathbb{R}, y \in \mathbb{Z}$

32 Aus: Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 135-136.
33 Vgl.: Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 102-109.
34 Vgl.: Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 102 Satz 4.1c.

$[x+y]=[x]+y$ ist. Da ferner gilt,[35] dass $[x]+[y]\leq[x+y]\leq[x]+[y]+1$ mit $x, y\in\mathbb{R}$ ist, ergibt sich die folgende Ungleichung für n:

$$-([-\frac{d}{a_1}y_0-\frac{d}{a_2}x_0]+1)\leq n\leq-[-\frac{d}{a_1}y_0-\frac{d}{a_2}x_0]$$

$$-([-\frac{d}{a_1a_2}y_0a_2-\frac{d}{a_1a_2}x_0a_1]+1)\leq n\leq-[-\frac{d}{a_1a_2}y_0a_2-\frac{d}{a_1a_2}x_0a_1]$$

$$-([-\frac{d}{a_1a_2}(y_0a_2+x_0a_1)]+1)\leq n\leq-[-\frac{d}{a_1a_2}(y_0a_2+x_0a_1)].$$

Und da x_0, y_0 eine Lösung zu $a_1x_1+a_2x_2=c$ ist:

$$-[-\frac{dc}{a_1a_2}]-1\leq n\leq-[-\frac{dc}{a_1a_2}].$$

Dies liefert zwei aufeinander folgende Werte für n, von denen eine der genauen Anzahl aller Lösungen der Gleichung in den natürlichen Zahlen entspricht. Ferner folgt, dass, sofern das Lösbarkeitskriterium $c|d$ erfüllt ist, mindestens eine Lösung in N existiert, wenn $dc>a_1a_2$ ist, da andernfalls $0<\frac{dc}{a_1a_2}<1$ und somit $n\leq[\frac{dc}{a_1a_2}]\leq0$ wäre.

4.3 Gleichungen mit mehr als zwei Unbekannten

Viele Aspekte des Lösens einer linearen diophantischen Gleichung mit den $k>2$ Unbekannten $x_1, x_2, \ldots, x_{k-1}, x_k$, welche die allgemeine Form

$$a_1x_1+a_2x_2+\ldots+a_{k-1}x_{k-1}+a_kx_k=c \quad a_i, c\in\mathbb{Z} \quad (3)$$

hat, lassen sich durch Zurückgriff auf die Gleichungen des Typs (1) mit zwei Unbestimmten gewinnen. So erweitert man das Kriterium für die Existenz ganzzahliger Lösungen auf $ggT(a_1, a_2, \ldots, a_{k-1}, a_k)|c$, wobei die Begründung analog zu 4.2.1 erfolgt.[36]

Um eine einzelne Lösung der Gleichung zu finden, verfährt man wie folgt:[37]

a) Man reduziert die Ausgangsgleichung (3) mit k Unbekannten auf $a_1x_1+a_2x_2+\ldots+a_{k-2}x_{k-2}+b_1y_1=c$ mit $k-1$ Variablen $x_1, x_2, \ldots, x_{k-2}, y_1$. Hierzu setzt man $a_{k-1}x_{k-1}+a_kx_k=b_1y_1$ und $b_1=ggT(a_{k-1}, a_k)$. Dieses Vorgehen führt man weiter fort und es resultiert die Gleichung $a_1x_1+a_2x_2+\ldots+a_{k-3}x_{k-3}+b_2y_2=c$ mit $k-2$ Unbestimmten, wobei $a_{k-2}x_{k-2}+b_1y_1=b_2y_2$ und $b_2=ggT(a_{k-2}, b_1)$ gesetzt werden.

35 Vgl.: Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 102 Satz 4.1d.
36 Vgl.: Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 137.
37 Vgl.: Bundschuh, Peter: Einführung in die Zahlentheorie S. 33.

b) Nach $k-2$ Schritten erhält man schließlich die Reduktion von (3) auf $a_1 x_1 + b_{k-2} y_{k-2} = c$ (4) mit den zwei Unbekannten x_1, y_{k-2}, indem man $a_2 x_2 + b_{k-3} y_{k-3} = b_{k-2} y_{k-2}$ (5) sowie $b_{k-2} = ggT(a_2, b_{k-3})$ setzt.

c) Durch die von Gleichung (4) auf bekannte Weise erhaltenen Werte für x_1, y_{k-2} hat man nun zum einen bereits eine Lösung für x_1 der Ausgangsgleichung (3), zum anderen kann man jedoch mit dem erlangten Wert für y_{k-2} Gleichung (5) komplettieren und auflösen.

d) So ermöglicht die letzte Komponente y jeder nach diesem Schema erhaltenen Lösung x_i, y_{k-1-i} die vollständige Aufstellung und Auflösung der vorhergegangenen Gleichung der Form (5). Letztendlich erhält man auf diese Weise Werte für alle x_i der Ursprungsgleichung (3).

Die Darstellung der Gesamtheit aller Lösungen über eine gewisse Anzahl an Parametern betreffend folgt an dieser Stelle aufgrund des Umfangs des Themas nur der Verweis auf [38] und [39].

38 Bundschuh, Peter: Einführung in die Zahlentheorie S. 33-35.
39 Niven, I.; Zuckermann, H. S.: Einführung in die Zahlentheorie S. 137-139.

5 Ergebnisse

Zusammengefasst wurden im Hauptteil folgende Inhalte behandelt: Geschichtliche Hintergründe wurden kurz vorgestellt, elementare Aspekte der Teilbarkeitslehre wurden aufgerollt und in Zusammenhängen zu wichtigen Erkenntnissen wie dem Lemma von Bachet entwickelt. Anhand des Themas der linearen diophantischen Gleichungen, welches durch Unterteilung in Gleichungen mit einer, zwei und beliebig vielen Unbekannten logisch aufeinander aufbaut, wurden die gewonnenen Methoden zu konkreten Werkzeugen. Wenngleich diese Erkenntnisse nur einen kleinen Teil des Themenkomplexes der diophantischen Gleichungen repräsentieren, so sind sie doch als Grundlage für weitergehende Vertiefungen hilfreich. Die hier nicht vorkommenden quadratischen diophantischen Gleichungen, deren wohl bekanntester Vertreter das pythagoreische Tripel $a^2+b^2=c^2$ ist, sind dabei eine Möglichkeit. Abseits aller theoretischen Interessen kann die Bedeutung des Auffindens von Lösungen nur aus den natürlichen oder ganzen Zahlen auch daran gemessen werden, dass Zahlen aus diesen Mengen die wahrscheinlich am häufigsten im alltäglichen Leben anzutreffende Position einnehmen und die Mathematik aus der Beschreibung von Mengen in eben diesen alltäglichen Zusammenhängen entstanden ist.

Literaturverzeichnis

Bücher, Monographien

Bundschuh, Peter: Einführung in die Zahlentheorie.
5. Auflage. Berlin (u.a.): Springer 2002. Springer-Lehrbuch.

Frey, Gerhard: Elementare Zahlentheorie.
1. Auflage. Braunschweig/Wiesbaden: Friedr. Vieweg&Sohn 1984
Vieweg-Studium: Grundkurs Mathematik Nr. 56.

Gelfond, Aleksandr Osiporie: Die Auflösung von Gleichungen in ganzen Zahlen (Diophantische Gleichungen).
4. Auflage. Berlin: Dt. Verlag der Wissenschaft 1968.

Mankiewicz, Richard: Zeitreise der Mathematik. Vom Ursprung der Zahlen zur Chaostheorie. 1. Auflage. Köln: VGS 2000.

Niven, Ivan; Zuckermann, Herbert S.: Einführung in die Zahlentheorie.
3. Auflage. Mannheim: Bibliographisches Institut 1976.
B.I. Hochschultaschenbuch.

Rose, Harvey Ernest: A Course in Number Theory.
1. Auflage. Oxford: Clarendon Press 1988. Oxford Science publications.

Schreiber, Peter: Euklid.
1. Auflage. Leipzig: BSB Teubner 1987.
Biographien hervorragender Naturwissenschaftler, Techniker und Mediziner.

Internetquellen

Schreiber, Alfred (1996): Einführung in die Mathematik, Kapitel 4 „Teilbarkeit“ (PDF-Datei, erstellt am 29.03.2004). Internet: http://www.uni-flensburg.de/mathe/zero/veranst/arithalgebra/schreiber/einfmath1996/4_teilbarkeit.pdf (Zugriff: 18.02.2006, 14:24)

Wiesenbauer, Johann (2005): AKDIS Zahlentheorie und Anwendungen (PDF-Datei, erstellt am 4.04.2005).
Internet: http://www.algebra.tuwien.ac.at/institut/zthanw/ZthAnw1_1.pdf
(Zugriff: 7.03.2006, 18:38)