Zeitschrift: Elemente der Mathematik

Band: 59 (2004)

Artikel: Höhere Mathematik an der Balkenwaage

Autor: Elsner, Carsten

DOI: https://doi.org/10.5169/seals-9318

Elem. Math. 59 (2004) 151 – 170
0013-6018/04/040151-20
DOI 10.1007/s00017-004-0210-y

Elemente der Mathematik

Höhere Mathematik an der Balkenwaage

Carsten Elsner

C. Elsner studierte Mathematik und Physik an der Universität Hannover. Im Jahr 1990 promovierte er dort über eine Fragestellung zu diophantischen Gleichungen vom Waring-Typ. Im Jahr 1997 folgte die Habilitation, ebenfalls über ein zahlentheoretisches Thema. Gegenwärtig lehrt er an der Fachhochschule für die Wirtschaft in Hannover. In seiner Forschung beschäftigt er sich neben zahlentheoretischen Problemen mit Approximationsfragen bei reellen Funktionen.

In diesem Aufsatz kommen vor:

- komplexe Zahlen und die komplexe Exponentialfunktion;
- trigonometrische Funktionen und Additionstheoreme;
- Ableitungen hoher Ordnung und Integrale;
- lineare quadratische Gleichungssysteme, Matrizen und ihre Inversen;
- Vandermondesche Determinanten;
- Gitterpunkte auf einer Hyperebene in einem hochdimensionalen Würfel;
- Bernoulli-Polynome;
- homogene Polynome in vielen Veränderlichen;

und das alles nur wegen eines Wägeproblems mit 15 Gewichten an einer simplen Balkenwaage! Aber der zahlentheoretische Hintergrund vermag Analysis und lineare Algebra auf elegante Weise zueinander in Beziehung zu setzen.

Ausgangspunkt des nachfolgenden Beitrags ist ein einfaches Wägeproblem an der Balkenwaage. Die Formalisierung eines solchen Problems führt unmittelbar auf eine lineare diophantische Gleichung $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, wobei die Lösungen $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ innerhalb eines Würfels mit vorgegebener Kantenlänge m gesucht sind. Im folgenden werden die entsprechenden Lösungsanzahlen explizit bestimmt, und zwar im allgemeinen Fall durch effektiv berechenbare Polynome in den $n+2$ ganzzahligen Grössen $a_1, a_2, \ldots, a_n, b, m+1$, im konkreten Fall mittels eines einfachen Computerprogramms (MAPLE). Die hierbei verwendeten Methoden verbinden den zahlentheoretischen Ansatz (Exponentialsummen) mit Hilfsmitteln aus der Analysis und der linearen Algebra.

1 Das Problem

Vor uns steht eine Balkenwaage mit zwei Waagschalen, die es erlaubt, die Gleichheit zweier Gewichte festzustellen. Auf der rechten Waagschale ist ein 7 Gramm-Gewicht festgenagelt. Zur Verfügung stehen uns 15 Gewichte, und zwar 5 Stück zu je 2 Gramm, 5 Stück zu je 3 Gramm und 5 Stück zu je 5 Gramm. Auf wieviele Weisen können nun Gewichte auf beide Waagschalen verteilt werden, so daß die Waage im Gleichgewicht ist? Selbstverständlich müssen nicht immer alle Gewichte verwendet werden. Um jedoch nur wesentlich verschiedene Verteilungen zu zählen, ist es verboten, auf beide Waagschalen gleichzeitig Gewichte derselben Sorte (etwa 2 Gramm-Gewichte) zu stellen.

Die Antwort auf dieses Wägeproblem kann uns die elementare Zahlentheorie geben. Die Problemstellung ist nämlich gleichwertig mit der Frage nach der Lösungsanzahl der linearen diophantischen Gleichung

$$2x_1 + 3x_2 + 5x_3 = 7 \tag{1}$$

in ganzen Zahlen x_1, x_2, x_3 unter den Nebenbedingungen

$$|x_1| \leq 5\,, \quad |x_2| \leq 5\,, \quad |x_3| \leq 5\,. \tag{2}$$

In einem Lösungstripel (x_1, x_2, x_3) gibt nämlich x_1 die Anzahl der 2 Gramm-Gewichte, x_2 die Anzahl der 3 Gramm-Gewichte und x_3 die Anzahl der 5 Gramm-Gewichte an, die für eine Gleichgewichtslage verwendet werden können. Ist die jeweilige Anzahl positiv, kommen die zugehörigen Gewichte auf die linke Waagschale, anderenfalls auf die rechte.

Das Problem kann natürlich durch Ausprobieren aller möglichen Verteilungen gelöst werden. Jede Gewichtssorte kann unabhängig von der Verwendung von Gewichten der beiden anderen Sorten auf 11 Weisen ins Spiel gebracht werden: entweder wird überhaupt kein Gewicht dieser Sorte verwendet, oder es kommen 1, 2, 3, 4 oder 5 Gewichte nur auf die linke Schale oder nur auf die rechte. So ergeben sich insgesamt $11^3 = 1331$ Verteilungsmöglichkeiten. Ein Gleichgewichtszustand stellt sich aber nur bei 23 Verteilungen ein. Hier sind sie:

Nr.	x_1	x_2	x_3	Nr.	x_1	x_2	x_3
1	−5	−1	4	13	1	−5	4
2	−5	4	1	14	1	0	1
3	−4	0	3	15	1	5	−2
4	−4	5	0	16	2	−4	3
5	−3	−4	5	17	2	1	0
6	−3	1	2	18	3	−3	2
7	−2	−3	4	19	3	2	−1
8	−2	2	1	20	4	−2	1
9	−1	−2	3	21	4	3	−2
10	−1	3	0	22	5	−1	0
11	0	−1	2	23	5	4	−3
12	0	4	−1				

Mit einem einfachen BASIC-Programm, das alle 1331 Möglichkeiten durchprobiert, lassen sich die 23 Lösungen leicht finden. Wie verhält es sich aber mit der Lösungsanzahl, wenn mehr als nur fünf Gewichte von jeder Sorte verwendet werden, oder wenn noch weitere Gewichtsklassen hinzukommen? Kurzum: Wie kann man die Anzahl der n-Tupel $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ berechnen, die der linearen diophantischen Gleichung

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \tag{3}$$

unter den Nebenbedingungen

$$|x_\nu| \leq m \qquad (1 \leq \nu \leq n) \tag{4}$$

genügen? Hierbei bezeichnen $a_1, a_2, \ldots, a_n$, b und m vorgegebene nichtnegative ganze Zahlen. Gleichung (3) ist in *reellen* Zahlen $x_1, \ldots, x_n$ immer lösbar. Die Lösbarkeit in *ganzen* Zahlen hingegen ist nur genau dann gewährleistet, wenn der größte gemeinsame Teiler der Koeffizienten $a_1, \ldots, a_n$ die Zahl b teilt. Eine ausführliche Darstellung der Theorie zur diophantischen Gleichung (3) und ihrer Lösungsgesamtheit findet man in [5, Kap. 1, §3].

Das Anliegen dieses Aufsatzes ist es, neben einer effektiven und raschen (praktischen) Berechnung der Lösungsanzahl mittels eines einfachen MAPLE-Befehls den dabei verwendeten Ansatz weiter auszubauen und für Schulzwecke zugänglich zu machen. Es soll demonstriert werden, daß ein zahlentheoretisches Problem bestens geeignet ist, Interesse bei Schülern (an Gymnasien) für die Anwendungen der bisher erlernten mathematischen Techniken zu wecken. Eine zahlentheoretische Fragestellung, dargestellt anhand eines nur scheinbar einfachen Wägeproblems, kann zunächst vom Schüler praktisch mit selbstgebastelten Programmen (z.B. BASIC) und, wie in Abschnitt 2 erläutert, auch mit MAPLE in Angriff genommen werden, um zu ersten numerischen Ergebnissen zu gelangen. Gleichzeitig wird das Umfeld ein wenig erhellt: So wird das Gitter aus den Lösungspunkten der linearen diophantischen Gleichung (1) mit zahlentheoretischen Methoden ermittelt. Ebenso wird für solche Gitter allgemein die Anzahl der Lösungspunkte im n-dimensionalen Würfel $(t_1, t_2, \ldots, t_n) \in \mathbb{R}^n$ mit $-m \leq t_\nu \leq m$ $(1 \leq \nu \leq n)$ mit elementaren Methoden nach unten abgeschätzt. Für das spezielle Gitter zu (1), (2) berechnen wir auch eine obere Schranke. Hier streifen wir das Gebiet der Geometrie der Zahlen in einem solchen Rahmen, für den der euklidische Anschauungsraum völlig ausreicht. Die Anwendung der elementaren Analysis und Trigonometrie (wobei der unten beschrittene Königsweg über die komplexen Zahlen auch problemlos umgangen werden kann) bringt einen überraschenden Zugang zur Lösung eines geometrisch-diskreten Gitterproblems.

Für die geschlossene Darstellung der Lösungsanzahl von (3) und (4) werden die bereits oben erwähnten Hilfsmittel aus Analysis und linearer Algebra eingesetzt. Die Vorgehensweise bleibt weitgehend elementar. Besonderer Wert wird aber auf die (tatsächlich in einem weitaus umfassenderen Sinne gültige) Aussage gelegt, daß zur Lösung eines zahlentheoretischen Problems Analysis und lineare Algebra in gleichem Maße herangezogen werden. Hier zeigt sich, daß sich zwei meist einander als fremd empfundene Gebiete durchaus gegenseitig durchdringen können und daß diese Durchdringung auch von einem praktischen Wägeproblem ausgehen kann.

Eine kurze Anmerkung soll vorab noch zu einer naheliegenden Verallgemeinerung des diophantischen Problems gemacht werden. Man wird natürlich die Frage stellen, inwieweit die hier dargelegte Theorie auch für *lineare diophantische Systeme* ausgebaut werden kann. Die Antwort ist: Das ist möglich, nur werden vor allem die behandelten quadratischen Gleichungssysteme nicht nur ziemlich groß, sondern auch unübersichtlich. Außerdem benötigt man dann partielle Ableitungen und Volumenintegrale, und alles zusammen würde den hier gesteckten Rahmen sprengen. Jedoch überlegt man sich leicht andere Varianten der Problemstellung oder andere praktische Interpretationsmodelle linearer diophantischer Gleichungen.

2 Das Zählen von Gitterpunkten mittels Exponentialsummen

Im dreidimensionalen Anschauungsraum stellt die Lösungsmenge von (1) ohne die Größenbeschränkungen an x_1, x_2 und x_3 eine zweidimensionale Ebene dar, deren vektorielle Darstellung man mit zwei Parametern $x_1 = \lambda$ und $x_2 = \mu$ wegen $x_3 = \frac{7}{5} - \frac{2}{5}\lambda - \frac{3}{5}\mu$ sofort anschreibt:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} \lambda \\ \mu \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \frac{7}{5} \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ 0 \\ -\frac{2}{5} \end{pmatrix} + \mu \cdot \begin{pmatrix} 0 \\ 1 \\ -\frac{3}{5} \end{pmatrix} \qquad (\lambda, \mu \in \mathbb{R}).$$

Gesucht ist nun aber eine Vektordarstellung aller ganzzahligen Lösungstripel (x_1, x_2, x_3) von (1), die folgende Eigenschaft hat: Durchlaufen die Parameter unabhängig voneinander *alle* ganzen Zahlen, so sollen (x_1, x_2, x_3) *alle* ganzzahligen Lösungen von (1) durchlaufen. Um diese sog. *diophantischen Lösungen* zu erhalten, muß man nun gänzlich anders vorgehen als für eine Vektordarstellung der reellen Lösungen. Es wird hierfür zweimal der *Satz von Bezout* angewendet:

Sind a, b und c ganze Zahlen, bei denen der größte gemeinsame Teiler (a, b) von a und b die Zahl c teilt, so erhält man alle ganzzahligen Lösungen x, y der linearen Gleichung

$$ax + by = c \tag{5}$$

mittels

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \frac{\gamma}{(a, b)} \cdot \begin{pmatrix} b \\ -a \end{pmatrix} \qquad (\gamma \in \mathbb{Z}), \tag{6}$$

wobei (x_0, y_0) eine beliebige Lösung von (5) *ist* (*siehe* [5, S. 30f.]).

In (1) kürzt man zunächst $t = 3x_2 + 5x_3$ ab und löst mit Bezout die Gleichung $2x_1 + t = 7$. Da 3 und 5 teilerfremd sind, ist in der ersten Gleichung jede ganze Zahl t darstellbar. Man erhält als Lösungsgesamtheit der zweiten Gleichung:

$$\begin{pmatrix} x_1 \\ t \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix} + \alpha \cdot \begin{pmatrix} 1 \\ -2 \end{pmatrix} \qquad (\alpha \in \mathbb{Z}).$$

Für ein beliebiges ganzzahliges α lautet nun die erste Gleichung $3x_2 + 5x_3 = 1 - 2\alpha$. Ihre Lösungsgesamtheit ist durch

$$\begin{pmatrix} x_2 \\ x_3 \end{pmatrix} = (1 - 2\alpha) \cdot \begin{pmatrix} 2 \\ -1 \end{pmatrix} + \beta \cdot \begin{pmatrix} 5 \\ -3 \end{pmatrix} \qquad (\beta \in \mathbb{Z})$$

gegeben, so daß man in der Zusammenfassung endgültig

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \\ -1 \end{pmatrix} + \alpha \cdot \begin{pmatrix} 1 \\ -4 \\ 2 \end{pmatrix} + \beta \cdot \begin{pmatrix} 0 \\ 5 \\ -3 \end{pmatrix} \qquad (\alpha, \beta \in \mathbb{Z}) \tag{7}$$

erhält. Diese diskrete Teilmenge in der reellen Lösungsebene von (1) ist ein *Gitter*; die Anzahl der Gitterpunkte im Würfel mit den Eckpunkten $(\pm 5, \pm 5, \pm 5)$ soll nun gezählt werden. Der zahlentheoretische Zugang zum Zählen von Lösungen diophantischer Gleichungen geht nun allerdings nicht von einer Darstellung der Lösungen aus, wie sie eben ermittelt wurde. Vielmehr beruht der Ansatz auf folgendem Integral, bei dem im Integranden eine komplexe Exponentialfunktion vorkommt. Für jede ganze Zahl z gilt nämlich:

$$\int_0^1 e^{2\pi i z \alpha} \, \mathrm{d}\alpha = \begin{cases} 0\,, & \text{falls } z \neq 0, \\ 1\,, & \text{falls } z = 0. \end{cases} \tag{8}$$

Hierbei ist $i^2 = -1$. Die Anzahl $A = A_m$ der Gitterpunkte, die der linearen Gleichung (3) unter den Nebenbedingungen (4) genügen, wird von

$$A = \int_0^1 e^{-2\pi i b \alpha} \cdot \prod_{\nu=1}^{n} \Big(\sum_{-m \leq k_\nu \leq m} e^{2\pi i a_\nu k_\nu \alpha} \Big) \, \mathrm{d}\alpha \tag{9}$$

erfaßt. Diesem zunächst abschreckenden Integral sieht man aber sein Geheimnis sofort an, wenn man die n Summen ausmultipliziert und jeweils alle Terme im Exponenten der Exponentialfunktion zusammenfaßt. Es entsteht dann eine Summe über alle möglichen n-Tupel $k_1, k_2, \ldots, k_n$, deren Komponenten betragsmäßig durch m beschränkt sind:

$$A = \int_0^1 \sum_{-m \leq k_1, k_2, \ldots, k_n \leq m} e^{2\pi i (a_1 k_1 + a_2 k_2 + \cdots + a_n k_n - b)\alpha} \, \mathrm{d}\alpha\,. \tag{10}$$

Vertauscht man nun Summe und Integral (was wegen der Endlichkeit der Summe problemlos möglich ist!) und wendet die Identität aus (8) an, so ist die Übereinstimmung des Integrals mit der Lösungsanzahl A unmittelbar einsichtig.

Weil im vorliegenden Fall die zugrundeliegende diophantische Gleichung (3) linear ist und zudem in den Summen im Integranden von (9) mit $-k_\nu$ auch jeweils k_ν vorkommt, kann jede solche Summe in (9) als eine Summe von reellen Kosinus-Funktionen ausgedrückt werden. Wegen der bekannten Darstellung

$$\cos t = \frac{e^{it} + e^{-it}}{2} \qquad (t \in \mathbb{R})$$

erhält man nämlich aus (9) durch Abspalten des Terms 1 (für $k_\nu = 0$) und Zusammenfassen von Termen, die zu $\pm k_\nu$ gehören:

$$A = \int_0^1 e^{-2\pi i b \alpha} \cdot \prod_{\nu=1}^{n} \Big(1 + 2 \cdot \sum_{k_\nu = 1}^{m} \cos(2\pi a_\nu k_\nu \alpha) \Big) \, \mathrm{d}\alpha\,.$$

A ist eine reelle Größe. (Tatsächlich ist ja A eine nichtnegative ganze Zahl.) Drückt man den Faktor $e^{-2\pi i b\alpha}$ durch $\cos(2\pi b\alpha) - i \cdot \sin(2\pi b\alpha)$ aus, bleibt demnach folgendes übrig:

$$A = \int_0^1 \cos(2\pi b\alpha) \cdot \prod_{\nu=1}^{n} \Big(1 + 2 \cdot \sum_{k_\nu=1}^{m} \cos(2\pi a_\nu k_\nu \alpha)\Big)\, \mathrm{d}\alpha\,. \tag{11}$$

Es gibt noch eine summenfreie Darstellung des Integranden, die zwar recht elegant ist, aber für die weitere Analyse des Integrals nicht viel nützt. Man kann nämlich die Summen in (9) als endliche geometrische Reihen mit komplexen Summanden auffassen und diese dann durch die entsprechende Summenformel ausdrücken. Ersetzt man anschließend noch die komplexen Exponentialterme durch trigonometrische Funktionen und wendet die Additionstheoreme an, so gelangt man unter Verwendung der Abkürzung $M := 2m+1$ zu

$$A = \int_0^1 \cos(2\pi b\alpha) \cdot \prod_{\nu=1}^{n} \frac{\sin(\pi M a_\nu \alpha)}{\sin(\pi a_\nu \alpha)}\, \mathrm{d}\alpha\,. \tag{12}$$

Bemerkenswert ist, daß der Integrand keine Pole, aber zahlreiche hebbare Unstetigkeitsstellen hat. Ist die Gleichung in (3) ganzzahlig nicht lösbar, verschwindet das Integral in (12) *für jedes beliebige* ungerade M.

Es läßt sich aber für den Integranden in (11) eine Stammfunktion angeben, wenn konkrete Werte für die Parameter $a_1, a_2, \dots, a_n$, b und m vorliegen. Man denke sich auch hier das Produkt über die trigonometrischen Summen ausmultipliziert. Jedes Produkt $2 \cdot \cos x \cdot \cos y$ kann durch $\cos(x-y) + \cos(x+y)$ ausgedrückt werden. Mittels vollständiger Induktion nach der Anzahl der Kosinusfaktoren beweist man so leicht die folgende Darstellung:

$$\cos(2\pi b\alpha) \cdot \prod_{\nu=1}^{n} \Big(1 + 2 \cdot \sum_{k_\nu=1}^{m} \cos(2\pi a_\nu k_\nu \alpha)\Big) = \sum_{\substack{\mu=0 \\ 2|\mu}}^{2(a_1+\cdots+a_n)m+2b} c_\mu \cdot \cos(\pi\mu\alpha)\,. \tag{13}$$

Eine besondere Bedeutung kommt hier auf der rechten Seite dem ersten Summanden c_0 zu: Integriert man nämlich die ganze Summe über α von 0 bis 1, so verschwinden alle Summanden bis auf den ersten, und es bleibt

$$A = c_0\,. \tag{14}$$

Wem nun der Umweg über die komplexen Exponentialfunktionen zu weitschweifig ist, der kann auch mit einem scharfen Blick unmittelbar in (13) die Bedeutung von c_0 ablesen. Jedes Produkt

$$2^{r-1} \cdot \cos\beta_1 \cdot \ldots \cdot \cos\beta_r$$

kann in der Form einer Summe von Termen der Gestalt $\cos(\pm\beta_1 \pm \cdots \pm \beta_r)$ geschrieben werden. Wenn das Argument dieser Funktion verschwindet, reduziert sich ein solcher Term auf 1, und dies geschieht oben genau bei den Lösungen von (3) und (4).

Mit einem MAPLE-Programm können nun problemlos alle Koeffizienten c_μ in (13) ermittelt werden. Zur Demonstration greifen wir auf das Eingangsbeispiel zurück und schreiben hierfür den Integranden aus (11) an. Dabei wird der Kürze halber noch $2\pi\alpha$ durch t abgekürzt.

$> s := \cos(7*t)*(1+2*sum(\cos(2*t*k)\,,\ k=1..5))*(1+2*sum(\cos(3*t*k)\,,$
$k=1..5))*(1+2*sum(\cos(5*t*k)\,,\ k=1..5))\ :$

MAPLE bestimmt hiervon eine Stammfunktion mit dem Befehl:

$$> \ int(s,t)\,;$$

Das Programm gibt das Ergebnis als eine Summe der Gestalt

$$23t + \sum_{h=1}^{57} \frac{c_{2h}}{h} \cdot \sin(ht)$$

an, wie man es für eine Stammfunktion der rechten Seite von (13) bezüglich der Variablen $t = 2\pi\alpha$ auch erwartet. Die gesuchte Lösungsanzahl 23 von (1) und (2) steht ganz links. Man liest aus dieser Darstellung aber auch folgende Werte für $c_2, c_4, c_6, \ldots, c_{114}$ ab:

$$\begin{aligned}
c_2,\ldots,c_{40} &= 47,47,47,46,46,45,46,45,44,43,43,42,42,40,39,38,38,36,35,34\,,\\
c_{42},\ldots,c_{80} &= 32,32,31,28,28,26,25,24,22,20,20,18,17,16,14,13,13,11,10,9\,,\\
c_{82},\ldots,c_{114} &= 8,7,7,5,5,4,4,3,3,2,2,2,1,1,1,0,1\,.
\end{aligned}$$

Die Summe dieser Zahlen $c_2 + c_4 + \cdots + c_{114}$ steht mit der Zahl A in einem einfachen Zusammenhang, wie man aus der Gleichung (13) für $\alpha = 0$ und aus (14) abliest:

$$A = c_0 = 11^3 - (c_2 + c_4 + \cdots + c_{114}) = 1331 - 1308 = 23\,.$$

Im allgemeinen Fall lautet diese wichtige Identität

$$A = (2m+1)^n - \sum_{\substack{\mu=0\\ 2|\mu}}^{2(a_1+\cdots+a_n)m+2b} c_\mu = (2m+1)^n - \sum_{h=1}^{(a_1+\cdots+a_n)m+b} c_{2h}\,. \tag{15}$$

Ehe nun mit den Hilfsmitteln der linearen Algebra aus (13) und (15) eine integralfreie, geschlossene algebraische Darstellung von A hergeleitet wird, wollen wir uns im nächsten Abschnitt zunächst mit der Größenordnung von A für alle hinreichend großen Lösungsschranken m beschäftigen.

3 Die Größenordnung von A

Der in diesem Abschnitt bewiesene Satz über Gitterpunkte eines d-dimensionalen Gitters in einem n-dimensionalen Würfel enthält eine etwas allgemeinere Aussage als es für die Lösungsanzahl des Systems (3), (4) benötigt wird. Hierfür ist $d = n-1$ ausreichend. Ein spezielles Vorwissen wird nicht vorausgesetzt. Zunächst werden einige Bezeichnungen eingeführt. Es seien d, n und m natürliche Zahlen mit $1 \le d \le n$, und

$$\vec{a}_1 := \begin{pmatrix} a_{11} \\ \vdots \\ a_{1n} \end{pmatrix}, \quad \vec{a}_2 := \begin{pmatrix} a_{21} \\ \vdots \\ a_{2n} \end{pmatrix}, \ldots, \quad \vec{a}_d := \begin{pmatrix} a_{d1} \\ \vdots \\ a_{dn} \end{pmatrix}$$

bezeichnen über den reellen Zahlen linear unabhängige Vektoren mit ganzzahligen Komponenten. Der n-dimensionale Würfel

$$W_m := \{(t_1, t_2, \ldots, t_n) \in \mathbb{R}^n : \ |t_\nu| \leq m \ (\nu = 1, 2, \ldots, n)\}$$

hat die Eckpunkte $(\pm m, \pm m, \ldots, \pm m)$. Schließlich wird noch ein weiterer Vektor

$$\vec{b} := \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{Z}^n$$

benötigt. Das in $\vec{b}$ angeknüpfte und von $\vec{a}_1, \ldots, \vec{a}_d$ über $\mathbb{Z}$ erzeugte Gitter hat dann die Gestalt

$$G := \vec{b} + \mathbb{Z}\vec{a}_1 + \cdots + \mathbb{Z}\vec{a}_d\,.$$

Satz 1 *Es gibt eine natürliche Zahl m_0 und eine positive reelle Zahl C, die nicht von m abhängt, so daß die Ungleichung*

$$|G \cap W_m| \geq C \cdot m^d \qquad (m \geq m_0)$$

besteht.

Die Zahl C hängt natürlich vom Gitter ab. Der folgende Beweis zeigt, daß sie effektiv berechenbar ist.

Beweis: Es sei zuerst m_1 eine natürliche Zahl, so daß

$$|b_\nu| \leq \frac{m_1}{2} \qquad (1 \leq \nu \leq n) \tag{16}$$

garantiert ist. Weiterhin benötigen wir noch

$$C_1 := \max\{|a_{\delta\nu}|\,,\,|b_\nu| \,:\, (1 \leq \delta \leq d\,,\, 1 \leq \nu \leq n)\}\,.$$

Es werden nun für ein $m \geq m_1$ solche Gitterpunkte von G gezählt, die eine Darstellung

$$\vec{x} = \vec{b} + k_1\vec{a}_1 + \cdots + k_d\vec{a}_d \tag{17}$$

mit ganzen Koeffizienten $k_1, \ldots, k_d$ unter den Bedingungen

$$|k_\delta| \leq \frac{m}{2dC_1} \qquad (1 \leq \delta \leq d) \tag{18}$$

haben. In jeder Komponente erhält man so in (17) folgende Abschätzung:

$$\begin{aligned} |x_\nu| &= \left|b_\nu + \sum_{\delta=1}^{d} k_\delta a_{\delta\nu}\right| \leq |b_\nu| + \sum_{\delta=1}^{d} |k_\delta| \cdot |a_{\delta\nu}| \\ &\leq \frac{m_1}{2} + \sum_{\delta=1}^{d} \frac{m}{2dC_1} \cdot C_1 \leq \frac{m}{2} + \frac{m}{2} \cdot \sum_{\delta=1}^{d} \frac{1}{d} = m \qquad (1 \leq \nu \leq n)\,. \end{aligned}$$

Hierbei wurde neben (16) und (18) auch $m \geq m_1$ ausgenutzt. Damit ist unter der Voraussetzung (18) nun $\vec{x} \in W_m$ gezeigt. Jetzt benötigen wir die lineare Unabhängigkeit der Vektoren $\vec{a}_1, \ldots, \vec{a}_d$, aus der die Eindeutigkeit der Darstellung eines Vektors $\vec{x}$ mit Parametern $k_1, \ldots, k_d$ folgt. Durch eine Unterscheidung positiver und negativer Werte, die jedes k_δ neben der Null in (18) annehmen darf, ergibt eine einfache Zählung (hier steht $[\alpha]$ für die größte ganze Zahl $\leq \alpha$):

$$|G \cap W_m| \geq \left(1 + 2\left[\frac{m}{2dC_1}\right]\right)^d \geq \left(1 + 2\left(\frac{m}{2dC_1} - 1\right)\right)^d = \left(\frac{m}{dC_1} - 1\right)^d \geq \left(\frac{m}{2dC_1}\right)^d.$$

Für die letzte Abschätzung wurde noch $m \geq 2dC_1$ angenommen. Daher definieren wir nun $m_0 := \max\{m_1, 1 + 2dC_1\}$ und fordern $m \geq m_0$. Mit $C := \left(\frac{1}{2dC_1}\right)^d$ ist dann die Schranke im Satz bewiesen. □

Eine allgemeine obere Schranke für $A = |G \cap W_m|$ kann auch bewiesen werden, ist aber ein recht umfangreiches Unterfangen. Für das eingangs gestellte Problem an der Balkenwaage soll nun so eine Oberschranke für das in (7) ermittelte Gitter G konkret berechnet werden. Nach demselben Muster kann man auch bei höherdimensionalen Gittern vorgehen.

Zuerst führen wir die Abkürzungen

$$\vec{a}_1 := \begin{pmatrix} 1 \\ -4 \\ 2 \end{pmatrix}, \qquad \vec{a}_2 := \begin{pmatrix} 0 \\ 5 \\ -3 \end{pmatrix}$$

für die beiden erzeugenden Vektoren des Gitters G ein. Wir beginnen nun die Berechnung einer oberen Schranke, indem wir zunächst ein eindimensionales Gitter

$$\vec{x} := \vec{b} + k\vec{a}_1 = \begin{pmatrix} b_1 & + & k \\ b_2 & - & 4k \\ b_3 & + & 2k \end{pmatrix}$$

betrachten. Hierbei ist $\vec{b}$ ein völlig beliebiger Vektor im Anschauungsraum $\mathbb{R}^3$. Eine notwendige (aber nicht hinreichende) Bedingung für $\vec{x} \in W_m$ ist die Beschränktheit der zweiten Komponente von $\vec{x}$ nach unten durch $-m$ und nach oben durch $+m$, oder

$$-m \leq b_2 - 4k \leq m \quad \text{bzw.} \quad \frac{m + b_2}{4} \geq k \geq \frac{-m + b_2}{4}.$$

Deshalb ist die Anzahl der ganzzahligen Werte, die k für $\vec{x} \in W_m$ annehmen kann, nach oben beschränkt durch

$$1 + \frac{m + b_2}{4} - \frac{-m + b_2}{4} = 1 + \frac{m}{2}. \tag{19}$$

Es sei noch einmal daran erinnert, daß hierbei der Vektor $\vec{b}$ völlig beliebig gewählt werden kann.

Jeden Punkt $\vec{x}$ des Gitters G schreiben wir nun in folgender Gestalt an:

$$G_r : \vec{x} = \vec{b} + r\vec{a}_2 + k\vec{a}_1 = \begin{pmatrix} 3 \\ 2 \\ -1 \end{pmatrix} + r \cdot \begin{pmatrix} 0 \\ 5 \\ -3 \end{pmatrix} + k \cdot \begin{pmatrix} 1 \\ -4 \\ 2 \end{pmatrix}.$$

Die ganze Zahl r wird zunächst als ein *fest gewählter Parameter* vorausgesetzt, k wird als Variable aufgefaßt. In diesem Sinne ist G_r ein eindimensionales Gitter, bestehend aus äquidistanten Punkten auf einer Geraden. Es wird nun der Abstand $L(G_r)$ dieser Trägergeraden von G_r zum Nullpunkt analytisch bestimmt. Die Länge $|\vec{x}|$ eines beliebigen Ortsvektors $\vec{x}$ bestimmt man bekanntlich mit

$$|\vec{x}|^2 = (3 + k)^2 + (2 + 5r - 4k)^2 + (-1 - 3r + 2k)^2 . \tag{20}$$

Im folgenden wird k vorübergehend als eine kontinuierliche Variable angesehen. Gesucht ist nun eine *reelle Zahl* k, für die der Term rechts in (20) minimal wird. Schon anschaulich ist klar, daß k existiert und eindeutig bestimmt ist. Zu diesem Zweck wird die Ableitung von (20) nach k zum Verschwinden gebracht. Das führt auf die Gleichungen

$$2(3+k)+2(2+5r-4k)(-4)+2(-1-3r+2k)2 = 0 \quad \text{bzw.} \quad -7+21k-26r = 0 .$$

Die Auflösung nach k ergibt:

$$k = \frac{1}{3} + \frac{26}{21} \cdot r .$$

Trägt man nun diese Darstellung in (20) ein, so findet man für den gesuchten Abstand der Trägergeraden von G_r zum Nullpunkt:

$$\begin{aligned} L^2(G_r) &= \Big(\frac{10}{3} + \frac{26}{21} \cdot r\Big)^2 + \Big(\frac{2}{3} + \frac{1}{21} \cdot r\Big)^2 + \Big(-\frac{1}{3} - \frac{11}{21} \cdot r\Big)^2 \\ &= \frac{1}{21} \cdot (245 + 182r + 38r^2) > \frac{4r^2}{21}, \end{aligned}$$

also

$$L(G_r) > \frac{2|r|}{\sqrt{21}} \quad (r \in \mathbb{Z}) . \tag{21}$$

Die bisherigen Untersuchungen, die zur Ungleichung (21) führten, werden für das folgende Argument benötigt, das den Kerngedanken des Beweises darstellt. Es sind nämlich die Eckpunkte $(\pm m, \pm m, \pm m)$ des dreidimensionalen Würfels W_m gerade diejenigen Punkte des Würfels, die den größten euklidischen Abstand zum Nullpunkt haben. Dieser Abstand ist genau $m \cdot \sqrt{3}$. Wenn nun der Abstand der Eckpunkte des Würfels W_m immer noch geringer ausfällt als der Abstand der Trägergeraden von G_r zum Nullpunkt, so kann erst recht kein Gitterpunkt von G_r im Inneren oder auf der Oberfläche des Würfels W_m liegen. Wir haben also

$$G_r \cap W_m = \emptyset , \quad \text{falls} \quad \frac{2|r|}{\sqrt{21}} > m \cdot \sqrt{3} .$$

Das bedeutet, daß *höchstens* für alle ganzen Zahlen r, die

$$|r| \leq \frac{3\sqrt{7}}{2} \cdot m$$

genügen, das Gitter G_r den Würfel W_m schneidet. Diese Bedingung ist somit für höchstens

$$\left(1 + 3\sqrt{7} \cdot m\right) \quad \text{ganze Zahlen } r \text{ erfüllt}.$$

Aus (19) wissen wir zudem, daß es zu jedem solchen r-Wert höchstens

$$\left(1 + \frac{m}{2}\right) \quad \text{ganze Zahlen } k \text{ gibt},$$

die auf $G_r \cap W_m \neq \emptyset$ schließen lassen. Insgesamt gibt es also höchstens

$$\left(1 + \frac{m}{2}\right) \cdot \left(1 + 3\sqrt{7} \cdot m\right) \quad \text{Tupel } (k, r),$$

und folglich höchstens ebenso viele Punkte des Gitters G, die auch in W_m liegen. Man rechnet nach, daß für $m \geq 270$ dieses Produkt nach oben durch $4m^2$ abgeschätzt werden kann. Wir haben hier ausgenutzt, daß das zweidimensionale Gitter G aus den eindimensionalen Gittern G_r entsteht, indem r alle ganzen Zahlen durchläuft. Genauer ist

$$G = \bigcup_{-\infty < r < +\infty} G_r \,;$$

und wegen der linearen Unabhängigkeit der Vektoren $\vec{a}_1$ und $\vec{a}_2$ ist diese Vereinigung sogar disjunkt.

Eine untere Schranke für $A = |G \cap W_m|$ entnimmt man aus Satz 1, wo man im Beweis hier $d = 2$, $C_1 = 5$, $m_1 = 8$, $m_0 = \max\{8; 21\} = 21$ und $C = 1/20^2$ setzen kann. Damit ist insgesamt bewiesen:

Satz 2 *Für das Lösungsgitter G der diophantischen Gleichung* (1) *und den Würfel W_m gelten:*

$$\frac{m^2}{400} \leq |G \cap W_m| \leq 4m^2, \qquad \textit{falls } \ m \geq 270 \ \textit{ist}.$$

Es bleibt dem interessierten Leser unbenommen, durch einen anderen Ansatz oder feinere Abschätzungen die Konstanten 1/400 und 4 zu verbessern. Für das folgende Korollar ist jedoch allein die Größenordnung m^2 von A ausschlaggebend.

Korollar 1

$$\lim_{m \to \infty} \frac{\log |G \cap W_m|}{\log m} = 2\,.$$

4 Eine geschlossen-algebraische Darstellung von A

Wir kommen nun auf die am Schluß des zweiten Abschnitts angekündigte geschlossene Darstellung der Lösungsanzahl A zurück, die im folgenden mit algebraischen Methoden allein aus (13) und (15) hergeleitet wird. Es muß allerdings zuvor darauf hingewiesen werden, daß bei dieser Formel allein die *Existenz* im Vordergrund steht; zur praktischen Berechnung von A eignet sie sich wegen der Größe der vorkommenden Objekte (Matrizen und Summen) nicht! Zur konkreten Berechnung von A ist oben im zweiten Abschnitt alles gesagt worden. Es ist allein die Ästhetik des algebraischen Formalismus, die eine so unzugängliche Größe wie die Lösungsanzahl einer diophantischen Gleichung erschließt.

Während in (11) eine Integration die gesuchte Größe A aus der rechten Seite von (13) herausfiltert, gelingt dasselbe auch durch mehrfaches Ableiten! Die Grundidee ist ziemlich einfach: Man leitet die Gleichung (13) hinreichend oft nach α ab und bringt in jeder Ableitung dann α zum Verschwinden. So entstehen viele lineare Gleichungen in den Koeffizienten $c_2, c_4, \ldots$, wobei man die k-te Ableitung der linken Seite von (13) an der Stelle $\alpha = 0$ elegant mit Hilfe der verallgemeinerten Leibnizschen Ableitungsregel ausdrücken kann. So entsteht ein lineares inhomogenes quadratisches Gleichungssystem, das sich als eindeutig lösbar erweisen wird. Kennt man die Lösung $c_2, c_4, \ldots$ dieses Systems, so bekommt man mit (15) über die Summe der Lösungskomponenten sofort die gesuchte explizite algebraische Darstellung. Auf dem Weg zu diesem Ziel werden wir allerdings mit einigen Überraschungen konfrontiert.

Zunächst wird die Abkürzung

$$L := 2m(a_1 + a_2 + \cdots + a_n) + 2b \tag{22}$$

eingeführt. Wir werden mehrfach ausnutzen, daß L eine *gerade Zahl* ist. Weiter sei

$$V(\alpha) := \cos(2\pi b\alpha) \cdot \prod_{\nu=1}^{n} \Big(1 + 2 \cdot \sum_{k_\nu=1}^{m} \cos(2\pi a_\nu k_\nu \alpha)\Big) \qquad (\alpha \in \mathbb{R})\,. \tag{23}$$

Wegen $V(-\alpha) = V(\alpha)$ ist V eine gerade Funktion in α. Somit verschwindet $V^{(k)}(0)$ für jede ungerade Ableitungsordnung k. Daher interessieren wir uns im folgenden ausschließlich für alle *geraden Ableitungsordnungen* $k = 2, 4, 6, \ldots, L$. Wegen (13) hat man so:

$$V^{(k)}(\alpha) = \sum_{\substack{\mu=0 \\ 2|\mu}}^{L} (-1)^{k/2} \pi^k \mu^k c_\mu \cdot \cos(\pi\mu\alpha)\,,$$

und daher ist

$$\sum_{\substack{\mu=0 \\ 2|\mu}}^{L} \mu^k \cdot c_\mu = (-1)^{k/2} \cdot \frac{V^{(k)}(0)}{\pi^k} \qquad (k = 2, 4, 6, \ldots, L)\,. \tag{24}$$

Diese $L/2$ Gleichungen fassen wir als ein lineares inhomogenes Gleichungssystem in den $L/2$ Unbekannten $c_2, c_4, \ldots, c_L$ auf und klären zunächst die Frage der Lösbarkeit.

Hierzu wird die Koeffizientenmatrix

$$\mathcal{A} := \begin{pmatrix} 2^2 & 4^2 & 6^2 & \dots & L^2 \\ 2^4 & 4^4 & 6^4 & \dots & L^4 \\ \vdots & & & \vdots & \\ 2^L & 4^L & 6^L & \dots & L^L \end{pmatrix}$$

eingeführt, mit der das Gleichungssystem in (24) auch als Matrix-Vektorgleichung ausgedrückt werden kann:

$$\mathcal{A} \cdot \begin{pmatrix} c_2 \\ c_4 \\ \vdots \\ c_L \end{pmatrix} = \begin{pmatrix} d_2 \\ d_4 \\ \vdots \\ d_L \end{pmatrix} \quad \text{bzw.} \quad \mathcal{A} \cdot \vec{c} = \vec{d}. \tag{25}$$

Dabei stehen die Komponenten des Vektors $\vec{d}$ gemäß (24) für

$$d_k := (-1)^{k/2} \cdot \frac{V^{(k)}(0)}{\pi^k} \qquad (k = 2, 4, 6, \dots, L). \tag{26}$$

Nach den bekannten Determinantengesetzen hat man nun

$$\begin{aligned} \det \mathcal{A} &= 2^2 \cdot 4^2 \cdot 6^2 \cdot \ldots \cdot L^2 \cdot \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 2^2 & 4^2 & 6^2 & \dots & L^2 \\ \vdots & & & \vdots & \\ 2^{L-2} & 4^{L-2} & 6^{L-2} & \dots & L^{L-2} \end{pmatrix} \\ &= 2^L \cdot \left(\frac{L}{2}\right)! \cdot \left(\frac{L}{2}\right)! \cdot \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 4 & 16 & 36 & \dots & (L^2)^1 \\ 4^2 & 16^2 & 36^2 & \dots & (L^2)^2 \\ \vdots & & & \vdots & \\ 4^{L/2-1} & 16^{L/2-1} & 36^{L/2-1} & \dots & (L^2)^{L/2-1} \end{pmatrix}. \end{aligned}$$

Dies ist eine Vandermonde-Determinante, die offensichtlich nicht verschwindet. Damit ist das lineare Gleichungssystem in (25) eindeutig lösbar. Da in der zweiten Zeile dieser Determinante genau alle Zahlen $(2k)^2$ für $k = 1, 2, 3, \dots, L/2$ vorkommen, kann der Wert der Determinante ausgerechnet werden. Wir überlassen es dem Leser, das Resultat

$$\det \mathcal{A} = \left(\frac{L}{2}\right)! \cdot \left(\frac{L}{2}\right)! \cdot 2^{\frac{L}{2}(\frac{L}{2}+1)} \cdot 1! \cdot 3! \cdot 5! \cdot \ldots \cdot (L-1)!$$

nachzurechnen; benötigen werden wir es im folgenden nicht! Es existiert jedenfalls die inverse Matrix $\mathcal{A}^{-1}$. Hiermit können wir die Gleichung (25) formal nach dem Vektor $\vec{c}$ auflösen:

$$\vec{c} = \mathcal{A}^{-1}\vec{d}.$$

Mit (15) erhalten wir so eine *erste Darstellung* der Lösungsanzahl A:

$$A = (2m+1)^n - \sum_{\substack{\mu=2 \\ 2|\mu}}^{L} c_\mu = M^n - \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \cdot \begin{pmatrix} c_2 \\ \vdots \\ c_L \end{pmatrix} = M^n - \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \cdot \left(\mathcal{A}^{-1}\vec{d}\right). \quad (27)$$

Hier haben wir wieder die Abkürzung $M = 2m + 1$ verwendet. Die Summe über die Lösungskomponenten c_μ wurde mit Hilfe des Skalarprodukts ausgedrückt.

Für eine *zweite Darstellung* von A definieren wir zunächst den Vektor $\vec{x}$ als die (eindeutige) Lösung des linearen Gleichungssystems

$$\mathcal{A}^T \cdot \vec{x} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}. \quad (28)$$

Da bei einer regulären Matrix die Reihenfolge beim Invertieren und Transponieren vertauscht werden darf, erhalten wir folgende Auflösung nach dem Vektor $\vec{x} = (x_2, x_4, \ldots, x_L)^T$:

$$\vec{x} = \left(\mathcal{A}^T\right)^{-1} \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \left(\mathcal{A}^{-1}\right)^T \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Hieraus liest man ab, daß die μ-te Koordinate $x_{2\mu}$ des Vektors $\vec{x}$ identisch ist mit der Summe über die Elemente des μ-ten *Spaltenvektors* der Matrix $\mathcal{A}^{-1}$. Indem man die Matrix-Vektormultiplikation für $\vec{c}$ in $\mathcal{A}^{-1}\vec{d}$ explizit mit den Komponenten $d_2, d_4, \ldots, d_L$ des Vektors $\vec{d}$ ausführt und bei der anschließenden Summation über alle Komponenten des so entstandenen Vektors $\vec{c}$ nach allen Termen mit demselben Faktor $d_{2\mu}$ sortiert, sieht man die Identität

$$c_2 + c_4 + c_6 + \cdots + c_L = \vec{x} \cdot \vec{d}$$

ein. Damit ist bewiesen:

$$A = M^n - \vec{x} \cdot \vec{d} = M^n - \sum_{\substack{\mu=2 \\ 2|\mu}}^{L} x_\mu d_\mu. \quad (29)$$

Nach dieser algebraischen Vorarbeit müssen nun noch die Zahlen $d_2, d_4, \ldots, d_L$ aus (26) eingehend untersucht werden. Hierfür wird zuerst die Funktion $V(\alpha)$ aus (23) mit der verallgemeinerten Leibnizschen Ableitungsregel k-mal nach α differenziert. Dadurch ergibt sich

$$V^{(k)}(\alpha) = \sum_{\substack{r_1+\cdots+r_{n+1}=k \\ 0\le r_1,\ldots,r_{n+1}\le k}} \binom{k}{r_1, r_2, \ldots, r_{n+1}} \cdot \prod_{\nu=1}^{n} \left[1 + 2 \cdot \sum_{k_\nu=1}^{m} \cos(2\pi a_\nu k_\nu \alpha)\right]^{(r_\nu)} \cdot \left[\cos(2\pi b\alpha)\right]^{(r_{n+1})}.$$

Erklärt man die Funktion $\varepsilon(r)$ für alle ganzen Zahlen $r \geq 0$ durch $\varepsilon(r) := 0$ für $r > 0$ und $\varepsilon(0) := 1$, so erhält man nach der Ableitung der trigonometrischen Terme für jedes gerade k an der Stelle $\alpha = 0$:

$$
\begin{aligned}
V^{(k)}(0) = & \sum_{\substack{r_1+\cdots+r_{n+1}=k \\ 0\leq r_1,\ldots,r_{n+1}\leq k \\ 2|r_1,\ldots,2|r_{n+1}}} \binom{k}{r_1, r_2, \ldots, r_{n+1}} \\
& \cdot \prod_{\nu=1}^{n} \left(\varepsilon(r_\nu) + 2 \cdot (-1)^{\frac{r_\nu}{2}} \cdot (2\pi a_\nu)^{r_\nu} \cdot \sum_{k_\nu=1}^{m} k_\nu{}^{r_\nu} \right) \cdot (-1)^{\frac{r_{n+1}}{2}} \cdot (2\pi b)^{r_{n+1}} .
\end{aligned}
\tag{30}
$$

Es wird nun der Term hinter dem Produktzeichen eingehend untersucht. Zuerst unterscheidet man die Fälle $r_\nu = 0$ und $r_\nu > 0$ und spaltet dementsprechend das Produkt auf. Weiterhin können die Summen $\sum k_\nu{}^{r_\nu}$ mit Hilfe der *Bernoulli-Polynome* ausgedrückt werden:

$$
\sum_{k_\nu=1}^{m} k_\nu{}^{r_\nu} = \frac{B_{1+r_\nu}(1+m)}{1+r_\nu} ,
$$

wobei bekanntermaßen die Bernoulli-Polynome durch

$$
B_q(x) := \sum_{\rho=0}^{q} B_\rho \cdot \binom{q}{\rho} \cdot x^{q-\rho} \qquad (q = 0, 1, 2, \ldots ; x \in \mathbb{R})
$$

mit den *Bernoulli-Zahlen*

$$
B_0 = 1 \,,\; B_1 = -\frac{1}{2} \,,\; B_2 = \frac{1}{6} \,,\; B_3 = B_5 = B_7 = \cdots = 0 \,,\; B_4 = -\frac{1}{30} \,,\; B_6 = \frac{1}{42} \,, \ldots
$$

erklärt sind. Die Bernoulli-Zahlen lassen sich wiederum schrittweise aus der Rekursionsformel

$$
B_0 := 1 \;, \quad \sum_{\rho=0}^{q-1} B_\rho \cdot \binom{q}{\rho} = 0 \qquad (q \geq 2)
$$

berechnen. Eine umfassende Darstellung der Bernoulli-Polynome und Bernoulli-Zahlen findet man im ersten Kapitel in [10]. Insgesamt kann man das Produkt rechts in (30) so folgendermaßen umformen:

$$
\begin{aligned}
\prod_{\nu=1}^{n} (\ldots) &= \prod_{\substack{\nu=1 \\ r_\nu=0}}^{n} (\ldots) \cdot \prod_{\substack{\nu=1 \\ r_\nu>0}}^{n} (\ldots) \\
&= \left(\prod_{\substack{\nu=1 \\ r_\nu=0}}^{n} (1+2m) \right) \cdot (-1)^{\frac{k}{2}} \cdot (2\pi)^k \cdot b^{r_{n+1}} \cdot \prod_{\substack{\nu=1 \\ r_\nu>0}}^{n} \left(2a_\nu^{r_\nu} \cdot \frac{B_{1+r_\nu}(1+m)}{1+r_\nu} \right) .
\end{aligned}
$$

Hierin wurde unter dem zweiten Produktzeichen mit der Forderung $r_\nu > 0$ auch die Randbedingung $r_1 + r_2 + \cdots + r_{n+1} = k$ ausgenutzt. Die in (26) eingeführten Zahlen $d_2, d_4, \ldots, d_L$ können nun unter Einbeziehung von (30) folgendermaßen dargestellt werden:

$$
\begin{aligned}
d_k = 2^k \cdot & \sum_{\substack{r_1+\cdots+r_{n+1}=k \\ 0\le r_1,\ldots,r_{n+1}\le k \\ 2|r_1,\ldots,2|r_{n+1}}} \binom{k}{r_1, r_2, \ldots, r_{n+1}} \cdot b^{r_{n+1}} \\
& \cdot \Big(\prod_{\substack{\nu=1 \\ r_\nu=0}}^{n} (1+2m) \Big) \cdot \prod_{\substack{\nu=1 \\ r_\nu>0}}^{n} \Big(2a_\nu^{r_\nu} \cdot \frac{B_{1+r_\nu}(1+m)}{1+r_\nu} \Big) .
\end{aligned}
\tag{31}
$$

Diese Größen d_k hängen also insgesamt neben k auch von $n, m, a_1, \ldots, a_n$ und b ab. Wir notieren sie nun als Werte gewisser Polynome in $n+2$ Variablen:

$$
\begin{aligned}
& H_{n,k}(t_1, t_2, \ldots, t_n; t_{n+1}, t_{n+2}) := \\
& 2^k \cdot \sum_{\substack{r_1+\cdots+r_{n+1}=k \\ 0\le r_1,\ldots,r_{n+1}\le k \\ 2|r_1,\ldots,2|r_{n+1}}} \binom{k}{r_1, r_2, \ldots, r_{n+1}} \cdot t_{n+1}^{r_{n+1}} \\
& \cdot \Big(\prod_{\substack{\nu=1 \\ r_\nu=0}}^{n} (2t_{n+2}-1) \Big) \cdot \prod_{\substack{\nu=1 \\ r_\nu>0}}^{n} \Big(2t_\nu^{r_\nu} \cdot \frac{B_{1+r_\nu}(t_{n+2})}{1+r_\nu} \Big) .
\end{aligned}
\tag{32}
$$

Wegen (31) ist dann offensichtlich

$$
d_k = H_{n,k}(a_1, a_2, \ldots, a_n; b, 1+m) . \tag{33}
$$

Die Polynome $H_{n,k}$ sind in den Variablen $t_1, t_2, \ldots, t_{n+1}$ *homogen vom Grad* k, d.h. es besteht für jedes t_{n+2} und jede reelle Zahl λ die Identität

$$
H_{n,k}(\lambda t_1, \lambda t_2, \ldots, \lambda t_n; \lambda t_{n+1}, t_{n+2}) = \lambda^k \cdot H_{n,k}(t_1, t_2, \ldots, t_n; t_{n+1}, t_{n+2}) .
$$

Wir fassen nun die bisherigen Resultate sowie die Identitäten aus (27), (29) und (33) zusammen.

Satz 3 *Zu jeder natürlichen Zahl n gibt es eine unendliche Folge*

$$
\big(H_{n,k}(t_1, t_2, \ldots, t_{n+2})\big)_{k=2,4,6,\ldots}
$$

explizit berechenbarer Polynome mit rationalen Koeffizienten, mit denen die Lösungsanzahl einer linearen diophantischen Gleichung in n Unbekannten explizit ausgedrückt werden kann:

Sind $a_1, a_2, \ldots, a_n, b$ und m natürliche Zahlen, so ist die Anzahl A der ganzzahligen Lösungen $x_1, x_2, \ldots, x_n$ der linearen diophantischen Gleichung $a_1x_1 + a_2x_2 + \cdots + a_nx_n =$

b unter der Nebenbedingung $|x_\nu| \le m$ für $\nu = 1, 2, \ldots, n$ auf jede der beiden folgenden Weisen darstellbar:

(i)
$$A = (1+2m)^n - \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \cdot \left[\mathscr{A}^{-1} \cdot \begin{pmatrix} H_{n,2}(a_1, \ldots, a_n\,;\, b, 1+m) \\ \vdots \\ H_{n,L}(a_1, \ldots, a_n\,;\, b, 1+m) \end{pmatrix} \right].$$

Hierbei ist $L := 2m(a_1 + a_2 + \cdots + a_n) + 2b$, und die Elemente der Matrix

$$\mathscr{A} := \begin{pmatrix} 2^2 & 4^2 & 6^2 & \ldots & L^2 \\ 2^4 & 4^4 & 6^4 & \ldots & L^4 \\ \vdots & & & \vdots & \\ 2^L & 4^L & 6^L & \ldots & L^L \end{pmatrix}$$

hängen nur von L ab.

(ii)
$$A = (1+2m)^n - \sum_{\substack{\mu=2 \\ 2|\mu}}^{L} x_\mu \cdot H_{n,\mu}(a_1, \ldots, a_n\,;\, b, 1+m).$$

Hierin sind die natürlichen Zahlen $x_2, x_4, \ldots, x_L$ die Komponenten der eindeutigen Lösung des linearen Gleichungssystems

$$\mathscr{A}^T \cdot \begin{pmatrix} x_2 \\ \vdots \\ x_L \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Für die $(n =)$ 3 Gewichtsklassen an der Balkenwaage, wie sie in der Einleitung verwendet wurden, erhält man beispielsweise für $k = 2$ und $k = 4$ die beiden Polynome

$$H_{3,2}(t_1, \ldots, t_5) = \frac{8}{3}(2t_5 - 1)^2(t_1^2 + t_2^2 + t_3^2)B_3(t_5) + 4(2t_5 - 1)^3 t_4^2$$

und

$$\begin{aligned} &H_{3,4}(t_1, \ldots, t_5) = \\ &\frac{32}{5}(2t_5 - 1)^2(t_1^4 + t_2^4 + t_3^4)B_5(t_5) + 16(2t_5 - 1)^3 t_4^4 + 64(2t_5 - 1)^2 t_4^2(t_1^2 + t_2^2 + t_3^2)B_3(t_5) \\ &\qquad + \frac{128}{3}(2t_5 - 1)(t_1^2 t_2^2 + t_1^2 t_3^2 + t_2^2 t_3^2)B_3^2(t_5). \end{aligned}$$

Die hierin verwendeten Bernoulli-Polynome sind

$$B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x \quad \text{und} \quad B_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x.$$

5 Schlußbemerkungen und Literaturverweise

Die Lösungsanzahl einer *beliebigen* diophantischen Gleichung kann normalerweise nicht geschlossen ausgedrückt werden, schon gar nicht durch einen algebraischen Term. Insofern hat das Resultat in Satz 3 seine besondere Bedeutung, wenn es sich auch nicht für praktische Berechnungen eignet. Zum Vergleich mit derartigen Resultaten sollen Satz 3 die Lösungsanzahlen zu einigen diophantischen Gleichungen gegenübergestellt werden.

1.) Nach dem *Vier-Quadrate-Satz* von Lagrange ist jede natürliche Zahl b als Summe von vier Quadraten ganzer Zahlen darstellbar; die Gleichung

$$b = w^2 + x^2 + y^2 + z^2 \tag{34}$$

besitzt also Lösungen $w, x, y, z \in \mathbb{Z}$. Mittels *Theta-Reihen* kann man die Lösungsanzahl bestimmen:

> *Die natürliche Zahl b ist so oft als Summe von vier Quadraten ganzer Zahlen darstellbar, als das 8-fache der Summe derjenigen positiven Teiler von b beträgt, die nicht durch 4 teilbar sind.*

Für $w, x, y, z \in \{-1, 0, 1\}$ findet man so beispielsweise die $8(1+3) = 32$ Darstellungen von 3, in der immer genau ein Summand verschwindet. Da hier in (34) die Lösungsanzahl beschränkt ist, erübrigen sich zunächst weitere Einschränkungen an w, x, y und z. Das zitierte Ergebnis über die Lösungsanzahl in (34) findet man in [5, S. 163ff.]; schränkt man die Zahlen w, x, y und z noch auf eine Restklasse ein, kann man über die Lösbarkeit einiges in [6] nachlesen. Weitere Resultate zur Darstellbarkeit mit Quadraten findet man in [8].

2.) Ist D eine natürliche Zahl, die keine Quadratzahl $1, 4, 9, \ldots$ darstellt, so ist die sog. *Pellsche Gleichung*

$$x^2 - Dy^2 = 1 \tag{35}$$

immer durch unendlich viele Paare ganzer Zahlen x und y lösbar. Diese Gitterpunkte liegen dann auf den in (35) definierten Hyperbelästen. Der Einfachheit halber betrachten wir jetzt nur positive Lösungen x und y. Kennt man die Lösung x_1, y_1, die dem Nullpunkt im ersten Quadranten am nächsten liegt, so kann man alle weiteren Lösungspaare x_n, y_n mit dem Ansatz

$$x_n + \sqrt{D}y_n = \left(x_1 + \sqrt{D}y_1\right)^n \qquad (n \geq 1)$$

bestimmen, indem man die rechte Seite ausmultipliziert und nach rationalen und irrationalen Termen sortiert. Die irrationalen Terme sind alle ganzzahlige Vielfache von $\sqrt{D}$. Man kann aber keine allgemeingültige Aussage treffen, wo die kleinste Lösung x_1, y_1 liegt. Insofern kennt man auch keinen geschlossenen Ausdruck für die Lösungsanzahl in einem gewissen Bereich.

Die später nach Pell benannte Gleichung (35) hat eine bis in die Antike auf Archimedes und Eratosthenes zurückgehende Geschichte. Es sei hier nur noch angemerkt, daß die Lösungen x_n, y_n von (35) eng mit den rationalen Näherungen von $\sqrt{D}$ zusammenhängen.

Über diese Näherungen weiß man aus der Kettenbruchtheorie einiges. Wir verweisen auf [9] und [5]. P. Bundschuh schreibt in seinem Buch auf Seite 184 auch einiges zur Geschichte der Pellschen Gleichung.

3.) Aus dem *Goldbach-Problemkreis:*
Vinogradov bewies 1937 (im Anschluß an Vorarbeiten von Hardy und Littlewood), daß jede hinreichend große ungerade natürliche Zahl b als Summe von drei Primzahlen darstellbar ist. Für die Anzahl der Darstellungen gilt (siehe z.B. [13, Theorem 3.4, S. 32]; man beachte hierbei auch die Formeln (3.5) und (3.15) in [13]):

$$\begin{aligned} &|\{(p_1,p_2,p_3)\in\mathbb{P}^3 : b = p_1+p_2+p_3\}| \\ &\sim \frac{b^2}{2\log^3 b}\cdot \prod_{b\not\equiv 0 \bmod p}\left(1+\frac{1}{(p-1)^3}\right)\cdot \prod_{b\equiv 0 \bmod p}\left(1-\frac{1}{(p-1)^2}\right). \end{aligned}$$

Die Produkte rechts erstrecken sich jeweils über alle Primzahlen p, die b nicht teilen bzw. teilen. Das Symbol $\sim$ drückt aus, daß der Quotient der linken und rechten Seite für wachsendes ungerades b gegen 1 konvergiert. Dies ist also nur eine *asymptotische Formel* für die Lösungsanzahl, worauf man sich bei vielen diophantischen Gleichungen beschränken muss. So findet man beispielsweise in Verallgemeinerung des Lagrangeschen Vier-Quadrate-Satzes in [13, Theorem 2.2, S. 18] auch eine asymptotische Formel für die Anzahl der Darstellungen aller hinreichend großen natürlichen Zahlen als eine Summe von g natürlichen Zahlen, die ihrerseits wiederum k-te Potenzen natürlicher Zahlen sind. Hier berührt man den *Waringschen Problemkreis.*

Ergänzend zum Darstellungsproblem mit Primzahlen muß die noch unentschiedene Goldbach-Vermutung erwähnt werden, nach der jede gerade Zahl oberhalb 2 die Summe von zwei Primzahlen sein soll.

4.) In der analytischen Zahlentheorie, speziell in der Theorie transzendenter Zahlen, spielen lineare, *homogene* diophantische Gleichungssysteme eine enorm wichtige Rolle. Man ist hier aber nicht an der Lösungsanzahl innerhalb eines gewissen Bereichs des Lösungsgitters interessiert, sondern an möglichst kleinen, *nichttrivialen* Lösungen. Diese werden durch das berühmte *Siegelsche Lemma* garantiert ([11, Hilfssatz 27], oder: [5, S. 273ff.], wo das Siegelsche Lemma in allgemeinerer Fassung für ganzalgebraische Koeffizienten bewiesen wird). Das Siegelsche Lemma wird sowohl für den *Satz von Gel'fond-Schneider* ([5, Kap. 6, §5]) über die Transzendenz von Zahlen der Gestalt α^β (mit algebraischen Größen α,β) als auch für A. Bakers berühmte *Abschätzungen für Linearformen in Logarithmen* ([1, Kap. 2, 3]) verwendet; die letztgenannten Arbeiten von Baker wurden mit der Fields-Medaille ausgezeichnet. Man sollte also die Bedeutung linearer diophantischer Gleichungen nicht unterschätzen.

Bombieri und Vaaler haben in [2] sogar kleine Basen linearer, homogener diophantischer Gleichungssysteme gefunden (Theorem 2, S. 12). Eine weitere Abschätzung der Lösungsanzahl einer einzigen inhomogenen, linearen diophantischen Gleichung mit ganzen, positiven Koeffizienten für *ganze, nichtnegative Lösungen* wird in [12, Lemma 3.1] angegeben. Der Beweis dieses Lemmas ist wieder elementar und benutzt das Verfahren der vollständigen Induktion.

Bei linearen, *inhomogenen* diophantischen Systemen bestehend aus m Gleichungen in n Unbekannten können ganzzahlige Lösungen, falls das System überhaupt lösbar ist, nur in der Größenordnung des größten m-reihigen Minors aus der um die Inhomogenität als $(n+1)$-te Spalte erweiterten Koeffizientenmatrix garantiert werden. Hierzu haben Borosh, Treybig und andere zwei Problemtypen behandelt:

i) Ein lineares inhomogenes System besitze eine ganzzahlige Lösung mit nicht verschwindenden Komponenten. Gibt es dann auch eine kleine Lösung?

ii) Für ein lineares inhomogenes System sei die Existenz einer nichttrivialen Lösung mit nichtnegativen Komponenten vorausgesetzt. Gibt es dann auch eine ebensolche, zusätzlich aber kleine Lösung?

Diese Probleme werden in [3] und [4] behandelt. Eine Übersicht über diesen Fragenkreis findet man in [7]. Diese Ergebnisse finden ihre Anwendung bei der sogenannten ganzzahligen Optimierung.

Literatur

[1] Baker, A.: *Transcendental Number Theory.* Cambridge University Press, 1975.

[2] Bombieri, E.; Vaaler, J.: On Siegel's Lemma. *Inventiones Mathematicae* 73 (1983), 11–32.

[3] Borosh, I.; Flahive, M.; Treybig, B.: Small solutions of linear diophantine equations. *Discrete Math.* 58 (1986), 215–220.

[4] Borosh, I.; Flahive, M.; Rubin, D.; Treybig, B.: A sharp bound for solutions of linear diophantine equations. *Proc. Amer. Math. Soc.* 105 (1989) 4, 844–846.

[5] Bundschuh, P.: *Einführung in die Zahlentheorie.* 2. Auflage, Springer-Verlag, 1992.

[6] Elsner, C.: On the Representation of Integers by Sums of Squares with Terms from an Arithmetic Progression. *Nieuw Archief voor Wiskunde* 17 (1999) 3, 331–341.

[7] Flahive, M.E.: Integral solutions of linear systems. *Proc. Int. Number Theory*, Laval, July 5–18, 1987, 213–219.

[8] Grosswald, E.: *Representation of Integers as Sums of Squares.* Springer-Verlag, Berlin-Göttingen-Heidelberg-New York 1985.

[9] Perron, O.: *Die Lehre von den Kettenbrüchen.* Teubner, Leipzig-Berlin 1929, (3. Auflage, Bände I, II, Teubner, Stuttgart 1954, 1957).

[10] Rademacher, H.: *Topics in Analytic Number Theory.* Springer-Verlag, Berlin-Heidelberg-New York 1973.

[11] Schneider, Th.: *Einführung in die transzendenten Zahlen.* Springer-Verlag, Berlin-Göttingen-Heidelberg 1957.

[12] Schwarz, W.: Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen I. *J. Reine Angew. Math.* 205 (1960), 21–47.

[13] Vaughan, R.C.: *The Hardy-Littlewood Method.* Cambridge University Press, 1981.

Carsten Elsner
Institut für Mathematik
Universität Hannover
Welfengarten 1
D-30167 Hannover, Deutschland
e-mail: elsner@math.uni-hannover.de