Elemente der Mathematik 79 (2024), 98–108
DOI 10.4171/EM/506

Geometrie der Zahlen

D. Kotschick

D. Kotschick wurde 1989 in Oxford promoviert. Nach Stellen in Cambridge und Princeton wurde er 1991 auf ein Ordinariat an der Universität Basel und 1998 auf den Lehrstuhl für Differentialgeometrie an der LMU München berufen. Seine Forschungsinteressen liegen in der Geometrie und Topologie.

Der Titel dieses Vortrags ist der Titel eines berühmten Buches von Hermann Minkowski [6], dessen erster Teil 1896 erschien und das 1910 posthum erstmals vollständig publiziert wurde. Minkowski selbst hat das Thema charakterisiert als einen Zugang zur Zahlentheorie, der sich auf die geometrische Anschauung stützt. Anders gesagt wird die Intuition, die jedermann für elementare geometrische Sachverhalte in der Ebene hat, nutzbar gemacht um algebraische Zusammenhänge sichtbar zu machen.

Die Wurzeln der Geometrie der Zahlen liegen schon vor Minkowski in den Arbeiten von Gauss, Dirichlet und anderen. Minkowski selbst wurde dazu geführt durch seine Betrachtungen zu quadratischen Formen, die er als 17-jähriger Student anstellte, um eine Preisaufgabe der Pariser Akademie zu bearbeiten. Er hat diese Betrachtungen später verallgemeinert und abstrahiert und hat ausser der *Geometrie der Zahlen* [6] ein zweites Buch [5] dazu geschrieben, mit dem Titel *Diophantische Approximationen*. Das Gebiet wurde nach Minkowski von vielen anderen Mathematikern weiterentwickelt, u. a. von H. F. Blichfeldt, J. W. S. Cassels, J. G. van der Corput, E. Hlawka, C. G. Lekkerkerker,

Die Geometrie der Zahlen geht bis in die antike Mathematik zurück, denn sicherlich ist die Entdeckung der Inkommensurabilität der Diagonale eines Quadrates mit seiner Seitenlänge, also die Irrationalität von $\sqrt{2}$, ihr erster Meilenstein. In der modernen Mathematik tritt sie seit Gauss und seinen Arbeiten zum Kreisproblem immer wieder auf. Der Name wurde schliesslich von Minkowski geprägt und popularisiert. Der Minkowskische Gitterpunktsatz ist das Aushängeschild der Geometrie der Zahlen schlechthin, aber es sind nach dem Gitterpunktsatz viele neue Dinge in der Geometrie der Zahlen ans Licht gekommen, nicht zuletzt Beziehungen zu anderen Zweigen der Mathematik von der Kombinatorik bis zur Funktionalanalysis. Der Autor des vorliegenden Artikels gibt eine elementare Einführung in die Geometrie der Zahlen in der Ebene. Als illustrative Anwendungen werden der Dirichletsche Approximationssatz und der Zwei-Quadrate-Satz von Fermat und Euler bewiesen.

K. Mahler, L. J. Mordell und C. L. Siegel. Inzwischen ist die Geometrie der Zahlen ein eigenes, reifes, mathematisches Gebiet, das nicht mehr nur ein besonderer Zugang zur Zahlentheorie ist, sondern auch vielfältige Beziehungen zu anderen Gebieten der Mathematik hat. Moderne Darstellungen und Entwicklungen die erst nach Minkowski entstanden sind, sind z. B. in den Büchern von Cassels [3] und Lekkerkerker [4] enthalten.

Mein Ziel ist es hier, einen Einblick in die Geometrie der Zahlen zu geben, der keine Vorkenntnisse in höherer Mathematik voraussetzt. Alles soll schon für Schüler in den mittleren Jahren des Gymnasiums verständlich sein. Aus diesem Grund beschränke ich mich darauf, die Grundideen nur in der Ebene und nicht in höheren Dimensionen zu präsentieren. Als illustrative Anwendungen beweise ich den Dirichletschen Approximationssatz und den Zwei-Quadrate-Satz von Fermat und Euler.

1 Gitterpunkte und Flächeninhalte

In der Ebene $\mathbb{R}^2$ hat jeder Punkt zwei Koordinaten, und die Punkte mit ganzzahligen Koordinaten bilden das Gitter $\mathbb{Z}^2 \subset \mathbb{R}^2$. Wir betrachten Teilmengen $K \subset \mathbb{R}^2$, die regulär genug sind, um einen wohl-definierten Flächeninhalt $A(K)$ zu haben, also sogenannte messbare Mengen. In unseren Anwendungen wird K immer eine Kreisscheibe oder ein Parallelogramm sein, so dass die Messbarkeit klar ist. Es war mindestens seit Gauss bekannt, dass es Zusammenhänge zwischen der Anzahl Gitterpunkte in K und dem Flächeninhalt $A(K)$ gibt, zumindest wenn K eine Kreisscheibe ist, oder sonst eine einfache Form hat.

Die folgende einfache Aussage zu so einem Zusammenhang wurde von Blichfeldt erstmals im Rahmen der Geometrie der Zahlen explizit hingeschrieben. Sie betrifft zunächst nicht Gitterpunkte in K, sondern Paare von Punkten, die sich um einen Gitterpunkt unterscheiden.

Blichfeldt Lemma. *Falls $K \subset \mathbb{R}^2$ Flächeninhalt $A(K) > 1$ hat, so enthält K zwei verschiedene Punkte P und Q mit $P - Q \in \mathbb{Z}^2$, d. h., der eine Punkt geht aus dem anderen durch eine ganzzahlige Verschiebung hervor.*

Beweis. Wir zerlegen die Ebene in die Gittermaschen des ganzzahligen Gitters, s. Abbildung 1. Für jede Gittermasche $[a, a+1) \times [b, b+1)$ mit $(a, b) \in \mathbb{Z}^2$ betrachten wir ihren Durchschnitt mit K und verschieben diesen, indem wir (a, b) subtrahieren, in das Einheitsquadrat $[0, 1) \times [0, 1)$. Die Verschiebung erhält den Flächeninhalt, also landen im Einheitsquadrat Stücke deren Flächeninhalte sich zu $A(K) > 1$ addieren. Da aber der Flächeninhalt des Einheitsquadrates gleich 1 ist, müssen sich mindestens zwei verschiedene der translatierten Stücke von K im Einheitsquadrat schneiden. Das heisst, es gibt verschiedene Punkte $P, Q \in K$, so dass

$$P - (a, b) = Q - (c, d), \quad \text{also} \quad P - Q = (a, b) - (c, d) \in \mathbb{Z}^2.$$

Dies bedeutet, dass P aus Q durch eine ganzzahlige Verschiebung hervorgeht. ∎

Wir möchten nun K nicht nur als messbar voraussetzen, sondern noch zwei zusätzliche Eigenschaften fordern. Die erste ist die Punktsymmetrie bezüglich des Ursprungs des Koordinatensystems, d. h., für jedes $P \in K$ gilt auch $-P \in K$, kurz $K = -K$. Die zweite

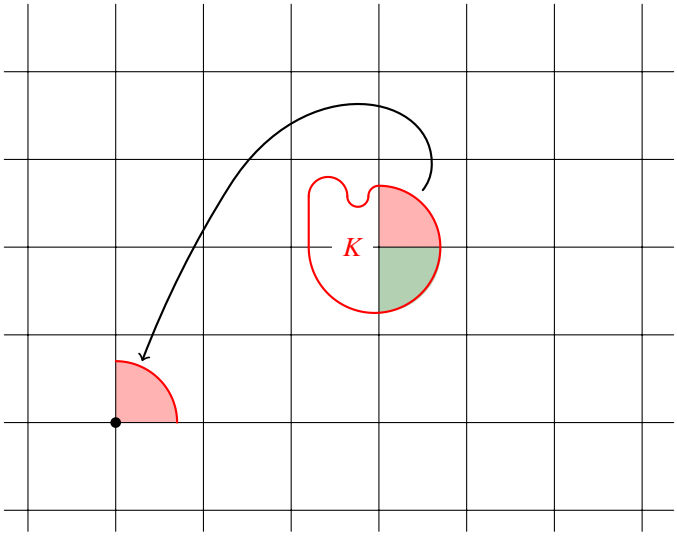

Abbildung 1. Zum Beweis des Blichfeldt Lemmas

Eigenschaft ist die Konvexität, die besagt, dass K für je zwei seiner Punkte die ganze Verbindungsstrecke zwischen ihnen enthält. Eine solche punktsymmetrische konvexe Menge enthält immer den Ursprung $(0,0)$.

Mit diesen Begriffen können wir den berühmten Gitterpunktsatz von Minkowski formulieren und beweisen, der der Anfang und die Grundlage der Geometrie der Zahlen ist.

Minkowskischer Gitterpunktsatz. *Sei $K \subset \mathbb{R}^2$ konvex und punktsymmetrisch bezüglich des Ursprungs. Wenn der Flächeninhalt $A(K) > 4$ ist, dann enthält K mindestens einen Gitterpunkt $R \in \mathbb{Z}^2$, der nicht der Ursprung ist.*

Wegen der Symmetrie folgt natürlich, dass auch $-R \neq R$ in K ist.

Die Annahme $A(K) > 4$ kann nicht abgeschwächt werden, wie das Beispiel des Quadrates mit den Ecken $(\pm 1, \pm 1)$ zeigt. Das Innere dieses Quadrates mit Seitenlänge 2 ist konvex und punktsymmetrisch um den Ursprung und hat Flächeninhalt 4. Das Innere enthält aber keinen Gitterpunkt ausser dem Ursprung!

Beweis. Betrachte die skalierte Menge

$$\frac{1}{2}K = \left\{ \frac{1}{2}x \;\middle|\; x \in K \right\}.$$

Für ihren Flächeninhalt gilt

$$A\left(\frac{1}{2}K\right) = \frac{1}{4}A(K) > 1,$$

also ist das Blichfeldt Lemma auf $\frac{1}{2}K$ anwendbar. Daher gibt es verschiedene Punkte $P, Q \in \frac{1}{2}K$ mit $P - Q = R \in \mathbb{Z}^2$. Dann sind also $2P$ und $2Q$ in K, und wegen der

Punktsymmetrie ist auch $-2Q \in K$. Wegen der Konvexität von K liegt der Mittelpunkt der Verbindungsstrecke von $2P$ und $-2Q$ ebenfalls in K, also

$$\frac{1}{2}(2P + (-2Q)) = P - Q = R \in K.$$

Dieses R ist ein Gitterpunkt in $\mathbb{Z}^2$, und es ist nicht der Ursprung, weil P und Q verschiedene Punkte sind. ∎

Man mag an dieser Stelle einwerfen, dass alle bisherigen Betrachtungen doch so extrem elementar sind, dass es kaum vorstellbar ist, dass sie in der höheren Mathematik nützlich sein können. Es gibt sicher mehrere Antworten darauf, ich beschränke mich auf zwei. Erstens ist es, wie immer in der Mathematik, so, dass die einfachsten Ideen am universellsten und damit auch am weittragendsten sind. Es ist gerade die Einfachheit der obigen Überlegungen, die bewirkt, dass sie in vielen verschiedenen Zusammenhängen angewendet werden können. Zweitens sind die obigen Aussagen nur die Spitze des Eisbergs, man kann tatsächlich diese grundlegenden Ideen noch substantiell verallgemeinern. Als ersten Schritt in dieser Richtung bemerkt man, dass man das ganzzahlige Gitter $\mathbb{Z}^2 \subset \mathbb{R}^2$ durch ein beliebiges anderes Gitter ersetzen kann.

Sind $v, w \in \mathbb{R}^2$ weder Null noch v ein Vielfaches von w, so ist

$$\Lambda = \{av + bw \mid a, b \in \mathbb{Z}\}$$

das von v und w erzeugte Gitter. Der Fall $\Lambda = \mathbb{Z}^2$ entsteht, indem man $v = (1, 0)$ und $w = (0, 1)$ wählt, aber auch auf unendlich viele andere Weisen, z. B. mit $v = (3, 2)$ und $w = (2, 1)$. Die Grundmasche von Λ ist das von v und w aufgespannte Parallelogramm. Das Blichfeldt Lemma gilt für Λ an Stelle von $\mathbb{Z}^2$, wenn man die Annahme $A(K) > 1$ ersetzt durch die Annahme, dass $A(K)$ strikt grösser als der Flächeninhalt dieses Parallelogramms ist. Der Beweis ist, mutatis mutandis, derselbe. Damit folgt auch der Minkowskische Gitterpunktsatz für Λ an Stelle von $\mathbb{Z}^2$, wenn man die Annahme, dass die konvexe punktsymmetrische Menge K Flächeninhalt strikt grösser als 4 hat, ersetzt durch die Annahme, dass der Flächeninhalt strikt grösser ist als 4 mal der Flächeninhalt des von v und w aufgespannten Parallelogramms.

Man kann natürlich viel weiter gehen und Gitter und konvexe punktsymmetrische Körper in beliebig hohen Dimensionen betrachten. Tatsächlich hat Minkowski das schon in [6] getan. Heutzutage kann man das in der Sprache der linearen Algebra sicher schon im ersten Semester eines Mathematik-Studiums verstehen.

2 Diophantische Approximation

Bei der diophantischen Approximation geht es darum, eine beliebige reelle Zahl α möglichst gut durch rationale Zahlen $\frac{x}{y}$ anzunähern. Hier sind also x und y ganze Zahlen mit $y > 0$. Dabei ist auch zu diskutieren, wie man die Güte einer Annäherung messen soll. Intuitiv ist klar, dass man immer bessere Approximationen bekommen kann, wenn man immer grössere Nenner y zulässt. Die Güte einer Approximation wird also von y abhängen.

Denkt man sich die Zahlengerade aufgeteilt in Intervalle der Länge $\frac{1}{y}$ mit Endpunkten der Form $\frac{z}{y}$, wobei z über alle ganzen Zahlen läuft, so ist klar, dass α in eines dieser Intervalle fällt, d. h., es ist möglich ein $x \in \mathbb{Z}$ zu wählen, so dass

$$\left|\alpha - \frac{x}{y}\right| \leq \frac{1}{2y}. \tag{1}$$

In dem Fall, dass $y = 10^k$ eine Potenz von 10 ist, ist dies nichts anderes als das Runden von α auf k Nachkommastellen, zusammen mit der offensichtlichen Abschätzung des Rundungsfehlers.

Man sieht sofort, dass in (1) nur dann Gleichheit auftreten kann, wenn α selbst rational ist. Dies ist tatsächlich der Fall, in dem Approximationen durch (andere) rationale Zahlen besonders schlecht sind. Sei $\alpha = \frac{p}{q} \in \mathbb{Q}$ mit kleinstmöglichem positivem Nenner $q \in \mathbb{Z}$. Es gilt dann

$$\alpha - \frac{x}{y} = \frac{p}{q} - \frac{x}{y} = \frac{py - qx}{qy}. \tag{2}$$

Es gibt nun zwei Möglichkeiten. Entweder ist $\frac{x}{y} = \alpha$, d. h., der Bruch $\frac{x}{y}$ entsteht durch Erweitern von $\frac{p}{q}$, und der Fehler der Approximation ist daher gleich 0. Oder, wenn $\frac{x}{y} \neq \alpha$, dann ist der Zähler der rechten Seite in (2) eine ganze Zahl ungleich 0, also im Betrag mindestens 1. Daher gilt im Fall $\frac{x}{y} \neq \alpha$ die Ungleichung

$$\left|\alpha - \frac{x}{y}\right| \geq \frac{1}{qy}. \tag{3}$$

Dies besagt also, dass für rationales α jede Approximation durch ein $\frac{x}{y} \neq \alpha$ einen Fehler hat, der mindestens ein konstantes Vielfaches von $\frac{1}{y}$ ist.

Schon vor Minkowski war bekannt, dass man diese Diskussion verschärfen kann, indem man Approximationen betrachtet, deren Fehler die Grössenordnung $\frac{1}{y^2}$ hat und nicht die Grössenordnung $\frac{1}{y}$. Dies ergibt sich auch ganz einfach aus dem Minkowskischen Gitterpunktsatz.

Dirichletscher Approximationssatz. *Für jede reelle Zahl α und jede Schranke S gibt es ganze Zahlen $x, y \in \mathbb{Z}$ mit $y > S$, so dass*

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^2}.$$

Die Aussage ist für rationale $\alpha = \frac{p}{q}$ trivial, weil man einfach mit beliebig grossen natürlichen Zahlen n erweitern kann und der Fehler der Approximation von $\frac{p}{q}$ durch $\frac{np}{nq}$ Null ist. Ungleichung (3) zeigt, dass dies für rationales α im Wesentlichen die einzigen Approximationen sind, die Fehler höchstens $\frac{1}{y^2}$ haben.

Beweis. Für eine beliebige natürliche Zahl n betrachten wir das folgende Parallelogramm in der Ebene $\mathbb{R}^2$, s. Abbildung 2:

$$K_n = \left\{(x, y) \in \mathbb{R}^2 \;\middle|\; |y| < n + \frac{1}{2},\ |x - y \cdot \alpha| < \frac{1}{n}\right\}.$$

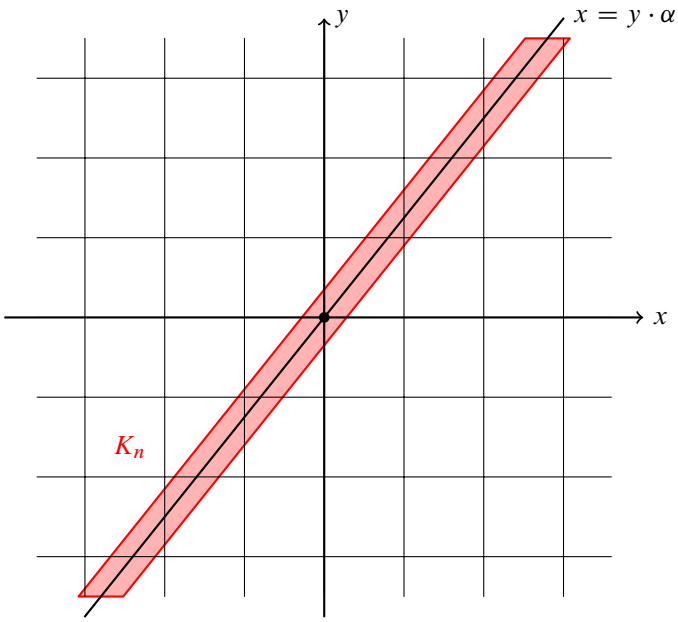

Abbildung 2. Zum Beweis des Approximationssatzes

Dies ist, wie jedes Parallelogramm, konvex und, weil die definierenden Ungleichungen die Beträge auf der linken Seite enthalten, auch punktsymmetrisch um den Ursprung. Sein Flächeninhalt ist

$$A(K_n) = 2\Big(n + \frac{1}{2}\Big) \cdot 2\frac{1}{n} = 4 + \frac{2}{n} > 4.$$

Nach dem Minkowskischen Gitterpunktsatz enthält K_n also einen Gitterpunkt $(x_n, y_n) \in \mathbb{Z}^2$, der nicht der Ursprung ist. Da y_n ganz ist mit $|y_n| < n + \frac{1}{2}$, gilt $|y_n| \leq n$. Ausserdem ist $y_n \neq 0$, weil sonst auch x_n Null wäre, aber (x_n, y_n) ist ja nicht der Ursprung. Wegen der Punktsymmetrie von K_n um den Ursprung dürfen wir $y_n > 0$ annehmen. Damit ist

$$\Big|\alpha - \frac{x_n}{y_n}\Big| = \frac{1}{y_n} \cdot |x_n - y_n \cdot \alpha| < \frac{1}{y_n} \cdot \frac{1}{n} \leq \frac{1}{y_n^2}.$$

Es bleibt noch zu zeigen, dass die y_n grösser als jede Schranke S werden. Nach der Bemerkung vor dem Beweis dürfen wir dazu annehmen, dass α irrational ist. Dann ist $|x - y \cdot \alpha|$ für alle ganzen x und y positiv und mit beschränktem y sogar von Null weg beschränkt. Da aber $|x_n - y_n \cdot \alpha| < \frac{1}{n}$ gilt, können die y_n nicht beschränkt sein. ∎

Mit der Version des Minkowskischen Gitterpunktsatzes in beliebigen Dimensionen, die am Ende des letzten Abschnitts angedeutet wurde, kann man diesen Approximationssatz zu einem Satz über die simultane Approximation einer beliebigen endlichen Anzahl von reellen Zahlen verallgemeinern.

3 Summen von zwei Quadraten

Wir betrachten nun folgende Frage, die so alt ist wie die Zahlentheorie selbst.

Frage. Welche natürlichen Zahlen n sind als Summen von zwei Quadratzahlen darstellbar?

Oder, äquivalent dazu, für welche n hat die Gleichung $x^2 + y^2 = n$ ganzzahlige Lösungen?

Ein Produkt von Summen von zwei Quadratzahlen ist wegen der Formel

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{4}$$

wieder eine solche Summe. Daher ist es naheliegend, sich erst mal auf den Fall dass $n = p$ eine Primzahl ist zu beschränken. Probiert man die ersten Primzahlen durch, so sieht man einerseits

$$1^2 + 1^2 = 2, \quad 1^2 + 2^2 = 5, \quad 2^2 + 3^2 = 13, \quad 1^2 + 4^2 = 17$$

und andererseits, dass für die Primzahlen 3, 7 und 11 keine solche Darstellung existiert.

Diese empirischen Bemerkungen lassen sich am besten in der Sprache der Kongruenzen formalisieren. Zwei ganze Zahlen a und b heissen kongruent modulo m, symbolisch

$$a \equiv b \pmod{m},$$

wenn sie beim Teilen durch m denselben Rest haben. Äquivalent dazu ist, dass m ein Teiler der Differenz $a - b$ ist. Damit verallgemeinern wir die obige Bemerkung zu den Primzahlen 3, 7 und 11 wie folgt.

Lemma 1. *Falls $n \equiv 3 \pmod 4$, so ist n nicht Summe von zwei Quadratzahlen.*

Beweis. Das Quadrat einer geraden Zahl ist durch 4 teilbar, also kongruent zu 0 modulo 4. Das Quadrat einer ungeraden Zahl ist wegen

$$(2k + 1)^2 = 4k(k + 1) + 1$$

kongruent zu 1 modulo 4. Zwei Summanden, die beide 0 oder 1 modulo 4 sind, können sich nicht zu 3 modulo 4 addieren. ∎

Das bedeutet nun, dass man für die Darstellbarkeit von Primzahlen als Summe von zwei Quadratzahlen nur noch diejenigen Primzahlen betrachten muss, die kongruent zu 1 modulo 4 sind. Für diesen Fall hat man den folgenden Satz, den Fermat als erster behauptet hat – wie so oft bei ihm, ohne Beweis. Der erste bekannte Beweis stammt wohl von Euler.

Zwei-Quadrate-Satz. *Ist die Primzahl $p \equiv 1 \pmod 4$, so ist p eine Summe von zwei Quadratzahlen.*

Wir werden das folgende Lemma aus der elementaren Zahlentheorie benutzen. Da das Rechnen mit Kongruenzen nicht zum Schulstoff gehört, lagere ich den Beweis in den Anhang aus.

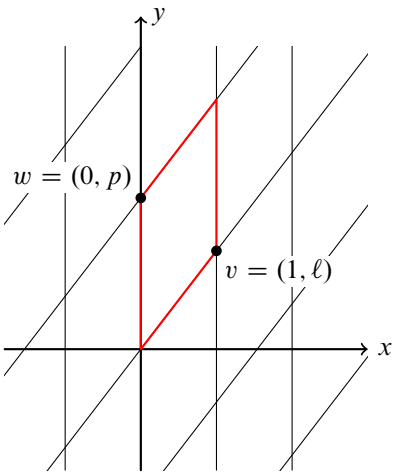

Abbildung 3. Zum Beweis des Zwei-Quadrate-Satzes

Lemma 2. *Sei p eine ungerade Primzahl. Es gilt*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p-3}{2}} \pmod{p}. \tag{5}$$

Für den Beweis des Zwei-Quadrate-Satzes fixieren wir eine Primzahl $p \equiv 1 \pmod 4$. In diesem Fall ist die rechte Seite in (5) gleich -1. Die linke Seite gibt also ein ℓ mit $\ell^2 \equiv -1 \pmod p$. Für dieses ℓ betrachten wir das Gitter $\Lambda \subset \mathbb{R}^2$, das durch $v = (1, \ell)$ und $w = (0, p)$ erzeugt wird. Seine Grundmasche ist ein Parallelogramm mit Flächeninhalt p, s. Abbildung 3.

Die Kreisscheibe

$$K = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 2p\}$$

ist natürlich konvex und punktsymmetrisch um den Ursprung. Ihr Flächeninhalt ist

$$A(K) = 2p\pi > 4p.$$

Nach dem Minkowskischen Gitterpunktsatz gibt es also einen Gitterpunkt $(x, y) \in \Lambda$ in K, der nicht der Ursprung ist. Das bedeutet

$$0 < x^2 + y^2 < 2p. \tag{6}$$

Aus $(x, y) \in \Lambda$ folgt, dass es $a, b \in \mathbb{Z}$ gibt, so dass

$$(x, y) = av + bw = (a, a\ell + bp).$$

Es gilt also $x = a$ und $y = a\ell + bp$ und damit

$$x^2 + y^2 = a^2(1 + \ell^2) + 2ab\ell p + b^2p^2 \equiv 0 \pmod p,$$

weil $\ell^2 \equiv -1 \pmod{p}$. Das heisst, $x^2 + y^2$ ist durch p teilbar. Damit folgt $x^2 + y^2 = p$ aus (6), womit der Zwei-Quadrate-Satz bewiesen ist.

Benutzt man den Minkowskischen Gitterpunktsatz in Dimension 4 statt in der Ebene, so kann man ganz ähnlich zeigen, dass jede Primzahl Summe von vier Quadratzahlen ist, und diese Schlussfolgerung folgt dann auch für alle natürlichen Zahlen.

4 Diskussion

Die beiden beispielhaften Anwendungen für die Geometrie der Zahlen, die wir hier besprochen haben, der Dirichletsche Approximationssatz und der Zwei-Quadrate-Satz, werden beide oft mit Hilfe des Schubfachprinzips bewiesen. So ist einer der beiden als besonders elegant geltenden Beweise für den Zwei-Quadrate-Satz im *Buch der Beweise* „eine bemerkenswerte Anwendung des Schubfachprinzips“ [1, S. 23]. Der Beweis von Dirichlet selbst für den Approximationssatz war historisch sogar der erste Fall eines formalen Beweises, in dem ganz explizit der Schubfachschluss als solcher benutzt wurde.

Das Blichfeldt Lemma, auf dem wir den Minkowskischen Gitterpunktsatz aufgebaut haben, ist eine geometrische Form des Schubfachprinzips. Tatsächlich hat Minkowski seinen Satz ursprünglich anders bewiesen, und das Blichfeldt Lemma kam erst später [2]. Trotzdem sind bei Minkowski schon Packungsargumente vorhanden, die man als Analoga des Schubfachprinzips für Flächeninhalte oder höherdimensionale Volumina verstehen kann. Scherrer [8] hat einen Beweis für das Blichfeldt Lemma gefunden, der das Dirichletsche Schubfachprinzip benutzt. Noch später hat dann Mordell [7], scheinbar in Unkenntnis der Arbeiten von Scherrer, sogenannte arithmetische Methoden in die Geometrie der Zahlen eingeführt, die a posteriori die geometrischen Argumente von Minkowski und Blichfeldt ersetzen durch Schubfachschlüsse über Restklassen. So schliesst sich der Kreis, und die geometrischen Ideen, die ursprünglich die Algebra sichtbar gemacht hatten, können durch Schubfachschlüsse mit Restklassen ersetzt werden, und am Ende werden die geometrischen Aussagen arithmetisch bewiesen.

Anhang: Kongruenzen modulo einer Primzahl

Sei p eine ungerade Primzahl und a eine ganze Zahl, die nicht durch p teilbar ist. Wir betrachten die Produkte

$$1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a.$$

Sind zwei solche Produkte, sagen wir $x \cdot a$ und $y \cdot a$, kongruent modulo p, so folgt, dass p die Differenz $x \cdot a - y \cdot a = (x - y) \cdot a$ teilt. Dies kann nur passieren, wenn $x = y$ gilt. Also sind die $p - 1$ Produkte in paarweise verschiedenen Restklassen modulo p. Da keines der Produkte durch p teilbar ist, bilden die Produkte eine Permutation der Restklassen von 1 bis $p - 1$. Insbesondere gibt es genau eine Restklasse x für die $a \cdot x \equiv 1 \pmod{p}$ gilt. Wir nennen diese Restklasse $\bar{a}$.

Falls für ein a gilt, dass $a \equiv \bar{a} \pmod{p}$, so ist $a^2 \equiv 1 \pmod{p}$, also ist $a^2 - 1 = (a - 1) \cdot (a + 1)$ durch p teilbar. Dies bedeutet $a \equiv \pm 1 \pmod{p}$.

Wir betrachten nun das Produkt

$$P = 2 \cdot 3 \cdot \ldots \cdot (p-2) = (p-2)!$$

und bestimmen seine Restklasse modulo p auf zwei Arten. Einerseits besteht P nach obiger Diskussion aus lauter Paaren der Form a und $\bar{a}$, und daher gilt $P \equiv 1 \pmod{p}$. Andererseits besteht P aus $\frac{p-3}{2}$ vielen Paaren der Form

$$k \cdot (p-k) \equiv -k^2 \pmod{p},$$

wobei k von 2 bis $\frac{p-1}{2}$ läuft. Also ist

$$P \equiv (-1)^{\frac{p-3}{2}} \cdot \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}.$$

Damit ist (5) bewiesen.

Der Zwei-Quadrate-Satz ist der wesentliche Teil bei der Beantwortung der Frage nach der Darstellbarkeit beliebiger natürlicher Zahlen als Summe von zwei Quadraten. Um das zu diskutieren, schreiben wir eine natürliche Zahl n als

$$n = k^2 \cdot q,$$

wobei k^2 die maximale Quadratzahl ist, die n teilt. Der zweite Faktor ist dann durch keine Quadratzahl grösser 1 teilbar und heisst der quadratfreie Kern von n. Die Antwort auf die Eingangsfrage lautet dann:

Eine natürliche Zahl n ist genau dann Summe von zwei Quadratzahlen, wenn ihr quadratfreier Kern q keine Primzahl p mit $p \equiv 3 \pmod{4}$ in seiner Primfaktorzerlegung enthält.

Nehmen wir an, n erfüllt die genannte Bedingung an q. Da sowohl 2 als auch die Primzahlen p, die $p \equiv 1 \pmod{4}$ erfüllen, Summen von zwei Quadraten sind, folgt durch wiederholte Anwendung der Formel (4), dass $q = x^2 + y^2$ mit ganzen x und y. Damit ist dann $n = (kx)^2 + (ky)^2$. Damit ist gezeigt, dass die genannte Bedingung hinreichend ist für die Darstellbarkeit von n als Summe von zwei Quadraten.

Umgekehrt, nehmen wir an, dass $n = a^2 + b^2$ mit a und b ganz. Sei p eine ungerade Primzahl, die n teilt. Falls a nicht durch p teilbar ist, so gibt es ein $\bar{a}$ wie oben. Multiplizieren wir die Kongruenz $a^2 + b^2 = n \equiv 0 \pmod{p}$ mit $\bar{a}^2$, so erhalten wir

$$1 + (b \cdot \bar{a})^2 \equiv 0 \pmod{p},$$

d. h., es gibt ein ℓ mit $\ell^2 \equiv -1 \pmod{p}$. Daraus folgt mit dem Beweis des Zwei-Quadrate-Satzes, dass p eine Summe von zwei Quadraten ist. Aber dies ergibt $p \equiv 1 \pmod{4}$ wegen Lemma 1. Im anderen Fall, wenn $p \equiv 3 \pmod{4}$, folgt also, dass a durch p teilbar ist, und dann ist auch b durch p teilbar und n durch p^2. Also kann man die Gleichung $a^2 + b^2 = n$ durch p^2 teilen und dieses Argument wiederholen. So erreicht man nach endlich vielen Schritten eine Situation, wo a nicht mehr durch p teilbar ist, also ist jedes $p \equiv 3 \pmod{4}$ in n mit geradem Exponenten enthalten, tritt also nicht im quadratfreien Kern auf.

Danksagung. Dies ist die Ausarbeitung zweier Vorträge, gehalten am 11. Februar 2023 in der Reihe *Mathematik am Samstag* an der LMU bzw. am 29. März 2023 im Wahlkurs *Enrichment* am Wilhelm-Hausenstein-Gymnasium in München. Ich danke beiden Institutionen für die Gelegenheit vorzutragen. Meinem Sohn Ferran danke ich für die Anregung zu dem Thema und für das sorgfältige Korrekturlesen des Textes. Dem Herausgeber der *Elemente*, N. Hungerbühler, ein herzliches Dankeschön für die Verwandlung meiner Handzeichnungen in Hightech-Abbildungen.

Literatur

[1] M. Aigner und G. M. Ziegler, *Das Buch der Beweise*. 5. Auflage, Springer, 2018 Zbl 71294.01001

[2] H. F. Blichfeldt, A new principle in the geometry of numbers, with some applications. *Trans. Amer. Math. Soc.* **15** (1914), no. 3, 227–235 Zbl 45.0314.01 MR 1500976

[3] J. W. S. Cassels, *An introduction to the geometry of numbers*. Grundlehren Math. Wiss. 99, Springer, Berlin, 1959 Zbl 0086.26203 MR 0157947

[4] C. G. Lekkerkerker, *Geometry of numbers*. Bibl. Math. VIII, Wolters-Noordhoff Publishing, Groningen; North-Holland Publishing, Amsterdam-London, 1969 Zbl 0198.38002 MR 0271032

[5] H. Minkowski, *Diophantische Approximationen – Eine Einführung in die Zahlentheorie*. B. G. Teubner, Leipzig, 1927 Zbl 53.0165.01

[6] H. Minkowski, *Geometrie der Zahlen*. Chelsea Publishing Company, New York, 1953 Zbl 0050.04807 MR 0249269

[7] L. J. Mordell, On some arithmetical results in the geometry of numbers. *Compos. Math.* **1** (1935), 248–253 Zbl 0009.15303 MR 1556892

[8] W. Scherrer, Ein Satz über Gitter und Volumen. *Math. Ann.* **86** (1922), no. 1–2, 99–107 Zbl 48.0192.03 MR 1512080

D. Kotschick
Mathematisches Institut
Ludwig-Maximilians-Universität München
Theresienstr. 39, 80333 München, Germany
dieter@math.lmu.de