Sind Zahlen und Geometrie verwandt miteinander? Ja, sagt ein Mathematiker von der Uni Luxemburg

Vom Einheitskreis zu Fermats letztem Satz

Peter Feist

In der Geschichte der Mathematik kam das Zählen vermutlich vor dem Zeichnen von Formen. Es gibt Aufzeichnungen über die Benutzung von Zahlen, die bis in die Prähistorie zurückreichen. Vielleicht waren die alten Griechen die ersten, denen auffiel, dass Zahlen und Geometrie miteinander zusammenhängen müssen. Griechische Mathematiker betrieben die Mathematik nicht nur zu praktischen Zwecken, sondern auch um ihrer selbst willen: Als ein Spiel, aber als ein sehr ernsthaftes Spiel, denn wichtig war ihnen nicht nur, Lösungen zu finden, sondern obendrein zu beweisen, dass sie ohne Zweifel die richtigen sind.

Für diesen Ansatz stand ganz besonders Euklid, geboren um das Jahr 300 vor Christus. Es ist nicht klar, ob Euklid eine Person war oder ein Pseudonym für eine Gruppe von Mathematikern. Euklid jedenfalls schrieb die dreizehnbändigen *Elemente der Geometrie*, in denen versucht wurde, das gesamte mathematische Wissen der damaligen Zeit zusammenzufassen *und* es zu beweisen. Dieses *Opus magnum* zeigt aber nicht nur, wie geometrische Objekte konstruiert werden. Es enthält unter anderem auch eine Theorie der Musik, und es untersucht Zahlen und legt den Grundstein für die Zahlentheorie.

„Es gibt viele Zusammenhänge zwischen Zahlen und Geometrie", sagt Gabor Wiese, Mathematikprofessor und Zahlentheoretiker an der Universität Luxemburg. „Manche dieser Zusammenhänge sind offensichtlich. Andere dagegen sind ganz überraschend."

Ein einfaches Beispiel für die Verwandtschaft von Zahlen und Geometrie ist der Kreis: Zeichnet man einen „Einheitskreis" mit dem Radius r=1 um den Nullpunkt eines Koordinatensystems mit x- und y-Achse, dann hat man nicht nur eine geometrische Form abgebildet, die jeder kennt, sondern auch die Gleichung $x^2+y^2=1$. Oder $x^2+y^2-1=0$. Der fertige Einheitskreis ist die Menge aller Punkte mit Abstand 1 vom Nullpunkt aus (Abb. 1).

Doch schon dieses Beispiel enthält eine Portion Überraschendes. Denn wie viele sind „alle Punkte"? Die Antwort lautet, unendlich viele. Ein Punkt auf dem Kreis beispielsweise hat die Koordinaten ($\sqrt{1/2}$, $\sqrt{1/2}$), ein anderer ($-\sqrt{1/2}$, $-\sqrt{1/2}$). Die Quadratwurzel aus 1/2 aber ist eine irrationale Zahl. Sie kann nicht als Bruch geschrieben werden und lässt sich auf der y-Achse nur exakt lokalisieren, wenn man dafür $\sqrt{1/2}$ schreibt.

Dass es auf einem Kreis unendlich viele Punkte gibt oder man, anders gesagt, zwischen zwei Punkten stets einen dritten findet, ist intuitiv aber durchaus einleuchtend: Andernfalls sähe der Kreis nicht wie ein richtiger Kreis aus. In die Unendlichkeit führt auch die Kreiszahl Pi oder π (3,1415926...). Seit 1882 ist bewiesen, dass die gerade Länge von π sich nicht mit einem Zirkel und einem Lineal ohne Skala konstruieren lässt. π ist eine transzendente irrationale Zahl – im Unterschied zu $\sqrt{2}$ oder $\sqrt{1/2}$, die ebenfalls irrational sind und in Dezimalschreibweise nicht abbrechen, die man aber auch als Gleichung schreiben kann. Für $\sqrt{2}$ wäre das $x^2-2=0$.

Das Spiel mit den Zahlen und der Geometrie am Einheitskreis lässt sich noch weiter treiben. „Interessiert man sich nur für jene Punkte auf dem Kreis, die Bruchzahlen als Koordinaten haben, dann führt das direkt in die Zahlentheorie", sagt Gabor Wiese.

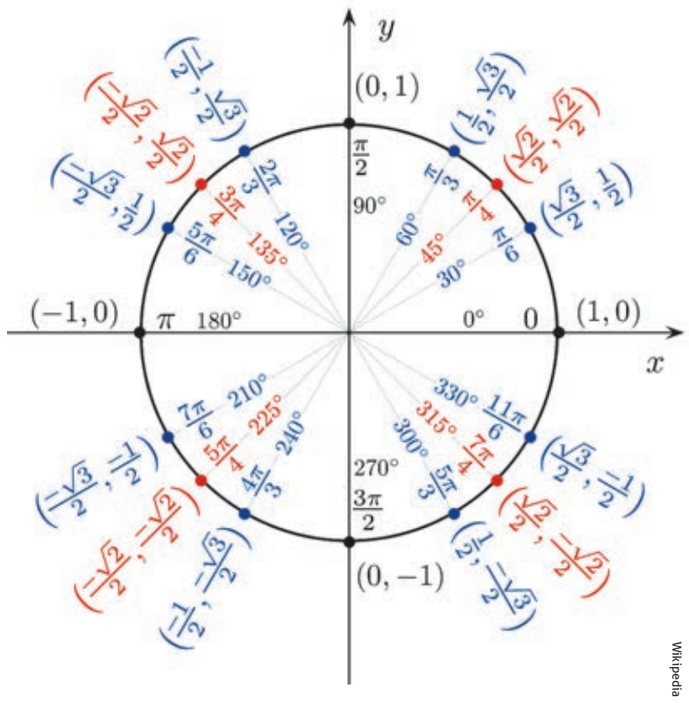

Abb. 1: Ausgewählte Punkte auf dem Einheitskreis

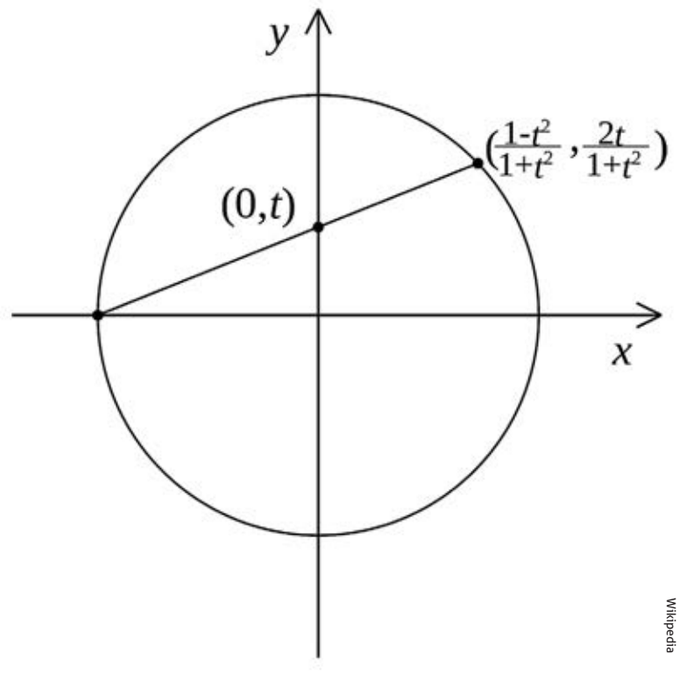

Abb. 2: Die „rationale Parametrierung" der Punkte auf dem Einheitskreis erlaubt die Berechnung Pythagoreischer Tripel

Gleichungen können „Codes" einer Kurve enthalten. In der Kryptografie macht man sich das zunutze

Hat solch ein Punkt die Koordinaten (a/c, b/c), dann wird die Einheitskreisformel zu $(a/c)^2+(b/c)^2=1$ oder $a^2+b^2=c^2$. Das erinnert an den Satz des Pythagoras für Rechnungen an rechtwinkligen Dreiecken, dem Generationen von Schülern begegnet sind. Am Einheitskreis kann man ihm ebenfalls begegnen, wenn man sich eine Strecke vom Nullpunkt aus zu einem Punkt auf dem Kreis vorstellt. Dann ist es gar nicht mehr so erstaunlich, dass aus manchen Zahlen, deren Quadrat addiert wird, eine dritte Quadratzahl entsteht.

Rechnet man in der Gleichung $a^2+b^2=c^2$ nur mit ganzen Zahlen – was besonders einfach ist –, dann studiert man eine Form der nach dem griechischen Mathematiker Diophant benannten „diophantischen Gleichung". Quadratzahlen-Trios, die sich aus dieser Gleichung ergeben, werden wegen des Zusammenhangs mit dem Satz des Pythagoras „Pythagoreische Tripel" genannt. Die Zahlen 3, 4 und 5 sind das kleinste Tripel: $3^2+4^2=5^2$ oder 9+16=25. Weitere kleine Tripel sind (5,12,13) und (8,15,17). Bereits 3 500 Jahre alte babylonische Tontafeln aus der Hamurabi-Dynastie enthalten 15 solche Tripel.

Damals aber wusste man noch nicht, dass die Tripel sich auch geometrisch über den Einheitskreis finden lassen. Stellt man sich vor, dass eine Gerade durch den Punkt (-1,0) verläuft und den Kreis ein zweites Mal schneidet (Abb. 2), dann kreuzt die Gerade unterwegs auch die y-Achse in einem Punkt (0,t) und es ergibt sich ein rechtwinkliges Dreieck. Von diesem Dreieck aus lässt sich berechnen, in welchem Punkt – abgesehen von (-1,0) – die Gerade den Kreis erneut schneidet. Auf diesem Weg findet man die Pythagoreischen Tripel ebenfalls. Und zwar unendlich viele: Läuft die Gerade nach und nach über den gesamten Kreis, passiert sie unendlich viele Punkte. Darunter sind auch unendlich viele, die solche Tripel ergeben.

Allerdings ist die Kreisgleichung eine Gleichung zweiten Grades, oder eine quadratische Gleichung. Das heißt, sie ist vergleichsweise einfach. „Die Zusammenhänge von Zahlen und Geometrie sind darin ziemlich offensichtlich", sagt Gabor Wiese. Die Frage, ob das auch für Gleichungen höheren Grades gilt, ist daher spannend.

Zahlentheoretiker rechnen unter anderem mit „Zahlkörpern". Das klingt stark nach Geometrie, meint aber keine Körper wie Zylinder oder einen Würfel, sondern eine „Menge" an Zahlen. Solche Mengen kann man addieren, subtrahieren, multiplizieren und dividieren, ohne dass die Grenzen der Menge andere würden. Allerdings dürfen in einem Zahlkörper nur bestimmte Zahlen vorkommen, zum Beispiel die in Dezimalschreibweise „unendliche" irrationale Zahl $\sqrt{2}$ (1,4121356237...). Schreibt man sie mittels einer Gleichung, sieht sie harmloser aus: $x^2-2=0$.

Solche Gleichungen nennt man allgemeiner „Polynome". Sie sehen so aus: $a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a0=0$. Hat ein Polynom nur ganze Zahlen a als Einträge, dann drückt dieses Polynom eine „algebraische Zahl" aus. Was nicht nur auf das Polynom für $\sqrt{2}$ zutrifft, sondern auch auf eine Bruchzahl wie 1/7. Als Dezimalbruch hat sie einen geheimnisvoll aussehenden Schwanz aus sechs immer wiederkehrenden Dezimalstellen: 0,142857*142857*142857... Als Polynom wird daraus 7x-1=0.

Alle Zahlen, mit denen wir alltäglich umgehen – ob ganze, ob rationale (Bruchzahlen) oder irrationale wie $\sqrt{2}$ oder π – kann man auch als so genannte Reihen schreiben. Das sind Summen, die unendlich lang werden können. 1,525 zum Beispiel ist die Summe aus 1+5/10+2/100+5/1000. Manche dieser Reihen haben kuriose Eigenschaften. Bildet man beispielswiese die aus den inversen Zweierpotenzen $1/2^n$ für alle n von 0 bis unendlich, dann erhält man 1+1/2+1/4+1/8+1/16+...

Diese Summe wird nicht immer größer, sondern nähert sich immer weiter 2 an, ohne sie je ganz zu erreichen. Der britische Mathematiker Matt Parker erzählt dazu einen Witz: Kommt eine unendliche Zahl von Mathematikern in einen Pub. Der erste bestellt ein Pint Bier, der zweite ein Half Pint, der dritte ein Viertel Pint und so weiter. Der verärgerte Bartender zapft zwei Pint-Gläser voll, stellt sie auf den Tresen und ruft: „You mathematicians have to know your limits!"[1]

Mit Geometrie hat das noch nicht viel zu tun. Das wird ein wenig anders mit den „komplexen Zahlen". Sie wurden entwickelt, damit quadratische Gleichungen immer zwei Lösungen haben können. Für $x^2-1=0$ klappt das: Die Lösungen sind 1 und -1. Für $x^2+1=0$ dagegen muss die Quadratwurzel aus -1 gezogen werden. Damit das funktioniert, wurde festgelegt, dass $\sqrt{-1}=i$ sei, die imaginäre Einheit. $x^2+1=0$ hat dann die Lösungen i und –i. Komplexe Zahlen werden mit einem „Realteil" und einem „Imaginärteil" mit i geschrieben: x+iy. Darstellen lassen sie sich nur in der Ebene eines kartesischen Koordinatensystems – wenn man so will, ein geometrisches Objekt.

Der Kreis, den man ebenfalls in die Ebene eines kartesischen Koordinatensystems zeichnen kann, um damit allerhand mathematische Spielereien anzustellen, wird durch eine Gleichung zweiten Grades beschrieben. Gleichungen dritten Grades, oder kubische Gleichungen, können „elliptische Kurven" beschreiben. Eine solche Gleichung könnte $y^2+y=x^3-x^2$ sein. Aus ihr ergibt sich der Verlauf in Abbildung 3.

„Man kann elliptische Kurven mit ganzen Koeffizienten aber auch durch ihre Modulformen ausdrücken", erläutert Gabor Wiese. „Seit den 1990-er Jahren ist das vollständig bewiesen."

Willkommen in der Welt der „komplexen Geometrie". Modulformen sind unendliche Reihen, die in die obere Halbebene des Koordinatensystems der komplexen Zahlen projiziert werden. Deshalb taucht in den Reihen der Modulformen obligatorisch die „komplexe Variable" $q=e^{2\pi i z}$ auf, die nicht nur die imaginäre Einheit enthält, sondern auch das geheimnisvolle π und die ebenso geheimnisvolle Eulersche Zahl e – wie π eine transzendente irrationale Zahl.

Die Modulform zu der Gleichung $y^2+y=x^3-x^2$ ist ein „unendliches Produkt". Es sieht auf den ersten Blick sehr repekteinflößend aus:

$$F(Z) = q \cdot \prod_{n=1}^{\infty} \left((1-q^n)\cdot(1-q^{11n})\right)^2$$

Die komplexe Variable q ist dieselbe wie im Absatz zuvor. Beginnt man dieses unendliche Produkt auszumultiplizieren, erhält man eine so genannte Potenzreihe, ein unendliches Polynom:

$F(z)= q-2q^2-q^3+2q^4+q^5+ ...$

„Die Koeffizienten diese Polynoms", sagt Gabor Wiese, „hängen mit Punkten auf der elliptischen Kurve modulo Primzahlen zusammen. In unserem Beispiel ist das für Primzahlen außer 11 möglich."

Für Primzahlen – alle natürlichen Zahlen, die größer sind als 1 und die nur durch sich selbst und durch 1 teilbar sind – interessierten sich schon die alten Griechen stark. Euklid erkannte, dass jede natürliche Zahl, die größer als 1 und selber keine Primzahl ist, sich als Produkt aus mindestens zwei Primzahlen darstellen lässt. Er erkannte ebenfalls, dass es unendlich viele Primzahlen und somit keine größte unter ihnen gibt. Die Suche nach der größten bekannten Primzahl dauert trotzdem ungebrochen an. Dieses Jahr wurde, wie *Wikipedia* schreibt, $2^{74\,207\,281}-1$ aufgespürt, ein Ungetüm von 22 338 618 Dezimalstellen.

Das Verfahren für den Zusammenhang zwischen Modulform und elliptischer Kurve ist schwierig zu beschreiben: Gezählt werden alle Punkte (x,y) der elliptischen Kurve „modulo einer Primzahl p". Für die kleinste Primzahl 2 zum Beispiel dürfen x und y zwischen 0 und p-1 (=1) betragen. Daraus ergeben sich für (x,y) die vier Fälle (0,0), (1,0), (0,1), (1,1), die nacheinander in die Kurvengleichung eingesetzt werden. Für alle vier Fälle wird dann überprüft, ob sich „modulo 2", das heißt bei Division durch 2, ein Rest ergibt. Ist das nicht der Fall, liegen die betreffenden Koordinaten auf der elliptischen Kurve modulo 2. Für unsere Kurve trifft das in allen vier Fällen zu. Die Anzahl der Punkte modulo 2 ist also N2 =4.

Der allgemeine Zusammenhang ist folgender: Der p-te Koeffizient der Modulform ist gleich p–Np. Für p=2 findet man also 2-4=-2. Umgekehrt sehen wir, dass der 3-te Koeffizient der Modulform gleich -1 ist. Wegen 3–N3=-1, muss es also 4 Punkte modulo 3 geben. Hier sind sie: (0,0), (0,2), (1,0), (1,2).

„Ist das mysteriös genug?", fragt Gabor Wiese. Kompliziert ist es allemal. „Das Überraschende daran ist", sagt der Zahlentheoretiker, „dass in dem unendlichen Produkt offenbar Informationen über die Kurve kodiert sind, die man gar nicht vermuten würde."

Modulformen kann man auch grafisch darstellen. Eine solche Darstellung, die aber nicht der Modulform der elliptischen Beispiel-Kurve entspricht, haben drei Studenten im ExperimentalMathLab der Universität Luxemburg angefertigt (Abb. 4).

Zusammenhänge zwischen Zahlen und Geometrie wie dieser fallen in Gabor Wieses Arbeitsgebiet: Er untersucht Beziehungen zwischen Modulformen und Verallgemeinerungen von elliptischen Kurven über Zahlkörpern – die bereits erwähnten speziell konstruierten Zahlenmengen. Das kann auch praktische Anwendungen haben: Schon seit den Achtzigerjahren werden Punkte auf elliptischen Kurven modulo Primzahlen in der Kryptografie benutzt. Wobei diese Primzahlen aber viel, sogar sehr, sehr viel größer sind als 2 oder 3.

Zahlentheorie einerseits und Geometrie andererseits spielen auch eine Rolle in „Fermats letztem Satz", einer jener Vermutungen, die jahrhundertelang unbewiesen bleiben mussten. Der französische Mathematiker Pierre de Fermat war von der diophantischen Gleichung $a^2+b^2=c^2$ und den Pythagoreischen Tripeln ausgegangen. Im Jahre 1621 schrieb er, erweitere man diese Gleichung auf Potenzen beliebigen Grades zu $a^n+b^n=c^n$, dann sei ab der dritten Potenz keine Lösung in positiven natürlichen Zahlen mehr zu finden. Den Beweis dafür trat Fermat selber nicht mehr an. Erst 1994 wies Andrew Wiles nach, dass Fermat mit seiner Vermutung Recht hatte. „Das", sagt Gabor Wiese, „hat die Zahlentheorie revolutioniert."

Es war nämlich Wiles, der den vorhin an einem Beispiel beschriebenen Zusammenhang zwischen elliptischen Kurven und Modulformen bewies. Dass dieser Zusammenhang den Beweis von Fermats Vermutung zur Folge haben würde, war schon bekannt gewesen. Die Idee dazu geht wohl auf den Mathematiker Gerhard Frey zurück: Man ordnet dabei einem hypothetischen Gegenbeispiel zu Fermats Vermutung $a^p + b^p = c^p$ mit positiven ganzen Zahlen a,b,c, und einer Primzahl p>2 eine potenzielle elliptische Kurve zu, nämlich: $y^2-x(x-a^p)(x+b^p)$. Zu dieser potenziellen elliptischen Kurve gibt es nach Wiles' Satz eine zugehörige potenzielle Modulform. Diese müsste bestimmte Eigenschaften haben. Durch explizite Rechnungen stellt man aber fest, dass es eine solche Modulform gar nicht geben kann. Da es die Modulform nicht gibt, kann es auch das potenzielle Gegenbeispiel zu Fermat nicht geben. Somit ist die Vermutung von Fermat bewiesen.

[1] Matt Parker, *Things to Make and Do in the Fourth Dimension*, Penguin Books, 2015

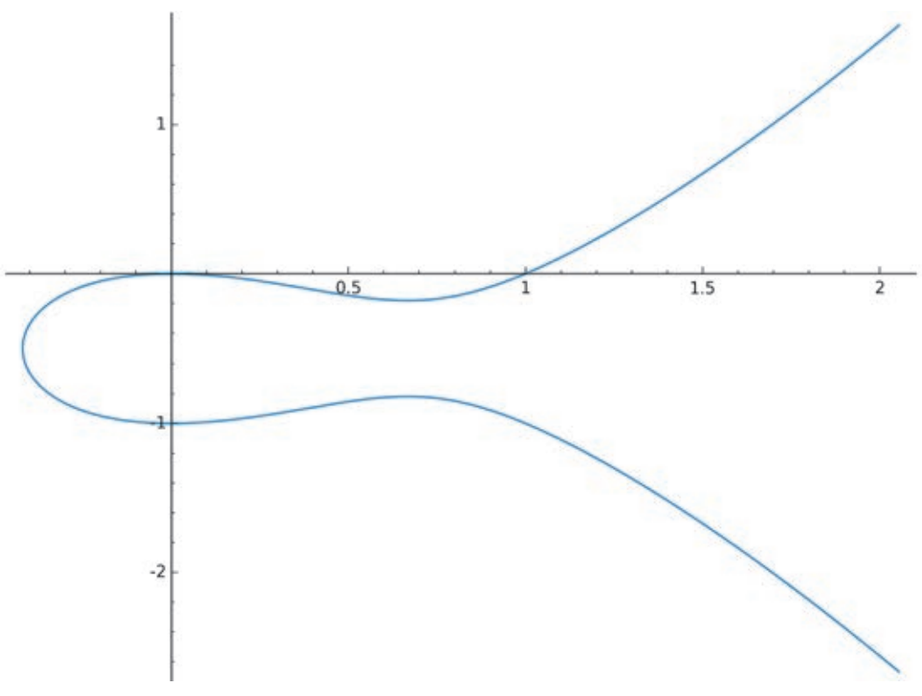

Abb. 3: Die elliptische Kurve $y^2+y=x^3-x^2$, erstellt von Gabor Wiese

Abb. 4: Eine Modulform auf der Einheitskreisscheibe mit einer zugrundeliegenden Kachelung wie bei Escher. Erstellt von Joel Costa, Loqman Salamatian und Alex Ferreira Costa vom ExperimentalMathLab der Universität Luxemburg