*Der Beweis der Serre-Vermutung, die einen Zusammenhang zwischen Zahlentheorie und Geometrie herstellt, ist erst vor kurzem gelungen. Gabor Wiese gibt einen Überblick über diese Vermutung, die für die Forschung am Institut für Experimentelle Mathematik eine nicht unerhebliche Bedeutung hat.*

# Der Zusammenhang von Modulformen und Zahlkörpern

## Zahlentheorie und Geometrie vereint in der Serre-Vermutung

Von Gabor Wiese

In den Jahren 2004 bis 2007 wurde zur großen Überraschung der mathematischen Gemeinde (der Autor eingeschlossen) eines der großen Probleme der reinen Mathematik der Gegenwart gelöst: die 'Serre-Vermutung'. Sie stellt einen Zusammenhang zwischen scheinbar grundverschiedenen Objekten her, die unterschiedlichen Gebieten der Mathematik entstammen: der Zahlentheorie und der Geometrie.

Diese Vermutung geht auf den französischen Mathematiker Jean-Pierre Serre (geboren 1926, emeritierter Professor am Collège de France) zurück, der einer der besten und einflussreichsten Mathematiker seit der zweiten Hälfte des 20. Jahrhunderts ist und zum Beispiel als erster mit dem höchst renommierten Abel-Preis ausgezeichnet wurde. Eine erste Version seiner Vermutung formulierte er zu Beginn der siebziger Jahre: Sie postuliert einen qualitativen Zusammenhang zwischen Modulformen (Geometrie) und bestimmten Klassen von Zahlkörpern (Zahlentheorie). Beide Begriffe zu erklären, ist ein Hauptanliegen dieses Artikels. Eine quantitative Präzisierung der Vermutung folgte in einem Artikel im Jahre 1987.[1] Diese neue Formulierung stützte sich übrigens bereits zum Teil auf Computerberechnungen. Sie war unter anderem motiviert durch die so genannte Taniyama-Shimura-Weil-Vermutung und liefert sogar eine weit reichende Verallgemeinerung dieser. Es war nämlich vom Mathematiker Gerhard Frey, der damals Professor in Saarbrücken war, aber seit der Gründung am Essener Institut für Experimentelle Mathematik tätig ist, suggeriert worden, dass die Taniyama-Shimura-Weil-Vermutung den so genannten letzten Satz von Fermat[2] (Abb. 2, nach Pierre de Fermat, etwa 1607 bis 1665) zur Folge hat. Serre beweist in seiner Präzisierung, dass seine Vermutung den Satz von Fermat direkt impliziert.

Die Serre-Vermutung hat den Fortgang der Forschung in Zahlentheorie und Geometrie in den letzten Jahren stark beeinflusst und wird ihn noch weiter beeinflussen, denn ihr Beweis ist natürlich kein Schlussstein in diesem Gebiet. Es scheint vielmehr so, dass sie nur der erste Fall viel umfassenderer Zusammenhänge ist.

Es gab, gibt und wird noch viele Essener Aktivitäten auf dem Gebiet rund um die Serre-Vermutung geben: Gerhard Frey hat neben seinem bereits erwähnten bahnbrechenden Beitrag viele Studien durchgeführt und initiiert[3], Gebhard Böckle hat einen entscheidenden Beitrag zum Beweis der Serre-Vermutung geleistet, indem er bestimmte *Deformationsringe* beschrieben hat; hierauf können wir leider in diesem Text

Gabor Wiese. Foto: Max Greve

(1) Jean-Pierre Serre im Gespräch mit Jean-Pierre Wintenberger.
Quelle: Xavier Taixés i Ventosa

nicht näher eingehen. Auch der Autor forscht auf diesem Gebiet, vor allem im Fall von *Gewicht eins*, und konnte einige Beiträge leisten.[4] Die Leserin oder der Leser ist nun eingeladen zu einer Reise durch einen kleinen Teil der großen Welt der Mathematik. Ziel ist es, nicht nur Begriffe zu verwenden, sondern diese so gut es geht zu erklären. Die Darstellung ist natürlich vereinfacht, aber dennoch wird versucht, vom Essentiellen so viel wie möglich beizubehalten. Wer sich für das ‚Wer, wann mit wem?' interessiert, wird hier aber nicht fündig.[5]

## Die Serre-Vermutung – ein Überblick

Die mathematischen Gebilde, die in der Serre-Vermutung Zahlentheorie und Geometrie verbinden, sind die Modulformen. Diesen widmen wir einen eigenen Abschnitt, in dem wir die verwendeten Begriffe erklären werden. Grob gesprochen sind *Modulformen* Funktionen, die der Geometrie entstammen und bestimmte Symmetrien erfüllen, die *Möbius-Symmetrien* nach August Ferdinand Möbius (1790 bis 1868). In diesem Text betrachten wir nur Modulformen, die noch eine zweite Klasse von Symmetrien aufweisen, die *Hecke-Symmetrien*, nach Erich Hecke (1887 bis 1947). Modulformen, die beide Symmetrien besitzen, nennen wir sehr *symmetrische Modulformen* oder *Hecke-Eigenformen.*

Die zahlentheoretischen Objekte in der Serre-Vermutung sind *Zahlkörper*, genauer ungerade $GL_2$-*Zahlkörper*, und ihre *Arithmetik*. Was wir darunter verstehen, wird im folgenden Abschnitt geklärt. Zahlkörper sind wichtige Hilfsmittel der algebraischen Zahlentheorie.

Eine erste allgemeine Verbindung zwischen Modulformen und Zahlkörpern wurde in einem ersten Fall von Goro Shimura (Princeton, geboren 1930) und im Allgemeinen von Pierre Deligne (Princeton, geboren 1944) mit Methoden der arithmetischen algebraischen Geometrie bewiesen. Eine grobe Formulierung der Verbindung ist die folgende: Jede sehr symmetrische Modulform enthält arithmetische Informationen zu bestimmten Zahlkörpern. Um die Verbindung präzisieren zu können, erinnern wir an den Begriff einer Primzahl. Das ist eine natürliche Zahl größer als 1, die nur durch 1 und sich selbst teilbar ist, wie zum Beispiel 2, 3, 5, 7, 11,..., 997,.... Die Präzisierung lautet wie folgt: *Jede sehr symmetrische Modulform enthält arithmetische Informationen zu je einem ungeraden $GL_2$-Zahlkörper pro Primzahl.*

Die Serre-Vermutung in ihrer ersten Formulierung aus den Siebzigern ist die kühne Aussage, dass die Umkehrung hiervon auch gilt: *Die arithmetische Information zu jedem ungeraden $GL_2$-Zahlkörper steckt in einer sehr symmetrischen Modulform.* Mit anderen Worten: *Die Arithmetik der ungeraden $GL_2$-Zahlkörper wird vollständig durch sehr symmetrische Modulformen bestimmt.*

Dies ist eine Strukturaussage von großer Bedeutung, denn die Welt der Zahlkörper ist sehr mysteriös und im Allgemeinen noch unzureichend verstanden. Hier wird also behauptet, dass einfache Funktionen, die der Geometrie und sogar dem 19. Jahrhundert entstammen, einen Teil der Welt der Zahlkörper beherrschen! Wie schon zu Anfang erwähnt, wissen wir seit kurzem, dass diese kühne Behauptung korrekt ist! Der Satz wurde bewiesen

Die Fermatsche Vermutung (Fermats letzter Satz) besagt, dass die Gleichung

$$a^n + b^n = c^n$$

für ganze Exponenten $n \geq 3$ keine Lösung in positiven natürlichen Zahlen $a, b, c$ hat. Sie wurde 1994 von Andrew Wiles mit Methoden bewiesen, die im Beweis der Serre-Vermutung weit reichende Verallgemeinerungen erfahren haben.

(2) Fermats letzter Satz.

von Chandrashekhar Khare (Los Angeles) und Jean-Pierre Wintenberger (Straßburg), wobei Mark Kisin (Chicago) und Richard Taylor (Harvard) eine sehr große Rolle gespielt haben. Aber noch viel besser: Nicht nur wurde die erste Formulierung der Vermutung bewiesen, sondern auch die sehr präzise zweite Formulierung aus dem Jahre 1987.

Die Stärke der Serre-Vermutung zeigt sich darin, dass sie eine ganze Reihe berühmter Probleme auf einen Schlag löst, die wir leider aus Platzgründen hier nicht erklären können und nur schlagwortartig auflisten.

• Artin-Vermutung für $GL_2$. In umfangreichen Arbeiten wurde diese Vermutung in den neunziger Jahren am Essener Institut für Experimentelle Mathematik in vielen, aber nur endlich vielen, Fällen überprüft.[6] Dass sie für unendlich viele Fälle richtig ist, wurde in einer ganzen Reihe von Arbeiten, initiiert von Richard Taylor, der auch ganz entscheidenden Anteil am Beweis der Taniyama-Shimura-Weil-Vermutung hatte, erst vor ein paar Jahren gezeigt. Dass sie in jedem Fall richtig ist, war nicht bekannt.

• Modulariät jeder Abelschen Varietät vom $GL_2$-Typ (bisher nicht bekannt); diese ist eine Verallgemeinerung der

• Taniyama-Shimura-Weil-Vermutung; diese wurde 1994 von Andrew Wiles (Princeton) erstmals gelöst in einer Arbeit, die es auf die erste Seite der New York Times gebracht hat, denn sie impliziert

• Fermats letzten Satz, den wir oben schon behandelt haben.

Der Autor dieses Artikels, der der Algorithmik sehr zugeneigt ist, wird nicht müde zu betonen, welche große Bedeutung die Serre-Vermutung für explizite Fragestellungen hat: Modulformen sind einfach berechenbar. Folglich sind mittels der Serre-Vermutung auch arithmetische Eigenschaften von ungeraden $GL_2$-Zahlkörpern einfach berechenbar!

Die Leserin oder der Leser wird die Begeisterung des Autors über diese große Entdeckung gespürt haben; sie wird geteilt von algebraischen Zahlentheoretikern weltweit. Auch wird die Leserin oder der Leser einen Eindruck von der strukturellen Bedeutung der Serre-Vermutung innerhalb der Zahlentheorie und der reinen Mathematik als solcher erhalten haben.

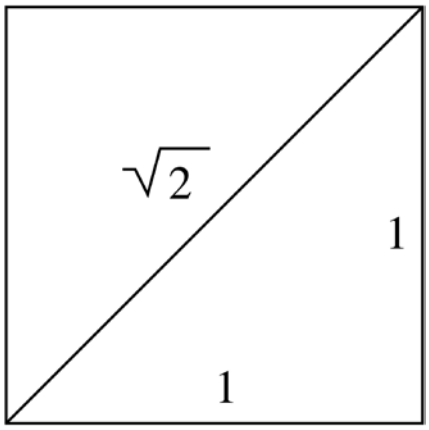
Nach diesem ersten Überblick beginnen wir nun die versprochene Reise durch die reine Mathematik, um uns ein genaueres Bild von der Serre-Vermutung zu verschaffen. Der erste und größte Teil ist der Welt der Zahlen gewidmet. Danach wenden wir uns der Geometrie, den verschiedenen Symmetrien und schließlich den Modulformen zu, bevor wir den Zusammenhang zwischen all diesen herstellen.

## Zahlen

### *Algebraische Zahlen und Zahlkörper*

Wir wollen und müssen unsere Geschichte früh beginnen. Weithin bekannt dürfte die Bestürzung der Pythagoräer sein, als sie feststellten, dass es Zahlen gibt, die keine Bruchzahlen sind. Genauer haben die Pythagoräer keine Zahlen sondern Längen beziehungsweise Längenverhältnisse betrachtet und herausgefunden, dass die Diagonale im Quadrat inkommensurabel mit den Seiten ist: Egal, wie viele Stäbe der Länge der Diagonale man hintereinander legt, nie wird man auf ein Vielfaches der Länge einer Seite kommen (vgl. Abb. 3). Ist nämlich die Seitenlänge $a$, dann ist nach dem Satz von Pythagoras das Quadrat der Länge einer Diagonalen gleich $2a^2$. Folglich ist das Verhältnis von Diagonale zu Seite gleich $\sqrt{2}$. Wir, ein paar Jahrtausende später, wissen natürlich, dass $\sqrt{2}$ kein Bruch ist.

Was ist also nun ein Zahlkörper? Zum einen handelt es sich um einen Körper: Das ist eine Menge von Zahlen, die man addieren, subtrahieren, multiplizieren und dividieren kann, ohne die Menge zu verlassen, wobei die üblichen Klammerregeln gelten sollen. Zum anderen wollen



(3) Quadrat und Diagonale.

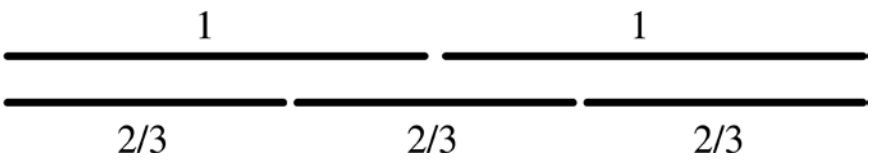
wir nur bestimmte Zahlen zulassen, zum Beispiel $\sqrt{2}$. Es ist eine ganz simple Eigenschaft, die man zu Grunde legt. In unserem Fall ist es die, dass $\sqrt{2}$ die Gleichung $x^2-2=0$ erfüllt (denn $(\sqrt{2})^2-2=2-2=0$).

Diesen Sachverhalt verallgemeinern wir jetzt wie folgt. Dabei halten wir uns vor Augen, dass es in der Zahlentheorie ja gerade um das Studium von Lösungen von Gleichungen mit ganzen Koeffizienten geht. Algebraische Zahlen bekommt man nun per Definition als Lösungen von Gleichungen mit ganzen Koeffizienten in einer Variablen. Genauer ist eine Zahl x eine algebraische Zahl, falls sie eine Gleichung (ein so genanntes Polynom)

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0 = 0$$

erfüllt, wobei all die $a_i$ ganze Zahlen sein sollen und jede natürliche Zahl als n erlaubt ist. Ein weiteres Beispiel ist der *goldene Schnitt* $\frac{1+\sqrt{5}}{2}$, der der Gleichung $x^2 - x - 1 = 0$ genügt (also n=2 und $a_2=1$, $a_1=-1$, $a_0=-1$), wie man durch Einsetzen und Ausmultiplizieren nachprüft.

Wie passen die rationalen Zahlen in diesen Zusammenhang? Sie erfüllen gerade Gleichungen mit n=1. Zum Beispiel ist ja für $x = \frac{2}{3}$, die Gleichung $3x-2=0$ wahr. Die ganzen Zahlen sind hierbei gerade diejenigen, die eine Gleichung $x-a_0=0$ erfüllen; dann ist natürlich $x=a_0$ und $a_n=1$. Es stellt sich heraus, dass dieses der Schlüssel für eine Verallgemeinerung des Begriffs der ‚ganzen Zahl'




(4) 1 und ⅔ sind kommensurabel.

auf Zahlkörper ist. Wir sagen, dass die Zahl $x$ eine *ganze algebraische Zahl* ist, wenn in obiger Gleichung $a_n=1$ gilt. Der goldene Schnitt und $\sqrt{2}$ sind somit sogar ganze algebraische Zahlen. Wir begegnen den algebraischen Zahlen im weiteren Verlauf als Koeffizienten von sehr symmetrischen Modulformen.

Nun können wir beschreiben, was ein Zahlkörper ist. Nach Definition ist dies ein Körper, der alle Potenzen einer algebraischen Zahl enthält und zudem auch alle Zahlen, die sich aus diesen durch beliebige Multiplikationen und Additionen mit Bruchzahlen ergeben.

*Kummers Idealtheorie*

Schon Euklid (365 bis 300 v. Chr.) war bekannt, dass es unendlich viele Primzahlen gibt und dass sich jede positive natürliche Zahl auf eindeutige Weise (bis auf Umordnung) als Produkt von Primzahlen schreiben lässt. Nun stellt sich natürlich die Frage, ob ähnliche Eigenschaften auch in Zahlkörpern erfüllt sind, genauer in den ganzen algebraischen Zahlen eines Zahlkörpers. Es stellt sich heraus, dass die naive Verallgemeinerung falsch ist. Jedoch hat Ernst Eduard Kummer (1810 bis 1893), auch motiviert von der Herausforderung von Fermats letztem Satz, eine andere Verallgemeinerung gefunden, die für alle Zahlkörper gilt.

In den ganzen algebraischen Zahlen eines Zahlkörpers kann man verschiedene Phänomene beobachten. Zum Beispiel kann es sein, dass sich eine Primzahl in dem Zahlkörper faktorisieren, also in das Produkt von zwei Zahlen (keine Einheiten) zerlegen lässt. Des Weiteren kann im Allgemeinen nicht jede Zahl auf eindeutige Weise als Produkt von Zahlen geschrieben werden, die sich nicht weiter zerlegen lassen.

Kummers große Einsicht war, von Zahlen zu bestimmten Mengen von Zahlen überzugehen, den *Idealen* (Kummer nannte diese ‚ideale Zahlen'). Er hat ein Produkt von Idealen definiert und es ist ihm gelungen zu beweisen, dass sich jedes Ideal als eindeutiges Produkt von nicht weiter zerlegbaren Idealen schreiben lässt. Letztere nennt man *Primideale*, in Analogie zu den Primzahlen. Die in den gewöhnlichen ganzen Zahlen geltende eindeutige Zerlegung in Primzahlen wird also in Zahlkörpern ersetzt durch die eindeutige Zerlegung jedes Ideals in Primideale. Man kann jeder ganzen Zahl ein Ideal zuordnen, das dann *Hauptideal* heißt. Jedes Hauptideal lässt sich nach Kummers Satz in ein eindeutiges Produkt von Primidealen faktorisieren. Dieses führt uns zu für das Folgende wichtigen Begriffen: Zerlegung und Verzweigung. Eine Primzahl heißt *verzweigt*, wenn das Quadrat oder eine höhere Potenz eines Primideals in der Faktorisierung des zur Primzahl gehörigen Hauptideals auftritt. Es ist ein klassischer Satz, dass für jeden Zahlkörper nur endlich viele Primzahlen verzweigt sind. Die verzweigten Primzahlen werden uns im Zusammenhang mit den Modulformen noch wieder begegnen. Eine Primzahl heißt *voll zerlegt*, wenn in der Faktorisierung des Hauptideals die maximal mögliche Anzahl von Primidealen auftritt (für diejenigen, die es genau wissen wollen: so viele wie der Grad des Zahlkörpers). Nach einem berühmten Satz von Nikolai Grigorjewitsch Tschebotarjow (1894 bis 1947) bestimmt die Menge der voll zerlegten Primzahlen den Zahlkörper eindeutig. Schließen wir diesen Abschnitt mit der Bemerkung, dass man die Eigenschaften der Primideale, also zum Beispiel Zerlegung und Verzweigung, häufig unter dem Begriff *Arithmetik* zusammenfasst.

*Endliche Körper*

Hier möchten wir jetzt auf eine ganz andere Klasse von Zahlen und Körpern eingehen, nämlich die endlichen. Der Hauptsatz über endliche Körper besagt, dass die Anzahl der Elemente jedes endlichen Körpers eine Primzahlpotenz ist, also von der Form $p^r$ mit $p$ einer Primzahl und $r$ einer positiven natürlichen Zahl. Umgekehrt gibt es für jede Primzahlpotenz einen endlichen Körper mit der gegebenen Anzahl an Elementen. Er sei mit $GF(p^r)$ bezeichnet.

Endliche Körper spielen in diesem Artikel zwei wichtige Rollen. Zum einen benötigen wir sie zur Definition von $GL_2$-Zahlkörpern. Zum anderen kann man von Zahlkörpern zu endlichen Körpern übergehen und zwar für jedes Primideal des Zahlkörpers.

*Reelle Zahlen und unendliche Reihen*

Nach der Betrachtung der Zahlen in endlichen Körpern wollen wir uns nun den reellen Zahlen zuwenden. Die reellen Zahlen sind die Zahlen, die wir im Alltag verwenden. Diese stellen wir zumeist in Dezimalschreibweise dar: 23,05 oder 1,979 oder $\sqrt{2}$ = 1,414213562373.... Was meinen wir mit 1,979? Natürlich: $1+\frac{9}{10}+\frac{7}{100}+\frac{9}{1000}$ .
Eine allgemeine reelle Zahl hat ja eine unendlich lange Dezimalschreibweise, wir haben es somit mit unendlich langen Summen zu tun, solche nennen wir *Reihen*. Wir können zum Beispiel jede reelle Zahl größer gleich 0 und kleiner als 1 schreiben als

$$0,z_1z_2z_3\ldots=\frac{z_1}{10}+\frac{z_2}{10^2}+\frac{z_3}{10^3}+\cdots=\sum_{i=1}^{\infty}\frac{z_i}{10^i}$$

wobei die Ziffern $z_i$ ganze Zahlen zwischen 0 und 9 sind. Der Ausdruck $\sum_{i=1}^{\infty} \frac{z_i}{10^i}$ bedeutet dann genau das, was davor steht, nämlich, dass man all die Brüche $\frac{z_i}{10^i}$ (für $i$ = 1,2,3,..., also unendlich viele) aufsummiert.

Betrachten wir als anderes Beispiel die Reihe

$$\sum_{n=1}^{\infty} \frac{1}{2^n} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots.$$

Man kann sie als ‚Null Komma Periode 1' im Binärsystem lesen. Erinnern wir uns, dass ‚Null Komma Periode 9' im Dezimalsystem gleich 1 ist, so können wir in Analogie hoffen, dass obige Reihe den Wert 1 hat. Das ist in der Tat so, und man kann sich dieses ganz einfach am Bild des Kuchens klar machen (Abb. 5). Das erste Stück gibt einen halben Kuchen, die ersten beiden einen drei Viertel Kuchen, die ersten drei einen sieben Achtel Kuchen, beziehungsweise allgemeiner die ersten $N$ einen $\frac{2^N-1}{2^N}$-tel Kuchen. Man sieht sofort, dass das fehlende Stück mit jedem Schnitt immer kleiner wird: Seine Größe kommt der 0 beliebig nah (man sagt, sie konvergiert gegen 0) und somit nimmt die Reihe den Wert 1 an.

Der Leser oder die Leserin sei gewarnt, dass nicht jede unendliche Reihe *konvergiert*, also einen wohl definierten Wert hat: Das unendlich oft Aufaddieren der 1 (also $\sum_{n=1}^{\infty} 1$) ergibt natürlich keine wohl definierte Zahl; man sagt, dass die Reihe *divergiert.*

Es gibt, wie wir ja wissen, unendlich viele natürliche Zahlen 1, 2, 3, ... und auch unendlich viele reelle Zahlen. Es war eine geniale Einsicht von Georg Cantor (1845 bis 1918), dass es trotzdem mehr reelle als natürliche Zahlen gibt. Die natürlichen Zahlen sind ja die ‚Zählzahlen'. Damit, dass es mehr reelle als natürliche Zahlen gibt, meinen wir, dass es unmöglich ist, die reellen Zahlen zu zählen. Wir sprechen davon, dass die Menge der reellen Zahlen *überabzählbar* ist. Die Menge der algebraischen Zahlen hingegen kann man abzählen. Die Konsequenz ist, dass es viel mehr reelle Zahlen als algebraische gibt. Somit ist die Eigenschaft, eine algebraische Zahl zu sein, etwas ganz Besonderes. Das berühmteste Beispiel einer reellen Zahl, die nicht algebraisch ist, ist die Kreiszahl π. Die nicht-Algebraiziät wurde erst im Jahre 1882 bewiesen.

*Komplexe Zahlen*

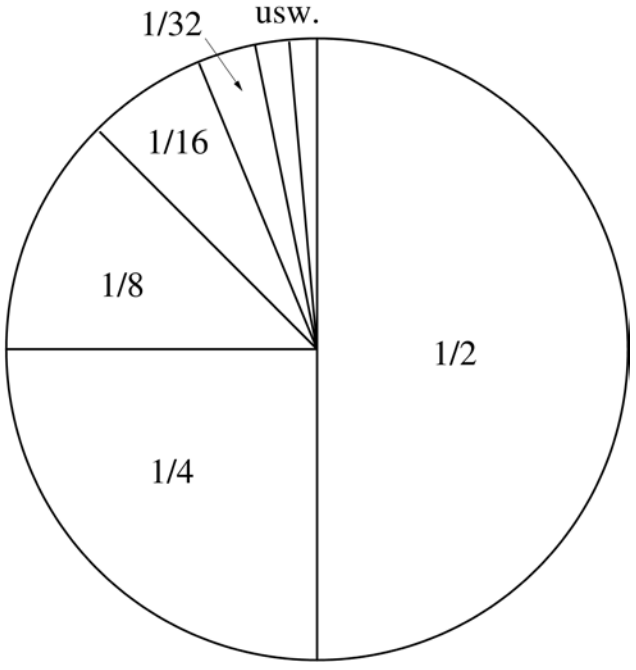
Komplexe Zahlen sind daraus entstanden, dass man gerne hätte, dass eine quadratische Gleichung $x^2+a \cdot x+b=0$ stets zwei Lösungen hat, die man eventuell mit Vielfachheiten zählen muss. Erinnern wir uns, dass zum Beispiel $x^2-1=0$ die Lösungen 1 und -1 hat. Die Gleichung $x^2+2x+1=(x+1)^2=0$ hat die Lösung -1 mit Vielfachheit 2. Die Lösungen von $x^2-2=0$ sind $\sqrt{2}$ und $-\sqrt{2}$. Wie sieht es mit $x^2+1=0$ aus? Da das Quadrat jeder reellen Zahl nicht negativ ist, kann diese Gleichung keine Nullstelle in den reellen Zahlen haben. Da es sich als sehr praktisch herausstellt, wenn jede quadratische Gleichung zwei Lösungen (mit Vielfachheiten) hat, führt man nun die Zahl $i=\sqrt{-1}$ formal ein; es ist keine reelle Zahl, es ist lediglich eine Zahl, deren Quadrat gleich -1 ist. Nun erhalten wir die Information, dass $x^2+1=0$ die Lösungen $i$ und $-i$ hat. Eine komplexe Zahl ist dann definiert als eine Zahl der Form $x+i \cdot y$ mit reellen Zahlen $x$ und $y$.

In den komplexen Zahlen hat nun jede quadratische Gleichung zwei Lösungen (mit Vielfachheiten). Zum Beispiel sind die Lösungen von $x^2+23=0$ gleich $\sqrt{-23}=\sqrt{-1} \cdot \sqrt{23}=i \cdot \sqrt{23}$ und $-i \cdot \sqrt{23}$. Der so genannte *Hauptsatz der Algebra* besagt nun, dass jede Gleichung $n$-ten Grades genau $n$ Lösungen (mit Vielfachheiten) in den komplexen Zahlen hat.

**Geometrie**

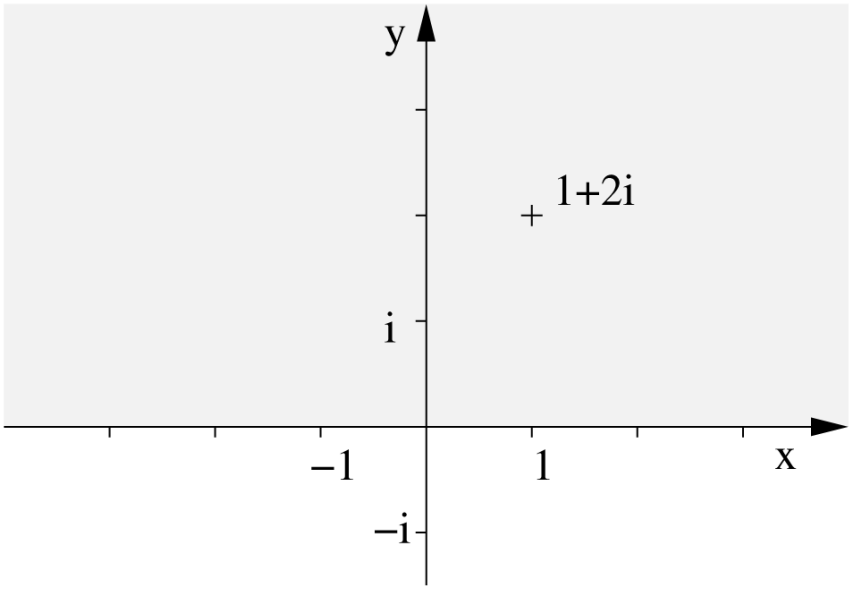
*Komplexe Geometrie*

Schließen wir für unsere geometrischen Betrachtungen direkt an die komplexen Zahlen an. Alle sind von der Form $x+i \cdot y$ mit reellen Zahlen $x,y$. Wir können $x$ und $y$ als kartesische Koordinaten ansehen und die komplexen Zahlen mit der Ebene identifizieren. Dieses ist bereits ein komplex geometrisches Objekt, in gewissem Sinne das einfachste.




(5) Kuchen als Illustration von $\sum_{n=1}^{\infty} \frac{1}{2^n} = 1$ .

Für die Theorie der Modulformen benötigen wir nur einen Teil hiervon, nämlich die *obere Halbebene*. Diese ist genauso definiert, wie der Name es suggeriert, nämlich als der Teil der Ebene, der oberhalb der $x$-Achse liegt. In der Sprache der komplexen Zahlen besteht die obere Halbebene also genau aus den komplexen Zahlen $x+i\cdot y$ mit $y>0$ (siehe Abb. 6).




(6) Obere Halbebene.

Um eine Idee von allgemeineren komplex geometrischen Objekten zu bekommen, betrachtet man am besten zunächst den Zusammenhang zwischen Erdkugel und Weltatlas. Die Erde ist eine Kugel und ihre Oberfläche ‚passt' nicht als Ganzes in ein Buch. Wenn wir uns allerdings auf kleine Ausschnitte (zum Beispiel die Stadt Essen) beschränken, dann merken wir gar nicht, dass wir auf einer Kugel stehen und wir können den Stadtplan als etwas ‚Plattes' auffassen, das dann wohl in ein Buch passt. Wenn wir nun so viele kleine Pläne in unseren Atlas aufnehmen, dass jeder Punkt der Erde in mindestens einem Plan liegt, dann haben wir die Oberfläche der Erde vollständig beschrieben. Genauso geht man vor bei den *Riemannschen Flächen*. Es sind dies geometrische Objekte (wie zum Beispiel die Kugeloberfläche), die im Kleinen so aussehen wie die komplexe Ebene, die man also mit Hilfe eines Atlas beschreiben kann. Betrachtet man nur die so genannten kompakten Riemannschen Flächen, dann kann man sie (bis auf glatte Transformationen) durch die Anzahl ihrer Löcher eindeutig charakterisieren: die Kugel hat kein Loch, der Fahrradreifen (Torus) aus Abbildung (7) hat ein Loch etc.

Die Riemannschen Flächen haben übrigens ihren Eingang in die große Weltliteratur gefunden: 'Near Shepherd's Bush two thousand Beta-Minus mixed doubles were playing Riemann-surface tennis.'[7] 'The nearest Riemann-surfaces were at Guildford.'[8]

Modulformen kann man als bestimmte Funktionen (Differentialformen) auf bestimmten Riemannschen Flächen ansehen. Damit sind Modulformen in der Geometrie verwurzelt. Wie viele essentiell verschiedene Modulformen (eines bestimmten Typs) es zu einer gegebenen Riemannschen Fläche gibt, kann man übrigens ganz einfach an der Anzahl der Löcher ablesen.

*Arithmetische algebraische Geometrie*

Der Ansatz der *arithmetischen algebraischen Geometrie*, vorangetrieben vor allem von Alexander Grothendieck (geboren 1928), ist, Zahlentheorie und Geometrie zu verbinden, indem man Geometrie über Zahlkörpern studiert und insbesondere viele klassische geometrische Sätze auch über Zahlkörpern beweist.

Viele geometrische Objekte, zum Beispiel alle (kompakten) Riemannschen Flächen, die ja zunächst komplex geometrischer Natur sind, haben nämlich eine Struktur über einem Zahlkörper. Das bedeutet, dass die Punkte auf dem Objekt Lösungen von einer oder mehrerer Gleichungen mit Einträgen im Zahlkörper sind (zum Beispiel sind die reellen Lösungen von $x^2+y^2-1=0$ die Punkte auf dem Kreis des Radius 1 um den Nullpunkt; die Einträge der Gleichung sind ganze Zahlen).

**Symmetrien**

*Geometrische Symmetrien*

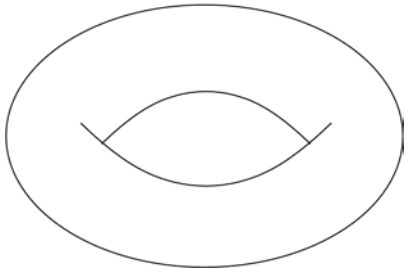
Eine sehr wichtige Methode zur Untersuchung von geometrischen Objekten ist die Betrachtung ihrer *Symmetrien*. Für Modulformen sind die *Möbius-Symmetrien* der oberen Halbebene von grundlegender Bedeutung. Sie sind ganz einfach definiert. Ist $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ ein Element der Modulgruppe (Abb. 8), dann ordnet man ihm die Möbius-Symmetrie zu, die den Punkt $z$ der oberen Halbebene auf den Punkt $\frac{az+b}{cz+d}$ schickt. Betrachten wir zwei Beispiele. Die Symmetrie zum Element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ ergibt sich als ‚$z$ geht auf $z+1$', es handelt sich also um die Verschiebung um 1. Das Element $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ ergibt die Abbildung, die $z$ auf $-\frac{1}{z}$ schickt.

Alle Symmetrien der Modulgruppe kann man durch einen Kunstgriff auch in einem geometrischen Objekt fassen, dem Quotienten beziehungsweise der *Modulkurve* (der Stufe 1). Dieses ist eine Riemannsche Fläche.

*Symmetrien von Zahlkörpern*

Die Betrachtung von Symmetrien von Körpern geht zurück auf Evariste Galois (1811 bis 1832). Eine *Galois-Symmetrie* ist eine Abbildung des Körpers in sich selbst, die die Addition und die Multiplikation respektiert (d.h. ist $\Phi$ die Abbildung und sind a,b Elemente des Körpers, dann gelten $\Phi(a+b)=\Phi(a)+\Phi(b)$ und $\Phi(a \cdot b)=\Phi(a) \cdot \Phi(b)$). Der Zahlkörper $Q(\sqrt{2})$ hat zum Beispiel neben der Identität noch die Galois-Symmetrie, die dadurch charakterisiert ist, dass sie $\sqrt{2}$ auf $-\sqrt{2}$ schickt.

Betrachten wir nun einen Zahlkörper (technische Voraussetzung: galoissch). Für jede unverzweigte Primzahl $p$ gibt es eine Galois-Symmetrie, die *p-Frobenius-Symmetrie*, nach Ferdinand Georg Frobenius (1849 bis 1917). Nun ist es aber so,



(7) Torus.

dass ein Zahlkörper stets nur endlich viele verschiedene Galois-Symmetrien hat. Es ist von großem Interesse zu wissen, welche der endlich vielen verschiedenen Galois-Symmetrien nun zur $p$-Frobenius-Symmetrie für eine gegebene Primzahl $p$ gehört. Denn daraus kann man zum Beispiel ablesen, wie viele Primideale in der Faktorisierung des zu $p$ gehörigen Hauptideals liegen. Die Zuordnung zwischen $p$-Frobenius-Symmetrien und Galois-Symmetrien speichert also die Arithmetik des Zahlkörpers.

Für den Fortgang dieses Artikels spielen Zahlkörper, deren Galois-Symmetriegruppen in einer gewissen großen Familie von Gruppen liegen, die Hauptrolle. Diese Zahlkörper bezeichnen wir als $GL_2$-*Zahlkörper*. Sie sind dadurch ausgezeichnet, dass ihre Galois-Symmetriegruppe aus Elementen der Matrix-Gruppe $GL_2$ über einem endlichen Körper $GF(p^r)$ besteht. Diese Matrix-Gruppe ist ganz genauso definiert wie die Modulgruppe aus Abbildung (8), mit dem einzigen Unterschied, dass die Einträge in den Matrizen (den Viertupeln) jetzt aus dem endlichen Körper $GF(p^r)$ sind und die Determinante jetzt auch jede Zahl ungleich null sein darf.

Es gilt noch viel mehr: Die Galois-Symmetrien eines Zahlkörpers geben auch Symmetrien auf den Punkten von geometrischen Objekten mit einer Struktur über diesem Zahlkörper. Diese Symmetrien sind ganz anderer Natur als die geometrischen Symmetrien, die wir eben behandelt haben.

**Modulformen**

Nun wollen wir genauer auf Modulformen eingehen. Modulformen sind Abbildungen von der oberen Halbebene in die komplexen Zahlen, die durch unendliche Reihen gegeben sind. Eine Modulform $f$ ordnet jedem Punkt $z$ aus der oberen Halbebene aufgrund einer bestimmten Regel einen Punkt $f(z)$ in den komplexen Zahlen zu. Die Regel ist stets von der Art $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$ mit komplexen Zahlen $a_n$. Dabei ist $e$ die Eulersche Zahl (ungefähr 2,71828). Unendlichen Reihen sind wir bereits vorne begegnet; hier sind die $a_n$ so gewählt, dass die Reihen konvergieren und eine komplexe Zahl $f(z)$ definieren.

Dieses alleine macht aber keine Modulform aus, sondern wir haben nur eine *Fourier-Reihe* beschrieben, nach Jean Baptiste Joseph Fourier (1768 bis 1830). Das Besondere an Modulformen ist, dass sie ein spezielles Verhalten bezüglich bestimmter Möbius-Symmetrien aufweisen. Jede Modulform hat eine *Stufe N* und ein *Gewicht k*; beides sind positive natürliche Zahlen.

Die Modulgruppe, bezeichnet mit $SL_2(\mathbb{Z})$, ist die Menge aller $2 \times 2$-Matrizen (d. h. Zahlenviertupel) $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ mit ganzen Zahlen als Einträgen (zum Beispiel $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$), so dass die *Determinante*, das ist die Zahl $ad - bc$, gleich 1 ist.
Man multipliziert zwei Matrizen wie folgt:

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) = \left(\begin{smallmatrix} ar+bt & as+bu \\ cr+dt & cs+du \end{smallmatrix}\right).$$

Ferner gelten

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$$

und

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Diese Eigenschaften, zusammen mit den üblichen Klammerregeln (Assoziativität), fasst man unter dem Namen *Gruppe* zusammen.

(8) Die Modulgruppe.

Bezüglich jeder Möbius-Symmetrie von so genannter Stufe $N$ verlangt man von einer Modulform nun, dass sie eine Symmetrie mit Gewicht $k$ hat (s. Abb. 9 für genauere Aussagen). Es sei noch einmal darauf hingewiesen, dass man Modulformen auch als Funktionen auf bestimmten Riemannschen Flächen, nämlich den Modulkurven (passender Stufe), betrachten kann. Das ist technisch schwieriger, aber der große Vorteil ist, dass die Geometrie deutlicher zum Vorschein kommt.

Modulformen spielen seit ihrer Einführung im 19. Jahrhundert eine zentrale Rolle in der Zahlentheorie. Zu Anfang wurden sie mit Hilfe der Funktionentheorie untersucht. Es wurde früh festgestellt, dass die zugehörigen Fourierkoeffizienten, das sind die $a_n$, häufig interessante zahlentheoretische Bedeutungen haben. So gibt es beispielsweise eine Modulform, deren $n$-ter Fourierkoeffizient angibt, wie oft die natürliche Zahl $n$ als Summe von vier Quadraten dargestellt werden kann.

Für unsere Zwecke stellen sich diejenigen Modulformen als besonders zugänglich heraus, die noch zusätzliche Symmetrien erfüllen.

Eine Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in der Modulgruppe ist von *Stufe* $N$, wenn $c$ durch $N$ teilbar ist. Eine Funktion $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$ ist eine *Modulform* von *Stufe* $N$ und *Gewicht* $k$, wenn für jede Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ von Stufe $N$

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$$

gilt und die technische Bedingung 'Holomorphizität in den Spitzen' erfüllt ist. Man bemerke die Möbius-Symmetrie in der Gleichung!

(9) Modulformen.

Diese zusätzlichen Symmetrien, die *Hecke-Symmetrien*, entstammen auch der Geometrie; sie sind so genannte Korrespondenzen der Modulkurven. Wir nennen Modulformen, die auch den *Hecke-Symmetrien* genügen, sehr *symmetrische Modulformen* oder *Hecke-Eigenformen*. Für sie gilt das wichtige Resultat, dass die $a_n$ in der unendlichen Reihe ganze algebraische Zahlen sind und nicht ‚nur' komplexe. Noch stärker gilt, dass man, wenn man alle möglichen Summen und Produkte aller Bruchzahlen und aller $a_2$, $a_3$, $a_4$ etc. bildet, einen Zahlkörper, den *Koeffizientenkörper* der Modulform, erhält.

## Zusammenhang von Zahlentheorie und Geometrie

### *Symmetrien als Schlüssel*

Kommen wir nun zum eigentlichen Gegenstand dieses Artikels, dem Zusammenhang zwischen Geometrie und Zahlentheorie, der durch Modulformen beschrieben wird, also dem Gegenstand der Serre-Vermutung. Dieser Zusammenhang beruht auf all den Symmetrien, die wir beschrieben haben.

Die Möbius-Symmetrien bewirken zunächst, wie oben schon herausgestellt, dass man eine gegebene Modulform als eine Funktion (Differentialform) auf einer (kompakten) Riemannschen Fläche, der Modulkurve (passender Stufe), betrachten kann. Diese kann als Lösungsmenge von Gleichungen beschrieben werden, deren Einträge ganze Zahlen sind. Damit kommt eine Modulform also von einem geometrischen Objekt mit einer Struktur über dem einfachsten Zahlkörper, den Bruchzahlen. Somit ergibt jede Galois-Symmetrie eines Zahlkörpers auch eine Symmetrie der Modulkurve, wie vorne erklärt wurde.

Der Zusammenhang zwischen Zahlentheorie und Geometrie, der auf Modulformen beruht, ist aber qualitativ noch viel weiter gehender Natur. Er basiert nämlich neben dem gerade Beschriebenen ganz entscheidend auf den zusätzlichen Symmetrien, den Hecke-Symmetrien, die eine sehr symmetrische Modulform erfüllt.

Eine sehr symmetrische Modulform weist also Hecke-Symmetrien und Galois-Symmetrien auf. Erstere sind geometrischer, letztere zahlentheoretischer Natur. Der Zusammenhang zwischen Geometrie und Zahlentheorie ergibt sich aus diesen, denn sie hängen eng zusammen: Die Hecke-Symmetrie $T_p$ für eine Primzahl $p$ bestimmt nämlich die Galois-Symmetrie, die von der $p$-Frobenius-Symmetrie kommt!

| $p$ | $a_p$ | Bedeutung |
|---|---|---|
| 2 | $-1$ | $1^2+23 = 24 = 2\cdot 12$ |
| 3 | $-1$ | $1^2+23 = 24 = 3\cdot 8$ |
| 5 | 0 | 5 teilt nie $n^2+23$ |
| 7 | 0 | 7 teilt nie $n^2+23$ |
| 11 | 0 | 11 teilt nie $n^2+23$ |
| 13 | $-1$ | $4^2+23 = 39 = 13\cdot 3$ |
| ... | ... | ... |
| 997 | 2 | $164^2+23 = 997\cdot 27$ |
| 1009 | 0 | 1009 teilt nie $n^2+23$ |
| ... | ... | ... |

Noch genauere Beschreibung (für Kenner): Der Koeffizient $a_p$ ist 2, wenn das Hauptideal $(p)$ in $\mathbb{Q}(\sqrt{-23})$ das Produkt zweier Hauptideale ist; es ist $a_p = -1$, wenn $(p)$ in zwei nicht-Hauptideale faktorisiert; es ist $a_p = 0$, wenn $(p)$ unzerlegt ist.

(10) Modulform von Stufe 23 und Gewicht 1 – Diskussion.

### *Ein kleines Beispiel*

Hier sei ein erstes ganz einfaches Beispiel des Zusammenhangs zwischen Zahlentheorie und Geometrie mittels Modulformen angeführt. Es ist so einfach, dass nicht alle Phänomene sichtbar werden, aber es gibt doch eine Idee von der Art zahlentheoretischer Information, die in jeder sehr symmetrischen Modulform gespeichert ist. Wie wir unten beschreiben werden, handelt die zahlentheoretische Aussage in voller Allgemeinheit von Zahlkörpern, deren Benutzung wir aber für das erste kleine Beispiel zunächst vermeiden können. Wir betrachten eine bestimmte sehr symmetrische Modulform (von Stufe 23 und Gewicht 1); ihre Fourierkoeffizienten sind stets 0, ±1 oder ±2 und genauer gilt, dass die Koeffizienten $a_p$ für jede Primzahl $p$ (mit der einzigen Ausnahme 23) stets 0, -1 oder 2 sind.

Eine vereinfachte Form des Zusammenhangs zwischen Geometrie und Zahlentheorie besagt das Folgende: Ist der Koeffizient $a_p$ für eine Primzahl $p \neq 23$ gleich -1 oder gleich 2, dann gibt es eine natürliche Zahl $n$, so dass $n^2$+23 durch $p$ teilbar ist. Ist der Koeffizient gleich 0, dann gibt es kein solches n (s. Abb. 10 für ein paar Beispiele). Selbst in diesem kleinen Beispiel sehen wir, welche überhaupt nicht offensichtliche Information in einer Modulform kodiert ist.

Die in diesem aller einfachsten Beispiel behandelten Fragen waren bereits Carl Friedrich Gauß (1777 bis 1855) klar, denn für sie entwickelte er sein Reziprozitätsgesetz. Aber die zahlentheoretische Information, die in den allermeisten anderen nicht so einfachen Fällen enthalten ist, kann man praktisch nur mittels Modulformen erlangen und hat man keine Alternative. Denn es ist sehr schwer, den zur Modulform gehörigen Zahlkörper auszurechnen, also eine definierende Gleichung anzugeben. Ein entsprechender Algorithmus

wurde erst in den letzten Jahren, hauptsächlich von Bas Edixhoven (Leiden), entwickelt. Aber selbst mit diesem Algorithmus erhält man nur in wenigen ‚kleinen' Fällen wirklich den Zahlkörper, denn die Berechnung würde häufig Jahrhunderte oder gar weit über die Lebensdauer des Universums hinausreichen, abgesehen davon, dass mehr Speicher notwendig wäre als es Atome im Universum gibt. Von der Modulform kann man aber trotzdem meist die ersten Koeffizienten berechnen. Die zugehörigen Zahlkörper werden beliebig groß: Gibt man eine beliebige Schranke vor, dann kann man eine Modulform mit zugehörigem Zahlkörper finden, dessen Grad größer als die Schranke ist. Zum Beispiel findet man schon in Stufe 3313 eine Modulform mit Zahlkörper vom Grad mindestens 492525077454 930990153488001251795172563496740880818083349353667553071522143698118524332281262888276797112614682624 (für Kenner, die Zerlegungsgruppe von 2 ist $SL_2$ von $GF(2^{127})$; die Elementanzahl dieser Gruppe ist obige Zahl). Die Modulform gibt aber Informationen über Zahlkörper preis, derer man sonst nie habhaft werden könnte.

### *$GL_2$-Zahlkörper zu einer sehr symmetrischen Modulform*

Wir beschreiben jetzt genauer den Zusammenhang zwischen Geometrie und Zahlentheorie, der von einer sehr symmetrischen Modulform $f(z)=\sum_{n=0}^{\infty} a_n e^{2\pi i n z}$ von Stufe $N$ und Gewicht $k$ herkommt. Zunächst dürfen wir ein beliebiges Primideal im Koeffizientenkörper von $f$ wählen. Wie wir wissen, kann man jede ganze algebraische Zahl im Koeffizientenkörper mittels des Primideals in einen endlichen Körper $GF(q)$ (mit $q$ einer Primzahlpotenz) abbilden, was wir im Folgenden auch tun werden.

Die Hauptaussage ist nun, dass es zur Modulform $f$ und dem gewählten Primideal einen Zahlkörper $K$ gibt, dessen Galois-Symmetriegruppe aus Matrizen in der Matrix-Gruppe $GL_2$ über $GF(q)$ besteht. Damit ist $K$ also ein $GL_2$-Zahlkörper, genauer ein ungerader $GL_2$-Zahlkörper, worauf wir hier aber nicht eingehen. Der versprochene Zusammenhang zwischen Hecke-Symmetrien und Galois-Symmetrien besagt nun das Folgende: Sei $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ die Matrix, die zur $p$-Frobenius-Symmetrie gehört. Dann ist $a+d$, die so genannte Spur, im endlichen Körper gleich der Zahl (dem Koeffizienten) $a_p$ aus der unendlichen Reihe von $f$. Letzterer kommt von der Hecke-Symmetrie $T_p$ (er ist ihr Eigenwert). Weiterhin ist ad-bc, die Determinante, gleich $p^{k-1}$. Übrigens genügen Spur und Determinante in den meisten Fällen, um die Matrix im Wesentlichen eindeutig zu bestimmen.

Damit erhalten wir die schon am Anfang erwähnten grundlegenden Aussagen. Formulieren wir das gerade Beschriebene noch einmal mit anderen Worten: *Die Arithmetik des Zahlkörpers K, die, wie wir oben gesehen haben, mit Hilfe der p-Frobenius-Symmetrien beschrieben werden kann, hängt von den Zahlen $a_p$ der Modulform ab!* Kürzer formuliert: *Die Modulform bestimmt die Arithmetik des Zahlkörpers K.* Anders herum gesehen: *Die Modulform speichert die Arithmetik des Zahlkörpers K.* Man kann sogar über den Zahlkörper $K$ noch mehr sagen, denn man kennt seine verzweigten Primzahlen: Alle diese teilen $N \cdot q$.

Vergessen wir auch nicht, dass wir zunächst ein Primideal *gewählt* haben. Wir hätten unendlich viele andere wählen können und für jedes andere hätten wir einen anderen Körper $K$ erhalten. Somit gibt uns eine sehr symmetrische Modulform eine ganze *Familie*, oder auch ein so genanntes *kompatibles System*, von Zahlkörpern zusammen mit ihrer Arithmetik.

### *Die Serre-Vermutung*

Die Serre-Vermutung beziehungsweise der Satz von Khare, Wintenberger und anderen liefert, wie zu Anfang bereits angedeutet, eine Umkehrung des gerade beschriebenen Sachverhaltes: *Jeder ungerade $GL_2$-Zahlkörper wird durch eine sehr symmetrische Modulform beschrieben.* Die quantitative Form der Vermutung besagt dabei sogar, dass sich die Stufe der Modulform und das Gewicht ausrechnen lassen. Erstere ist in etwa gleich dem Produkt der im Zahlkörper verzweigten Primzahlen, die $q$ nicht teilen. Letztere berechnet sich aus Eigenschaften der Primideale, die $q$ teilen.

Halten wir noch einmal die Hauptaussage fest: *Die Arithmetik aller ungerader $GL_2$-Zahlkörper lässt sich mit Modulformen fassen.*

### *Ein trickreicher Beweis*

Der Beweis der Serre-Vermutung ist sowohl technisch schwer und tief liegend als auch trickreich. Wir können ihn hier verständlicherweise nicht wiedergeben. Der Haupttrick hingegen ist ziemlich zugänglich. Er basiert darauf, dass eine Modulform nicht nur einen $GL_2$-Zahlkörper liefert sondern eine ganze Familie.

Ist $K$ ein ungerader $GL_2$-Zahlkörper, der laut der Serre-Vermutung von einer Modulform der Stufe $N$ herkommen sollte, dann sagen wir kurz, dass $N$ die *Stufe* von $K$ ist.

Zunächst ist es Chandrashekhar Khare gelungen, die Serre-Vermutung zu beweisen für $GL_2$-Zahlkörper von Stufe $N$=1.[9]

Außerdem haben Khare und Wintenberger, übrigens auch Luis Dieulefait (Barcelona), die folgende Reduktionsmethode erdacht, die nach harter technischer Arbeit und unter Zuhilfenahme vieler schwieriger Sätze, vor allem von Mark Kisin und Richard Taylor, schließlich zum Erfolg geführt hat: Sei ein ungerader $GL_2$-Zahlkörper $K$ der Stufe $N$ gegeben. Man kann zu einer Familie von $GL_2$-Zahlkörpern übergehen, zu der $K$ gehört. Dann

stellt man fest, dass diese Familie auch einen anderen ungeraden $GL_2$-Zahlkörper $L$ von Stufe $M$ enthält, wobei $M$ durch eine Primzahl weniger teilbar ist als $N$. Der entscheidende Schluss ist nun, dass, wenn der Zahlkörper $L$ von einer Modulform herkommt, bereits die ganze Familie von einer Modulform herkommt. Insbesondere kommt auch der Zahlkörper $K$ von einer Modulform her.

Dieses erlaubt einem dann ein schrittweises (induktives) Vorgehen. Für Stufe $N$=1 hat Khare die Serre-Vermutung bewiesen. Im nächsten Schritt beweist man die Serre-Vermutung für $GL_2$-Zahlkörper von Stufe $N$, wobei $N$ nur von einer einzigen Primzahl geteilt wird. Mittels der Reduktionsmethode kann man zu einem Zahlkörper $L$ von Stufe $M$=1 übergehen, der nach Khares Satz über Stufe 1 von einer Modulform kommt. Somit kommt auch $K$ von einer Modulform.

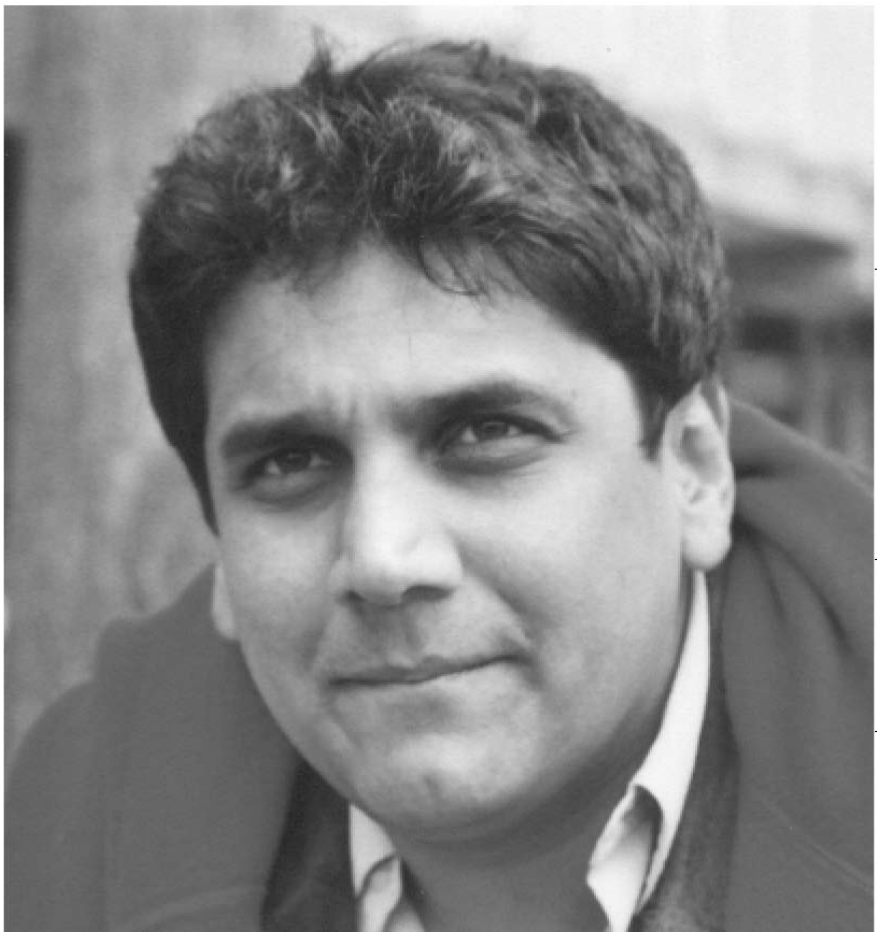
Im folgenden Schritt können wir die Serre-Vermutung für Zahlkörper $K$ zeigen, deren Stufe von genau zwei Primzahlen geteilt wird. Denn mit der Reduktionsmethode kann man zu einem Zahlköper $L$ übergehen, dessen Stufe nur aus einer einzigen Primzahl besteht. Dieser kommt aber von einer Modulform nach vorherigem Schritt. Folglich kommt wiederum $K$ auch von einer Modulform.

So fährt man fort und kann den Fall beliebiger Stufe behandeln.

## Abschließende Bemerkungen und Ausblick

Der hier dargestellte Zusammenhang zwischen Zahlentheorie und Geometrie passt sich in eine sehr große ‚Philosophie', um das Wort ‚Programm' zu vermeiden, ein: die *Langlands-Philosophie*. Diese geht zurück auf die Idee von Robert Langlands (Princeton, geboren 1936), dass automorphe Formen, das sind weit reichende Verallgemeinerungen von Modulformen, zu bestimmten Galois-Darstellungen, das sind Verallgemeinerungen von $GL_2$-Zahlkörpern, korrespondieren sollten. Hatte Langlands wohl hauptsächlich an komplexe Darstellungen gedacht, wurde seine Idee in verschiedenste Kontexte übertragen. Die Serre-Vermutung kann als ein Teil einer *mod p Langlands-Philosophie* aufgefasst werden.

Alle diese ‚Philosophien' suggerieren weitere tiefe und nützliche Zusammenhänge zwischen Geometrie und Zahlentheorie und werden die mathematische Forschung noch über lange Jahre bereichern.[10]



(11) Chandrashekhar Khare.
Quelle: Chandrashekhar Khare


### Summary

Recently one of the most important structural conjectures in pure mathematics, Serre's modularity conjecture, has become a theorem, proved mainly by Khare and Wintenberger. Serre's conjecture establishes a link between seemingly different areas: number theory and geometry. This link is made through modular forms, which are functions dating back to the 19th century.
The main aim of the article is to describe the content of Serre's conjecture in a non-technical language. Moreover, links to past and ongoing research in Essen are mentioned, as well as some consequences of Serre's conjecture.
The article first surveys the objects involved in Serre's conjecture: modular forms and Galois representations. According to a theorem by Deligne and Shimura, any Hecke eigenform gives an odd 2-dimensional Galois representation. This is illustrated by means of a simple example. Serre's

conjecture postulates that the converse is also true: any odd 2-dimensional irreducible Galois representation comes from a Hecke eigenform. The remainder of the article is devoted to explaining these objects in more detail. Different types of 'numbers' and 'fields' are introduced, discussed and compared: algebraic numbers, real numbers, complex numbers, number fields and finite fields. Subsequently, complex geometry, in particular Riemann surfaces, are touched upon, and geometry over number fields (arithmetic geometry) is mentioned. The article emphasizes the role played by symmetries. It takes the point of view that modular forms link geometry and number theory via symmetries: Möbius transforms, Hecke operators and Galois and Frobenius automorphisms are united as different kinds of symmetries. These objects are explained. Modular forms are presented as objects coming from and being rooted in geometry. The link between modular forms and Galois representations provided by Serre's modularity conjecture is finally explained in more detail and one small glimpse on its proof is provided. A final section puts Serre's conjecture into the context of Langlands' philosophy.

---

## *Anmerkungen*

1) Serre 1987.
2) Für einen allgemein verständlichen Überblick siehe Aczel 1997 und Singh 2000.
3) Siehe zum Beispiel Frey 1994.
4) Siehe zum Beispiel Wiese 2004, 2007a, 2007b.
5) Dafür siehe zum Beispiel die bereits erwähnten Bücher Aczel op. cit. und Singh op. cit.
6) Frey op. cit.
7) Huxley, Chapter 4.
8) ibid., Chapter 18.
9) Khare 2006.
10) Den Begriff der Symmetrie auch für Galois-Automorphismen zu verwenden, geht auf einen Vorschlag von Bas Edixhoven zurück. Wie nützlich dieser Hinweis von vor drei Jahren war, ist mir erst beim Schreiben dieses Artikels klar geworden. Für sehr konstruktive Bemerkungen möchte ich Gerhard Frey, Georg Hein und meinem Vater danken.

## *Literatur*

– Aczel, Amir D.: Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem, Delta, 1997.
– Frey, Gerhard (Hrsg.): On Artin's conjecture for odd 2-dimensional representations, Lecture Notes in Math., 1585, Springer, Berlin, 1994.
– Huxley, Aldous: Brave new world. Eine freie Version findet sich auf http://www.huxley.net/bnw/
– Khare, Chandrashekhar: Serre's modularity conjecture: the level one case. Duke Math. J. 134 (2006), no. 3, 557-589.
– Khare, Chandrashekhar und Wintenberger, Jean-Pierre: Serre's modularity conjecture (I and II). Vorveröffentlichung, 2007.
– Serre, Jean-Pierre: Sur les représentations modulaires de degré 2 de Gal($\overline{Q}$/Q), Duke Math. J. 54 (1987), no. 1, 179-230.
– Singh, Simon: Fermats letzter Satz: Die abenteuerliche Geschichte eines mathematischen Rätsels, DTV, 2000.
– Wiese, Gabor: Multiplicities of Galois representations of weight one. With an appendix by Niko Naumann. Algebra & Number Theory 1 (2007), no. 1, 67-85.
– Wiese, Gabor: On the faithfulness of parabolic cohomology as a Hecke module over a finite field. J. Reine Angew. Math. 606 (2007), 79-103.
– Wiese, Gabor: Dihedral Galois representations and Katz modular forms. Doc. Math. 9 (2004), 123-133.

## *Der Autor*

Gabor Wiese, geboren 1976, studierte Mathematik von1996 bis 2001 in Heidelberg und Cambridge (1999 bis 2000). Er begann mit seiner Promotion in Rennes und schloss sie in Leiden im Jahr 2005 ab. Danach war Wiese wissenschaftlicher Mitarbeiter an der Universität Regensburg. Seit März 2007 ist er Juniorprofessor für Arithmetische Geometrie am Institut für Experimentelle Mathematik der Universität Duisburg-Essen. Gabor Wieses Arbeitsgebiet ist die „explizite arithmetische Geometrie". Explizite Methoden, zum Beispiel Computerberechnungen, spielen dabei eine große Rolle, um einerseits Vermutungen zu überprüfen und andererseits solche aus der Kenntnis einer Vielzahl an Beispielen abzuleiten. Derzeit forscht er über verschiedene Fragestellungen zu zahlentheoretischen Anwendungen der im Text erwähnten Modulformen.

**DOI:** 10.17185/duepublico/73809
**URN:** urn:nbn:de:hbz:464-20210204-160202-8