Die Serresche Modularitätsvermutung und Computer-Algebra

Gabor Wiese*

5. Oktober 2010

In den Jahren 2004-2007 wurde die Serresche Modularitätsvermutung von Chandrashekhar Khare, Jean-Pierre Wintenberger und Mark Kisin ([9], [10], [12]) bewiesen. In meinen Augen stellt dies einen wichtigen Meilenstein in der arithmetischen Geometrie und Zahlentheorie dar. Dieses Resultat muss als eine weit reichende Verallgemeinerung des Satzes von Wiles und Taylor zur Modularität von rationalen elliptischen Kurven angesehen werden, der den großen Satz von Fermat impliziert. Auch für die Computer-Algebra ist die Serresche Modularitätsvermutung, kurz: Serre-Vermutung, von großer Bedeutung, wie wir in diesem Artikel ausführen wollen.

Ganz grob gesprochen stellt die Serre-Vermutung eine explizite Korrespondenz zwischen bestimmten komplexen Funktionen, den *Modulformen*, und *Zahlkörpern* einer bestimmten Bauart her. Da Modulformen mittels Computer-Algebra berechnet werden können, ergibt sich so ein Zugang, auch Eigenschaften der Zahlkörper, die mit anderen Methoden nicht zugänglich sind, explizit zu bestimmen.

Modulformen

Modulformen wurden bereits im 19. Jahrhundert in der Funktionen- und der Zahlentheorie unter anderen von Jacobi, Kronecker, Eisenstein und Weierstraß und später von Poincaré und Klein studiert. Ein berühmtes, wunderschönes Resultat dieser Zeit ist eine Formel für die Anzahl der Möglichkeiten, eine gegebene natürliche Zahl als Summe von vier Quadraten darzustellen. Man liest sie sofort durch Koeffizientenvergleich aus der auf Jacobi zurückgehenden Identität

$$\Big(\sum_{n=-\infty}^{\infty} q^{n^2}\Big)^4 = \sum_{a,b,c,d\in\mathbb{Z}} q^{a^2+b^2+c^2+d^2} = 1 + 8\sum_{m=1}^{\infty}\Big(\sum_{d|m,4\nmid d} d\Big)\, q^m \tag{1}$$

ab. Die linke Seite ist eine Theta- und die rechte eine Eisenstein-Reihe. Beides sind Modulformen und die Gleichheit folgt aus der Eindimensionalität des zugehörigen Vektorraums der Modulformen.

Die Definition einer Modulform ist sehr einfach. Jede Modulform hat zwei Invarianten; zunächst benötigen wir nur das *Gewicht*, eine ganze Zahl. Eine Modulform vom Gewicht k ist eine holomorphe (d. h. differentierbare) komplexwertige Funktion auf der oberen Halbebene $\mathbb{H} := \{z = x + iy \in \mathbb{C} \mid y > 0\}$, also $f : \mathbb{H} \to \mathbb{C}$, die die Transformationseigenschaft

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z) \tag{2}$$

für alle ganzzahligen Matrizen $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ der Determinante 1 erfüllt und die darüber hinaus auch in den Spitzen holomorph ist, was wir sofort erklären. Die Transformationsformel für $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ ergibt $f(z+1) = f(z)$, also eine Periodizität mit Periode 1, weshalb sich f in eine Fourier-Reihe

$$f(z) = \sum_n a_n(f)\, e^{2\pi i n z} = \sum_n a_n(f)\, q^n \tag{3}$$

*Ich danke Johan Bosman für eine kritische Lektüre des Artikels.

mit Fourier-Koeffizienten $a_n(f) \in \mathbb{C}$ entwickeln lässt, wobei wir $q = q(z) = e^{2\pi iz}$ als Abkürzung einführen. Die Holomorphie in den Spitzen bedeutet einfach, dass alle Koeffizienten $a_n(f)$ für negative n gleich 0 sind. Ist zudem $a_0(f) = 0$, dann nennt man f eine *Spitzenform*.

Die zweite Invariante einer Modulform ist ihre *Stufe*. Man verallgemeinert obige Definition, die der Stufe 1 entspricht, wie folgt zu Stufe N: Die Transformationsformel (2) wird nur für solche Matrizen gefordert, bei denen N sowohl c als auch $d-1$ teilt; außerdem muss die Holomorphie in den Spitzen etwas anders formuliert werden.[1]

Hecke-Operatoren

Erich Hecke führte in der ersten Hälfte des 20. Jahrhunderts eine wichtige algebraische Struktur auf Räumen von Modulformen ein, indem er lineare Operatoren definierte, die wir heute *Hecke-Operatoren* nennen. Für jede natürliche Zahl n gibt es einen Hecke-Operator T_n. Dieser kann durch eine einfache Formel auf den Koeffizienten der Fourier-Reihe definiert werden, hat aber auch eine geometrische Erklärung. Da die Hecke-Operatoren untereinander vertauschen, gibt es Modulformen, die Eigenfunktionen für alle Hecke-Operatoren sind. Diese nennen wir *Hecke-Eigenformen*. Ist f eine Hecke-Eigenform, so ist der Eigenraum zu den Eigenwerten der Hecke-Operatoren auf f eindimensional, wird also von f erzeugt. Wir nennen f normiert, falls $a_1(f) = 1$ gilt. Bemerkenswert ist, dass dann der Eigenwert von T_n gleich dem Fourier-Koeffizienten $a_n(f)$ ist. Für das Folgende wollen wir uns merken:

> **Die Kenntnis der Hecke-Operatoren ist äquivalent zur Kenntnis der Modulformen.**

Modulsymbole: Modulformen auf dem Computer

Die angenehmste Form, eine Modulform auf dem Computer darzustellen, ist, die ersten Koeffizienten der Fourier-Enwicklung abzuspeichern. Da für festes Gewicht und feste Stufe der Vektorraum der Modulformen endlichdimensional ist, ist dies auch genug und einfache Formeln geben an, wieviele Koeffizienten man höchstens abzuspeichern braucht.

Es gibt mehrere Methoden, Modulformen auszurechnen, von denen ich die am weitesten verbreitete hier kurz einführen möchte: *Modulsymbole*. Diese gehen auf Bryan Birch zurück; einen richtigen Aufschwung erlebten sie durch John Cremona, der sie zur Berechnung modularer elliptischer Kurven verwendet hat [6]. Der Hintergrund hierzu ist, dass die Hodge-Zerlegung einen Isomorphismus zwischen dem Vektorraum der ersten Homologie der sogenannten Modulkurve zu Stufe N und zwei Kopien des Raumes der Modulformen derselben Stufe und Gewicht 2 ergibt. Durch Einführung eines lokalen Systems kann man auch beliebiges größeres Gewicht erreichen.

Die oben erwähnte geometrische Beschreibung der Hecke-Operatoren lässt sie auch auf der Homologie linear operieren. Da die Kenntnis der Hecke-Operatoren ja genügt, um Modulformen zu beschreiben, brauchen wir also nur die Hecke-Operatoren auf der Homologie zu berechnen. Die erste Homologie hat eine kombinatorische Beschreibung mittels des Modulsymbolformalismus (siehe zum Beispiel [13]), die zu einer Darstellung des Vektorraums der ersten Homologie auf dem Computer verwendet wird. Hier sind zwei Punkte zu betonen:

> **Hecke-Operatoren sind explizit gegebene lineare Abbildungen auf dem Vektorraum der Modulsymbole.**

Homologie kann man mit rationalen Koeffizienten definieren, genauso wie Modulsymbole. Daraus kann man zum Beispiel schließen, dass der Vektorraum der Modulformen zu beliebigem Gewicht und beliebiger Stufe eine Basis bestehend aus Modulformen besitzt, deren sämtliche Fourier-Koeffizienten rationale Zahlen sind. Dieses hat zur Konsequenz:

> **Alle Rechnungen können mit rationalen Zahlen, also exakt, durchgeführt werden.**[2]

[1] Für die allgemeine Definition sei auf die Vielzahl an Lehrbüchern zu Modulformen verwiesen.

[2] Das ist bei den reellen Analoga, den Maaß-Formen, nicht der Fall.

Modulformen in MAGMA und SAGE

Die Berechnung von Modulformen mittels Modulsymbolen ist in den Computer-Algebra-Systemen MAGMA und SAGE implementiert. Beide Implementationen gehen auf William Stein, den Hauptinitiator von SAGE, zurück. In seinem Lehrbuch [13] beschreibt er sehr detailliert die verwendeten Algorithmen und gibt eine große Anzahl an Beispielen. Kilfords Lehrbuch zu Modulformen [11] enhält ebenfalls viele Beispiele zur Berechnung von Modulformen in MAGMA und SAGE.

Zahlkörper

Ein frühes Beispiel zur zahlentheoretischen Bedeutung von Modulformen haben wir oben bereits gesehen. Weitergehende Bedeutung erlangten Modulformen in der zweiten Hälfte des 20. Jahrhunderts, da sie zahlentheoretische Strukturen auf eine sehr tief liegende Weise beschreiben. Diese kann man leicht formulieren. Um dies zu tun, müssen wir allerdings etwas ausholen.

Ein ganz wichtiges Hilfsmittel der algebraischen Zahlentheorie sind sogenannte *Zahlkörper*. Man erhält einen Zahlkörper als diejenigen komplexen Zahlen, die sich als Linearkombination mit rationalen Koeffizienten von Potenzen der Nullstelle eines rationalen Polynoms schreiben lassen. Jeder Zahlkörper ist ein endlichdimensionaler $\mathbb{Q}$-Vektorraum; die Dimension nennt man den *Grad* des Zahlkörpers. Der berühmteste Zahlkörper ist wohl der der Gaußschen Zahlen, den man aus $\mathbb{Q}$ und $i = \sqrt{-1}$ erhält. Mit seiner Hilfe kann man under anderem zeigen, dass es genauso viele Primzahlen gibt, die beim Teilen durch 4 den Rest 1 lassen, wie solche deren Rest 3 ist.

Beim Rechnen in Zahlkörpern muss man aber etwas aufpassen, da man keine eindeutige Primzerlegung mehr hat. Wir erinnern uns an die Aussage des Hauptsatzes der elementaren Zahlentheorie, dass sich jede natürliche Zahl auf bis auf die Reihenfolge eindeutige Art als Produkt von Primzahlen darstellen lässt. Kummer hat, um diesem Mangel in Zahlkörpern abzuhelfen, sogenannte *Ideale* eingeführt und gezeigt, dass sich jedes Ideal eindeutig als Produkt von Primidealen schreiben lässt. Das ist dann so: Für jede Primzahl p gibt es ein oder mehrere eindeutig bestimmte paarweise verschiedene Primideale $P_1, \ldots, P_r$, so dass sich das Hauptideal zu p als Produkt

$$(p) = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r} \tag{4}$$

faktorisiert. Der Normalfall ist $e_1 = \ldots = e_r = 1$; diesen nennt man *unverzweigt*. In den Gaußschen Zahlen gilt zum Beispiel $(p) = P_1 P_2$ mit zwei verschiedenen Idealen genau dann, wenn p beim Teilen durch 4 den Rest 1 lässt; ist der Rest 3, dann gibt es genau ein Ideal; nur $p = 2$ ist verzweigt. Eine wichtige Frage der *Arithmetik eines Zahlkörpers* ist:

> **Wie faktorisiert (p) als Produkt von Primidealen in einem Zahlkörper?**

Galois-Symmetrien

In diesem Artikel möchte ich Selbstabbildungen eines Zahlkörpers als *Galois-Symmetrien* (nach Evariste Galois) bezeichnen. Die Gruppe aller Galois-Symmetrien heißt *Galois-Gruppe*.[3]

Um jetzt den Bezug zur Frage herzustellen, betrachten wir *Frobenius-Symmetrien*: Für jedes unverzweigte Primideal P im Zahlkörper gibt es die Galois-Symmetrie Frob_P: Wenn wir die ganzen Zahlen des Zahlkörpers modulo P nehmen, erhalten wir eine endliche Erweiterung des Körpers mit p Elementen, und die Galois-Symmetrie Frob_P ist dadurch charakterisiert, dass sie auf dem endlichen Körper als p-te Potenz operiert. Da Frob_P durch p bis auf Konjugation bestimmt ist, schreiben wir einfach Frob_p. Es gilt, dass die Anzahl r aus Gleichung (4) mal der Ordnung von Frob_p den Grad des Zahlkörpers ergibt.

> **Die Frobenius-Symmetrien Frob_p in der Galois-Gruppe eines Zahlkörpers beschreiben, wie sich Primzahlen im Zahlkörper in Primideale faktorisieren.**

Das wollen wir wissen und das können wir in bestimmten Fällen mittels Modulformen ausrechnen! Dazu kommen wir in Kürze. Für das Weitere bezeichne $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ die Galois-Gruppe des algebraischen Abschlusses von $\mathbb{Q}$ in $\mathbb{C}$: Es ist die Gruppe aller Galois-Symmetrien.

[3] Wir nehmen in diesem Artikel stets an, dass die Anzahl der Galois-Symmetrien der Zahlkörper gleich deren Grad ist, dass die Zahlkörper also *galoissch über* $\mathbb{Q}$ sind.

Galois-Darstellungen

Um Gruppen zu studieren, benutzt man Darstellungen. Ist die Gruppe eine Galois-Gruppe, so spricht man von einer *Galois-Darstellung*. Die Spur einer Darstellung nennt man *Charakter*, und der Charakter bestimmt absolut irreduzible Darstellungen eindeutig. Wir erinnern uns, dass die Spur einer Matrix als die Summe ihrer Diagonaleinträge definiert ist und dass sie unter Konjugation invariant ist. Daher können wir nun eindeutig vom Wert bei Frob_p des Charakters einer Galois-Darstellung reden. Man weiß, dass diese Werte den Charakter eindeutig festlegen, wenn p die Primzahlen durchläuft.[4]

Der Satz von Shimura und Deligne

Um die Verbindung zu den Modulformen herzustellen, blicken wir zurück auf deren Berechnung. Dazu werden, wie oben erwähnt, Modulsymbole, also die erste Homologie der entsprechenden Modulkurve, verwendet. Betrachtet man die Modulkurve genauer, stellt man fest, dass sie als Lösungsmenge von Polynomen mit rationalen Koeffizienten geschrieben werden kann. Somit ergibt jede Galois-Symmetrie, also jedes Element von $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, insbesondere Frob_p, eine Selbstabbildung der Modulkurve. Weiter hat dies zur Folge, dass Methoden der arithmetischen Geometrie, die auf Grothendieck zurückgehen, greifen und man statt Homologie auch ℓ-adische Etale-Kohomologie verwenden kann.[5] Insgesamt haben wir somit auf den Modulsymbolen zwei lineare Operationen: die der Hecke-Operatoren und die von $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Sei f eine normierte Hecke-Eigenform.[6] Da der Eigenraum zu den Hecke-Eigenwerten auf f im Raum der Modulformen eindimensional ist, folgt, dass der entsprechende Eigenraum in der ersten Homologie die Dimension 2 hat. Da die Hecke-Operatoren mit den Galois-Symmetrien vertauschen, erhält man eine stetige lineare $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-Operation auf diesem Raum, also eine (ℓ-adische) Galois-Darstellung

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell). \tag{5}$$

Durch Analyse der Reduktion der Modulkurve modulo p konnten Eichler, Shimura und Deligne zeigen, dass der Charakter $\Theta_{f,\ell}$ dieser Darstellung für alle unverzweigten p die bemerkenswert einfache Formel

$$\Theta_{f,\ell}(\mathrm{Frob}_p) = a_p(f) \tag{6}$$

erfüllt, dass er also durch die Koeffizienten der Modulform f gegeben ist! Weiter gilt, dass $\Theta_{f,\ell}$ bei der komplexen Konjugation den Wert 0 annimmt. Man sagt dafür, dass die Galois-Darstellung *ungerade* ist. Wir halten fest:

Jede Hecke-Eigenform beschreibt eine ungerade ℓ-adische Galois-Darstellung.

Zahlkörper zu residuellen Galois-Darstellungen

Für den Rest dieses Artikels beschränken wir uns auf eine Konsequenz hiervon: Durch Reduktion modulo ℓ erhalten wir die (residuelle) Darstellung

$$\overline{\rho}_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell). \tag{7}$$

Galois-Theorie zeigt, dass es dann einen Zahlkörper $K_{f,\ell}$ gibt, dessen Galois-Gruppe eine Untergruppe von $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ ist. Dieser Zahlkörper ist vollständig durch f bestimmt, seine Galois-Gruppe kann einfach berechnet werden, und für die meisten p kann man aus $a_p(f)$ modulo ℓ bestimmen, in wieviele Primideale p in K_f faktorisiert.

Die Fourier-Koeffizienten der Hecke-Eigenform f beschreiben für jede Primzahl ℓ die Arithmetik des Zahlkörpers $K_{f,\ell}$.

[4] Es dürfen sogar endlich viele Primzahlen ausgelassen werden.

[5] Hier und im Folgenden sei ℓ eine Primzahl.

[6] Wir sehen im Folgenden ihre Koeffizienten als Elemente von $\overline{\mathbb{Q}}_\ell$ via einer fixierten Einbettung $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$.

Normalerweise stellt man einen Zahlkörper als Quotienten des Polynomringes über $\mathbb{Q}$ modulo einem rationalen Polynom dar. Wir bezeichnen mit $\phi_{f,\ell}$ ein Polynom zu $K_{f,\ell}$. Die Zahlkörper $K_{f,\ell}$ und somit auch die Polynome $\phi_{f,\ell}$ werden allerdings sehr schnell sehr groß. Zum Beispiel würde selbst unter der Annahme, dass alle Koeffizienten nur 0 oder 1 sind, also durch ein Bit beschrieben werden können, das Polynom $\phi_{f,2}$ zu einer bestimmten Eigenform f in Stufe 3313 und Gewicht 2 bereits 10^{28} GB Speicher einnehmen. Ginge man weiter, überschritte man so sicherlich die Anzahl der Atome im Universum recht schnell. Umso erstaunlicher ist, dass wir mittels der Modulform über den Zahlkörper doch wichtige arithmetische Aussagen treffen können!

Der Algorithmus von Edixhoven et. al.

Umgekehrt, wenn man in kleinem Grad ist und ein Polynom $\phi_{f,\ell}$ zum Zahlkörper $K_{f,\ell}$ kennt, dann kann man es benutzen, um Modulformen modulo ℓ auszurechnen. Macht man dies für genügend viele ℓ, erhält man Koeffizienten der Modulform aus dem chinesischen Restsatz, da die Koeffizienten beschränkt sind. Die Berechnung von $a_p(f)$ aus dem Polynom besteht im Wesentlichen aus der Faktorisierung des Polynoms modulo p.

Die neueste sehr wichtige Entwicklung in diesem Gebiet ist ein Algorithmus, der in den letzten Jahren von Edixhoven, Couveignes und anderen [8] entwickelt und in einer Variante von Johan Bosman implementiert wurde: Zu einer Eigenform f und einer Primzahl ℓ wird das Polynom $\phi_{f,\ell}$ berechnet. Dieses erlaubt also insbesondere die Berechnung der Koeffizienten von Modulformen. In seiner gerade verteidigten Doktorarbeit beweist Peter Bruin [2], dass (unter der technischen Annahme quadratfreier Stufe und der verallgemeinerten Riemannschen Vermutung) die Komplexität der Berechnung von $a_p(f)$ mit dieser Methode polynomial in der Bitlänge von p, also $\log(p)$, ist. Die Komplexität im Modulsymbolalgorithmus ist polynomial in p, also exponentiell in $\log(p)$. Die obige Speicherabschätzung zeigt aber bereits, dass trotz dem theoretischen Vorteil bei diesem Verfahren praktische Probleme auftreten.

Man kann den neuen Algorithmus als einen Schritt hin zur Verallgemeinerung konstruktiver Klassenkörpertheorie auf GL_2 ansehen. Als kleine Illustration kann dienen, dass Johan Bosman [1] mit seiner Implementierung das erste bekannte Polynom mit Galois-Gruppe $\mathrm{SL}_2(\mathbb{F}_{16})$ gefunden hat.

Die Serresche Modularitätsvermutung

Nach diesem Exkurs über die Berechnung der Galois-Darstellungen zu einer Eigenform kommen wir jetzt zur Serre-Vermutung, also dem Satz von Khare, Wintenberger und Kisin:

> **Jede irreduzible[7] ungerade Galois-Darstellung** $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ **kommt von einer Eigenform f, ist also von der Form $\overline{\rho}_{f,\ell}$.**

Der Satz ist sogar noch viel stärker: Er gibt Formeln für die Stufe und das Gewicht der zugehörigen Modulform an. Die Stufe berechnet sich dabei aus der Verzweigung in Primzahlen ungleich ℓ und das Gewicht aus der Verzweigung bei ℓ. Eine Umformulierung ist, dass Hecke-Eigenformen zweidimensionale irreduzible ungerade Galois-Darstellungen parametrisieren.

Konsequenzen

Eine Motivation für Serre bei seiner Vermutung war, dass sie den *großen Satz von Fermat* impliziert. Somit gibt es jetzt auch einen neuen Beweis dieses Satzes.[8] Der Startpunkt ist auch hierbei die Idee von Gerhard Frey, einer hypothetischen ganzzahligen Lösung der Gleichung $a^p + b^p = c^p$ die elliptische Kurve $y^2 = x(x-a^p)(x+b^p)$ zuzuordnen; ihre p-Teilungspunkte geben eine irreduzible ungerade Galois-Darstellung. Nach der Serre-Vermutung gehört hierzu eine Hecke-Eigenform von Stufe 2 und Gewicht 2. Eine solche gibt es aber nicht, somit gibt es auch nicht die hypothetische Lösung. Von diesem Beweistyp sind viele Variationen mit ähnlichen Gleichungen möglich.

[7] Irreduzibilität ist keine Einschränkung, da reduzible halbeinfache Galois-Darstellungen vollständig durch Klassenkörpertheorie beschrieben werden können.

[8] Da die Methoden zum Beweis der Serre-Vermutung Weiterentwicklungen derer von Wiles sind, kann man aber nicht von einem grundsätzlich verschiedenen Beweis reden.

Die Serre-Vermutung hat aber auch die *Taniyama-Shimura-Vermutung*, die von Wiles und Taylor im Spezialfall semistabiler elliptischer Kurven für den ursprünglichen Beweis des Satzes von Fermat gelöst worden ist, samt ihrer Verallgemeinerung auf rationale abelsche Varietäten vom GL_2-Typ zur Folge: *Diese sind modular*, d. h. ihre L-Reihe stimmt mit der einer Modulform überein. Eine weitere Konsequenz der Serre-Vermutung ist die berühmte *Artin-Vermutung*, also die analytische Fortsetzbarkeit der L-Reihe von komplexen Galois-Darstellungen, im Spezialfall ungerader Darstellungen $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$.

Bedeutung in der Computer-Algebra

Die wichtigsten Konsequenzen der Serre-Vermutung für die Computer-Algebra wollen wir noch einmal auflisten:

1. **Modulformen, die mit Computer-Algebra berechnet werden können, parametrisieren Galois-Darstellungen obigen Typs.**
2. **Wichtige arithmetische Eigenschaften dieser Galois-Darstellungen lassen sich durch Rechnungen mit Modulformen bestimmen.**

Eine theoretische Konsequenz der Serre-Vermutung ist der Satz, dass es für jede Primzahl ℓ nur endlich viele Isomorphieklassen von irreduziblen ungeraden und außerhalb von ℓ unverzweigten Darstellungen $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ gibt. Mithilfe der Computer-Algebra kann man also all diese auflisten und das Wachstum ihrer Anzahl als Funktion von ℓ studieren (siehe [5] und [4] für neue Arbeiten).

Ich beschäftige mich derzeit unter anderem, theoretisch und mittels Computer-Algebra, mit der Rolle von Modulformen vom Gewicht eins und arbeite zusammen mit Panagiotis Tsaknias daran, Eigenschaften ℓ-adischer Galois-Darstellungen durch Modulformen modulo ℓ^n zu bestimmen.

Ausblick

Mit dem Beweis der Serre-Vermutung wurde zwar ein Kapitel abgeschlossen; es ist aber nur das erste Kapitel eines großen Buches, dessen Umfang wir noch nicht abschätzen können. Emerton versteht die Serre-Vermutung als eine Lokal-Global-Kompatibilitätsaussage im mod-p-Langlands-Programm von Breuil und Colmez. Auch gibt es Formulierungen von "Serre-Vermutungen" für Hilbertsche Modulformen [3] und für Modulformen über imaginär-quadratischen Zahlkörpern [14]. Für all diese gibt es einige numerische Evidenz, die mittels Computer-Algebra gewonnen wurde (z. B. [7]). Wir dürfen gespannt sein, wie die Entwicklungen fortschreiten. Die Computer-Algebra wird dabei ihre Rolle spielen.

Literatur

[1] Johan Bosman. *A polynomial with Galois group* $\mathrm{SL}_2(\mathbb{F}_{16})$. LMS J. Comput. Math. 10 (2007), 378–388.

[2] Peter Bruin. *Modular curves, Arakelov theory, algorithmic applications.* Dissertation, Universiteit Leiden, 2010.

[3] Kevin Buzzard, Fred Diamond and Frazer Jarvis. *On Serre's conjecture for mod l Galois representations over totally real fields.* arXiv:0810.2106.

[4] Tommaso Giorgio Centeleghe. *Computing the number of certain Galois representations mod* p. 28 Seiten, arXiv:1008.2059.

[5] Craig Citro and Alexandru Ghitza. *Enumerating Galois representations in Sage.* 4 Seiten, arXiv:1006.4084v2.

[6] J. E. Cremona. *Algorithms for modular elliptic curves.* Second edition. Cambridge University Press, Cambridge, 1997. Online-Version: http://www.warwick.ac.uk/∼masgaj/book/fulltext/index.html

[7] Lassina Dembélé. *Anhang zum Artikel "Sur une question de compatibilité local-global modulo p" von Christophe Breuil*. Preprint, 2009.

[8] Bas Edixhoven, Jean-Marc Couveignes, Robin de Jong, Franz Merkl, Johan Bosman. *Computational aspects of modular forms and Galois representations.* 438 Seiten, erscheint als Buch in der Serie 'Annals of Mathematics Studies' bei Princeton University Press, arXiv:math/0605244v3.

[9] Chandrashekhar Khare and Jean-Pierre Wintenberger. *Serre's modularity conjecture. I.* Invent. Math. 178 (2009), no. 3, 485–504.

[10] Chandrashekhar Khare and Jean-Pierre Wintenberger. *Serre's modularity conjecture. II.* Invent. Math. 178 (2009), no. 3, 505–586.

[11] L. J. P. Kilford. *Modular Forms. A classical and computational introduction.* Imperial College Press, London, 2008.

[12] Mark Kisin. *Modularity of 2-adic Barsotti-Tate representations.* Invent. Math. 178 (2009), no. 3, 587–634.

[13] William Stein. *Modular forms, a computational approach.* With an appendix by Paul E. Gunnells. Graduate Studies in Mathematics, 79. American Mathematical Society, Providence, RI, 2007.

[14] Rebecca Torrey. *On Serre's Conjecture Over Imaginary Quadratic Fields.* Dissertation, King's College London, 2009.