Zusammenfassung der Doktorarbeit

Modular Forms of Weight One Over Finite Fields

von Gabor Wiese.

In dieser kurzen Zusammenfassung möchte ich eine möglichst allgemein verständliche Einführung in das Gebiet der vorliegenden Arbeit und einen Überblick über diese geben.

Modulformen spielen seit ihrer Einführung im 19. Jahrhundert eine zentrale Rolle in der Zahlentheorie. Zu Anfang wurden sie mit Hilfe der Funktionentheorie untersucht, da die zugehörigen Fourierkoeffizienten häufig interessante zahlentheoretische Bedeutungen haben. So gibt es z. B. eine Modulform, deren n-ter Fourierkoeffizient angibt, wie oft die natürliche Zahl n als Summe von 8 Quadraten dargestellt werden kann. Seit den 60er Jahren hat sich die Sprache der algebraischen Geometrie, besonders der *arithmetischen algebraischen Geometrie*, in vielen Bereichen der Zahlentheorie als sehr nützlich erwiesen. Auf Grund von Einsichten von Shimura, Weil, Serre und Deligne wurde diese neue Sprache mit viel Erfolg auch auf die Theorie der Modulformen angewandt und hat einige tief liegende Zusammenhänge zu Tage gebracht. Als spektakulärer bisheriger Höhepunkt ist der Beweis der Fermatschen Vermutung zu nennen, den Andrew Wiles 1994 gefunden hat. Diese Vermutung 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.

Den Zusammenhang zwischen Zahlentheorie und Geometrie möchte ich an einem einfachen Beispiel andeuten. Nehmen wir die Gleichung

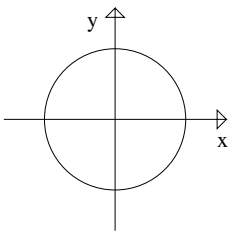
$$a^2 + b^2 = c^2.$$

Im Gegensatz zum Fermatproblem hat diese Gleichung Lösungen, nämlich die wohlbekannten Pythagoräischen Tripel, z. B. $3^2 + 4^2 = 5^2$ oder $5^2 + 12^2 = 13^2$. Schreiben wir $x = \frac{a}{c}$ und $y = \frac{b}{c}$, dann erhalten wir durch einfache Umformungen die Gleichung

$$x^2 + y^2 - 1 = 0.$$

Wir können zunächst alle reellen Lösungen betrachten (d. h. wir erlauben Zahlen mit beliebiger, also auch unendlicher und nicht periodischer Dezimalschreibweise).

Mittels der Parametrisierung $x = \cos(\varphi)$ und $y = \sin(\varphi)$ sehen wir, dass die reellen Lösungen gerade den Einheitskreis bilden (d. h. den Kreis von Radius 1 um den Ursprung der Koordinatenebene). Damit sind wir nun ganz offensichtlich in der Welt der Geometrie! Unsere Frage nach den Pythagoräischen Tripeln übersetzt sich dann in die Frage nach Punkten auf dem Einheitskreis, deren Koordinaten Bruchzahlen (diese nennen wir *rationale Zahlen*) sind.



Es stellt sich heraus, dass sich die Gleichung $a^2 + b^2 = c^2$ leichter untersuchen lässt, wenn man nicht nur Bruchzahlen zulässt, sondern auch die Zahl i, welche als eine Wurzel von -1 definiert ist, also als eine Lösung der Gleichung

$$X^2 + 1 = 0.$$

Nach dem Hauptsatz der Algebra hat nämlich jede solche Gleichung über den komplexen Zahlen so viele Lösungen (mit Multiplizitäten gezählt) wie der Grad ist; hier also zwei, und die Lösungen sind i und $-i$.

Wir werden in den Gaußschen Zahlen rechnen. Das sind alle Zahlen, die man durch Addition und Multiplikation von ganzen Zahlen und der Zahl i erhält. Es ist einfach einzusehen, dass sich jede Gaußche Zahl schreiben lässt als $a + ib$ mit ganzen Zahlen a und b. Erinnern wir uns, dass eine positive natürliche Zahl ungleich 1 *Primzahl* heißt, wenn die einzigen positiven Teiler 1 und die Zahl selbst sind. Jede ganze Zahl ungleich 0 lässt sich auf bis auf die Reihenfolge eindeutige Weise als plus oder minus einem Produkt von Primzahlen schreiben, z. B. ist $12 = 2 \cdot 2 \cdot 3$. Etwas ganz Ähnliches gilt in den Gaußschen Zahlen. Die einzigen Gaußschen Zahlen, die jede beliebige Gaußsche Zahl teilen, sind $1, -1, i, -i$; diese heißen Gaußsche Einheiten. Eine Gaußsche Primzahl ist eine Gaußsche Zahl ungleich 1, die im Quadraten rechts oben einschließlich dem positiven Teil der x-Achse ohne die y-Achse liegt und nur von den Gaußschen Einheiten und von sich selbst mal einer Gaußschen Einheit geteilt wird. Jede Gaußsche Zahl lässt sich auf bis auf die Reihenfolge eindeutige Weise als Produkt einer Gaußschen Einheit mit einem Produkt von Gaußschen Primzahlen schreiben. Es gilt ferner Folgendes: Wenn die ganze Primzahl p beim Teilen durch 4 den Rest 3 ergibt (z. B. $p = 3$, $p = 7$ oder $p = 11$), dann ist $p = p + i \cdot 0$ auch eine Gaußsche Primzahl. Wir sagen dann, dass p *träge* ist. Lässt p aber beim Teilen durch 4 den Rest 1, dann kann man ganze Zahlen u, v finden, derart dass $p = u^2 + v^2$ gilt, und daher kann man p in den Gaußschen Zahlen faktorisieren:

$$p = (u + iv)(u - iv) = u^2 - (iv)^2 = u^2 - (i)^2v^2 = u^2 - (-1)v^2 = u^2 + v^2.$$

Daher ist in diesem Fall p keine Gaußsche Primzahl, stattdessen aber $u + iv$ und $u - iv$ (evtl. bis auf eine Einheit). Wir sagen, dass p in den Gaußschen Zahlen *zerlegt* ist. Eine besondere Rolle spielt die Primzahl 2, sie ist

$$2 = -i(1 + i)^2,$$

d. h. eine Gaußsche Einheit mal einem Quadrat einer Gaußschen Primzahl. Die ganze Primzahl 2 heißt deswegen in den Gaußschen Zahlen *verzweigt*.

Kommen wir zurück zur Gleichung $a^2 + b^2 = c^2$. In den Gaußschen Zahlen können wir diese nun so schreiben:

$$a^2 + b^2 = (a + ib)(a - ib) = c^2.$$

Wenn wir annehmen, dass a, b, c keine gemeinsamen Teiler haben (wir suchen dann nur primitive Pythagoräische Tripel; durch das Herausteilen des gemeinsamen Faktors kann jedes Pythagoräische Tripel auf ein primitives zurückgeführt werden), dann sind $a + ib$ und $a - ib$ teilerfremde Gaußsche Zahlen, d. h. dass ihre gemeinsamen Teiler nur die Gaußschen Einheiten sind. Wegen der eindeutigen Primfaktorzerlegung in den Gaußschen Zahlen muss dann aber $a + ib$ schon selbst ein Quadrat sein, also muss gelten

$$\epsilon(a + ib) = (u + iv)^2 = u^2 - v^2 + i2uv,$$

mit einer Gaußschen Einheit ϵ und ganzen Zahlen u, v. Ist $\epsilon = \pm 1$, dann erhalten wir also $a = \pm(u^2 - v^2)$ und $b = \pm 2uv$. Ist $\epsilon = \pm i$, dann ist es gerade umgekehrt $a = \pm 2uv$ und $b = \mp(u^2 - v^2)$. Andersherum ist es ganz einfach nachzuprüfen, dass die Zuordnung

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2$$

Pythagoräische Tripel erzeugt, nämlich:

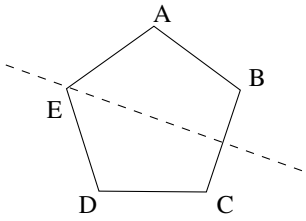
$$a^2 + b^2 = (u^2 - v^2)^2 + (2uv)^2 = u^4 + 2u^2v^2 + v^4 = (u^2 + v^2)^2 = c^2.$$

Damit haben wir alle primitiven Pythagoräischen Tripel bestimmt, indem wir den Zahlenbereich, in dem wir rechnen, geschickt erweitert haben. Dies ist eine Hauptmethode der algebraischen Zahlentheorie. Allgemeiner studiert man unter Multiplikation und Addition abgeschlossene Erweiterungen der ganzen Zahlen bzw. der Bruchzahlen, die durch Hinzufügen von Lösungen von Gleichungen der Form

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$$

mit ganzen Zahlen a_i entstehen. Solche Lösungen nennt man *ganze algebraische Zahlen*. An die Stelle der eindeutigen Primfaktorzerlegung tritt dann jedoch im Allgemeinen nur noch die eindeutige Primidealzerlegung. Begriffe wie Trägheit, Zerlegung und Verzweigung hat man jedoch auch im erweiterten Sinn. Sie werden zusammengefasst im Begriff *Arithmetik der Zahlkörper*.

Bevor wir zu Symmetriegruppen von Zahlkörpern (den sogenannten *Galoisgruppen*) kommen, behandeln wir ein Beispiel von Symmetriegruppen aus der ebenen euklidischen Geometrie. Wir betrachten das regelmäßige Fünfeck (Pentagon).



Welche abstandserhaltenden umkehrbaren Transformationen gibt es, die das Pentagon in sich selbst überführen? Es sind dies die Drehungen um $n \cdot 72$ Grad mit $n \in \{0, 1, \ldots, 4\}$ und die Spiegelungen an den Achsen, die durch einen Eckpunkt gehen und senkrecht auf der gegenüber dem Eckpunkt liegenden Seite stehen. Insgesamt gibt es also 10 solche Transformationen. Das Hintereinanderausführen von zwei solchen liefert eine dritte. Außerdem kann man die Transformationen wieder rückgängig machen (die Rotation um $n \cdot 72$ Grad durch Rotation um $(5-n) \cdot 72$ Grad, und die Spiegelung durch nochmaliges Ausführen). So etwas nennt man eine Gruppe. Wir haben also gerade die Symmetriegruppe des regelmäßigen Fünfecks beschrieben. Im Allgemeinen nennt man die Symmetriegruppe des regelmäßigen n-Ecks die n-te *Diedergruppe*. Diese hat $2n$ Elemente.

In der Zahlentheorie betrachtet man Symmetriegruppen von Zahlkörpern und nennt diese Galoisgruppen. Schließen wir an das Beispiel von oben an. Die gebrochenen Gaußschen Zahlen sind alle Zahlen $a + ib$, wobei a, b nun Bruchzahlen sind. Eine Symmetrie der gebrochenen Gaußschen Zahlen ist eine umkehrbare Selbstabbildung, die die Multiplikation und die Addition respektiert. Sie ist dann automatisch die Identität auf den Bruchzahlen. Neben der identischen Symmetrie gibt es eine weitere. Diese ist dadurch gegeben, dass die Zahl $a + ib$ auf die Zahl $a - ib$ abgebildet wird. Führt man diese Abbildung zweimal nacheinander aus, so erhält man wieder die Identität. Die Galoisgruppe der gebrochenen Gaußschen Zahlen enthält genau diese zwei Elemente.

Es gibt aber auch Zahlkörper, deren Symmetriegruppe denselben Gesetzen folgt wie die Symmetriegruppe des Fünfecks (allgemeiner gilt dies für jedes regelmässige n-Eck). Z. B. ist dies der Fall beim Zahlkörper, den man erhält, indem man zu den Bruchzahlen noch alle Lösungen der Gleichung

$$X^5 - 2X^4 + 2X^3 - X^2 + 1$$

hinzufügt und alle Zahlen, die man aus diesen durch Multiplikation und Addition erhält.

Die Symmetriegruppe der Menge aller algebraischen Zahlen überhaupt nennt man die *absolute Galoisgruppe der rationalen Zahlen* und bezeichnet sie mit dem Symbol $G_{\mathbb{Q}}$. Aus ihr kann man im Prinzip alle Informationen zu allen Zahlkörpern und deren Arithmetik ablesen! Daher ist $G_{\mathbb{Q}}$ das zentrale Objekt der algebraischen Zahlentheorie. Allerdings ist die Struktur von $G_{\mathbb{Q}}$ sehr mysteriös (sie hat z. B. überabzählbar viele Elemente, d. h. viel mehr als es ganze Zahlen gibt) und sie ist nur sehr schlecht verstanden.

An dieser Stelle kommt nun das tiefliegende Zusammenspiel von algebraischer Geometrie und algebraischer Zahlentheorie in der Theorie der Modulformen voll zum Tragen. Es gibt nämlich einen Satz von Shimura, Deligne und Serre, der einer Modulform (die eine Eigenform ist, d. h. u. a. wenn sie geschrieben wird als unendliche Reihe $e^{2\pi i\tau}+\sum_{n=2}^{\infty} a_n e^{2\pi i n\tau}$, dass dann $a_n \cdot a_m = a_{nm}$ gilt für n und m ohne gemeinsamen Faktor) für eine vorgegebene Primzahl p eine *Galoisdarstellung* (das ist eine stetige Abbildung von Gruppen, d. h. sie respektiert die Geometrie und das Hintereinanderausführen)

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

zuordnet (genauer: diese ist ungerade und halbeinfach). Die rechte Seite der Formel ist noch zu erklären. Hier ist $\overline{\mathbb{F}_p}$ die Menge aller Lösungen von Gleichungen

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 = 0,$$

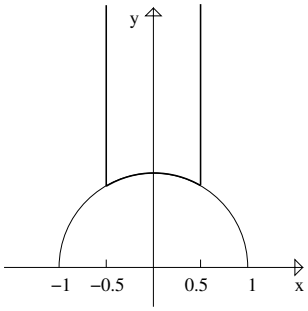
wobei wir nun von den Koeffizienten nur den Rest betrachten, den sie beim Teilen durch p lassen. Ferner ist $\mathrm{GL}_2(\overline{\mathbb{F}_p})$ die Gruppe der umkehrbaren linearen Abbildungen der Ebene mit Koordinaten in $\overline{\mathbb{F}_p}$. Vereinfacht ausgedrückt bedeutet dies, dass uns eine solche Galoisdarstellung "ebene Stücke" von $G_{\mathbb{Q}}$ in Charakteristik p liefert. Davon existiert keine gute, anschauliche Vorstellung, und die Sprache wird nur in Analogie zur gewöhnlichen reellen Geometrie gebraucht. Die Topologie, d. h. die Art, wie wir uns die Geometrie auf $\overline{\mathbb{F}_p}$ definieren, nämlich diskret, hat zur Folge, dass die "ebenen Stücke" von $G_{\mathbb{Q}}$ endlich sind, d. h. nur aus einer endlichen Anzahl Elementen bestehen. Das wiederum bedeutet, dass uns die Modulform, von der wir ausgegangen sind, einen Zahlkörper liefert. Das Wichtige dabei ist, dass die Arithmetik dieses Zahlkörpers (zumindest zum Teil) an den Koeffizienten der Modulform abzulesen ist (diese können wir ausrechnen; wir können sie sogar gleich in $\overline{\mathbb{F}_p}$ nehmen)! Damit gewähren uns Modulformen einen kleinen Einblick in die mysteriöse absolute Galoisgruppe $G_{\mathbb{Q}}$!

Dies veranschaulichen wir uns an einem Beispiel. Es gibt eine Modulform von Stufe 229 und Gewicht 1, deren Koeffizienten a_n in der Menge $\{0, 1\}$ liegen (mit der Addition und Multiplikation $1+0=1, 1+1=0, 1\cdot 1=1, 1\cdot 0=0$, mit anderen Worten dem endlichen Körper $\mathbb{F}_2$). Sei K der Zahlkörper, der aus den Bruchzahlen durch Hinzunehmen einer Quadratwurzel der Primzahl 229 gebildet wird. Sei l eine Primzahl, die nicht 2 und nicht 229 ist. Dann ist der l-te Koeffizient unserer Modulform gleich 0 genau dann, wenn l träge in K ist (mit anderen Worten, wenn keine Quadratzahl beim Teilen durch l denselben Rest lässt wie 229) oder l in zwei Hauptideale zerfällt. Sonst ist der Koeffizient gleich 1.

Wir haben also gesehen, dass eine Modulform uns ebene Stücke von $G_{\mathbb{Q}}$ in Charakteristik p gibt. Der berühmte Mathematiker Jean-Pierre Serre (2003 der erste Gewinner des neuen Abel-Preises, der der "Nobelpreis" für Mathematik werden soll) hat die Vermutung ausgesprochen, dass umgekehrt alle ebenen Stücke von $G_{\mathbb{Q}}$ in Charakteristik p durch Modulformen beschrieben werden können. Er hat sogar noch eine Formel angegeben, wo die Modulformen zu suchen sind (die Stufe, den Charakter und

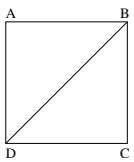
das Gewicht). Ist diese Vermutung war, dann können wir alle solche ebenen Stücke von $G_{\mathbb{Q}}$ mit dem Computer berechnen, denn wir können Modulformen berechnen! Serres Vermutung ist daher sowohl von ungeheuerer struktureller als auch von rechnerischer Bedeutung. Allerdings ist nicht bekannt, ob Serres Vermutung wahr ist. Aber vor wenigen Monaten wurde ein wichtiger Fall gelöst, so dass die Forschung gerade stark in Bewegung ist.

Als nächstes wollen wir kurz Modulkurven betrachten. Diese können als der geometrische Aspekt von Modulformen angesehen werden. Außerdem bilden sie das Verbindungsglied zwischen Modulformen, Modulsymbolen (siehe unten) und Galoisdarstellungen. Modulkurven sind zunächst komplexe Kurven, d. h. Flächen in der Anschauung. Die allereinfachste ist gegeben als die Punkte in der Koordinatenebene, deren x-Koordinate zwischen $-\frac{1}{2}$ und $\frac{1}{2}$ liegt und die auf bzw. über dem Einheitskreis liegen. Dabei muss man nun den linken Rand mit dem rechten Rand verkleben (das ist ganz wörtlich vorstellbar: wir schneiden diesen Bereich mit der Schere aus; dann kleben wir die beiden langen Geraden zusammen; schließlich kleben wir noch die linke Hälfte des Bogenstücks mit der rechten zusammen; dann hat man einen Zylinder mit einem etwas komischen Boden). Die so erhaltene (Ober-)Fläche ist oben offen. Man kann diese durch Hinzufügen eines Punktes, einer sogenannten *Spitze*, kompaktifizieren (auch das ist ganz bildlich: wir drücken den Zylinder oben zu einem Punkt zusammen; dann sehen wir die Spitze ganz deutlich). Die so entstandene Fläche ist eine kompakte Riemannsche Fläche, d. h. kleine Stücke haben dieselbe Geometrie wie die komplexe Zahlenebene. Modulformen findet man auf den Modulkurven wieder als sog. Differentialformen (diese gebraucht man z. B. zum Integrieren auf der Riemannschen Fläche). Der entscheidende Punkt für die Zahlentheorie ist, dass die Modulkurven eine recht tiefliegende algebraische Struktur haben, d. h. dass ihre Punkte auch Lösungen von Gleichungen mit ganzen Koeffizienten sind, allerdings in vielen Variablen. Auch die Differentialformen haben ein algebraisches Analogon, das uns die sogenannten *Katz-Modulformen* liefert, die in der vorliegenden Arbeit benutzt werden. Auch die Galoisdarstellungen werden mit Hilfe der algebraischen Beschreibung der Modulkurven konstruiert.



Dem Studium von Flächen (und höherdimensionalen Varietäten) dient die (Ko-)Homologietheorie. Die Homologietheorie von Riemannschen Flächen mit trivialen Koeffizienten wollen wir kurz vorstellen. In der vorliegenden Arbeit werden aber auch Kohomologietheorien von Schemas (das sind weitreichende algebraische Verallgemeinerungen von Riemannschen Flächen), Stacks (das sind noch andere Verallgemeinerungen) und von Gruppen und dann im allgemeinen mit nicht-trivialen Koeffizienten benutzt.

Eine Riemannsche Fläche kann man triangulieren, d. h. sie in endlich viele Dreiecke aufteilen (dabei dürfen die Seiten "krumm" sein, aber keine Knicke enthalten). Zur Aufteilung in Dreiecke werden Seiten gezogen, d. h. jedes Dreieck hat drei Seiten und zwei aneinander grenzende Dreiecke haben (mindestens) eine gemeinsame Seite. Außerdem betrachten wir die Menge der Schnittpunkte der Seiten.



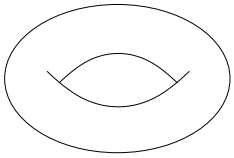
Wir beschreiben nun eine Triangulation des Fahrradreifens (des sog. *Torus*). Dabei gehen wir konstruktiv vor. Wir beginnen mit dem nebenstehenden Rechteck, das wir in zwei Dreiecke aufgeteilt haben. Durch Zusammenkleben wird sich die Anzahl

der Seiten verkleinern. Zunächst kleben wir die Seite AD an die Seite BC. Auf diese Weise erhalten wir einen Zylinder. Nun kleben wir den Deckel an den Boden (dazu stellen wir uns Gummi als Baumaterial vor).

Die Eulercharakteristik einer Fläche ist definiert als $\chi = d - s + p$, wobei d die Anzahl der Dreiecke, s die Anzahl der Seiten und p die Anzahl der Punkte bezeichnen. Die Eulercharakteristik ist unabhängig von der Triangulation. Außerdem gilt die berühmte Beziehung

$$\chi = 2 - 2g,$$

wobei g das Geschlecht der Fläche ist, d. h. die Anzahl der Löcher.



Im Beispiel des Fahrradreifens finden wir in der Tat $g = 1$. Wir haben nämlich noch immer die beiden Dreiecke, von denen wir ausgegangen waren. Da wir die Seite AD mit BC und ferner auch AB mit DC identifiziert haben, ist die Anzahl der Seiten unserer Triangulation des Torus 3. Außerdem fallen durch obige Verklebungen alle vier Punkte zusammen zu einem. Somit ergibt sich tatsächlich $\chi = 2 - 3 + 1 = 0$.

Die oben beschriebene Modulkurve hat kein Loch. Daher gilt für sie $g = 0$. Wir können auch die Modulkurve einfach triangulieren. Dazu falten wir sie wieder auseinander. Wir benutzen nur ein Dreieck. Dieses besteht aus den beiden Punkten unten links und unten rechts und einem gedachten Punkt ganz oben (der Punkt der durch das Zusammendrücken des Zylinders entstanden ist). Dann haben wir nach dem Zusammenkleben noch drei Punkte, zwei Seiten (die senkrechte und das Bogenstück) und das Dreieck. Damit ergibt sich $\chi = 1 - 2 + 3 = 2$. Allgemeinere Modulkurven, wie z. B. die in der Arbeit behandelte Modulkurve $X_1(N)$, haben in der Regel viele Löcher.

Die Homologiegruppen stehen zur Eulercharakteristik in enger Beziehung (die Eulercharakteristik wird aus diesen abgeleitet). Die nullte und die zweite Homologiegruppe sind freie Gruppen vom Rang gleich der Anzahl der Zusammenhangskomponenten. In unserem Fall ist der Rang beider also 1. Die erste Homologiegruppe ist wiederum eine freie Gruppe. Ihr Rang ist $2g$, wobei g wie oben die Anzahl der Löcher ist.

Nachdem wir versucht haben, eine erste, sehr stark vereinfachte Idee von den in der vorliegenden Arbeit untersuchten Objekten zu geben, wenden wir uns nun dem Inhalt zu.

Das erste Kapitel ist bereits als eigenständiger Artikel erschienen. Es geht in ihm um eine leicht modifizierte Version von Serres Vermutung. In tief liegenden Arbeiten einer Vielzahl Mathematiker wurde gezeigt, dass für ungerade Charakteristik p Serres Formeln für die Stufe, den Charakter und das Gewicht der vorhergesagten Modulform richtig sind. Genauer, wenn irgendeine Modulform existiert, die ein vorgegebenes ebenes Stück von $G_{\mathbb{Q}}$ gibt, dann gibt es auch eine da, wo Serres Formeln diese voraussagen. Der Fall $p = 2$ ist jedoch zum Teil noch offen.

In dem Artikel beschränke ich mich auf "ebene Stücke" in Charakteristik p von $G_{\mathbb{Q}}$ (also zweidimensionale Galoisdarstellungen), deren Symmetriegruppe eine Diedergruppe, also eine Symmetriegruppe eines regelmässigen n-Ecks ist. Von diesen zeige ich die modifizierte Serre-Vermutung ohne Ausnahme, d. h. einschließlich $p = 2$. Dass solche Galoisdarstellungen von irgendeiner Modulform kommen, war im Prinzip schon Erich Hecke bekannt, zumindest wenn $p \neq 2$ ist. Im Beweis mache ich unendlich viele solche Modulformen, so dass ich dann mittels des Schubfachprinzips (verteile 10

Briefe auf 5 Schubfächer, dann liegen in einem mindestens zwei Breife) zwei wählen kann, die sich mit Hilfe algebraisch geometrischer Methoden zu der gewünschten Form kombinieren lassen.

Im Kapitel II berechne und vergleiche ich verschiedene Arten von (Ko-)Homologiegruppen, die alle mit der Modulkurve $X_1(N)$ (einer etwas allgemeineren als der oben vorgestellten Riemannschen Fläche) zusammenhängen, mit dem Modulsymbolformalismus, der an die Homologie angelehnt ist. Dabei ist der Koeffizientenring beliebig. Es werden jeweils explizite Beschreibungen in Termen von linearer Algebra abgeleitet.

Modulsymbole betrachten wir aus praktischen Gesichtspunkten: sie sind im weit verbreiteten Computeralgebrasystem Magma implementiert. Ich habe Computerprogramme erstellt, die hierauf beruhen.

Im dritten Kapitel werden neue Fälle bewiesen, in denen die Katz-Modulformen über $\mathbb{F}_p$ mit Hilfe der expliziten Beschreibungen der Kohomologiegruppen aus Kapitel II direkt über dem endlichen Körper $\mathbb{F}_p$ berechnet werden können. Dieses bringt einen Geschwindigkeitszuwachs im Vergleich zu Methoden, die mit ganzen Zahlen rechnen. Unter Benutzung einer Idee von Edixhoven erhalten wir auch einen Algorithmus zur Berechnung von Katz-Modulformen von Gewicht eins (diese sind nicht direkt zugänglich!) mittels Modulsymbolen über $\mathbb{F}_p$.

Ausgenutzt wird im Beweis eine erstaunliche Parallelität im Verhalten der Modulformen von Gewicht 2 und Stufe Np über $\mathbb{F}_p$ und der ersten Kohomologiegruppen der Riemannschen Fläche $X_1(Np)$ mit $\mathbb{F}_p$-Koeffizienten. In beiden spiegeln sich nämlich die Modulformen bzw. die ersten Kohomologiegruppen wider, die zu Stufe N und Gewicht $k \in \{2, \ldots, p+1\}$ gehören.

Der Übergang von komplexer Geometrie zu algebraischer Geometrie über $\mathbb{F}_p$ wird dabei mit Hilfe der Jakobischen der Modulkurve bewerkstelligt. Die erste Kohomologiegruppe kann nämlich mit der p-Torsion der komplexen Jakobischen identifiziert werden. Geht man dann zum Néronmodell der Jakobischen über, so gelingt es, Eigenschaften von der generischen Faser (sogar der Riemannschen Fläche) zur speziellen Faser (also nach $\mathbb{F}_p$) zu übertragen.

Das vierte Kapitel enthält eine Beschreibung der Algorithmen, die sich aus der Theorie der beiden vorangehenden Kaptiel ergeben. Schließlich wird im fünften Kapitel von Computerberechnungen berichtet, die mit Hilfe der vorgestellten Algorithmen ausgeführt wurden. Dabei wurde zum Beispiel festgestellt, dass die ebenen Stücke von $G_{\mathbb{Q}}$ in Charakteristik 2 erstaunlich schnell sehr groß werden. Desweiteren wurden noch andere Beobachtungen gemacht, die einige interessante theoretische Zusammenhänge suggerieren. Das Studium dieser kann Gegenstand zukünftiger Arbeiten sein.