Samenvatting behorende bij het proefschrift

Modular Forms of Weight One Over Finite Fields

van Gabor Wiese.

In deze samenvatting zal ik eerst een zo begrijpelijk mogelijke, elementaire inleiding geven tot het gebied van de wiskunde waarover mijn proefschrift gaat. Daarna volgt een overzicht van de inhoud van deze dissertatie.

Modulaire vormen spelen al sinds hun introductie in de 19de eeuw een belangrijke rol in de getaltheorie. In het begin werden zij met behulp van de complexe analyse bestudeerd, omdat de bijbehorende Fouriercoëfficiënten vaak getaltheoretische interpretaties bezitten. Bijvoorbeeld bestaat er een modulaire vorm waarvan de n-de Fouriercoëfficiënt gelijk is aan het aantal mogelijkheden het getal n als som van acht kwadraten te schrijven. Sinds de jaren zestig is de taal van de algebraïsche meetkunde, in het bijzonder die van de *aritmetische algebraïsche meetkunde*, in veel gebieden van de getaltheorie heel nuttig gebleken. Op grond van inzichten van Shimura, Weil, Serre en Deligne werd deze nieuwe taal met veel succes ook op de theorie van modulaire vormen toegepast en er werden enige diepe samenhangen ontdekt. Als hoogtepunt tot nu toe is het bewijs van het vermoeden van Fermat te noemen, dat in 1994 door Andrew Wiles gevonden werd. Dit vermoeden zegt dat de vergelijking

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

met gehele machten $n \geq 3$ geen oplossing heeft voor positieve natuurlijke getallen a, b, c.

De samenhang tussen getaltheorie en meetkunde wil ik met behulp van een eenvoudig voorbeeld aanduiden. Laten we de vergelijking

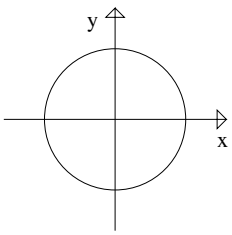
$$a^2 + b^2 = c^2$$

beschouwen. Anders dan in het vermoeden van Fermat heeft deze vergelijking wel oplossingen, namelijk de bekende Pythagoreïsche drietallen, zoals $3^2 + 4^2 = 5^2$ of $5^2 + 12^2 = 13^2$. Als we $x = \frac{a}{c}$ en $y = \frac{b}{c}$ schrijven, dan verkrijgen we middels een eenvoudige manipulatie de vergelijking

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

Beschouwen we nu eerst alle reële oplossingen (d.w.z. we staan getallen toe die oneindig veel cijfers achter de komma mogen hebben en niet periodiek hoeven te zijn).

Met behulp van de parametrisatie $x = \cos(\varphi)$ en $y = \sin(\varphi)$ zien we dat de reële oplossingen precies de eenheidscirkel vormen (d.w.z. de cirkel om de oorsprong van het coördinatenvlak met straal 1). Nu zijn we heel duidelijk in de wereld van de meetkunde! Onze vraag naar de Pythagoreïsche drietallen kan nu worden vertaald in de vraag naar punten op het eenheidscirkel waarvan de coördinaten breuken (d.w.z. *rationale getallen*) zijn.



We zullen zien dat de vergelijking $a^2 + b^2 = c^2$ makkelijker te bestuderen is, als men niet alleen met breuken werkt maar ook met het getal i dat als een wortel van -1 gedefiniëerd is, d.w.z. als een oplossing van de vergelijking

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

Volgens de hoofdstelling van de algebra heeft namelijk iedere zulke vergelijking over de complexe getallen even veel oplossingen (met multipliciteiten) als haar graad aangeeft; in dit geval dus twee, namelijk i en $-i$.

We zullen in de getallen van Gauß rekenen, dit zijn alle getallen die men door optellen en vermenigvuldigen van gehele getallen en het getal i verkrijgt. Het is makkelijk in te zien dat men iedere getal van Gauß als $a + ib$ met gehele getallen a en b kan schrijven. Laten we ons herinneren dat een positief natuurlijk getal ongelijk 1 een *priemgetal* heet, als zijn enige positieve delers 1 en het getal zelf zijn. Ieder geheel getal ongelijk 0 kan op de volgorde na op eenduidige manier geschreven worden als plus of min een product van priemgetallen, bijv. is $12 = 2 \cdot 2 \cdot 3$. Zoiets is ook voor de getallen van Gauß geldig. De enige getallen van Gauß die ieder willekeurig getal van Gauß delen zijn $1, -1, i, -i$; deze worden de Gaußeenheden genoemd. Een Gaußpriemgetal is een getal van Gauß ongelijk 1 die in de kwadrant rechts boven met de positieve x-as en zonder de y-as ligt en alleen door de Gaußeenheden en door zichzelf keer een Gaußeenheid gedeeld word. Ieder getal van Gauß kan op de volgorde na op eenduidige manier geschreven worden als product van Gaußpriemgetallen en een Gaußeenheid.

Bovendien is het volgende geldig: Als een priemgetal p bij deling door 4 rest 3 heeft (bijv. $p = 3$, $p = 7$ of $p = 11$), dan is $p = p + i \cdot 0$ ook een Gaußpriemgetal. We zeggen in dat geval dat p *inert* is. Als p gedeeld door 4 rest 1 heeft, dan kan men gehele getallen u, v vinden, zodat $p = u^2 + v^2$ geldig is, en dus kan men p in de getallen van Gauß factoriseren:

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

Daarom is in dat geval p geen Gaußpriemgetal, maar $u + iv$ en $u - iv$ zijn dat wel (op een eenheid na). We zeggen dat p in de getallen van Gauß *gespleten* is. Een bijzondere rol speelt het priemgetal 2. Het is

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

dus een Gaußeenheid keer het kwadraat van een Gaußpriemgetal. Het gehele priemgetal 2 heet daarom in de getallen van Gauß *vertakt*.

Laten we teruggaan naar de vergelijking $a^2 + b^2 = c^2$. In de getallen van Gauß kunnen we nu schrijven:

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

Als we aannemen dat a, b, c geen gemeenschappelijke delers hebben (we zoeken dus alleen primitieve Pythagoreïsche drietallen; door delen door de gemeenschappelijke factor kan men ieder Pythagoreisch drietal in een primitieve veranderen), dan zijn $a + ib$ en $a - ib$ getallen van Gauß waarvan de gemeenschappelijke delers alleen de Gaußeenheden zijn. Wegens de unieke priemfactorisatie in de getallen van Gauß moet dan $a + ib$ zelf een kwadraat zijn. Dus er moet gelden

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

met een Gaußeenheid ϵ en gehele getallen u, v. Is $\epsilon = \pm 1$, dan verkrijgen we dus $a = \pm(u^2 - v^2)$ en $b = \pm 2uv$. Is $\epsilon = \pm i$, dan is het precies andersom, namelijk $a = \pm 2uv$ en $b = \mp(u^2 - v^2)$. Het is ook makkelijk te verifiëren dat door

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

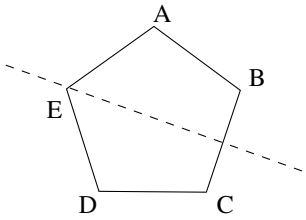
Pythagoreïsche drietallen gegenereerd worden, namelijk:

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

Dus hebben we alle primitieve Pythagoreïsche drietallen bepaald door het getalbereik waarin we rekenen slim uit te breiden. Dit is een van de belangrijkste methoden van de algebraïsche getaltheorie. In het algemeen bestudeert men onder vermenigvuldiging en optellen afgesloten uitbreidingen van de gehele getallen resp. de breuken, die door bijvoegen van oplossingen van vergelijkingen van de vorm

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

met gehele getallen a_i ontstaan. Zulke oplossingen noemt men *gehele algebraïsche getallen*. In plaats van unieke priemfactorisatie heeft men echter in het algemeen alleen nog unieke priemideaalfactorisatie. Begrippen als inertie, splijten en vertakking bestaan ook in deze algemene context. Dit wordt *aritmetiek van getallenlichamen* genoemd.



Voordat we het over symmetriegroepen van getallenlichamen (de *Galoisgroepen*) hebben, behandelen we een voorbeeld van symmetriegroepen uit de platte euclidische meetkunde. We beschouwen de regelmatige vijfhoek (pentagoon). Welke afstandsbehoudende omkeerbare transformaties bestaan er, die de pentagoon op zichzelf afbeelden? Het zijn de rotaties over $n \cdot 72$ graden met $n \in \{0, 1, \ldots, 4\}$ en de spiegelingen door de assen die door een hoekpunt lopen en loodrecht op de tegenoverliggende zijde staan. Bij elkaar bestaan er dus 10 zulke transformaties. Het samenstellen van twee zulke levert altijd een derde op. Bovendien kan men de transformaties weer omkeren (de rotatie over $n \cdot 72$ graden door de rotatie over $(5 - n) \cdot 72$ graden, en de spiegeling door hem nog een keer te doen). Zoiets noemt men een groep. We hebben dus net de symmetriegroep van de regelmatige vijfhoek beschreven. In het algemeen noemt men de symmetriegroep van de regelmatige n-hoek de n-de *diëdergroep*. Zij heeft $2n$ elementen.

In de getaltheorie bekijkt men de symmetriegroepen van getallenlichamen en noemt deze *Galoisgroepen*. Laten we met het voorbeeld van boven doorgaan. De rationale getallen van Gauß zijn alle getallen $a + ib$ waarbij nu a en b breuken zijn. Een symmetrie van de rationale getallen van Gauß is een omkeerbare afbeelding van de rationale getallen van Gauß naar zichzelf die vermenigvuldiging en optellen behoudt. Zij is dan automatisch de identiteit op de breuken. Naast de identieke symmetrie bestaat er één andere. Deze wordt gegeven door het getal $a + ib$ op het getal $a - ib$ af te beelden, dus door complexe conjugatie. Past men deze afbeelding twee keer toe dan verkrijgt men weer de identiteit. De Galoisgroep van de rationale getallen van Gauß bevat precies deze twee elementen.

Maar er zijn ook getallenlichamen waarvan de symmetriegroep dezelfde vermenigvuldiging heeft als de symmetriegroep van de vijfhoek (in het algemeen geldt dit voor iedere regelmatige n-hoek). Bijvoorbeeld is dit het geval voor het getallenlichaam dat men verkrijgt door aan de breuken nog alle oplossingen van de vergelijking

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

toe te voegen en ook nog alle getallen die door vermenigvuldiging en optellen hieruit ontstaan.

De symmetriegroep van de verzameling van alle algebraïsche getallen samen heet de *absolute Galoisgroep van de rationale getallen* en wordt door het symbool $G_{\mathbb{Q}}$ aangeduid. Uit deze groep kan men in principe alle informatie over alle getallenlichamen en hun aritmetiek aflezen! Dus is $G_{\mathbb{Q}}$ het centrale object van de algebraïsche getaltheorie. Helaas is de structuur van $G_{\mathbb{Q}}$ heel mysterieus (zij heeft bijv. overaftelbaar veel elementen, d.w.z. veel meer dan er gehele getallen bestaan) en zij is zeer slecht begrepen.

Op deze plaats speelt de diepe samenwerking van algebraïsche meetkunde en algebraïsche getaltheorie in de theorie van de modulaire vormen een heel belangrijke rol. Er is namelijk een theorema van Shimura, Deligne en Serre dat bij een modulaire vorm (die een eigenvorm is, dat betekent bijv. als de vorm als oneindige reeks $e^{2\pi i\tau} + \sum_{n=2}^{\infty} a_n e^{2\pi i n\tau}$ geschreven is dat dan $a_n \cdot a_m = a_{nm}$ geldt voor n en m zonder gemeenschappelijke factor) voor een gegeven priemgetal p een *Galoisrepresentatie* (dat is een continuë afbeelding, d.w.z. zij respecteert de meetkunde en het samenstellen)

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

maakt (deze is oneven en semi-simpel). De rechterkant van de formule moet nog worden uitgelegd. Hier is $\overline{\mathbb{F}_p}$ de verzameling van alle oplossingen van vergelijkingen

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

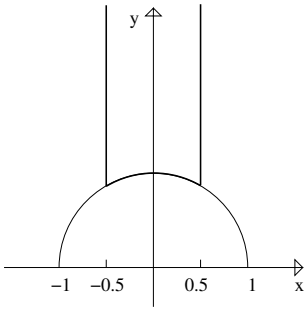
waar we nu van de coëfficiënten alleen de rest bekijken die zij bij het delen door p geven. Daarenboven is $\mathrm{GL}_2(\overline{\mathbb{F}_p})$ de groep van omkeerbare lineaire afbeeldingen van het vlak met coördinaten in $\overline{\mathbb{F}_p}$. Eenvoudig gezegd betekent dit dat we platte stukken van $G_{\mathbb{Q}}$ in karakteristiek p beschouwen. Hiervoor bestaat geen goede, intuïtieve aanschouwing, en de taal wordt alleen in analogie met de gewone, reële meetkunde gebruikt. De topologie, d.w.z. de manier waarop we de meetkunde op $\overline{\mathbb{F}_p}$ definiëren, namelijk diskreet, heeft als gevolg dat de "platte stukken" van $G_{\mathbb{Q}}$ eindig zijn, dus alleen maar uit eindig veel elementen bestaan. Dit betekent dan dat de modulaire vorm, waarmee we begonnen waren, een getallenlichaam oplevert. Het belangrijke is nu dat de aritmetiek van het getallenlichaam (ten minste gedeeltelijk) aan de coëfficiënten van de modulaire vorm kan worden afgelezen (die kunnen we berekenen; we kunnen ze zelf direct in $\overline{\mathbb{F}_p}$ nemen)! Op deze manier verlenen ons de modulaire vormen een klein inzicht in de mysterieuze absolute Galoisgroep $G_{\mathbb{Q}}$!

Laten we een voorbeeld bekijken. Er is een modulaire vorm van niveau 229 en gewicht 1 waarvan de coëfficiënten in de verzameling $\{0, 1\}$ liggen (met de optelling en vermenigvuldiging $1 + 0 = 1, 1 + 1 = 0, 1 \cdot 1 = 1, 1 \cdot 0 = 0$ dus in het eindige lichaam $\mathbb{F}_2$). Zij K het getallenlichaam dat uit de breuken door bijvoegen van een wortel van het priemgetal 229 gemaakt wordt. Zij l een priemgetal ongelijk aan 2 en 229. Dan is de l-de coëfficiënt van de modulaire vorm gelijk aan 0 dan en slechts dan als l in K inert is (d.w.z. dat geen kwadraat bij delen door l dezelfde rest heeft als 229) of dat l in twee hoofdidealen splijt. Anders is de coëfficiënt gelijk aan 1.

We hebben dus gezien, dat een modulaire vorm "platte stukken" van $G_{\mathbb{Q}}$ in karakteristiek p oplevert. De beroemde wiskundige Jean-Pierre Serre (in 2003 de eerste winnaar van de nieuwe Abelprijs die de Nobelprijs voor de wiskunde zal worden) heeft het vermoeden uitgesproken dat andersom alle "platte stukken" van $G_{\mathbb{Q}}$ in karakteristiek p door modulaire vormen kunnen worden beschreven. Hij heeft zelfs een formule aangegeven waarmee men naar de modulaire vormen moet zoeken (d.w.z. het niveau, het karakter en het gewicht). Als dit vermoeden waar is, dan kunnen we alle zulke platte

stukken van $G_{\mathbb{Q}}$ met de computer berekenen, omdat we modulaire vormen kunnen berekenen! Serres vermoeden is dus zowel van groot structureel als van computationeel belang. Echter is het niet bekend of Serres vermoeden waar is. Maar enkele maanden geleden werd een belangrijk geval opgelost zodat het onderzoek tegenwoordig sterk in beweging is.

Nu zullen we kort modulaire krommen bespreken. Deze kunnen als het meetkundige aspect van modulaire vormen worden beschouwd. Bovendien geven zij de verbinding tussen modulaire vormen, modulaire symbolen (zie beneden) en Galoisrepresentaties. Modulaire krommen zijn voorlopig complexe krommen, dus vlakken in de aanschouwing. De eenvoudigste modulaire kromme is gegeven als de punten in het coördinatenvlak, waarvan de x-coördinaat tussen $-\frac{1}{2}$ en $\frac{1}{2}$ ligt en die op of boven de eenheidscirkel liggen. Nu moet men de linkerrand op de rechterrand plakken (letterlijk: we knippen dit gebied met een schaar uit; dan plakken we de twee lange lijnen aan elkaar; tenslotte plakken we nog de linkerhelft van de boog aan de rechterhelft; zo verkrijgt men een cilinder met een ietwat vreemde bodem).

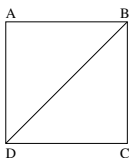


Het op deze manier verkregen vlak is boven open. Men kan hem door bijvoegen van een punt, van een *spits*, compactificeren (ook dit is aanschouwelijk te maken: we duwen de cilinder aan de bovenkant tot een punt samen; dan zien we de spits heel duidelijk). Het zo ontstane vlak is een compact Riemannoppervlak, d.w.z. dat kleine stukken meetkundig er hetzelfde uitzien als het complexe getallenvlak. Modulaire vormen vindt men op de modulaire krommen terug als differentiaalvormen (deze heeft men bijv. nodig om op Riemannoppervlakken te integreren). Het belangrijke voor de getaltheorie is dat de modulaire krommen ook een vrij diepe algebraïsche structuur hebben, d.w.z. dat hun punten oplossingen van vergelijkingen met gehele coëfficiënten zijn, maar dan in meerdere variabelen. Ook de differentiaalvormen hebben een algebraïsche analogon, die de *Katz modulaire vormen* oplevert, die in dit proefschrift gebruikt worden. Ook de Galoisrepresentaties worden met behulp van de algebraïsche beschrijving van de modulaire kromme gemaakt.

Voor de studie van oppervlakken (en ook hogerdimensionale variëteiten) gebruikt men de (co-)homologietheorie. We zullen kort de homologietheorie van Riemannoppervlakken met triviale coëfficienten beschrijven. Maar in het proefschrift worden ook (co-)homologietheorieën van schema's (dat zijn algebraïsche generalisaties van Riemannoppervlakken), stacks (dat zijn nog verdere generalisaties) en van groepen gebruikt en dan in het algemeen met niet-triviale coëfficiënten.

Men kan ieder Riemannoppervlak trianguleren, d.w.z. hem in eindig veel driehoeken opdelen (de zijden mogen krom zijn maar geen knikken bevatten). Voor het opdelen in driehoeken worden zijden getekend. Iedere driehoek heeft drie zijden en twee elkaar aanrakende driehoeken hebben ten minste een gemeenschappelijke zijde. Bovendien bekijken we de verzameling van snijpunten van zijden.

We beschrijven nu een triangulatie van de fietsband (de *torus*). Dit doen we constructief. We beginnen met de rechthoek uit het plaatje die we in twee driehoeken opgedeeld hebben. Door plakken zal het aantal zijden dalen. Eerst plakken we de zijde AD aan de zijde BC. Op deze manier verkrijgen we een cilinder. Nu plakken we het deksel op de bodem (we stellen ons de cilinder uit rubber voor).

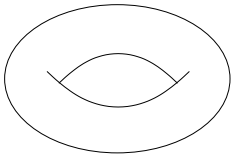


De Eulerkarakteristiek van een oppervlak is $\chi = d - z + p$, waar d het aantal

driehoeken, z het aantal zijden en p het aantal hoekpunten aanduidt. De Eulerkarakteristiek is onafhankelijk van de triangulatie. Bovendien geldt de beroemde formule

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

waar g het geslacht van het oppervlak is, d.w.z. het aantal gaten.



In het voorbeeld van de fietsband vinden we inderdaad $g = 1$. We hebben namelijk nog altijd de twee driehoeken, waarmee we begonnen zijn. Omdat we de zijde AD met BC en ook AB met DC geïdentificeerd hebben, is het aantal zijden van onze triangulatie van de torus 3. Bovendien vallen alle vier hoekpunten onder het plakken samen tot één punt. Dus verkrijgen we inderdaad $\chi = 2 - 3 + 1 = 0$.

De modulaire kromme die we boven beschreven hebben heeft geen gat. Dus geldt voor haar $g = 0$. We kunnen ook de modulaire kromme makkelijk trianguleren. We vouwen haar weer uiteen en gebruiken maar één driehoek. Dit bestaat uit de twee hoekpunten beneden links en beneden rechts samen met een denkbeeldig punt helemaal boven (dit is het punt dat door het samenduwen van de cilinder ontstaan is). Dan hebben we na het plakken nog drie hoekpunten, twee zijden (de verticale en het stuk van de boog) en de driehoek. Dus verkrijgen we $\chi = 1 - 2 + 3 = 2$. Wat algemenere modulaire krommen, bijv. de in het proefschrift gebruikte modulaire kromme $X_1(N)$, hebben meestal veel gaten.

De homologiegroepen staan in nauwe relatie tot de Eulerkarakteristiek (de Eulerkarakteristiek wordt met behulp van de homologiegroepen afgeleid). De nulde en de tweede homologiegroep zijn vrije groepen van rang gelijk aan het aantal samenhangscomponenten. In ons geval is de rang van allebei dus 1. De eerste homologiegroep is ook een vrije groep. Haar rang is $2g$ met g het geslacht.

Nadat we nu geprobeerd hebben een eerste, heel erg vereenvoudigd idee te geven van de objecten die in het proefschrift behandeld worden, zullen we nu de inhoud ervan beschrijven.

Het eerste hoofdstuk is inmiddels als artikel verschenen. Er wordt een aangepaste versie van Serres vermoeden behandeld. Diepe resultaten van verschillende wiskundigen zeggen dat voor oneven karakteristiek p Serres formules voor het niveau, het karakter en het gewicht van de gepostuleerde modulaire vorm inderdaad juist zijn. Dit wil zeggen dat als er een modulaire vorm bestaat die een gegeven "plat stuk" van $G_{\mathbb{Q}}$ geeft, dan bestaat er ook een modulaire vorm die aan Serres formule voldoet. Het geval $p = 2$ is echter nog gedeeltelijk open.

In het artikel beperk ik me tot "platte stukken" in karakteristiek p van $G_{\mathbb{Q}}$ (dus twee-dimensionale Galoisrepresentaties) waarvan de symmetriegroep een Diëdergroep, dus een symmetriegroep van een regelmatige n-hoek is. Voor deze toon ik het aangepaste Serrevermoeden aan zonder uitzondering, dus inclusief het geval $p = 2$. Dat zulk een Galoisrepresentatie van een modulaire vorm komt was in principe al Erich Hecke bekend, ten minste als $p \neq 2$ is. In het bewijs maak ik oneindig veel zulke modulaire vormen, zodat ik dan met behulp van het ladenprincipe (verdeel 10 letters over 5 laden, dan is er een lade waarin er ten minste twee liggen) er twee kan kiezen, die zich met methoden van de algebraïsche meetkunde tot de gewenste modulaire vorm laten combineren.

In het Hoofdstuk II bereken en vergelijk ik verschillende soorten cohomologiegroepen die alle met de modulaire kromme $X_1(N)$ (dit is een iets algemener Riemannoppervlak dan de hiervoor beschreven modulaire kromme) samenhangen, met het formalisme van de modulaire symbolen dat van de

homologie afgeleid is. In deze berekeningen is de coëfficiëntenring willekeurig. Er worden expliciete beschrijvingen in termen van lineaire algebra gegeven.

We bekijken modulaire symbolen om praktische redenen: zij zijn in het ver verspreide computeralgebrasysteem Magma geïmplementeerd. Ik heb computerprogramma's geschreven die hierop werken.

In het derde hoofdstuk worden nieuwe gevallen bewezen, wanneer de Katz modulaire vormen over $\overline{\mathbb{F}_p}$ met behulp van de expliciete beschrijvingen van de cohomologiegroepen uit Hoofdstuk II direct over het eindige lichaam $\mathbb{F}_p$ kunnen worden berekend. Dit betekent een snelheidswinst in vergelijking tot methoden die gehele getallen gebruiken. Met behulp van een idee van Edixhoven verkrijgen we zo ook een algoritme voor de berekening van Katz modulaire vormen van gewicht één (deze zijn niet direct berekenbaar) met behulp van modulaire symbolen over $\mathbb{F}_p$.

Het bewijs gebruikt het opmerkelijke parallel gedrag tussen de modulaire vormen van gewicht 2 en niveau Np over $\mathbb{F}_p$ en de eerste cohomologiegroepen van de Riemannoppervlakken $X_1(Np)$ met $\mathbb{F}_p$-coëfficiënten. In allebei vindt men namelijk de modulaire vormen resp. de eerste cohomologiegroepen terug, die bij het niveau N en het gewicht $k \in \{2, \ldots, p+1\}$ horen.

De overgang van de complexe meetkunde naar de algebraïsche over $\mathbb{F}_p$ vindt met behulp van de Jakobiaan van de modulaire kromme plaats. De eerste kohomologiegroep kan namelijk met de p-torsie van de complexe Jakobiaan geïdentificeerd worden. Gaat men dan naar het Néronmodel van de Jakobiaan, dan kan men eigenschappen van de generieke vezel (zelfs van het Riemannoppervlak) naar de speciale vezel (dus naar $\mathbb{F}_p$) overdragen.

Het vierde hoofdstuk bevat een beschrijving van de algoritmen die voortkomen uit de theorie van de twee voorgaande hoofdstukken. Tenslotte wordt in het vijfde hoofdstuk over computerberekeningen gerapporteerd die met behulp van de voorgestelde algoritmen zijn uitgevoerd. Er wordt bijvoorbeeld geconstateerd dat de platte stukken van $G_{\mathbb{Q}}$ in karakteristiek 2 opmerkelijk sterk groeien. Bovendien worden ook observaties gemaakt, die enkele interessante theoretische samenhangen suggereren. Hun studie zou het onderwerp van toekomstige projecten kunnen zijn.