Explicit computations with modular Galois representations

Bosman, J.G.

Samenvatting

Expliciete berekeningen met modulaire Galoisrepresentaties

De tekst van deze samenvatting is gebaseerd op het door de auteur geschreven populairwetenschappelijke artikel [8].

Galoistheorie

Op de middelbare school leert iedereen een kwadratische vergelijking $ax^2+bx+c=0$ oplossen met behulp van de *abc*-formule:

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

Voor vergelijkingen van graad 3 bestaat er een soortgelijke formule, in 1545 gepubliceerd door Cardano, na het gestolen te hebben van Tartaglia: de nulpunten van het polynoom ax^3+bx^2+cx+d zijn gelijk aan

$$x=\sqrt[3]{C+\sqrt{D}}+\sqrt[3]{C-\sqrt{D}}-\frac{b}{3a},$$

waarbij

$$C=\frac{-b^3}{27a^3}+\frac{bc}{6a^2}-\frac{d}{2a},\quad D=C^2+\left(\frac{c}{3a}-\frac{b^2}{9a^2}\right)^3$$

en de derdemachtswortels geschikt gekozen dienen te worden. We zien dat de nulpunten van tweedegraads- en derdegraadspolynomen gegeven kunnen worden als uitdrukkingen in de coëfficiënten, waarbij we de operaties $+$, $-$, $\cdot$, $/$ en $\sqrt[n]{}$ gebruiken. We zullen in zo'n geval zeggen dat het polynoom *oplosbaar* is. We kunnen ons afvragen of dit ook geldt voor polynomen van willekeurige graad. Ferrari, een student van Cardano, had in 1540 al aangetoond dat vierdegraadsvergelijkingen oplosbaar zijn, onder de voorwaarde dat derdegraadsvergelijkingen oplosbaar zijn.

Naar een formule voor de nulpunten van polynomen van graad 5 en hoger heeft men sindsdien eeuwenlang tevergeefs gezocht. In 1799 vond de Italiaanse wiskundige Ruffini zelfs een bewijs dat zo'n formule in het algemeen niet bestaat! Niemand geloofde hem echter,

totdat Abel in 1826 eveneens een bewijs vond. Zelfs vandaag de dag zijn er nog ongelovige thomassen die, uiteraard zonder succes, formules voor oplossingen van vijfdegraadsvergelijkingen proberen te vinden. Laten we hierbij wel opmerken dat het niet zo is dat geen enkele vergelijking van graad 5 of hoger opgelost kan worden. De nulpunten van $x^5 - x - 1$ kun je weliswaar niet uitdrukken in elementaire formules, maar die van $x^5 - 2$ wel: dat zijn alle waarden van $\sqrt[5]{2}$.

In 1832 vond Galois een nieuw bewijs voor het feit dat vergelijkingen vanaf graad 5 niet op te lossen zijn met $+$, $-$, $\cdot$, $/$ en $\sqrt[n]{}$. Het bewijs van Galois is zeer interessant omdat het veel meer inzicht en structuur aan een polynoom geeft dan alleen 'ja, het kan' of 'nee, het kan niet'.

Laten we eens kijken hoe Galois het deed. Kies je favoriete polynoom

$$P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Q}[x] \quad \text{met nulpunten } \alpha_1, \ldots, \alpha_n \in \mathbb{C}.$$

We zullen veronderstellen dat de nulpunten *verschillend* zijn; dit is geen grote belemmering want we kunnen meervoudige factoren makkelijk vinden. Er zijn allerlei relaties tussen de nulpunten. Zo kunnen we het product uitwerken in de identiteit

$$a_n(x - \alpha_1) \cdots (x - \alpha_n) = a_n x^n + \cdots + a_0$$

en dan vinden we bij elke coëfficiënt een symmetrische relatie, bijvoorbeeld

$$\alpha_1 + \cdots + \alpha_n = \frac{-a_{n-1}}{a_n} \quad \text{en} \quad \alpha_1 \cdots \alpha_n = \frac{(-1)^n a_0}{a_n}.$$

Afhankelijk van het polynoom kunnen er meerdere relaties tussen de nulpunten zijn dan degenen die je direct uit de symmetrische relaties kunt afleiden. Galois kwam op het idee om de groep van alle permutaties van de nulpunten te bekijken die alle relaties tussen deze nulpunten vasthouden; deze groep heet vandaag de dag de *Galoisgroep* van het polynoom P en noteren we met $\mathrm{Gal}(P)$. Als er niet meer relaties tussen de nulpunten zijn dan degenen die je uit de symmetrische relaties kunt afleiden, dan zal $\mathrm{Gal}(P)$ uit alle mogelijk permutaties tussen de nulpunten bestaan en dus isomorf zijn met S_n, de volledige symmetrische groep van graad n. Als er echter meer relaties zijn, dan leggen deze restricties op de permutaties op en zal $\mathrm{Gal}(P)$ dus kleiner zijn.

De oplosbaarheid van een polynoom P kan nu worden uitgedrukt in abstracte eigenschappen van de Galoisgroep $G = \mathrm{Gal}(P)$. We gaan een rij

$$G = G_1 \supset G_2 \supset \cdots$$

van ondergroepen van G maken aan de hand van het volgende recept: Begin met $G_1 = G$ en neem daarna telkens de *commutatorondergroep*:

$$G_{i+1} = [G_i, G_i] := \langle ghg^{-1}h^{-1} : g, h \in G \rangle.$$

Men kan laten zien dat P oplosbaar is dan en slechts dan als ergens in deze rij de triviale groep voorkomt. We zeggen in zo'n geval ook wel dat de groep G *oplosbaar* is.

Een groep die erg cruciaal is in deze context is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, de automorfismengroep van het lichaam van algebraïsche getallen. Het is een topologische groep waarin de Galoisgroepen van alle polynomen in $\mathbb{Q}[x]$ gecodeerd zitten. Voor eindige groepen G is het geven van een polynoom met Galoisgroep G (grofweg) equivalent met het geven van een continu surjectief homomorfisme $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to G$. De groep $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is binnen deze theorie dus een soort allesomvattend object en daarmee ook meteen heel moeilijk te begrijpen.

Modulaire vormen en Galoisrepresentaties

Modulaire vormen spelen een belangrijke rol in de getaltheorie. Grofweg zijn het holomorfe functies op het complexe bovenhalfvlak $\mathfrak{H}$ die aan bepaalde groeivoorwaarden en aan bepaalde symmetrierelaties ten aanzien van transformaties van de vorm $z \mapsto \frac{az+b}{cz+d}$ voldoen.

Een belangrijk voorbeeld van een modulaire vorm die veel wiskundigen heeft beziggehouden is de functie

$$\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24}, \quad \text{waarbij } q = e^{2\pi iz}. \tag{4.3}$$

De groeivoorwaarde voor deze functie is $\lim_{\Im z\to\infty}\Delta(z) = 0$ en de symmetrierelatie luidt in dit geval dat $\Delta(z)$ voldoet aan

$$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\Delta(z)$$

voor alle $z \in \mathfrak{H}$ en $a,b,c,d \in \mathbb{Z}$ met $ad-bc = 1$. We kunnen deze transformaties visualiseren in een plaatje dat laat zien hoe het complexe bovenhalfvlak in driehoeken wordt opgedeeld; zie de figuur op bladzijde 2. Als we het product in (4.3) uitwerken dan krijgen we een machtreeks

$$\Delta(z) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 + \cdots = \sum_{n\geq 1}\tau(n)q^n,$$

met $\tau(n)$ geheel. De functie $\tau : \mathbb{Z}_{>0} \to \mathbb{Z}$ die op deze manier gedefinieerd is heet de *Ramanujan tau-functie*. Ramanujan merkte een aantal merkwaardige eigenschappen van zijn tau-functie op. Onder andere waren daar de volgende drie eigenschappen, die hij niet kon bewijzen:

- Als m en n ondeelbaar zijn dan geldt $\tau(mn) = \tau(m)\tau(n)$.
- Voor priemmachten geldt de recursie $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$.
- Voor priemgetallen hebben we een ongelijkheid $|\tau(p)| \leq 2p^{11/2}$.

De eerste twee eigenschappen zijn in 1917 door Mordell bewezen, maar de derde is lange tijd onopgelost geweest.

Behalve de bovengenoemde eigenschappen vond Ramanujan ook nog congruenties voor $\tau(n)$ modulo (machten van) de priemgetallen 2, 3, 5, 7, 23 en 691, bijvoorbeeld

$$\tau(n) \equiv 1 + n^{11} \quad \text{voor alle } n.$$

Serre begon zich af te vragen waarom zulke congruenties niet bestaan modulo andere priemgetallen. In 1968 formuleerde hij een vermoeden waarin werd gesteld dat $\tau(p)$ uit te drukken is in termen van 2-dimensionale Galoisrepresentaties, dat wil zeggen continue homomorfismen $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K)$ waarbij K een zeker lichaam is. Hij bracht op die manier het modulo ℓ gedrag van $\tau(p)$ in verband met de grens $|\tau(p)| \leq 2p^{11/2}$. Het lukte Deligne in 1969 om het bestaan van zulke representaties aan te tonen en in 1974 slaagde hij erin om hiermee $|\tau(p)| \leq 2p^{11/2}$ te bewijzen. Het bewijs van Deligne gebruikt diepe resultaten uit de algebraïsche meetkunde; het totale aantal pagina's dat je krijgt als je alles helemaal vanaf het begin zou uitschrijven wordt geschat op ongeveer 2000.

De vorm Δ is niet uniek hierin. Eigenschappen die vergelijkbaar zijn met die voor de vorm Δ gelden voor veel meer modulaire vormen. De modulaire vormen in kwestie heten *eigenvormen* omdat het eigenvectoren zijn voor bepaalde lineaire operatoren op ruimten van modulaire vormen, de zogenaamde Heckeoperatoren. Bij elke eigenvorm blijken er Galoisrepresentaties gemaakt te kunnen worden.

De afgelopen decennia is het verband tussen eigenvormen en Galoisrepresentaties zeer intensief bestudeerd. Een van de grote resultaten die hieruit voortkwam is Wiles' bewijs voor de Laatste Stelling van Fermat. Een ander groot resultaat, dat sterk in verband staat met het werk van Wiles, is het bewijs voor het Serrevermoeden, gegeven door Khare, Wintenberger en Kisin. Dit Serrevermoeden stelt dat een representatie $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K)$ met K een eindig lichaam slechts aan een paar hele milde voorwaarden hoeft te voldoen om al van een eigenvorm afkomstig te zijn.

Het berekenen van $\tau(n)$

Een vraag die René Schoof aan Bas Edixhoven stelde is of het mogelijk is om $\tau(n)$ efficiënt uit te rekenen. Als we $\tau(p)$ kunnen uitrekenen voor priemgetallen p en n kunnen factoriseren in priemgetallen dan kunnen we, wegens de observaties van Ramanujan, $\tau(n)$ uitrekenen. Het zou mooi zijn om $\tau(n)$ snel te kunnen uitrekenen zonder te hoeven factoriseren; in dat geval zou het bekende en veelgebruikte cryptosysteem RSA namelijk gekraakt zijn. Voorlopig is het echter niet duidelijk hoe dit aangepakt zou kunnen worden en kunt u nog veilig internetbankieren.

Als we nu $\tau(p) \bmod \ell$ uitrekenen voor zo veel priemgetallen ℓ dat hun product groter dan $4p^{11/2}$ is, dan ligt, gezien de grens voor $|\tau(p)|$ hiermee $\tau(p)$ zelf vast. Met dit in het achterhoofd is Edixhoven een project gestart waarin hij het probleem tracht aan te pakken door de bijbehorende Galoisrepresentaties uit te rekenen. Dit proefschrift vormt een onderdeel van het project. Het basisidee van de berekeningen komt uit de meetkunde: de Galoisrepresentatie die bij $\tau(p) \bmod \ell$ hoort voor een gegeven ℓ kan worden gerealiseerd in een variëteit

die $J_1(\ell)$ genoemd wordt en dimensie $(\ell-5)(\ell-7)/24$ heeft. Jean-Marc Couveignes had het idee om hierbij numerieke berekeningen te gebruiken. Om deze ideeën hard te maken lijkt het echter onvermijdelijk om *Arakelovmeetkunde* te gebruiken; op dit punt kon Robin de Jong zijn steentje bijdragen aan het project. Hierbij is gebruikgemaakt van een resultaat van Franz Merkl, iemand uit de kansrekening.

Een nadeel van het algoritme van Edixhoven, Couveignes en De Jong is dat het praktisch niet goed werkt. Zo is de rekenprecisie te hoog en moeten we in plaats van $J_1(\ell)$ de variëteit $J_1(5\ell)$ gebruiken, waarvan de dimensie $(\ell-2)^2$ is.

In de praktijk kunnen we deze bezwaren negeren en gewoon gaan rekenen. We krijgen polynomen met coëfficiënten van een hoge precisie (denk hier aan enkele duizenden decimalen). We weten dat de coëfficiënten benaderingen zijn van rationale getallen. Als de benadering sterk genoeg is, dan gokken we dat de rationale getallen waar ze dichtbij liggen de daadwerkelijke coëfficiënten zijn van de polynomen die bij de representaties horen. We moeten dan wel nog achteraf nagaan dat het verkregen polynoom correct is. Dankzij het feit dat het Serrevermoeden nu bewezen is, is dit allemaal goed te doen. Uiteraard geldt ook hier dat we niet tot de tau-functie beperkt zijn. De rekenmethoden werken met eigenvormen in het algemeen.

Dit proefschrift

In Hoofdstuk 1 van dit proefschrift zullen wij de theorie van modulaire vormen behandelen. Voorts zullen wij in Hoofdstuk 2 bespreken hoe er gerekend kan worden aan modulaire vormen en Galoisrepresentaties. In de Hoofdstukken 3 en 4 zullen we enkele resultaten van de berekeningen presenteren die zijn uitgevoerd.

In Hoofdstuk 3 betreft deze berekening de oplossing van een probleem uit de *computationele inverse Galoistheorie* dat Jürgen Klüners, een van de grote wereldexperts op dit gebied, mij had voorgelegd. In de computationele inverse Galoistheorie tracht men voor zo veel mogelijk groepen G een polynoom te vinden waarvan G de Galoisgroep is. De groep in Hoofdstuk 3 betreft $\mathrm{SL}_2(\mathbb{F}_{16})$, de groep van 2 bij 2 matrices met determinant 1 en coëfficiënten in het lichaam van 16 elementen. Verschillende mensen waren naar zo'n polynoom op zoek. Of er ook voor elke groep G een polynoom bestaat met Galoisgroep G is een zeer moeilijk onopgelost probleem in de getaltheorie.

De resultaten van Hoofdstuk 4, betreffen enkele berekeningen aan Galoisrepresentaties voor de tau-functie en daaraan gerelateerde functies. In dat hoofdstuk zullen we projectieve representaties voor deze functies modulo de priemgetallen $\ell \geq 23$ geven. Als toepassing verbeteren we de grens waarvoor het *Lehmervermoeden* geverifiëerd is met meer dan een factor duizend. Dit vermoeden stelt dat de tau-functie nergens de waarde nul aanneemt. Het resultaat van het hoofdstuk is interessant omdat het een toepassing geeft van het Serrevermoeden, een theoretisch resultaat, in een computationele context.