Bas Edixhoven
Mathematisch Instituut
Universiteit Leiden
bas@edixhoven.net

Onderzoek Vici-project

Aritmetische meetkunde

Bas Edixhoven vroeg in 2002 een Vici-subsidie aan voor het project 'Arithmetic geometry, motives: computational aspects'. Deze aanvraag werd *niet* gehonoreerd. In 2004 was dezelfde aanvraag *wel* succesvol. In dit artikel blikt hij terug op zowel de aanvraag- als op de uitvoeringsperiode, en geeft hij enkele adviezen aan NWO.

Verslag doen is een goede zaak. Zeker als er $1{,}25$ miljoen euro aan publieke middelen is gestoken in een individueel onderzoeksproject. Natuurlijk worden er verslagen voor de grootste geldschieter, NWO, geschreven, elk jaar zolang het project loopt, *en* op het midden, *en* aan het eind. Maar die verslagen bereiken maar een zeer klein publiek. En het zijn grotendeels weinig inspirerende opsommingen van proefschriften, publicaties, voordrachten en andere vormen van 'output'. Zulke verslagen belanden al gauw in een digitale map, van waaruit ze dan hopelijk nog eens worden opgevraagd wanneer de uitvoerder een nieuwe aanvraag indient. Ik ben een groot voorstander van het beoordelen van aanvragers op prestaties uit het verleden, en niet op beloften voor de toekomst. Het is dan interessant (NWO-bestuurders, lezen jullie mee?) om te kijken hoeveel van de heldhaftige plannen uit de vorige aanvraag daadwerkelijk zijn gerealiseerd.

Ik neem dus nu graag mijn laptop op schoot om aan het verzoek van de redactie van dit blad te voldoen en een verslag te schrijven over het door mij uitgevoerde Vici-project, niet voor *alle* belastingbetalers, maar wel voor alle lezers van het *Nieuw Archief voor Wiskunde* en, laten we zeggen, voor allen die zich wiskundigen kunnen noemen.

Het schrijven van de aanvraag

Het was niet mijn eigen idee om een Vici project aan te vragen bij NWO. Het idee kwam van de toenmalige directie van het Leidse Mathematisch Instituut (en met name van Gerrit van Dijk) in december van 2001, toen ik daar vanuit Frankrijk solliciteerde naar een hoogleraarspositie. Ook toen was dit soort geld al belangrijk voor het overleven van de Nederlandse wiskunde-instituten, die geteisterd werden door lage studentenaantallen. Aangezien het mijn ambitie was in Leiden een sterke groep op mijn vakgebied 'aritmetische meetkunde' op te zetten, zowel voor onderzoek als voor onderwijs, kwamen onze belangen overeen. Na enig onderhandelen kreeg ik een aanbod uit Leiden dat ik aannam, en begon ik met nadenken over de aanvraag. Een eerste versie, vooraanmelding geheten, moest al per 1 april bij NWO zijn ingediend. Ik had al een goede onderzoeksvraag, gebaseerd op een vraag van René Schoof uit 1995. Over die vraag had ik al af en toe nagedacht, maar kwam pas weer verder na een cruciale suggestie van Jean-Marc Couveignes in 1999 (gebruik geen algebra, maar numerieke analyse!). In oktober 2000 had ik een kansrijke strategie gevonden, die ik samen met Couveignes zou uitwerken. Onze taken waren goed gescheiden: Jean-Marc werkte aan benaderingen met behulp van numerieke analyse, en ik aan afschattingen van de benodigde precisie. In december 2000 had ik over dit project gesproken tijdens een conferentie in Berkeley voor een publiek van aritmetisch meetkundigen (zie [22]), maar daarna had ik er nog niet verder aan gewerkt omdat het een meerjarenklus zou worden, en aan werk had ik geen gebrek.

Bij het schrijven van de vooraanmelding besteedde ik de meeste tijd aan de beschrijving van het voorgenomen onderzoek, in $300 + 800$ woorden (waarover later meer; wie ongeduldig is *en* voldoende bekwaam is in de aritmetische meetkunde kan ook direct door naar [6] en [3], die samen gezien kunnen worden als het ultieme wetenschappe-

lijke verslag van het project). In overleg met Fred Bakker werd de begroting opgesteld: vijf jaar mijn gehele eigen salaris, acht postdocjaren, twee promovendi en wat bijkomstigheden als bezoekers, reiskosten, computers en software, een programmeur, en wat geld voor het populariseren van de wiskunde (denk aan steun voor de stichting Vierkant voor Wiskunde en het opzetten van een WIMS-mirror, zie [21]). De universiteit Leiden zorgde voor een 'inbeddingsgarantie', waarin ze beloofde de onderzoekslijn van het project structureel in te bedden in haar toekomstplannen. Het gaat hier om een blijvende stevige invloed van de subsidie. In mijn geval was dat niet zo moeilijk, want ik had immers al de hoogleraarsplaats gekregen, met daarbij de belofte twee UD/UHD-posities in te kunnen vullen.

Op 2 juli 2002 kreeg ik van Lex Zandee het goede nieuws dat ik werd uitgenodigd een uitgewerkt Vici-voorstel in te dienen: $300+8000$ woorden dit keer. De deadline was 1 september 2002. Ik herinner me nog dat ik een flink aantal dagen in augustus, na de verhuizing naar Leiden, op het instituut aan de aanvraag heb gewerkt. Uiteindelijk was ik zeer tevreden met het resultaat. In die 8000 woorden had ik uitgelegd welk probleem aangepakt zou worden, waarom het een interessant probleem was, hoe het aangepakt zou worden, en waarom de kans van slagen groot was.

Daarna was NWO weer aan zet, met het raadplegen van adviseurs en verzamelen van de reacties van de kandidaten op de adviezen. Op 23 oktober 2002 kreeg ik van Petra de Bont de rapporten van vijf referenten, waarop ik binnen zes dagen diende te reageren. Het lezen van de vijf rapporten was een spannende ervaring. Gelukkig kon ik tevreden zijn met het resultaat. Alle vijf referenten beoordeelden de aanvraag als excellent, ze vonden de plannen interessant en de aanpak overtuigend. Er was voor mij geen reden om te reageren.

Het interview, wat ging er mis?

De volgende stap in de aanvraagprocedure was een interview van vijftig minuten van de overgebleven kandidaten met een commissie ingesteld door het gebiedsbestuur van Exacte Wetenschappen (EW) van NWO, waarin wiskunde, informatica, sterrenkunde en toen ook nog natuurkunde vertegenwoordigd waren. Direct na de interviews, die op een of twee dagen in november plaatsvonden, maakte deze commissie een 'ranking' van de kandidaten, zodat het algemene NWO-bestuur (geleid door de excellente, nu legendarische en welhaast mythische topeconoom Peter Nijkamp) de uiteindelijke beslissing kon nemen. (Hoe kan zo iemand als Nijkamp zo hoog terecht komen? Dateert zijn fraude al van voor zijn prijzen en benoemingen? Extra controle van bovenaf, en extra cursussen integriteit lossen dit probleem niet op — bestuurders, lezen jullie mee? De controle moet van collega's uit het vakgebied zelf komen, daar zit de expertise. Laten vooral degenen die verantwoordelijk zijn voor zijn prijzen en benoemingen zich eens bezinnen op de vraag hoe dit alles heeft kunnen gebeuren. De schuld voor de misdragingen ligt natuurlijk bij Nijkamp zelf.)

Als voorbereiding werd er voor mij in Leiden een proef-interview georganiseerd. Daar kreeg ik veel nuttige maar uiteenlopende suggesties. Het echte interview verliep stroef. Eigenlijk liep het uit op een clash, maar dat besef drong pas na enige tijd door. Na al die jaren nu terugkijkend zie ik twee oorzaken. Zelf had ik het belang van het interview onderschat. Ik verkeerde teveel in de veronderstelling dat de commissie haar oordeel grotendeels op de CV's en de rapporten van de referenten zou baseren, en dat het interview meer een soort 'sanity check' was (zo ging dat toen in Frankrijk). Gezien de uiterst positieve rapporten dacht ik niet dat een andere uitkomst dan toekenning mogelijk was. Maar zo gaat het dus niet. De commissie gaf haar eigen oordeel over de kandidaten meer gewicht dan ik toen dacht. Mijn presentatie, waarmee het interview begon, bestond teveel uit intimidatie met grote namen, prijzen, en wiskundige objecten dan op inhoudelijke overtuiging. Bijvoorbeeld noemde ik belangrijke resultaten van Faltings, Wiles, Lafforgue en Voevodsky zonder die concreet te maken. Er kwam geen 'klik' met de commissie. Aan de andere kant begon de voorzitter van de commissie, H.A.M. van Eekelen, een natuurkundige die voor Shell had gewerkt (of werkte), na de presentatie met mij te vragen waarom ik maar zo weinig citaties had (hij had zijn huiswerk gedaan, zei hij). Was de groep van wiskundigen met interesse in mijn werk misschien heel klein? Ik gaf hierop het weinig diplomatieke antwoord dat er wel degelijk veel wiskundigen in mijn werk geïnteresseerd waren, dat de referenten toch duidelijk overtuigd waren, en dat hij een fout maakte met zijn citatie-argument. Ook liet Van Eekelen blijken dat hij cryptografie niet belangrijk vond, en niet geloofde dat mijn onderzoek relevant zou kunnen zijn voor cryptografie.

Ongeveer een maand na het interview werd mij de uitslag van de procedure meegedeeld. Niet toegekend, dus. Ondanks de negatieve sfeer tijdens het interview, die ik zelf kennelijk grotendeels verdrongen had, was ik toch nog verbaasd, en kwaad.

Tussen twee aanvragen

Natuurlijk was het de bedoeling om de aanvraag nog een keer in te dienen. Maar een periode van afkoeling kon geen kwaad. Vandaar het besluit om een jaar over te slaan, in 2004 zou ik een tweede poging doen.

Nu ik zo'n duidelijk onderzoeksplan had liggen, maar nog geen promovendi en geen postdocs, begon ik er zelf alvast maar aan te werken. Aan zijn kant maakte Jean-Marc Couveignes vorderingen, dus ik was wel verplicht om ook aan mijn kant aan de kar te trekken. Een andere goede reden om te beginnen was om een voordracht over dit onderwerp voor te bereiden die ik in een workshop 'Future directions in algorithmic number theory' in Palo Alto zou gaan geven.

Bij een voordracht in het Nederlandse Intercity Number Theory Seminar in April 2003 liet Robin de Jong, toen promovendus bij Gerard van der Geer, zijn interesse en deskundigheid in het onderwerp blijken. In de drie maanden daarna maakten we samen een goed begin met het project, we bewezen een deelresultaat (Stelling 9.2.5 in [6]). Met dat resultaat in de hand werd het duidelijker wat er allemaal nog te doen was. Een van deze taken was het afschatten van zogenaamde Arakelov–Green-functies op Riemann-oppervlakken. Voor mijzelf was dit probleem te analytisch, dus benaderde ik Peter Sarnak. Hij gaf de vraag door aan Jay Jorgenson, die er vanaf januari 2004 aan ging werken, samen met Jürg Kramer in Berlijn. Ook sprak ik in december 2003 met Franz Merkl over dit probleem, hij was dat jaar postdoc in de statistiekgroep in Leiden. Franz zei meteen dat hij wist hoe hij dit probleem kon oplossen. En inderdaad kwam hij in februari 2004 met een tekst die met weinig aanpassingen geworden is tot hoofdstuk 10 in [6]. Jorgenson en Kramer losten het probleem wat later ook op, op een andere manier. Voor mij betekende dit dat het laatste serieuze obstakel in mijn hele project was weggenomen, en was ik er zeker van dat ik de rest zou kunnen afmaken. Het bleef nog wel een meerjarenklus.

De tweede aanvraag, wel succes

Inmiddels was het 2004, dus tijd om opnieuw een aanvraag bij NWO in te dienen. De eerste keer had de mislukking niet aan het geschreven voorstel gelegen, dus dit keer had ik weinig werk. Ik diende het voorstel in zoals het was, met toevoeging van een beschrijving van

het werk dat sinds de eerste keer was gedaan, en met een verandering van de begroting. Dit laatste punt verdient wel enige uitleg, aangezien er een conflict van belangen was tussen die van de aanvrager en die van zijn instituut en universiteit. De totale omvang van het project was $1{,}25$ miljoen euro, waarvan NWO 67 procent voor haar rekening nam, en de overige 33 procent moest worden 'gematcht' door de Universiteit Leiden. Dit soort matching is later afgeschaft. In mijn eerste aanvraag had ik 100 procent van mijn eigen salaris in de begroting van het project gezet. Doordat ik in de jaren 2002–2004 voor NWO in commissies had gezeten waar projecten werden beoordeeld, had ik ook ingezien dat projecten aantrekkelijker waren naarmate er meer uitkwam, bijvoorbeeld in aantallen opgeleide promovendi. Door mijn eigen salaris (de universiteit moest het toch al betalen) voor maar 40 procent in de begroting op te nemen, kwam er ruimte voor een derde promovendus. Ook was het natuurlijk niet realistisch dat ik 100 procent van mijn tijd in het project kon gaan steken: er moest immers ook onderwijs worden gegeven, en ik was een van de twee managing editors van *Compositio Mathematica*. Mijn begroting was kostenneutraal voor de universiteit (het salaris van Johan Bosman, die in juni 2004 als promovendus was begonnen, zat er ook in). Natuurlijk zou de universiteit van mijn project enorm profiteren in de vorm van extra promovendi, postdocs en activiteiten. Ik kreeg wel een telefoontje van het bestuursbureau met de vraag of er niet een promovendus minder kon, maar het was niet moeilijk om daar nee op te zeggen.

Ook deze keer werd ik uitgenodigd om een uitgewerkt voorstel in te dienen. Het resultaat daarvan is [19], nagenoeg identiek aan het voorstel uit 2002. NWO zocht en vond vijf nieuwe referenten. Vier van hen beoordeelden het project met 'excellent'. Referent nummer 5 schreef: "As the above report clearly shows, for me this is THE most important work presently being done in explicit arithmetic geometry. I have no doubt that the authors will achieve at least part of their goals, and that it will be an important landmark on the subject. In addition, the cryptographic applications are immediately clear, even if they are not the main motivation for the reasearch. I am surprised that an earlier proposal of the applicant was not accepted 2 or 3 years ago: of course the research was not as advanced as it is now, but I am sure that the referees must have been unanimous in saying that the potential of the work was outstanding. I give the highest possible marks to this proposal."

Maar referent nummer 4 vond het maar niets dat ik voltijds zou werken aan computationele aspecten, want ik zou er mijn intuïtie voor 'bona fide theorems' mee verliezen. Ook vond hij of zij het maar niets dat ik wat samenwerking had met een bedrijf, Canon Recherche France, en met het Franse CELAR (Centre Electronique de l'Armement, een afdeling van het Franse ministerie van defensie). Hij ging ervan uit dat de in die samenwerking verkregen resultaten geheim zouden zijn. Zijn rapport eindigde aldus: "As far as I am concerned, I feel that Edixhoven is basically lost for number theory, and I cannot recommend him for your fellowship."

Dit keer schreef ik dus wel een weerwoord. Ik schreef dat mijn project bijna geheel bestond uit het bewijzen van 'bona fide theorems', dat zijn conclusies over de bovengenoemde samenwerking die ik had, gebaseerd waren op onjuiste aannamen (in het contract voor de samenwerking stond bijvoorbeeld dat ik alle daarin door mij verkregen resultaten op mijn eigen homepage moest publiceren), en ik eindigde met: "Finally, to think that I would be lost for number theory just proves that this report cannot be taken seriously."

Nu is het zo dat zo'n weerwoord niet naar de referenten gaat, maar naar de commissie die de kandidaten moet 'ranken'. Die commissie moet dan beslissen of het weerwoord de bezwaren van de referent voldoende weerlegt. Maar als het een technische kwestie wordt, heeft ze vaak de daarvoor benodigde expertise niet (NWO-bestuurders, kan dit beter?).

Deze keer nam ik het interview serieuzer. Door mijn ervaring als lid van andere beoordelingscommissies snapte ik beter dat je als kandidaat op *inhoudelijke* zaken echt overtuigend moet zijn. Dat je de commissie moet overtuigen juist aan *jou* die enorme pot geld toe te kennen, door te laten zien dat zij *waar* voor haar geld krijgt door de *meerwaarde van het project* duidelijk te maken.

Het interview, dat aan het eind van de middag plaatsvond, begon met een presentatie van 25 minuten, waarvan de slides (voor overheadprojector, en inclusief aantekeningen voor mijzelf — tussen de slides) te vinden zijn in [20]. De sfeer was ontspannen. De voorzitter, Emile Aarts, heette mij hartelijk welkom. Ik had mij de hele dag mentaal zitten voorbereiden op mijn presentatie, die daardoor liep als een trein. Ik wist precies wat ik allemaal wilde zeggen, en het kwam er zo vloeiend uit dat ik adem tekortkwam. Daarna volgde de discussie, waarin de voorzitter begon met de mededeling dat ook de commissie het rapport van referent nummer 4 terzijde had geschoven. Van de 25 minuten discussie herinner ik me weinig, behalve dat aan het eind er de vraag kwam, nu van Annejet Meijler (NWO, directeur gebied EW, met een achtergrond in de medische fysica), die ook bij het eerste interview aanwezig was geweest, waarom mijn werk relevant zou zijn voor de cryptografie. Kennelijk waren de twijfels van Van Eekelen toch nog blijven hangen. Nu had ik echter mijn antwoord klaar. Ik haalde even diep adem, ging *rustig* een aantal slides terug (naar slide 4, om precies te zijn) en liet zien dat het daar stond, en dat ik het had uitgelegd.

Na het interview volgde een spannende periode van wachten. De ranking van de commissie blijft natuurlijk een proces met een kans-aspect, want het is als appels en peren vergelijken. Er zijn veel aanvragen en maar weinig toekenningen, en je weet zelf niet wie je concurrenten zijn. Voor je eigen gezondheid is het dan maar beter om ervan uit te gaan dat je de subsidie *niet* krijgt. En dat is ook de meest realistische houding. Uiteindelijk kwam op 16 december 2004 het goede nieuws in de vorm van een email (normaal word je gebeld, maar ik was juist bij Couveignes in Toulouse) van Petra de Bont: bij EW (wiskunde, informatica en sterrenkunde; de natuurkunde was eruit gestapt) werden drie aanvragen gehonoreerd, en het mijne was daar één van.

De wiskunde dan, eindelijk; context

Nu kon ik medewerkers gaan aanstellen. De eersten waren Johan Bosman, die al promovendus was, en Robin de Jong die direct na zijn promotie als postdoc in dienst kwam. Ik had al twee andere promovendi, Gabor Wiese en Theo van den Bogaart, maar die werkten aan andere zaken. Met Peter Bruin en Arjen Stolk had ik twee heel goede kandidaten voor de overige twee promotieplaatsen. Zij moesten nog wel eerst afstuderen. Een voordeel daarbij was dat ze in hun afstudeerscripties al werden voorbereid op het latere werk.

Laten we dan nu eindelijk naar de *wiskunde* in het voorstel kijken. (NWO-medewerkers in EW en andere béta-bestuurders: haak nu nog niet af! Als u het volgende niet grotendeels kunt begrijpen, bent u aan wat bijscholing toe. Er zijn vast wiskundigen in uw omgeving die u daar graag bij helpen, en zo niet, dan bent u welkom bij mij.) Eerst een schets van het landschap waarin het onderzoek plaatsvond: de algebraïsche meetkunde, en Grothendiecks étale cohomologie. Laat $n \geq 0$ een geheel getal zijn, en laat $X \subset \mathbb{C}^n$

de oplossingsverzameling zijn van een systeem van veeltermvergelijkingen met complexe coëfficiënten:

$$\begin{aligned} f_1(x_1, x_2, \ldots, x_n) &= 0 \\ f_2(x_1, x_2, \ldots, x_n) &= 0 \\ &\vdots \\ f_r(x_1, x_2, \ldots, x_n) &= 0. \end{aligned}$$

Zulke deelverzamelingen van $\mathbb{C}^n$ heten *complex affien algebraïsch*. We zijn met name geïnteresseerd in de topologische eigenschappen van X, waarbij we X voorzien van de geïnduceerde topologie als deelverzameling van $\mathbb{C}^n$, die zelf de gebruikelijke (euclidische) topologie heeft. Een voorbeeld is de vergelijking $x_1+x_2=0$; dan is de oplossingsverzameling X gelijk aan $\{(z,-z) : z \in \mathbb{C}\}$, een complexe lijn, dus homeomorf met $\mathbb{C}$. Een ander voorbeeld is de vergelijking $x_1^2+x_2^2=0$, waarbij X gelijk is aan de vereniging van twee complexe lijnen die snijden in de oorsprong (want $x_1^2+x_2^2=(x_1+ix_2)(x_1-ix_2)$). Iets interessanter is de vergelijking $x_1^2+x_2^2=1$, waarbij X homeomorf is met $\mathbb{C}$ minus één punt: schrijf de vergelijking als $(x_1+ix_2)(x_1-ix_2)=1$, dan zie je dat de afbeelding $X \to \mathbb{C}$ die (a,b) naar $a+ib$ stuurt injectief is, met beeld $\mathbb{C}-\{0\}$. De inverse afbeelding stuurt t naar $((t+t^{-1})/2, (t-t^{-1})/2i)$, een continue afbeelding. Topologisch gezien is deze X interessanter dan de voorgaande, want deze X is niet samentrekbaar. Sterker, deze X is homotopie-equivalent met de cirkel S^1.

Nog interessanter wordt het met vergelijkingen van de vorm $x_2^2=x_1^3+ax_1+b$, met a en b in $\mathbb{C}$ complexe parameters (elliptische krommen!). Als de veelterm $x_1^3+ax_1+b$ geen meervoudige nulpunten heeft (hetgeen equivalent is met $4a^3+27b^2 \neq 0$), dan is X homeomorf met een torus ($S^1 \times S^1$) minus één punt. Dit is minder eenvoudig in te zien, maar al wel minstens 150 jaar standaardwiskunde (denk aan Gauss, Jacobi, Riemann,...).

In het begin van twintigste eeuw hebben algebraïsch topologen (Henri Poincaré (intuïtief), onze eigen Luitzen Egbertus Jan Brouwer (precies)) voor alle topologische ruimten X cohomologiegroepen $H^j(X,\mathbb{Z})$ gedefinieerd, voor j in $\mathbb{Z}$ (die met $j<0$ zijn nul). (Dit lijkt me een redelijk punt om even af te haken, voor degenen die niet het equivalent van een bachelor wiskunde hebben gedaan. Maar lees vooral weer door vanaf de voorlaatste paragraaf.) Deze groepen geven niet alleen interessante informatie over de topologische complexiteit van X, maar zijn ook nuttig voor het tellen van vaste punten van continue afbeeldingen $f: X \to X$ via de spoorformule van Lefschetz (onder zekere voorwaarden op X en f).

Een van de mijlpalen in het werk van Alexander Grothendieck is een *algebraïsche definitie* van $H^j(X,\mathbb{Z}/m\mathbb{Z})$, voor $m \neq 0$ en j geheel, en $X \subset \mathbb{C}^n$ complex affien algebraïsch. Zelfs voor elliptische krommen X als hierboven kunnen cohomologiegroepen $H^1(X,\mathbb{Z})$ *niet* algebraïsch gedefinieerd worden. Als groep zijn al deze $H^1(X,\mathbb{Z})$ isomorf met $\mathbb{Z}^2$. Voor de kenner: neem X met 'complexe vermenigvuldiging', zie die cohomologiegroep als moduul over de endomorfismenring, de cohomologiegroep heeft dan een klasse in de Picard-groep van de endomorfismenring, deze klassen zouden dan behouden moeten zijn door automorfismen van $\mathbb{C}$ die de identiteit induceren op de endomorfismenring, quod non.

Wat is dat precies, in dit geval, een *algebraïsche definitie*? Het antwoord is: een definitie die compatibel is met algebraïsche isomorfismen. Dat betekent dat we moeten zeggen wat de algebraïsche isomorfismen zijn tussen complexe affiene algebraïsche X en Y. Welnu, terwijl ik dit schrijf, realiseer ik me ineens dat zelfs *dat* in eenvoudige termen uit te leggen is, zonder sjoemelen!

Voor $X \subset \mathbb{C}^n$ complex affien algebraïsch, laat $A(X)$ de verzameling van functies $f: X \to \mathbb{C}$ zijn, die de beperking tot X zijn van complexe veeltermfuncties op $\mathbb{C}^n$. Deze verzameling $A(X)$ is gesloten onder het puntsgewijs optellen en vermenigvuldigen van functies: het is een commutatieve ring, met een eenheidselement, namelijk de constante functie met waarde 1. Ieder element x van X geeft een evaluatie-afbeelding $\mathrm{ev}_x: A(X) \to \mathbb{C}$, $f \mapsto f(x)$. David Hilbert liet al zien (zijn Nullstellensatz) dat de kernen van deze evaluatieafbeeldingen precies de maximale idealen van $A(X)$ zijn (de afbeelding $x \mapsto \ker(\mathrm{ev}_x)$ is een bijectie tussen de betreffende verzamelingen). Dus als verzameling kunnen we X terugvinden uit $A(X)$.

Voor $X \subset \mathbb{C}^n$ en $Y \subset \mathbb{C}^m$ complex affien algebraïsch, is dan een algebraïsch isomorfisme van X naar Y hetzelfde als een isomorfisme van ringen van $A(Y)$ naar $A(X)$. Wat Grothendieck heeft laten zien (met veel medewerking van Michael Artin), is dat er voor ieder geheel getal $m \neq 0$ en ieder geheel getal j een functor is van ringen naar abelse groepen, $A \mapsto H^j_{\mathrm{et}}(A,\mathbb{Z}/m\mathbb{Z})$, zodat voor X complex affien algebraïsch $H^j_{\mathrm{et}}(A(X),\mathbb{Z}/m\mathbb{Z})$ hetzelfde is (isomorfisme van functoren...) als de door de topologen gedefinieerde $H^j(X,\mathbb{Z}/m\mathbb{Z})$. Voor de volledigheid is het goed te melden dat Grothendieck zijn functor definieerde (hoe kan het ook anders) voor *willekeurige ringen*. En eigenlijk is die definitie tegenwoordig geen verrassing meer; zozeer zijn Grothendiecks technieken gemeengoed geworden. Wat wel verrassend is, is dat die definitie redelijke resultaten oplevert (dat was het werk met Artin).

Laten we nu eens kijken naar de automorfismen van $\mathbb{C}$. Let wel, dit gaat om automorfismen van $\mathbb{C}$ als *lichaam*, we moeten (en dat is voor iemand die dat voor het eerst doet niet zo makkelijk) de topologie van $\mathbb{C}$ *vergeten*. De enige continue automorfismen van $\mathbb{C}$ zijn de identiteit en de complexe conjugatie (makkelijke opgave voor eerstejaars studenten). Laten we nu degenen die denken dat e en π speciale getallen zijn eens wat plagen. De getallen e en π zijn beide transcendent over $\mathbb{Q}$ (Hermite, Lindemann), dus zijn er (transcendentiebases, Zorn...) automorfismen σ en τ van $\mathbb{C}$ met $\sigma(\pi)=e$ en $\tau(e)=\pi$. Dus voor een algebraïcus zijn e en π niet verschillend. Het schijnt niet bekend te zijn of men τ en σ aan elkaar gelijk kan nemen. Men verwacht dat e en π algebraïsch onafhankelijk over $\mathbb{Q}$ zijn, en dan is $\sigma=\tau$ mogelijk.

De cruciale opmerking is nu dat ieder automorfisme σ van $\mathbb{C}$ een algebraïsch isomorfisme geeft van X, oplossingsverzameling van $f_1,\ldots,f_r$, naar $\sigma(X)$, de oplossingsverzameling van $\sigma(f_1),\ldots,\sigma(f_r)$ (pas σ toe op de coëfficiënten van $f_1,\ldots,f_r$), als volgt. Voor $(a_1,\ldots,a_n)$ in $\mathbb{C}^n$ is het nul zijn, voor alle j, van $f_j(a_1,\ldots,a_n)$, equivalent met het nul zijn, voor alle j, van $\sigma(f_j(a_1,\ldots,a_n))=\sigma(f_j)(\sigma(a_1),\ldots,\sigma(a_n))$. Kortom, σ coördinaatsgewijs toepassen geeft een bijectie tussen X en $\sigma(X)$, en een isomorfisme van ringen $A(\sigma(X)) \to A(X)$, $h \mapsto \sigma^{-1} \circ h \circ \sigma$.

Laten we vanaf nu aannemen dat alle coëfficiënten van alle f_j in $\mathbb{Q}$ liggen. Dan is $\sigma(X)$ gelijk aan X, en $A(\sigma(X))$ is gelijk een $A(X)$. We concluderen dat de automorfismengroep van $\mathbb{C}$ werkt op alle $H^j(X,\mathbb{Z}/m\mathbb{Z})$. Dit heet de *Galois-actie* van $\mathrm{Aut}(\mathbb{C})$, en het maakt de cohomologiegroepen tot zogenaamde *Galois-representaties*.

Laten we dit concreet maken. Voor iedere X, m en j is $H^j(X,\mathbb{Z}/m\mathbb{Z})$ eindig, en is er een polynoom f in $\mathbb{Q}[t]$, en een bijectie b tussen $H^j(X,\mathbb{Z}/m\mathbb{Z})$ en de verzameling nulpunten van f in $\mathbb{C}$, die compatibel is met de Galois-acties aan beide kanten: voor alle elementen h van $H^j(X,\mathbb{Z}/m\mathbb{Z})$ en voor alle σ in $\mathrm{Aut}(\mathbb{C})$ geldt dat $b(\sigma(h))=\sigma(b(h))$. Echter, in niet-triviale gevallen is het meestal ongelooflijk moeilijk om zo'n f te vinden. Voorbeelden

van triviale tot conceptueel niet zo erg moeilijke gevallen zijn:

- die waar $H^j(X, \mathbb{Z}/m\mathbb{Z})$ cyclisch is (rang één motieven),
- die waar $j = 0$,
- die waar X een rationale of elliptische kromme is (gebruik delingspolynomen),
- die waar X een Riemann-oppervlak van begrensd geslacht minus een eindig aantal punten is (in dit geval kijken we naar een oneindige rij van X'en),
- die waar het beeld van de Galois-representatie (een eindige groep) oplosbaar is (geïtereerde klasselichamentheorie).

De wiskunde, het project

Het project bestond eruit om het vinden van een f zoals aan het eind van de vorige sectie in het eenvoudigste niet-triviale geval aan te pakken: het geval van rang twee motieven, dat wil zeggen, Galois-stabiele ondergroepen van $H^j(A, \mathbb{Z}/m\mathbb{Z})$ die als commutatieve groep isomorf zijn met $(\mathbb{Z}/m\mathbb{Z})^2$, waar f dus graad m^2 heeft. Sinds werk van Hecke, Eichler, Shimura, Deligne (ongeveer van 1920 tot 1970) en nog veel anderen is het bekend dat modulaire vormen (we gaan dit begrip nu niet uitleggen) een bron zijn voor dit soort Galois-representaties. En sinds het werk van Khare-Wintenberger en Kisin (en veel werk dat daar weer aan ten grondslag ligt, denk aan Wiles en Taylor, en laten we Fontaine en ook Serre niet vergeten) weten we precies welke tweedimensionale Galois-representaties van modulaire vormen komen: de determinant van de actie van complexe conjugatie moet -1 zijn.

Kort samengevat heeft het project opgeleverd dat zulke f komend van modulaire vormen, berekend kunnen worden in een rekentijd begrensd door een vaste macht van de som van m, het 'gewicht' en het 'niveau' van f. Het geval van niveau 1 is in groot detail opgeschreven in [6]. Peter Bruin generaliseerde het in zijn proefschrift [3] naar algemenere niveaus (Ariyan Javanpeykar bewees de nodige afschattingen in Arakelov theorie voor *alle* niveaus in zijn proefschrift [7]). Arjen Stolk begon met een analoog geval: functielichamen, maar de klus was groter dan redelijk. Onder begeleiding van Joost Batenburg en in mindere mate van mij paste hij zijn verworven kennis in de algebra toe op de discrete tomografie in [13].

Naast de net genoemde theoretische resultaten over de asymptotiek van de rekentijd zijn er in 2004–2008 ook echte berekeningen gedaan door Johan Bosman, zie hoofdstukken 6 en 7 van [6], en ook zijn proefschrift [1]. Zie vooral ook zijn eigen verslag [2] in dit tijdschrift. Kort geleden zijn Johans berekeningen uitgebreid door Nicolas Mascot, een promovendus van Couveignes, in [10] en [11]. En ook door Maarten Derickx, Mark van Hoeij en Jinxiang Zeng, en Peng Tian: zie [4], [16], en [14].

Grothendiecks algebraïsche definitie van $H^j(X, \mathbb{Z}/m\mathbb{Z})$ voor $j > 1$ is niet geschikt om direct ermee te kunnen rekenen, laat staan er *snel* mee te kunnen rekenen. Standaardtechnieken uit de étale cohomologie maken het mogelijk om berekeningen te reduceren naar gevallen met $j = 1$, en uiteindelijk ook $j = 0$, waarin Grothendiecks definitie *wel* geschikt is om mee te rekenen. Maar de prijs die daarvoor wordt betaald is een toename van de dimensie van X met een factor ongeveer gelijk aan m^2 in de gevallen die in het project bestudeerd werden. Exacte berekeningen (computeralgebra) van oplossingen van stelsels veeltermvergelijkingen in zoveel variabelen kosten een rekentijd die exponentieel in m groeit (dit is een manifestatie van de 'curse of dimensionality'). Hier had Couveignes het idee om numeriek te werken, met een voldoend grote precisie zodat de gezochte f exact bepaald kon worden. Inderdaad zijn de coëfficiënten van dergelijke f rationale getallen, dus van de vorm a/b met a en b geheel en onderling ondeelbaar. Als men een a priori bovengrens kent voor $|a|$ en $|b|$, zeg M, dan is een benadering x (reëel, zeg) van a/b met $|x - a/b| < 1/(2M^2)$ voldoende om a/b uit te bepalen.

Couveignes' idee splitst dan het probleem in twee deelproblemen. Het eerste is om te laten zien dat de aantallen cijfers van tellers en noemers van de coëfficiënten van de f niet harder groeien dan een vaste macht van m. Dit is uitgevoerd door Robin de Jong en mij, gebruikmakend van Franz Merkls bovengrenzen voor Greense functies (hoofdstukken 8–11 in [6]). Het tweede deelprobleem is te laten zien dat de benaderingen met de nodige precisie uitgerekend kunnen worden in rekentijd die niet harder groeit dan een vaste macht van m. Dat is uitgevoerd door Couveignes (hoofdstukken 5, 12 en 13 van [6]). Hij behandelt daar benaderingen met complexe getallen, maar ook benaderingen met behulp van veel eindige lichamen. Peter Bruin generaliseerde die laatste methode in zijn proefschrift en ook het begrenzen van de benodigde precisie. Alles samengevoegd hebben we op die manier de 'curse of dimensionality' overwonnen, door hem te omzeilen.

Kort geleden, zie [12] en [9], is aangetoond dat, ook voor $j > 1$, $H^j(X, \mathbb{Z}/m\mathbb{Z})$ inclusief Galois-actie berekenbaar is. Maar de technieken die daar gebruikt worden, berusten op aftellen van alle mogelijkheden in aftelbare verzamelingen, dus redelijke bovengrenzen voor de rekentijd zijn nog ver te zoeken. Jinbi Jin werkt in Leiden aan directere technieken.

Tastbare gevolgen

Coëfficiënten van modulaire vormen komen veel voor in oplossingen van telproblemen. Eenvoudige telproblemen leiden tot machtsfuncties, of binomiaalcoëfficiënten, en lineaire combinaties en multiplicatieve combinaties daarvan, en de bijbehorende genererende functies zijn dan rationale functies, algebraïsche functies, of hypergeometrische functies. Het volgend niveau van moeilijkheid leidt dan tot modulaire vormen en hun coëfficiënten. Natuurlijk zijn er ook weer moeilijkere telproblemen. In ieder geval is het zo dat het hier besproken Vici-project de berekening in polynomiale tijd van coëfficiënten van modulaire vormen mogelijk heeft gemaakt, door, behalve de interne symmetrie van de modulaire vormen zelf, óók de symmetrieën in de getaltheorie te gebruiken (Galois-representaties). Voor een hele klasse van telproblemen kan (in theorie) het antwoord nu heel snel worden uitgerekend.

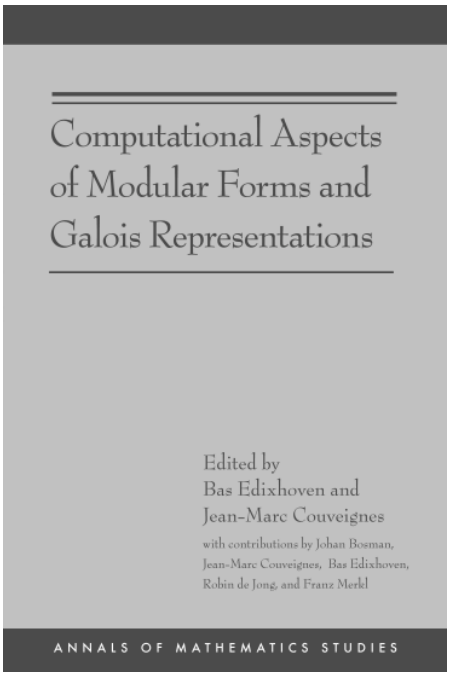
Laat ik hier twee voorbeelden geven, die beide als mijlpalen bekend staan: aantallen punten in $\mathbb{Z}^{2n}$ op gegeven afstand van de oorsprong, en Ramanujans τ-functie. Het eerste voorbeeld wordt in meer detail behandeld in [5], van waaruit ik me nu ga bezondigen aan een beetje zelfplagiaat, en het tweede in [2].

Het eerste probleem dan. Voor $d \geq 0$ en $n \geq 0$ geheel, laat $r_d(n)$ het aantal punten $(x_1, \ldots, x_d)$ in $\mathbb{Z}^d$ zijn met $x_1^2 + \cdots + x_d^2 = n$, dat wil zeggen, het aantal punten waarvan het kwadraat van de afstand tot $(0, \ldots, 0)$ gelijk is aan n.

Beroemde wiskundigen zoals Diophantus, Fermat, Legendre, Gauss, Jacobi, Eisenstein en Liouville hebben voor d gelijk aan $2, 4, 6, 8$ of 10 formules gegeven waarmee deze aantallen snel berekend kunnen worden. Daarna is zonder succes geprobeerd dit uit te breiden naar grotere even getallen. Door ons werk begrijpen we nu dat er dan geen dergelijke formules meer bestaan (zie [15]), maar dat de gezochte aantallen *toch* snel kunnen worden uitgerekend. Even snel als wanneer de formules *wel* hadden bestaan. Een algoritmische kijk op dit probleem geeft dus een bevredigender antwoord.

Het tweede probleem. We bekijken het oneindig product

$$x \prod_{n \geq 1} (1 - x^n)^{24} = \sum_{n \geq 1} \tau(n) x^n.$$



Omslag van het boek dat uit het project is voortgekomen [6]

De zo gedefinieerde functie $\tau\colon \mathbb{N} \to \mathbb{Z}$ is bekend als Ramanujans τ-functie. De bovenstaande machtreeks is een typisch voorbeeld van een niet-triviale modulaire vorm. In [6] is bewezen dat voor priemgetallen p, men $\tau(p)$ kan uitrekenen in een tijd begrensd door een vaste macht van $\log(p)$. Daarvóór was de benodigde rekentijd minstens een positief getal keer $p^{1/2}$.

Eindsituatie, aanbevelingen, dank

De belangrijkste van de in de aanvraag beoogde resultaten zijn behaald. De beoogde aanpak heeft gewerkt. Ik ben bijzonder trots op de publicatie van de resultaten in [6], in de prestigieuze boekenreeks *Annals of Mathematics Studies*, waaraan dit de eerste Nederlandse bijdrage is (zie [18]). In Leiden is er nu een sterke groep voor onderzoek en onderwijs in de algebraïsche en aritmetische meetkunde, getaltheorie en algebra. Dit laatste is niet alleen te danken aan het Vici-project, denk bijvoorbeeld ook aan het Akademiehoogleraarschap van Hendrik Lenstra, de Veni's van Robin de Jong, Lenny Taelman en Peter Bruin, de Vidi van Ronald van Luijk, en aan promovendi, studenten en bezoekers gefinancierd door de Erasmus Mundus master- en PhD-programma's 'ALGANT'. Het gaat goed met het Mathematisch Instituut in Leiden als geheel. De nabije toekomst ziet er florissant uit. Op de langere termijn is de belangrijkste vraag of de vaste staf mee kan groeien. Voor een goed onderwijsprogramma is dat zeker nodig.

Heeft het project mijn status verhoogd? Buiten Nederland niet, denk ik, maar binnen Nederland waarschijnlijk wel, en dan met name buiten de wiskunde, want binnen de wiskunde weten we zelf meestal wel wat iemand waard is. In dit themanummer van het NAW staan veel mooie zaken die bereikt zijn door succesvolle Vernieuwingsimpulskandidaten. Het is dan verleidelijk te concluderen dat het programma goed heeft gewerkt. Maar om *echt* te evalueren moet je het vergelijken met wat degenen die *niet* succesvol waren hebben bereikt, en met wat ze misschien zouden hebben bereikt als ze succesvol waren geweest.

Graag eindig ik met wat gedachten over de huidige trend in subsidieland, voor zover het de wiskunde betreft. Die trend is om steeds grotere subsidievormen op te zetten, waarbij natuurlijk steeds minder projecten gehonoreerd kunnen worden. Dit verstoort het hele ecosysteem. Maar als dat dan toch moet, dan pleit ik voor maar één project in de wiskunde in Nederland, namelijk de wiskunde zelf, als geheel. Dat heeft het bijkomende voordeel dat er geen selectie meer hoeft plaats te vinden bij NWO. De wiskundegemeenschap in Nederland is prima in staat om zelf het geld te verdelen, en daarvoor verantwoording af te leggen. De globale verdeling van de middelen van NWO over de verschillende wetenschapsgebieden kan gedaan worden in een jaarlijks overleg tussen uit de wetenschapsgebieden afgevaardigde wetenschappers (laat vooral ook de universiteitsbestuurders erbuiten, het moet om de wetenschap gaan). Mijn gevoel is dat zo'n systeem betere resultaten zal opleveren dan wat er nu is: directeuren en politici die zich laten adviseren door 'beleidswetenschappers' (dat *is* geen wetenschap). In een groter en meer direct overleg zoals ik voorstel komen de grootverbruikers van NWO-middelen directer in confrontatie met de kleinere maar meer talrijke en ook meer diverse gebruikers, waarvoor ik zelf meer sympathie heb.

Leest u vooral ook Klaas Landsmans artikel [8] in het vorige nummer van dit tijdschrift over de problematiek van de financiering van wetenschappelijk onderzoek. Ik ben het van harte met hem eens!

Ten slotte dank aan NWO voor de subsidie die me is toegekend, en aan mijn medewerkers voor hun bijdragen aan het project, en voor de fijne tijd die ze me hebben gegeven.

Referenties

1 J.G. Bosman, *Explicit Computations with Modular Galois Representations*, proefschrift, Universiteit Leiden, 2008, online onder [17].

2 J.G. Bosman, Modulaire vormen en berekeningen in Galoistheorie, *Nieuw Archief voor Wiskunde* 5/9(3) (2008), 184–187.

3 P.J. Bruin, *Modular Curves, Arakelov Theory, Algorithmic Applications*, proefschrift, Universiteit Leiden, 2010, online onder [17].

4 M. Derickx, M. van Hoeij en Jinxiang Zeng, Computing Galois representations and equations for modular curves $X_H(\ell)$, arxiv.org/abs/1312.6819.

5 S.J. Edixhoven, Snelle algoritmen in de getaltheorie, Vacantiecursus PWN/CWI, 2011, pub.math.leidenuniv.nl/~edixhovensj/talks/2011/2011_08_26_vacantiecursus/text.pdf.

6 S.J. Edixhoven en J.-M. Couveignes, eds., *Computational Aspects of Modular Forms and Galois Representations*, met bijdragen van Johan Bosman, Jean-Marc Couveignes, Bas Edixhoven, Robin de Jong en Franz Merkl, Annals of Mathematics Studies, Vol. 176, Princeton University Press, 2011, www.math.u-bordeaux1.fr/~jcouveig/book.htm; versies 1 en 2 op arxiv.org/abs/math/0605244 hebben een interessant 'personal historical account'.

7 A. Javan Peykar, *Arakelov Invariants of Belyi Curves*, proefschrift, Universiteit Leiden, 2013, online onder [17].

8 N.P. Landsman, Wetenschap en welvaart, een paradoxaal krachtenveld, *Nieuw Archief voor Wiskunde* 5/15(2) (2014), 89–95.

9 D. Madore en F. Orgogozo, Calculabilité de la cohomologie étale modulo ℓ, arxiv.org/abs/1304.5376.

10 N. Mascot, Computing modular Galois representations, arxiv.org/abs/1211.1635.

11 N. Mascot, Tables of modular Galois representations, arxiv.org/abs/1312.6418.

12 B. Poonen, D. Testa en R. van Luijk, Computing Néron-Severi groups and cycle class groups, arxiv.org/abs/1210.3720.

13 A.P. Stolk, *Discrete Tomography for Integer-Valued Functions*, proefschrift, Universiteit Leiden, 2011, online onder [17].

14 P. Tian, Computations of Galois representations associated to modular forms of level one, *Acta Arithm.* 164 (2014), 399–411.

15 I. Varma, Finding elementary formulas for theta functions associated to even sums of squares, *Indag. Math. (N.S.)* 22 (2011), 12–26, www.math.leidenuniv.nl/nl/theses/196.

16 J. Zeng en L. Yin, On the computation of coefficients of modular forms: the reduction modulo p approach, arxiv.org/abs/1211.1124.

17 openaccess.leidenuniv.nl.

18 press.princeton.edu/catalogs/series/am.html.

19 pub.math.leidenuniv.nl/~edixhovensj/FormVICIdetail_2004.pdf.

20 pub.math.leidenuniv.nl/~edixhovensj/talks/2004/vicipres2.pdf.

21 wims.math.leidenuniv.nl/wims.

22 www.msri.org/realvideo/ln/msri/2000/arithgeo/edixhoven/1/index.html