Wat heb je nu aan algebra

Wat heb je nu aan algebra

INTREEREDE

Prof.dr. Arjeh M. Cohen

Technische Universiteit Eindhoven

INTREEREDE

Uitgesproken op vrijdag 5 november 1993 aan de Technische Universiteit Eindhoven

Prof.dr. Arjeh M. Cohen

Mijnheer de Rector Magnificus,
Dames en heren,

In een Western, die niet lang geleden op TV verscheen, staat een stevige twintiger te klungelen met een lasso, die hij maar niet om de horens van een stier kan gooien. Een ervaren persoon komt hoofdschuddend aanlopen en zegt: "dat lukt je niet met al die algebra die je geleerd hebt; dat leer je alleen in de harde praktijk."[1]

Een al even duidelijke typering van algebra komt naar voren in het een aantal jaren geleden populaire liedje "Algebra"[2] met de regels:
"Wat heb ik nou aan algebra
nu ik voor de keuze sta".

De keuze betrof een liefdesprobleem.Uit beide aanhalingen spreekt enige twijfel over het nut van het abstracte vak algebra. Nu wordt de vraag naar het nut van de algebra niet alleen gesteld door leken. Ook beoefenaars van het vak wiskunde, staan wel bij deze vraag stil, getuige het volgende citaat van Kloosterman.[3]
"[...] Wat is b.v. het practische nut van de moderne getallentheorie? Toch kunnen ook hier nog wel directe toepassingen aangegeven worden. Zoo is b.v. de theorie der partities, die zich bezig houdt o.a. met de vraag naar het aantal manieren, waarop een geheel positief getal als een som van geheele positieve getallen is te schrijven, in de statistische mechanica toegepast. Zoo spelen ook de polygonaalgetallen een rol in de waarschijnlijkheidsrekening en in toepassingen daarvan. Maar belangrijker is het om te wijzen op het verband, dat tusschen de verschillende onderdeelen der wiskunde bestaat en op de invloed, die deze onderdeelen op elkaar uitoefenen. Zoo heeft b.v. Fermat het bekende vermoeden uitgesproken, dat een som van twee n-de machten van geheele positieve getallen nooit weer een n-de macht van een geheel positief getal kan zijn, als n minstens 3 is. Voor Kummer is dit probleem echter aanleiding geweest, om zijn theorie der ideale getallen op te stellen.
Deze theorie heeft weer den stoot gegeven tot moderne algebra, en deze staat weer via representatietheorie van hypercomplexe systemen in verband met problemen uit de quantenmechanica."

Kloosterman sprak deze woorden in 1947 uit bij zijn ambtsaanvaarding in Leiden. Hoewel de wiskunde grote vooruitgang heeft geboekt sinds deze rede, blijft de vraag naar het nut van de zuivere wiskunde actueel.

Vooruitgang

Om eerst eens die vooruitgang in de wiskunde toe te lichten kom ik nog even terug op het bekende vermoeden van Fermat. Iets anders geformuleerd, ziet het vermoeden er als volgt uit voor een natuurlijk getal $n > 2$: van iedere gehele oplossing x, y, z van de vergelijking

$$x^n + y^n - z^n = 0$$

is tenminste één de drie getallen x, y, z gelijk aan 0. Het linkerlid van deze verge-

lijking is een uitdrukking die men *veelterm* noemt.

Fermat's uitspraak dateert van rond 1630 en is, zonder bewijs, opgetekend in de marge van een exemplaar van de ongeveer 1750 jaar oude "Arithmetica" van Diophantus. Zij is daarna op veel verschillende plaatsen aangehaald, vaak onder de naam de *laatste stelling van Fermat*. Na de intreerede van Kloosterman werd ze bijvoorbeeld in 1968 genoemd door Oort [4] en in 1959 door U, Rector Magnificus.[5] Dit is niet verwonderlijk, want de verwikkelingen rond de oplossing vormen een prachtig voorbeeld van de stimulans die de verschillende onderdelen van de wiskunde elkaar toedienen.

De laatste jaren is er een grote activiteit op gang gekomen in de aritmetische algebraïsche meetkunde.[6] Afgelopen juni leidde dit tot een hoogtepunt: Wiles kondigde in Cambridge een bewijs van Fermat's uitspraak aan. Nu is dat al vaker gebeurd, maar dit keer maakt het bijbehorende manuscript op de experts een zeer overtuigende indruk.[7] Het is dus te verwachten dat intreeredenaars vanaf nu een alternatief moeten vinden voor de laatste stelling van Fermat als een eenvoudig te formuleren maar zeer moeilijk te bewijzen open probleem. Ik zal zo meteen een bescheiden poging daartoe wagen.

Overigens is er morgen in Utrecht een symposium over "De laatste stelling van Fermat," dat voor een algemeen publiek toegankelijk is.

Het thema toepassingen

Kloosterman sprak ook over het nut van de ene tak van de wiskunde voor de andere aan de hand van de laatste stelling van Fermat. Daar kan nu het volgende aan toegevoegd worden. Het resultaat van Wiles in de richting van Fermat's laatste stelling betreft nauwelijks meer de vergelijking

$$x^n + y^n - z^n = 0$$

maar doet uitspraken over de aritmetische algebraïsche meetkunde die van groter belang geacht worden dan het vermoeden van Fermat zelf.

Het bewijs van Wiles gebruikt elliptische krommen.[8] Bij de studie van elliptische krommen komen weer andere gebieden kijken, zoals die van de automorfe vormen. De verwijzing van Kloosterman naar het nut van het ene deelgebied van de wiskunde voor het andere heeft niets aan geldingskracht ingeboet.

Elliptische krommen zijn ook een goede illustratie voor de al vaak gehoorde uitspraak dat niet van tevoren is aan te geven voor welke maatschappelijke toepassingen de zuivere wiskunde nuttig kan zijn. Deze krommen worden gebruikt bij zeer snelle algoritmen om vast te stellen of een natuurlijk getal priem is. Een natuurlijk getal heet *priem*, als het groter is dan 1 en niet deelbaar door andere natuurlijke getallen dan 1 en zichzelf. Deze priemtest komt zeer goed van pas in de cryptografie, een vakgebied dat van direct nut is voor het bankwezen en andere instellingen die

elektronische boodschappen voor buitenstaanders geheim willen houden. Lang voordat iemand hun nut voor de cryptografie kon bevroeden, waren de elliptische krommen al ontdekt.

Dit alles neemt niet weg dat men zich in de wiskunde, en zelfs in de zuivere wiskunde (tegenwoordig vaak met de neutralere term fundamentele wiskunde aangeduid) wel degelijk meer kan richten op toepassingen. Algebra leent zich uitstekend tot het toelichten van deze stelling. Kloosterman's thema aanhoudend, zal ik niet alleen de waarde van de algebra voor de wiskunde, maar ook voor de directe toepassingen bespreken.

Dit geeft meteen de tweedeling aan die ik in de rest van mijn rede heb aangebracht. In het eerste deel wil ik het hebben over de betekenis van algebra en de betekenis van het vak voor de wiskunde. In het tweede deel van deze rede kom ik toe aan het praktische nut.

Algebra voor de wiskunde

Wat is algebra? In woordenboeken komt men al gauw drie of meer betekenissen tegen. Twee daarvan zijn voor mijn betoog relevant. De eerste wordt door Van Dale als volgt omschreven: algebra is het deel van de wiskunde dat zich bezighoudt met de betrekkingen van grootheden die voorgesteld worden door symbolen (letters).

Een voorbeeld van zo'n grootheid die voorgesteld wordt door symbolen, is een veelterm. Zo is Fermat's vergelijking voor $n = 3$ een betrekking die de veelterm $x^3 + y^3 - z^3$ gelijk nul stelt. De symbolen x, y, z uit deze veelterm zijn variabelen die elementen uit een verzameling als de gehele getallen vertegenwoordigen. Op die verzameling onderscheiden we operaties als machtsverheffen en optellen. Het voorbeeld $x^3 + y^3 - z^3$ is opgebouwd uit x, y en z met behulp van drie derde machtsverheffingen, een optelling en een aftrekking.

De algebra is allereerst een wiskundige manier van redeneren door middel van het manipuleren van uitdrukkingen met formele symbolen. Als we bijvoorbeeld, de haakjes uitwerken in de veelterm

$$(9x^4)^3 + (3x - 9x^4)^3 - (9x^3 - 1)^3,$$

dan zien we dat de uitdrukking 1 oplevert. We concluderen dan dat deze veelterm gelijk is aan 1. De bewerkingen die schuil gaan achter het 'haakjes uitwerken,' stoelen op wetten die gelden voor de operaties 'vermenigvuldiging en optelling van veeltermen.' Het zal duidelijk zijn dat de manipulatieregels in het algemeen sterk van de context afhangen.

Zoals ik heb aangegeven, zijn optelling en vermenigvuldiging van getallen voorbeelden van algebraïsche operaties. De onderliggende verzameling zou die van de gehele getallen, van de natuurlijke getallen, of van de reële getallen kunnen zijn. Het maakt verschil welke onderliggende verzameling je kiest. Bijvoorbeeld, in de natuurlijke getallen heeft de vergelijking

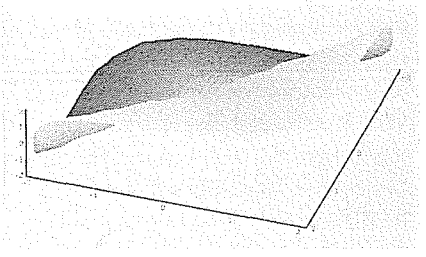
$$x + 5 = 3$$

geen oplossing: je kunt 5 niet van 3 aftrekken. In de gehele getallen kun je wel aftrekken; $x = -2$ is een oplossing van de vergelijking $x + 5 = 3$. In de reële getallen kun je niet alleen aftrekken, maar ook delen door een getal ongelijk 0.

De vergelijkingen waarvan volgens Fermat voor n=3 geen gehele oplossingen met waarden ongelijk nul te vinden zijn, hebben wel oplossingen als de variabelen uit de reële getallen afkomstig zijn: voor elke x en y is er de oplossing met z -waarde

$$z = \sqrt[3]{x^3 + y^3}.$$

De keuze van de onderliggende verzameling is dus van groot belang voor het al of niet bestaan van oplossingen van vergelijkingen. Deze verschillende onderliggende verzamelingen komen tot uitdrukking in de soort operaties die beschikbaar zijn en in de wetten waaraan die operaties voldoen. Voor de natuurlijke getallen, de gehele getallen en de reële getallen gelden achtereenvolgens steeds meer wetten die van belang zijn voor het herschrijven en vereenvoudigen van vergelijkingen en, uiteindelijk, voor het vinden van oplossingen.



Figuur 1. De reële nulpunten van $x^3 + y^3 - z^3$.

Modulo rekenen

Ik wil nu een voorbeeld behandelen van optellen, aftrekken, vermenigvuldigen en machtsverheffen op een iets andere verzameling dan die van de gehele of de reële getallen. De verzameling waarop we onze operaties laten werken bestaat uit de getallen 0 tot en met 23. Deze verzameling zal ik aanduiden als de getallen modulo 24. Wanneer we een willekeurig geheel getal tegenkomen, bijvoorbeeld 80, dan zal ik verstaan onder "80 modulo 24" het unieke getal tussen 0 en 23 (0 en 23 meegerekend) dat de rest is bij deling van dat getal door 24. In ons voorbeeld levert deling van 80 door 24 een rest ter grootte 8, dus 80 modulo 24 is 8.

Optellen van getallen modulo 24 geschiedt zoals gebruikelijk voor gehele getallen, met dien verstande dat het resultaat modulo 24 genomen moet worden. Een interpretatie hiervan in de alledaagse praktijk gaat als volgt: als het nu 16:00 uur is, dan zal het over 80 uur (96 modulo 24) :00 uur, dat wil zeggen 00:00 uur zijn. Vandaar, dat modulo 24 of modulo 12 rekenen ook wel klokrekenen genoemd wordt.

Aldus kunnen we getallen modulo 24 optellen. Beperken we ons tot de gehele getallen modulo 24, dan kunnen we ze ook vermenigvuldigen zoals we dat bij gehele getallen gewend zijn. Aftrekken is evenzeer mogelijk, maar delen niet.[9]

Vanzelfsprekend kunnen we 24 ook door een ander getal (de modulus) vervangen. De modulus van de kilometerteller van uw auto is waarschijnlijk 100.000 of 1.000.000,

de modulus van de optelling in de centrale besturingseenheid van computers waarschijnlijk een macht van 2 (vaak 2^{32}).

Deze 'modulo'-structuren zijn grondig onderzocht, maar de studie ervan is allesbehalve afgerond. Ik kom daar dadelijk op terug.

De tweede betekenis van algebra

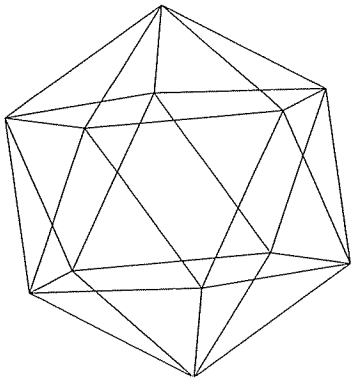
Maar eerst wil ik de tweede betekenis van algebra bespreken.

Zoals al opgemerkt, komen de manipulatieregels voor symbolische uitdrukkingen vaak af van wetten die voor bepaalde operaties gelden. Denk hierbij aan haakjes uitwerken (distributiviteit) of het verwisselen van volgorde (commutativiteit). De wetten waaraan operaties als optellen, vermenigvuldigen, aftrekken en delen in verschillende contexten voldoen, worden als uitgangspunt genomen voor geaxiomatiseerde theorieën. Een natuurlijk vervolg is de studie en classificatie van systemen die aan dergelijke axiomastelsels voldoen. Vanzelfsprekend is de algebraïcus niet zomaar in axiomatische systemen geïnteresseerd, maar in stelsels die in de praktijk vaak voorkomen.

Groepen

Een typisch voorbeeld van zo'n axiomatisch systeem is dat van een groep. Daarvan zijn de operaties een associatieve vermenigvuldiging, een element dat zich als de 1 onder vermenigvuldiging gedraagt, en deling.[10] Voorbeelden van groepen worden gevonden in de symmetrieën van meetkundige objecten.

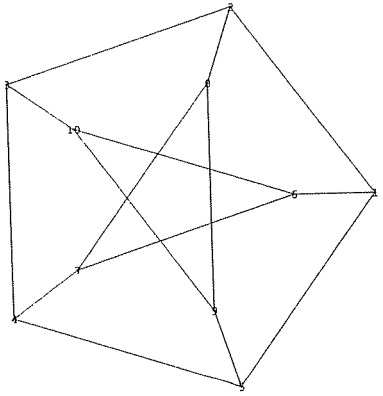
Mooie meetkundige exemplaren in de Euclidische ruimte zijn de vijf Platonische lichamen: de tetraëder, de octaëder, de kubus, de dodecaëder en de icosaëder. De bijbehorende groepen bestaan uit alle draaiingen en spiegelingen van de ruimte die het lichaam in zichzelf overvoeren. Deze groepen zijn eindig: de onderliggende verzameling bestaat uit eindig veel elementen, voor de icosaëder zijn dit er bijvoorbeeld 120. De studie van de eindige groepen is een algebraïsch onderdeel van de discrete wiskunde, het vakgebied waarin ik ben benoemd.



Figuur 2. De icosaëder

Groepentheorie wordt gebruikt om de symmetrieën van een regelmatige figuur algebraïsch te beschrijven. De abstracte groep, d.w.z. de structuur van de symmetrie los gezien van de concrete figuur, manifesteert zich vervolgens niet alleen als groep van symmetrieën van de oorspronkelijke figuur, maar ook van ver-

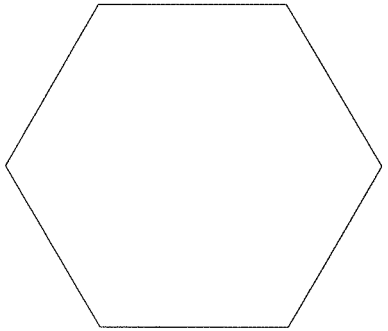
schillende andere objecten, op verschillende plaatsen in de wiskunde. De groep van de icosaëder bijvoorbeeld, kan ook gezien worden als groep van alle permutaties van een verzameling van 5 elementen, of als groep van alle symmetrieën van de in figuur 3 afgebeelde graaf. Het begrip 'groep' legt dus verrassende verbanden tussen verschillende meetkundige objecten. Deze observatie is in zekere zin terug te voeren tot de illustere intreerede die Klein hield in het jaar 1872 aan de Universiteit van Erlangen. Daarin unificeerde hij de Euclidische, de projectieve, en de hyperbolische meetkunde door ze vanuit de symmetriegroepen te beschouwen. Dit gezichtspunt, dat bekend is geworden als het Erlanger Program, heeft grote invloed gehad op de meetkunde in de er op volgende jaren.



Figuur 3. De Petersengraaf

Ik geef als voorbeeld nog een oneindige serie groepen. Voor elk getal p bestaat er een eenvoudige groep, de *cyclische groep* genaamd, die precies p elementen heeft. Deze groep heeft een element, dat *voortbrenger* heet, met de eigenschap dat alle andere elementen te verkrijgen zijn door de voortbrenger herhaald met zichzelf te vermenigvuldigen. Deze groep is voor te stellen als de groep van draaiingen van een regelmatige p-hoek in het vlak. Als voortbrenger kan men dan de draaiing om de kleinst mogelijke hoek kiezen.

Net zoals getallen te ontbinden zijn in priemfactoren, zo zijn eindige groepen op te delen in 'priemfactoren'. Deze groepsanaloga van priemgetallen heten *enkelvoudige groepen.*



Figuur 4. De regelmatige 6-hoek

Eén van de grote wiskundige prestaties van deze eeuw is dat deze bouwstenen van de eindige groepen zijn geclassificeerd: alle enkelvoudige groepen zijn bekend. De lijst is te ingewikkeld om hier te beschrijven. Een opmerkelijk feit is dat, op een 26-tal groepen na, elke enkelvoudige groep in een oneindige serie thuis hoort. Een van die oneindige series wordt gevormd door de cyclische groepen waarvan de onderliggende verzameling een priemgrootte heeft. De 26 'sporadische' groepen hebben veel weg van een periodiek systeem

uit de scheikunde, of zo U wilt, van een stel elementaire deeltjes uit de natuurkunde, maar dan voor de groepentheorie.

De grootste sporadische groep heet het Monster.[11] De onderliggende verzameling bestaat uit ongeveer

$$0{,}8 \times 10^{54}$$

elementen, dus meer dan het aantal elementaire deeltjes waaruit de aarde bestaat. Het zal duidelijk zijn dat er het een en ander aan techniek en inzicht nodig is om zo'n groot object te beschrijven, laat staan te bestuderen.

De betrekkingen tussen groepen en meetkundige objecten vormen een gebied dat mij zeer aan het hart gaat, en waarin ik een groot deel van mijn werk in de discrete wiskunde hoop te kunnen uitvoeren.

Hier eindigt mijn bespreking van groepen als voorbeeld van een axiomatisch systeem.

Algebra binnen de wiskunde

Laat ik terugkeren van de groepen naar de algebra in zijn algemeenheid. Binnen de wiskunde vormt de algebra een groot en centraal onderdeel dat overlappingen vertoont met vele deelgebieden, zoals de discrete wiskunde, de analyse, de statistiek, de meetkunde en de topologie.

Dit patroon komt al naar voren in het middelbaar onderwijs, waar meetkundige problemen als "Bepaal de snijpunten van een gegeven rechte en een gegeven kegelsnede" worden vertaald in algebra door het opstellen van een stel vergelijkingen.

De algebra speelt zelfs een rol bij differentiëren of primitiveren, begrippen die uit de 'continue' analyse komen. De bijbehorende handelingen worden beschreven door een stel mechanisch toepasbare regels. Een aantal ervan wordt in het middelbaar en hoger onderwijs behandeld. Deze operaties zijn volledig algebraïsch.[12]

Algebra levert de taal en de machinerie om vele wiskundige bewerkingen te beschrijven. Het is vaak het communicatiemiddel tussen deelgebieden en tussen personen, het middel om karakteristieke eigenschappen vast te leggen en om noodzakelijke berekeningen uit te voeren.

Algebra is echter niet alleen notatie en herschrijfwerk. Het behelst ook diepgaand onderzoek in structuren als de eindige groepen, waar het tot de besproken classificatie leidde. De bijdragen van de algebra aan diepe resultaten over elliptische krommen zijn niet strikt te scheiden van die van de andere gebieden, en het zou zinloos zijn die scheidslijn te willen trekken. Dergelijke resultaten komen tot stand dankzij een mengeling van gebieden, waarop de algebra wellicht als bindend middel werkt. Hoewel de taal en het formalisme per definitie tot de algebra gerekend kunnen worden, kan de 'visie' uit een heel andere wereld komen (bijvoorbeeld uit de topologie, de meetkunde, of de analyse).

Door de aard van de algebra, zijnde bewerkingen op formele uitdrukkingen, ligt het

voor de hand dat hij van nut is bij de formalisatie van de wiskunde en, in het vervolg hiervan, de verificatie van wiskundige uitspraken en bewijzen. Immers, niet alleen alle uitspraken, maar ook alle afleidingsregels die wiskundigen voor hun redeneringen gebruiken, zijn zó eenduidig op te schrijven, dat ze machinaal leesbaar en verwerkbaar zijn. Deze naar de logica neigende aspecten van de algebra hebben de laatste jaren een grote ontwikkeling doorgemaakt.[13] Ik zal hier echter niet verder op ingaan en de bespreking van de betekenis van algebra afsluiten met de beloofde simpele vraag.

Het vermoeden van Artin

De vraag staat bekend als het vermoeden van Artin. Om de vraag te appreciëren nemen we een priemgetal p in gedachten en gaan we na welke getallen ongelijk 0 een macht van 2 modulo p zijn. Voor $p = 5$ zijn de achtereenvolgende machten van 2, te beginnen bij de nulde macht: 1,2, 4 en 3, want dat is 8 modulo 5. De daarop volgende macht is weer 1, waarna de rij zich blijft herhalen. Onderhand is elk getal modulo 5 ongelijk 0 als macht van 2 modulo 5 geschreven.

Dit lukt niet als we $p = 7$ nemen, want 3 is geen macht van 2 modulo 7. Immers, de machten van 2 zijn achtereenvolgens 1, 2, 4 en 1 (want dat is 8 modulo 7). Daarna blijft de rij zich weer herhalen, dus 3 komt nooit aan bod.

Laten we kortweg een getal *voortbrenger modulo p* noemen als elk natuurlijk getal ongelijk 0 modulo p een macht van dat getal modulo p is. Aldus is 2 wel een voortbrenger modulo 5, maar géén voortbrenger modulo 7. De terminologie is zo gekozen dat 2 precies dan een voortbrenger modulo p is als de vermenigvuldigingsgroep van de elementen ongelijk 0 modulo p een cyclische groep is met 2 als voortbrenger.

Enig rekenwerk voor kleine moduli p leert dat 2 een voortbrenger modulo p is voor

$$p = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, \ldots$$

Zo lijken we oneindig door te kunnen gaan. En dat is nu precies de vraag: bewijs dat deze rij niet stopt, dus dat er oneindig veel priemgetallen p zijn zo dat 2 een voortbrenger modulo p is.

Deze vraag kan teruggevoerd worden tot Gauss, die rond 1800 op dit gebied actief was. Maar ze is vernoemd naar Artin, die enige tientallen jaren geleden een kwantitatieve versie ervan presenteerde.[14]
De uitspraak dat er oneindig veel priemgetallen p zijn zodat 2 een voortbrenger modulo p is, vormt het voorbeeld dat ik nog wilde geven van een eenvoudig te formuleren vermoeden dat uiterst moeilijk te bewijzen is.

Ook hier lijkt de oplossing trouwens niet ver weg. In 1986 heeft Heath-Brown[15] bewezen dat tenminste één van de drie getallen 2, 3 of 5 een voortbrenger modulo p is voor oneindig veel priemgetallen p. Het zou een grote verrassing zijn, als er een eenvoudig bewijs voor zo'n eenvoudig

vermoeden zou verschijnen. Ik acht de kans erop niet groot.

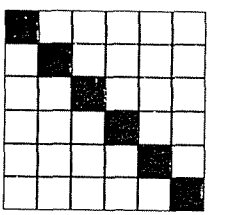
Het praktische nut van algebra

Dan kom ik nu toe aan het tweede deel van mijn rede, waarin ik het praktische nut van algebra bespreken zal. Het karakter van de algebra brengt met zich mee dat praktische toepassingen van de algebra vaak tot stand komen via andere deelgebieden van de wiskunde. Ik stipte zo'n toepassing al aan toen ik het over cryptografie had, waar priemtesten gebruikt worden. Ik wil U graag nog een praktische discreet-wiskundige toepassing van deze soort schetsen.[16]

Een radarprobleem

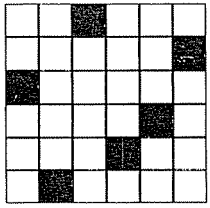
Bij gebruik van radar wordt een signaal uitgezonden en, na terugkaatsing op het te lokaliseren object, laten we zeggen een passerend vliegtuig, weer opgevangen. Het tijdverschil tussen opvang en verzending zegt iets over de plaats van het object. De verschuiving in frequentie, veroorzaakt door het Doppler-effect, zegt iets over de snelheid waarmee het zich voortbeweegt. Door niet een signaal, maar een aantal in frequentie en tijd verschillende signalen uit te zenden en op te vangen, kan een grotere precisie bereikt worden. Dus, in plaats van één signaalstoot met een vaste frequentie, zenden we een pakket van n in frequentie verschillende signalen op n verschillende opeenvolgende tijdsintervallen uit. We hebben nog de keuze welke frequentie eerst, en welke daarna wordt uitgezonden, enzovoort. Zo komen we tot een uitzendpatroon dat 2-dimensionaal is weer te geven: de uitgezonden signalen corresponderen met zwarte hokjes op een n x n vierkant; horizontaal is de tijd uitgezet, verticaal de frequentie. Afstand en snelheid van het passerende vliegtuig zorgen voor een verplaatsing van het ontvangen patroon in het tijd, frequentie vlak. Bij juist gekozen schaling, kunnen we van een uniforme verschuiving in het vlak uitgaan. Om nu de afstand en snelheid nauwkeuriger dan met één enkel signaal te bepalen, moeten we de verschuiving van het binnengekomen patroon ten opzichte van het uitgezonden patroon zo goed mogelijk vaststellen. Hiertoe is het van belang dat de identificatie van het binnengekomen patroon met een verschuiving van het oorspronkelijke patroon zo zuiver mogelijk is. Dit kan bereikt worden door het uitzendpatroon zo te kiezen dat elke verschuiving tot een groot onderscheid met het oorspronkelijke patroon leidt.

Als we het volgende patroon kiezen



waar $n = 6$ en de tonen bij elk volgend interval een stapje afnemen in frequentie, dan is een diagonale verschuiving richting zuid-oost slecht te onderscheiden van het oorspronkelijke patroon. Dit speelt natuurlijk nog sterker voor diagonaalpatronen waarin n groter is.
Een zeer goede kandidaat bij grootte $n = 6$,

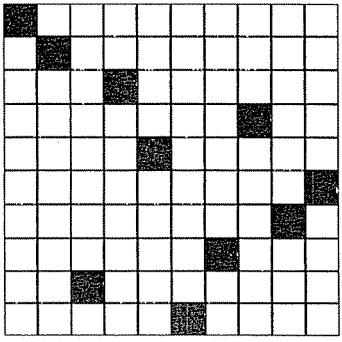
waar elke verschuiving in het vlak weinig overeenkomst vertoont met het oorspronkelijke patroon, is hieronder weergegeven.



Nu heeft elke verschuiving ten hoogste één hokje gemeen met het oorspronkelijke uitzendpatroon. Beter kunnen we ons niet wensen.[17]

Met behulp van de algebra kunnen we voor elke n van de vorm $p-1$, waar p een priemgetal is, zo'n patroon construeren.[18] Om die constructie uit te voeren, moeten we een voortbrenger modulo p kiezen. Voor het gemak kies ik p zó dat 2 een voortbrenger modulo p is. Het patroon bestaat dan precies uit die paren van tijd i en frequentie j waarvoor geldt dat j gelijk is aan de $(i-1)$ste macht van 2 modulo p.

Voor $p = 11$ levert dit bijvoorbeeld het onderstaande uitzendpatroon.[19]



Het bestaan van een voortbrenger modulo p is essentieel om via deze constructie een uitzendpatroon met ten hoogste één hokje overlap na verschuiving te verkrijgen.

Dit typeert de rol die de algebra vaker speelt. Het helpt ons met groot gemak een eind op weg. Maar we komen er niet mee tot een volledige oplossing. In dit geval missen we nog constructies voor grootten van het uitzendpatroon die niet van de vorm p - 1 met p een priemgetal zijn. Andere discreet-wiskundige technieken zullen dan te hulp moeten komen. Maar die zal ik hier niet verder bespreken.

Er zit nog een interpretatie van het vermoeden van Artin in dit probleem die ik ter afsluiting van de radarsignalen graag nog even vermeld. Als Artin's vermoeden waar is, dan zal er altijd een geschikt uitzendpatroon met 2 als voortbrenger geconstrueerd kunnen worden dat voldoende groot is. Dankzij het resultaat van Heath-Brown voldoet de constructie zeker aan die eis als we naast 2 ook nog 3 en 5 als mogelijke voortbrengers nemen.

Modelvorming

Tot zover een toepassing van de algebra in de discrete wiskunde, die op haar beurt weer van direct nut is voor praktische toepassingen.

In het algemeen zien we bij toegepast wiskundig werk vaak het volgende patroon. Vanuit de praktijk komt een wiskundig model naar voren. Daarnet was dat een discreet-wiskundig model van uit-

zendpatronen. Binnen dit model is dan een probleem geformuleerd. Dat kan de vraag naar een configuratie zijn die aan bepaalde eisen voldoet. In het radarvoorbeeld is het de vraag naar een uitzendpatroon met minimale overlap bij verschuivingen.

Het woord 'probleem' staat hier eigenlijk voor een hele klasse van problemen, voor elke waarde van de parameters in het model één. Bij de uitzendpatronen bijvoorbeeld is er één parameter, namelijk de grootte n van het uitzendpatroon. Ook het vermoeden van Fermat kent zo'n parameter, daar is het de exponent n.

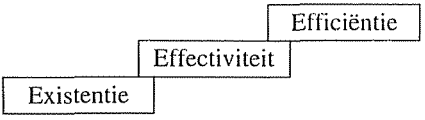
De gevonden constructie voor uitzendpatronen in deze optiek samenvattend, hebben we een mechanische methode, ofwel *algoritme*, om het probleem op te lossen mits de grootte $p-1$ bedraagt met p een priemgetal. Op deze algoritmische kant wil ik wat nader ingaan.

Implementeerbaarheid

Algebra, zo hoorde U, betreft het manipuleren van uitdrukkingen met formele symbolen, die operaties op verzamelingen voorstellen. Daar waar de elementen van zo'n verzameling en de bijbehorende operaties goed op een computer zijn weer te geven, staat ons weinig in de weg om de algebra te automatiseren. Het formele aspect van de algebra vergemakkelijkt dit. In de zestiger en ten dele zeventiger jaren waren computergeheugens nog niet groot genoeg om grote symbolische uitdrukkingen comfortabel te bewerken. Nu is die situatie sterk verbeterd.

Dientengevolge is de afgelopen jaren veel aandacht besteed aan het bruikbaar maken van algebraïsche operaties op computer. Dit vraagt om een benadering van de algebra, waarbij men zich niet slechts om existentie bekommert maar ook om constructie, en vervolgens om snelheid van constructie. Zo zijn er drie fasen die een algoritme in wording op weg van theorie naar praktijk doorloopt.

Het is niet altijd mogelijk om een efficiënte oplossing te vinden. Daarom luidt een wat realistischer streven: zo ver mogelijk te komen op de trap met de drie treden Existentie, Effectiviteit en Efficiëntie, die ik voor het gemak de E-trap zal noemen:



Figuur 5. De E-trap

Ter illustratie passen we deze driedeling toe op de stevige twintiger uit het begin van mijn rede, wiens probleem bestond uit het werpen van een lasso om de horens van een stier. Eerst is de existentie van een oplossing aan de orde: de werper stelt zich zo op dat het touw de horens haalt en maakt de lus groot genoeg. Aldus wordt aan de noodzakelijke en liefst voldoende voorwaarden voor een geslaagde worp voldaan. In de wiskunde is het bestaan van gehele oplossingen van de vergelijking

$$x^3 + y^3 - z^3 = 30$$

een onopgelost probleem, voor de oplos-

sing waarvan geen algoritme bekend is.[20]

In de effectieve fase wil de lassowerper een methode vinden die de lasso op de gewenste plaats brengt. Onze twintiger is daar duidelijk blijven steken.

In de wiskunde is het vinden van reële oplossingen van een stel veeltermvergelijkingen met gehele coëfficiënten een effectief, maar lang niet altijd praktisch oplosbaar probleem.[21]

Mocht de lassowerper ooit aan de efficiëntie van zijn werpprobleem toekomen, dan zal hij zich bekwamen in het uitvoeren van een geslaagde worp zonder zelf om te vallen of anderszins teveel energie te verliezen.

Als een wiskundig probleem algoritmisch voldoende efficiënt is, kan het in een bruikbaar computerprogramma uitmonden. Via de E-trap zien we hoe de abstracte algebra, veelal opererend op de existentie tree, via de efficiëntie tree in verbinding gebracht kan worden met de praktische kant van de zaak. De aard van het werk in de drie fasen verschilt. De existentiefase is abstract algebraïsch van karakter. Is er eenmaal een efficiënte oplossing, dan zal het implementeren ervan nog een apart stuk vakmanschap vereisen.

De ingenieur

Zo kom ik tot een interpretatie van wat je nù aan algebra hebt, wellicht meer dan ooit te voren. Daarbij richt ik me voornamelijk tot de ingenieur die wiskunde toepast.

Zoals gezegd, komen de toepassingen vanuit de praktijk de wiskunde binnen via een wiskundig model. Dit model kan bestaan uit een stel veeltermvergelijkingen, een stel differentiaalvergelijkingen, of een andere wiskundige structuur, zoals de uitzendpatronen van radarsignalen waar ik eerder over sprak.

Bij de oplossing van in dat model geformuleerde problemen zou de algebra een bijdrage kunnen leveren op een of meer van de volgende drie manieren, die ik kort heb samengevat in een 'alternatieve' ABC-formule:

A. De A stelt 'Algoritmische plaatsbepaling' voor. Daarbij gaat de ingenieur na hoe het geparametriseerde probleem op de E-trap gesitueerd kan worden. Zo wordt vastgesteld of het probleem überhaupt wel een oplossing heeft, en zo ja of er een effectieve, dan wel een efficiënte oplossing is. Zonodig wordt het model bijgesteld om hoger op de E-trap uit te komen. Hier is sprake van een afweging van belangen: aan de ene kant moet het wiskundige probleem efficiënt oplosbaar zijn, aan de andere kant moet het wiskundig model de werkelijkheid voldoende nauwkeurig weergeven. Voor efficiënte oplosbaarheid is in de regel eenvoud van het model vereist, een vereiste dat op gespannen voet staat met de wens van nauwkeurige weergave.

B. De B staat voor 'Bouwstenen'. Ik bedoel hiermee de mogelijke constructies die de algebra kan leveren voor een oplossing. Denkt U aan de elliptische krommen voor een priemtest bij cryptografie, of

aan de voortbrengers modulo p voor radarsignalen.

C. De C staat voor 'Computerondersteund algebraïsch werk' of kortweg *computeralgebra*. Dit is het gebruik van de bestaande, op de computer geïmplementeerde algoritmen. Zij geven ruimschoots de gelegenheid tot het uitvoeren van allerlei algebraïsche standaardbewerkingen, variërend van het oplossen van kleine stelsels veeltermvergelijkingen en het ontwikkelen van Taylorreeksen, tot het vinden van primitieven bij integratie. Daarin zit veel algebraïsche kennis, waarvan een deel pas tot stand kwam nadat de grote symbolische rekencapaciteit van de huidige computers duidelijk werd.

De onderdelen A, B en C hoeven niet noodzakelijk in de gepresenteerde volgorde afgewerkt te worden. Zij geven alleen categorieën aan waarin algebra van betekenis kan zijn voor toepassingen.

Toegepaste wiskunde

Maar, vraagt U zich wellicht af, hoe zit dat met de belangrijke rol en de gevestigde reputatie van vakken als de analyse en de numerieke wiskunde? Zijn die nu volledig aan de kant gezet door algebraïsche manipulatie? Integendeel, de computeralgebra zal in toepassingen goed kunnen samenwerken met deze vakken, en zal ze zeker niet vervangen!

Bijvoorbeeld voor numeriek-wiskundige toepassingen kan programmatuur aangemaakt worden in dezelfde computeromgeving als waar de algebraïsche formules bewerkt worden. In die omgeving kunnen foutenschattingen voor numerieke berekeningen met behulp van computeralgebra bepaald worden. De integratie van numerieke wiskunde en algebra in een computerwerkomgeving is nabij.

De algebraïsche speurtocht naar oplossingen van een stel differentiaalvergelijkingen zal vaak blijven steken in de existentiefase van de E-trap. Alle gebruikelijke transformaties en substituties, daarentegen, al het herschrijfwerk tot een normaalvorm en de test of er toevallig een algebraïsche oplossing is, worden door computeralgebra tot een stel eenvoudige handelingen gereduceerd.

Het gebruik van algebra

Moeten ingenieurs vanwege de ABC-formule de hele algebra kennen? Het antwoord luidt: nee, maar ze moeten er wel voldoende vertrouwd mee zijn om de goede weg te vinden. Zoals de autorijder het functioneren van de motor nauwelijks hoeft te kennen om te kunnen rijden, zo hoeft de gebruiker van veel wiskundige algoritmen alleen de invoer en de uitvoer wiskundig te herkennen.

Het doet er voor gebruikers niet toe dat factorisatie van een getal in priemgetallen elliptische krommen gebruikt. Het is voor hen van belang te kunnen verifiëren dat het resultaat correct is. In het geval van factorisatie betekent dit dat aan de gebruiker (op aanvraag) een bewijs gepresenteerd wordt dat de factoren priem zijn en

dat het produkt van de priemfactoren weer het ingevoerde getal geeft.

Evenzo voor het primitiveren. Het doet er niet toe dat er zeer geavanceerde algoritmen gebruikt worden om een gesloten vorm voor de integraal van een uitdrukking te vinden: de gebruiker kan zelf eenvoudig nagaan dat differentiëren van het eindresultaat weer de ingevoerde functie oplevert.

De parallel van de algoritmische algebra met de auto kan doorgetrokken worden. Zoals er automonteurs zijn die weten wat er onder de motorkap te vinden is, zo zullen er ook wiskundigen en ingenieurs zijn die de programma's kennen en kunnen bijstellen. Zoals er automakers zijn, zo zullen er computergeschoolde algebraïci zijn om nieuwe algoritmische verworvenheden van de algebra te implementeren.

De computer-werkomgeving

Veel van wat nuttig is voor ingenieurs die algebra toepassen is ook van betekenis voor wiskundigen. Voor de wiskundige is de algebra een leefwereld op zich, waar eindige groepen als het Monster wonen, en waar meer dan voldoende uitdaging en bevrediging gevonden kan worden om de echte wereld te vergeten. Ook in deze wereld dringt de computer door in zijn functie van leverancier van rekenfaciliteit, van hulp bij experimenten en bij visualisatie.

In de toekomst zal hij waarschijnlijk ook behulpzaam zijn als bewijsverificator, als hulp bij het vinden van afleidingen, en als hulp bij de specificatie van wiskundige problemen. Er is sprake van een bescheiden begin in deze richting, dat mijns inziens kan leiden tot inspirerende computer-werkomgevingen voor wiskundigen en ingenieurs. Ik hoop ook aan deze ontwikkelingen bij te kunnen dragen.

Onderwijs

De laatste jaren is de waardering voor het bedrijven van wiskunde om de wiskunde onder druk komen staan vanwege de grote nadruk op maatschappelijke toepasbaarheid.

Door bezuinigingen en externe redenen (zoals het enorme aanbod uit oostelijke landen) is er voor een betrekkelijk groot aantal zeer goede gepromoveerden geen geschikte academische baan te vinden.

Gegeven deze moeilijkheid, dienen vormgevers van het universitaire wiskunde-onderwijs er voor te zorgen dat de aangeboden wiskunde goed aansluit bij de toepassingen. In de onderzoeksschool EIDMA voor de discrete wiskunde en haar toepassingen, die we dit jaar hebben opgericht, zullen we ons slechts ten dele op de academische wereld als baangever richten. Het vertrouwen dat we hebben in een goede aansluiting bij de niet-universitaire arbeidsmarkt voor wiskundigen ligt verankerd in de toepassingsmogelijkheden voor de discrete wiskunde.

Conclusie

Concluderend wil ik twee dingen stellen; en wel

- in de eerste plaats dat het abstracte vak algebra onverminderd tot de verbeelding van zijn beoefenaars blijft spreken,

- en in de tweede plaats dat, via de E-trap van abstracte existentie naar computerimplementatie, er betere verbindingen tussen algebra en zijn toepassingen komen dan er ooit geweest zijn.

In Van Dale komt onder het kopje 'algebra' de uitdrukking 'dat is algebra voor mij' voor. Ik hoop dat U na de rede deze woorden niet in de mond zult nemen, want volgens Van Dale betekenen ze 'daar begrijp ik niets van'.

Dank

Ik wil deze rede besluiten met enkele woorden van dank.

Hooggeleerde Rector Magnificus, beste Jack van Lint. Ik waardeer het ten zeerste dat U, tezamen met de overige leden van het College van Bestuur, mij aan deze Universiteit hebt willen benoemen.
Tezamen met De Bruijn en Seidel hebt U het gezicht van de discrete wiskunde in Eindhoven, in Nederland, en zelfs in de wereld op erg oorspronkelijke en kwalitatief indrukwekkende wijze bepaald. Daardoor is de vakgroep Discrete Wiskunde, waar ik nu werk, een zeer levendige en gerenommeerde geworden. Ik beschouw het als een voorrecht er te mogen werken en een uitdaging het grote voorbeeld dat U, De Bruijn en Seidel alle drie hebt gegeven, na te volgen. Daarbij prijs ik me te meer gelukkig alle drie regelmatig op de werkvloer aan te treffen.

Ik ben ook zeer vele anderen aan deze Universiteit dankbaar voor hun open houding en vriendelijke ondersteuning bij het werk. Dit geldt in het bijzonder voor de leden van de vakgroep Discrete Wiskunde, de studenten incluis. Het is me een grote vreugde dat zij zo'n plezierige werkomgeving vormen.

Kort geleden heb ik al de gelegenheid gehad om het instituut CWI, en de hoogleraren Baayen, Buekenhout, Hazewinkel en Springer te bedanken voor hun belangrijke rol in mijn leven. Ik wil daaraan toevoegen dat er aan het CWI veel mensen verbonden zijn met wie ik nu al jarenlang met veel genoegen samenwerk. Gelukkig kan deze samenwerking, mede via het onderzoeksinstituut RIACA, voortgezet worden.

Nu ik stil sta bij dit bijzonder moment van mijn leven, wil ik mijn ouders laten weten dat hun aanwezigheid deze intreerede tot een zeer intense belevenis maakt.

Speciale dank gaat naar Christel, die er bijna altijd is voor onze kinderen als geen van beide ouders aanwezig is. Als 'derde ouder' heb je de afgelopen twaalf jaren het gezin perfect aangevuld.

Dan wil ik nog dank betuigen aan mijn gezin, al zou ik niet weten hoe. De stabiliserende en vitaliserende werking die van jullie, Peggy, Eleonore en Max, uitgaat is te goed voor woorden. Ik kan alleen maar wensen dat het nog lang zo gelukkig blijven mag.

Geachte collegae, studenten, vrienden, kennissen, familie en andere toehoorders, ik dank U dat U deze gelegenheid met Uw aanwezigheid hebt willen vereren, en dank U voor Uw aandacht.

Ik heb gezegd.

Aantekeningen

[1] Maandag 19 juli 1993, BRTN 1, 20:40 ,
" Gunsmoke: The last Apache," Deel 1.

[2] Het lied is gezongen door Loeki Knol, op tekst van Rob Chrispijn,
muziek van Leo Unger (oorsponkelijke tekst: "It isn't really like they say"),
Polydor 2104604.

[3] H.D. Kloosterman, "Waarde en waardeering der wiskunde,"
rede uitgesproken bij de aanvaarding van het hoogleeraarsambt aan de
Rijksuniversiteit Leiden op 2 mei 1947,
P. Noordhoff N.V., 1947, Groningen-Batavia.

[4] F. Oort, "Vlijt, Visie, Verificatie, aspecten van wiskundebeoefening,"
rede uitgesproken bij de aanvaarding van het ambt van gewoon hoogleraar in de
zuivere wiskunde aan de Universiteit van Amsterdam op 27 mei 1968,
Wolters Noordhoff, Groningen, 1968.

[5] J.H. van Lint, "Een blik in de getaltheorie,"
rede uitgesproken bij de aanvaarding van het ambt van gewoon hoogleraar in de
wiskunde aan de Technische Hogeschool te Eindhoven op vrijdag 20 november 1959,
Tjeenk Willink, Zwolle, 1959.

[6] Tien jaar geleden bewees Faltings [G. Faltings, Endlichkeitssätze für abelsche
Varietäten über Zahlkörpern, Inventiones Math. 73 (1983) 349-366] een zeer
algemeen resultaat in dit gebied waaruit volgt dat er bij elke keuze van n groter dan
of gelijk aan 3, hoogstens eindig veel essentieel verschillende oplossingen voor
Fermat's vergelijking zijn.

[7] Een bericht hierover verscheen in NRC van 1 juli 1993. Zie K.A. Ribet, "Wiles proves
Taniyama's conjecture; "Fermat's last theorem follows,"
Notices of the Amer. Math. Soc., 40 (1993), 575, 576.

[8] Deze meetkundige objecten worden beschreven door veeltermvergelijkingen in twee
onbekenden van de graad 3, net zo als kegelsneden worden beschreven door
veeltermvergelijkingen in twee onbekenden van de graad 2.

[9] Met andere woorden, er is wel een inverse operatie voor de optelling, maar niet voor
de vermenigvuldiging. Het zal de kenner niet ontgaan zijn dat we hier expliciete
vermelding van de begrippen 'ring' en 'lichaam' vermijden.

[10] De formele definitie van een groep wordt gegeven door de volgende wetten op een operatie $*$, waarbij aan vermenigvuldiging gedacht kan worden.

(all x x*e =x).

(all x e*x=x).

(all x (all y (all z (x*y)*z= x(y*z)))).

(all x x*h(x)=e).

(all x h(x)*x=e).

Hier speelt *e* de rol van een speciaal element uit de verzameling en *h* de rol van een operator die aan een element *x* het element *h(x)* toevoegt.

[11] De term 'Monster' is afkomstig van J.H. Conway. De groep is ontdekt en geconstrueerd door R.L. Griess, Jr. Om precies te zijn, het aantal elementen is

808017424794512875886459904961710757005754368000000000.

Zie bijvoorbeeld D. Gorenstein, "Finite simple groups, An introduction to their classification," Plenum Press, New York, 1982, ISBN 0-306-40779-5.

[12] Ik doel hier op het Risch algoritme. De eerste observatie in deze richting wordt toegeschreven aan Liouville (1841). Zie K.O. Geddes, S.R. Czapor, G. Labahn. "Algorithms for Computer Algebra," Kluwer, Dordrecht,1992.

[13] Bijvoorbeeld, door de groepswetten in een formele taal op te schrijven en in te voeren in een daartoe door logici ontworpen programma, is het mogelijk interactief een formeel bewijs te zoeken voor wetten die uit de groepswetten volgen. Een elementaire eigenschap van groepen als de schrapwet

$a * b = a * c \implies b = c$

is op die manier zeer eenvoudig van een bewijs te voorzien. Om dit in te zien, vervangen we de uitspraak $x * y = z$ door $p(x, y, z)$. Vervolgens formuleren we de groepswetten (zie aantekening 10) als abstracte uitspraken en voeren ze in het computerprogramma OTTER in. (Ik bedank Mark Bezem voor de OTTER-sessie.)

(all x p(x,e,x)).

(all x p(e,x,x)).

(all x (all y (all z (all u (all v (all w

((p(x,y,u) & p(y,z,w)) $\implies$ (p(x,w,v) $\iff$ p(u,z,v))))))))).

(all x p(x,h(x),e)).

(all x p(h(x),x,e)).

We willen een formeel bewijs voor de schrapwet. Daartoe voegen we als axioma's toe de aannames a $*$ b = d en a $*$ c = d en de ontkenning van hetgeen te bewijzen is, dus $\neg$ (c $*$ e = b). Eerste bewerking van deze invoer door het programma geeft:

1 [ ] p(x,e,x).

2 [ ] p(e,x,x).

3 [ ] $\neg$ p(x,y,u) | $\neg$ p(y,z,w) | $\neg$ p(x,w,v) | p(u,z,v).

4 [ ] $\neg$ p(x,y,u) | $\neg$ p(y,z,w) | p(x,w,v) | $\neg$ p(u,z,v).

5 [ ] p(x,h(x),e).

6 [ ] p(h(x),x,e).

7 [ ] $\neg$ p(c,e,b).

8 [ ] p(a,b,d).

9 [ ] p(a,c,d).

De rol van *a,b,c,d,e* verschilt van de rest: deze zijn vast gekozen.
Het programma vindt nu:

2 [ ] p(e,x,x).

3 [ ] $\neg$ p(x,y,u) | $\neg$ p(y,z,w) | $\neg$ p(x,w,v) | p(u,z,v).

4 [ ] $\neg$ p(x,y,u) | $\neg$ p(y,z,w) | p(x,w,v) | $\neg$ p(u,z,v).

5 [ ] p(x,h(x),e).

6 [ ] p(h(x),x,e).

7 [ ] $\neg$ p(c,e,b).

8 [ ] p(a,b,d).

9 [ ] p(a,c,d).

10 [hyper,8,4,6,2] p(h(a),d,b).

15 [hyper,10,3,6,9] p(e,c,b).

20 [hyper,15,4,5,6] p(c,e,b).

21 [binary,20,7] .

Dit levert een bewijs, dat beter als 'gewoon bewijs' te lezen is als de volgende substituties meegenomen worden:

Bij 10: $x = a^{-1}$, $y = a$, $z = d$, $u = e$, $v = d$, $w = b$,

Bij 15: $x = a^{-1}$, $y = a$, $z = c$, $u = e$, $v = b$, $w = d$,

Bij 20: $x = c$, $y = c^{-1}$, $z = c$, $u = e$, $v = c$, $w = e$.

[14] Zie M. Ram Murthy, "Artin's conjecture for primitive roots,"
Math. Intelligencer, 10 (1988)59-67.
In 1967, liet Hooley [C. Hooley, On Artin's conjecture, J. reine u. angew. Math. 226 (1967) 209-220] zien dat Artin's vermoeden volgt uit de zogenaamde gegeneraliseerde Riemann hypothese, waarvan de speciale versie, als we Fermat als opgelost beschouwen, wellicht het beroemdste open probleem in de wiskunde is. De Riemann hypothese is 117 jaar oud.

[15] D.R. Heath-Brown, "Artin's conjecture for primitive roots,"
Quarterly J. Math. Oxford 37 (1986) 27-38.

[16] Golomb & Taylor, "Two-dimensional synchronization patterns for minimum ambiguity, IEEE Transactions Information Theory," IT-28, pp. 600-604, 1982.

[17] Er zullen altijd verschuivingen zijn die ten minste één hokje gemeen hebben met de oorspronkelijke: verschuif het linkerboven hokje maar naar een ander hokje van het oorspronkelijke patroon.

[18] Deze constructie wordt door Golomb & Taylor toegeschreven aan L.R. Welch.

[19] Het bestaat uit de hokjes met coördinaten (1, 1), (2, 2), (3, 4), (4, 8), (5, 5), (6, 10), (7, 9), (8, 7), (9, 3), (10, 6).

[20] Deze uitspraak komt van L. Vaserstein, Combinatorial Seminar,
Eindhoven, 23 juni, 1993.

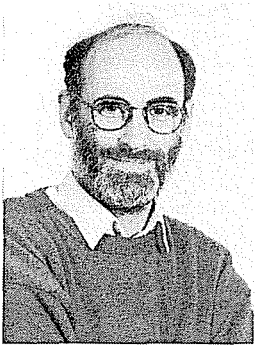
[21] Ik doel hier op het zogenaamde Buchberger-algoritme waarvan de complexiteit bekend slecht is. Zie K.O. Geddes, S.R. Czapor, G. Labahn. "Algorithms for Computer Algebra," Kluwer, Dordrecht, 1992.

[22] Ik bedank Peggy Cohen-Kettenis, Hans Cuypers, André Heck en Marc van Leeuwen voor hun hulp bij de voorbereiding van deze tekst.

Vormgeving en druk:
Reproduktie en Fotografie van de CTD
Technische Universiteit Eindhoven

Informatie:
Academische en Protocollaire Zaken
Telefoon (040-47)2250/4676

ISBN 90 38 60043 8



Arjeh M. Cohen werd in 1949 geboren in Haifa (Israel). Hij studeerde wiskunde aan de Universiteit van Utrecht, en werd daar benoemd tot wetenschappelijk medewerker. In 1975 promoveerde hij aan dezelfde universiteit in de algebra op een onderwerp in de groepentheorie. In datzelfde jaar aanvaardde hij een functie bij het Openbaar Lichaam Rijnmond.
Een jaar later trad hij als wetenschappelijk medewerker in dienst bij de vakgroep Fundamentele Wiskunde van de afdeling Toegepaste Wiskunde aan de Universiteit van Twente. In 1979 werd hij onderzoeker aan het Centrum voor Wiskunde en Informatica te Amsterdam, waaraan hij nog steeds voor een dag in de week verbonden is, en daarnaast vanaf 1991 deeltijd hoogleraar aan de Universiteit van Utrecht.
Hij was mede-initiatiefnemer en bestuurslid van de Stichting Computer Algebra Nederland. Per 1 augustus 1992 werd hij benoemd tot hoogleraar in de discrete wiskunde van de Technische Universiteit Eindhoven. Hij is voorzitter van het bestuur van de onderzoeksschool EIDMA en wetenschappelijk directeur van het onderzoeksinstituut RIACA te Amsterdam.