*Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.*

*The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.*

MC SYLLABUS 18

F. VAN DER BLIJ
H. FREUDENTHAL
J.J. DE IONGH
J.J. SEIDEL
A. VAN WIJNGAARDEN

# EEN KWART EEUW WISKUNDE 1946-1971

Serie voordrachten in het kader van de
Vacantiecursus 1971

MATHEMATISCH CENTRUM AMSTERDAM 1973

AMS (MOS) subject classification scheme (1970): 01A65

ISBN 90 6196 092 4

# INHOUD

# VOORWOORD

Op 11 februari 1946 werd het Mathematisch Centrum gesticht. Enige maanden later werd de eerste vakantiecursus gehouden.

In de kwart eeuw van zijn bestaan is door het Mathematisch Centrum veel meer gedaan voor de bevordering en de verspreiding van wiskundige kennis in Nederland, dan verwezenlijkt kan worden via vakantiecursussen. Maar dit is niet de plaats om op die andere activiteiten in te gaan, hoe belangrijk sommige ervan ook waren. Laten we hier liever erbij stil staan dat in 1971, het jaar waarin het MC zijn vijfentwintigjarig jubileum vierde, ook de vijfentwintigste vakantiecursus gegeven werd -de cursus waarvan de voordrachten hier gebundeld voor u liggen.*)

Vijfentwintig vakantiecursussen. Van de Didactiek van de Wiskunde via Grondslagenproblemen en Historische en Methodische Aspecten naar het Wiskunde-onderwijs in het V.H.M.O. van morgen. Topologie, groepentheorie, waarschijnlijkheidsrekening, besliskunde, computer en onderwijs - al deze onderwerpen zijn aan bod geweest. Een volledige lijst kunt u vinden op blz. 81 e.v. En dan nu als thema een terugblik op Een Kwart Eeuw Wiskunde.

Het is al zo vaak gezegd: de geschiedenis bevindt zich in een stroomversnelling. Dat geldt ook voor de evolutie van de wiskunde. Prof. Van WIJNGAARDEN mag zijn overzicht dan al in het jaar -1100 aanvangen, ook in zijn verhaal concentreren zich de ontwikkelingen in de jaren na 1945.

In die jaren valt meer te constateren dan een grote toename in onze wiskundige kennis. De richting van het onderzoek is gaan veranderen, en de hele wiskundige stijl raakt vernieuwd. Heel duidelijk wordt dit uiteengezet in de voordracht van Prof. FREUDENTHAL.

Overigens is die toename van onze kennis inderdaad groot. Uitgaande van HILBERT's vijfde probleem laat Prof. FREUDENTHAL zien hoe belangrijke ontwikkelingen plaatsvonden in de theorie van de topologische groepen, met grote consequenties voor de meetkunde. Daarnaast geeft hij een boeiend verslag van het ontstaan van de cohomologische algebra en van de categorietheorie, die beide van omstreeks 1945 dateren. Zijn persoonlijke evaluatie van de door hem beschreven resultaten maken Prof. FREUDENTHAL's bijdrage nog boeiender en belangwekkender.

---

*) In 1954 werd geen vakantiecursus gehouden, in verband met het feit dat in dat jaar het International Congres of Mathematicians te Amsterdam bijeenkwam.

Van twee andere problemen uit HILBERT's lijst van 1900, nl. het eerste en het tiende probleem, betreffende de onafhankelijkheid van CANTOR's continuumhypothese resp. betreffende het bestaan van rekenmethoden voor het oplossen van diophantische vergelijkingen, vertelt Prof. DE IONGH niet leen dat zij zijn opgelost in de laatste vijfentwintig jaar, maar hij weet ook in kort bestek een helder overzicht te geven van de bewijsmethoden. Het belang van het grondslagenonderzoek voor de verdere wiskunde is nog steeds groeiende. Sterke hulpmiddelen en methodieken zijn in de jongste kwart eeuw ontwikkeld. Een beroemde toepassing in de getaltheorie van ultraproducten -een hulpmiddel uit de modeltheorie- door AX en KOCHEN wordt vermeld in de voordrachten van Prof. FREUDENTHAL en van Prof. Van der BLIJ.

Daarmee komen we tot de getaltheorie, de koningin van de wiskunde. In een systematisch overzicht behandelt Prof. Van der BLIJ enerzijds "klassieke problemen, waarvan enkele werden opgelost, en bij andere nauwelijks vooruitgang werd geboekt", anderzijds noemt hij generalisaties en analogieen. Leerzaam en erg nuttig is telkens zijn evaluatie van "de vraag of de oplossing het resultaat was van een lange ontwikkeling (met bijvoorbeeld steeds betere methoden) of eigenlijk even goed al vóór 1946 gevonden had kunnen worden, omdat het materiaal voor de oplossing van het probleem al lang gereed lag".

Er zijn altijd nauwe relaties geweest tussen de getaltheorie en de combinatoriek. Die banden zijn waarneembaar uit de voordracht van Prof. SEIDEL, getiteld *Van recreatie naar ernst, van meetkunde naar codes, grafen en groepen.* Een andere relatie, nl. tussen de combinatoriek en de recreatieve wiskunde, komt ook duidelijk aan de orde. Toch is de combinatoriek veel meer dan "Spielerei", en de belangrijke ontwikkelingen in de vijfentwintig jaren waarmee wij hier bezig zijn, werden mede sterk gestimuleerd vanuit de techniek, vanuit de toepassingen. Aan de hand van een paar uitgelezen voorbeelden geeft Prof. SEIDEL ons van die ontwikkelingen een indruk.

Ieder die nadenkt over de betekenis van het wiskundig onderzoek sinds 1946 kan niet voorbijgaan aan de informatica. De getaltheorie mag dan de koningin van de wiskunde zijn - de informatica is inmiddels de majordomus geworden. Wellicht voelt hij zich nog niet zo heel goed thuis in deze hoge positie, en ontstaat daaruit de behoefte zich te voorzien van een lang en eerbiedwaardig voorgeslacht, dat verder terug gaat in het verleden dan dat van de heerseres zelve, tot HAN PIN HO in -1100?

In ieder geval, ook in de voordracht van Prof. Van WIJNGAARDEN ligt uiteindelijk het accent niet op het verre verleden, maar op de laatste vijfentwintig jaar. Zijn levendige en bijzonder boeiende beschrijving van de ontwikkeling van de computer, en met name van de programmatuur, toont duidelijk hoezeer Prof. Van WIJNGAARDEN deze ontwikkeling van nabij heeft meegemaakt. Vervolgens behandelt hij het ontstaan van de hogere programmeertalen -met name ALGOL 60 en ALGOL 68- en gaat in op de uitbouw van de semantiek van (formele) talen, om tenslotte aan een aantal voorbeelden te laten zien hoe de informatica met zijn rekenautomaten helpen kan om klassieke problemen nader tot een oplossing te brengen. Problemen die hij ontleent aan ... de getaltheorie.

Evenals bij alle vorige vakantiecursussen was het succes van deze vijfentwintigste cursus (en ontegenzeggelijk is deze cursus inderdaad een succes gebleken) afhankelijk van hen die hem "maakten": de docenten en de deelnemers. De deelnemers hebben steeds mede de themata van de diverse cursussen kunnen bepalen, via de Voorbereidingscommissie. Graag wil ik op deze plaats dank brengen aan deze commissie, en vooral aan die leden ervan die, uit het V.H.M.O. afkomstig, konden aangeven in welke richting de belangstelling en de behoeften van de leraressen en leraren ging. De deelnemers ook hebben door hun grote opkomst, en door hun participatie in de discussie, voor plezierige en levendige cursusdagen gezorgd. Toch -meer nog dan de deelnemers, meer nog dan de voorbereidingscommissie- hebben de docenten hun stempel op de vakantiecursussen gezet, en telkens weer het slagen van deze cursussen zeker gesteld. Het Mathematisch Centrum prijst zich gelukkig, dat het steeds weer zoveel bereidwilligheid heeft gevonden bij de Nederlandse wiskundigen om aan deze vakantiecursussen mede te werken. Aan de verschillende sprekers -niet alleen op de Vakantiecursus 1971, maar op alle vakantiecursussen- zij hierbij dan ook oprechte dank gebracht. De docenten van de Vakantiecursus 1971 komt dan zeker veelvoudige dank toe, want allen hebben ze al meerdere malen op vakantiecursussen gesproken: Prof. FREUDENTHAL voor het eerst op de tweede cursus, Prof. Van der BLIJ voor het eerst op de vierde, Prof. SEIDEL voor het eerst op de negende, Prof. De IONGH al op de derde, en Prof. Van WIJNGAARDEN op de zesde cursus. En in het totaal hebben deze vijf samen op de eerste vijfentwintig cursussen drieëntwintig voordrachten voor hun rekening genomen...

Ten gevolge van een aantal tegenslagen, gedeeltelijk van technische aard, verschijnt deze volledige tekst van de vijfentwintigste vakantiecur-

sus aanzienlijk later dan wij bedoelden. Wij hopen, dat voor de deelnemers aan de Vakantiecursus 1971 deze syllabus alsnog een prettige herinnering zal betekenen aan een leerzame en plezierige cursus, en dat zij en alle andere lezers van dit boek erdoor gestimuleerd zullen worden zich opnieuw, of nog meer, bezig te houden met dat schone spectrum van theorieën: de WISKUNDE.

P.C. Baayen.

MC SYLLABUS 18, 1973, 1-15

# VIJFENTWINTIG JAAR WISKUNDIGE IDEEEN EN METHODEN

H. FREUDENTHAL

Mijn Utrechtse inaugurale oratie droeg de titel *5000 jaren internationale wetenschap*, en daar was dan de wiskunde mee bedoeld. Toen het Mathematisch Centrum me uitnodigde over die 25 jaren wiskunde te spreken, die met het leven van deze instelling samenvallen, dacht men dus wel dat ik voor een kleintje niet vervaard zou zijn. Ik wil u vast verklappen dat -bij leven en welzijn- mijn Utrechtse afscheidsrede zal gaan over *Vijftig jaren wiskunde*. Ik zal de jaren, die me tot dan resten, besteden om me beter op de hoogte te stellen van wat in die vijftig jaren is gebeurd. Ik heb trouwens een tijd geleden een lustrum van een vereniging mee helpen vieren onder de titel -als ik me niet vergis- van 40 jaren wiskunde. Ik heb dus al met dat bijltje gehakt.

Excuses zoals "in de mij ter beschikking staande tijd" of "bij de ongekende omvang die de wiskunde heeft aangenomen" zijn goedkoop. Als je een taak aanvaardt, moet je je er goed van kwijten, d.w.z. zó dat tijdgenoten het goed vinden. Het nageslacht kun je het toch niet naar zijn zin doen. In zijn *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert* heeft F. KLEIN te veel nadruk gelegd op die ontwikkelingen, die in de 19e eeuw zijn afgesloten en heel weinig op de wortels, waaruit in de 20e eeuw nieuwe loten zouden schieten, zoals verzamelingenleer, ideaaltheorie, meetkundige axiomatiek. In 1951 hield H. WEYL een lezing over *A half-century of mathematics*; zonder hem te kort te doen, zullen velen zijn keuze van onderwerpen en de manier, waarop hij de accenten legt, niet meer goedkeuren.

Natuurlijk is elke dag de toekomst al weer begonnen, maar het is een grote kunst, om in het heden de tere wortels van de dag van morgen te herkennen. Ik heb me in dit opzicht in het verleden vaak genoeg vergist -en anderen deden dit met mij- om een les te hebben kunnen leren.

Hoe nu de afgelopen kwart eeuw te behandelen? Ik kan HILBERT's befaamde 23 Parijse problemen van 1900 een voor een de revue laten passeren en kijken wat er rondom deze in de laatste tijd zoal is gebeurd. Bijvoorbeeld RIEMANN's vermoeden over de nulpunten van de $\zeta$-functie: geen stap verder, ondanks computers die tot het zoveelste nulpunt het vermoeden hebben bevestigd. Of de grote Fermat, waar naarstige onderzoekers telkens nieuwe -eindige- pasjes vooruit doen. Maar er zijn zoveel problemen buiten HILBERT's keuze, die onderzoekers boeien. Denk even aan BIEBERBACH's vermoeden: bij een in de 1-cirkel een-eenduidige reguliere functie f met $f(0)=0$, $f'(0) = 1$ vervullen de coëfficiënten $a_n$ van de machtreeksontwikkeling $f(z) = \sum a_n z^n$ de ongelijkheden $|a_n| \leq n$. De historische lijst ziet er als volgt uit. Bewezen voor

$n = 2$, door L. BIEBERBACH in 1916,
$n = 3$, door K. LOEWNER in 1923,
$n = 4$, door GARABEDIAN-SCHIFFER in 1955,
$n = 6$, door PEDERSON in 1968; maar het geval
$n = 5$ is nog onopgelost.

Een aardige variatie op dit probleem, waartoe trouwens ook N.G. de BRUIJN een bijdrage heeft geleverd, is:

bij vaste f voor bijna alle n, door HAYMAN in 1968.

Een ander bewijs dat niet alle onopgeloste problemen door HILBERT zijn geregistreerd, is de befaamde vraag van BURNSIDE of er niet-cyclische enkelvoudige groepen zijn van oneven orde, m.a.w. of alle groepen van oneven orde oplosbaar zijn. De laatste vraag werd eindelijk in 1963 door W. FEIT en J.G. THOMPSON bevestigend beantwoord. Het bewijs beslaat meer dan 250 bladzijden.

Als ik dan toch één der Hilbertse problemen moet behandelen, kies ik het vijfde: *de analyticiteit van de continue groepen*. We zouden het tegenwoordig als volgt formuleren.

Het is duidelijk wat we een topologische groep gaan noemen: een verzameling met twee structuren; een structuur van groep en één van topologische ruimte, die compatibel moeten zijn, d.w.z. de groepbewerkingen moeten continu zijn. Bij de meest bekende topologische groepen is de ten grondslag

liggende topologie een variëteit, dus samenhangend locaal euclidisch. Maar in feite zijn het zelfs analytische variëteiten en zijn ook de groepbewerkingen analytisch - de zogenaamde Liegroepen. LIE wist al dat men alleen twee keer continue differentieerbaarheid hoeft te onderstellen om analyticiteit af te dwingen. HILBERT stelde de vraag of continuïteit alleen voldoende was. L.E.J. BROUWER deed daarna krachtige pogingen HILBERT's vraag te beantwoorden, maar de topologische werktuigen waarover hij toen kon beschikken, waren nog veel te zwak.

De eerste belangrijke stap werd door J. von NEUMANN (1927) gedaan; hij loste het probleem op voor lineaire groepen in eindig veel dimensies. Ik had in dezelfde tijd een zwakker resultaat gevonden, maar het, toen me in een gesprek met Von NEUMANN bleek, dat hij meer had, niet gepubliceerd. Feitelijk behelsde Von NEUMANN's methode nog meer, zoals E. CARTAN duidelijk maakte: elke afgesloten locale ondergroep van een Liegroep is locaal een Liegroep.

Inmiddels waren merkwaardige topologische groepen bekend geworden, die geen Liegroepen waren, de solenoïden van D. van DANTZIG, door ongewone completeringen van de optelgroep der reële getallen verkregen, of, zo men wil, als projectieve limieten van abelse Liegroepen. Het zijn samenhangende compacte groepen, maar geen Liegroepen.

De lineaire groepen nemen een sleutelpositie in. In een geschikte functieruimte $\Phi$, op de groep G gedefinieerd, induceert G een lineaire groep. Op Liegroepen is er een wezenlijk unieke invariante maat; naar zulk een maat kan men voor $\Phi$ de ruimte van de $L^2$-functies nemen; de in $\Phi$ door G geïnduceerde groep bestaat dan uit unitaire afbeeldingen. $\Phi$ is jammer genoeg oneindig dimensionaal, maar in het algemeen zal $\Phi$ ook reducibel zijn; is $\Phi$ misschien zelfs in eindig dimensionale onderdelen op te lossen?

Wel, voor compacte groepen lukte het F. PETER en H. WEYL met de integratiemethode van A. HURWITZ (1926); ze konden aldus de totaliteit der lineaire voorstellingen verkrijgen. Het gaat met een eigenwaardeprobleem van een -dankzij de compactheid van G- compacte lineaire operator; de eindige dimensie van die voorstellingen is door de eindige multipliciteit van die eigenwaarden verzekerd.

Om willekeurige compacte groepen met deze methode te behandelen, moest men er een invariante maat op hebben. Die werd in 1933 door A. HAAR, zelfs voor locaal compacte groepen, ontdekt, en daarmee kon J. von NEUMANN de samenhangende compacte groepen tot de Liegroepen terugbrengen.

Het lag voor de hand hoe men verder moest. Het juiste medium van onderzoek waren de samenhangende locaal compacte groepen, en de stelling waar men

naar toe moest, was, dat deze als projectieve limieten van Liegroepen verkregen konden worden.

De volgende stap werd door L. PONTRJAGIN (1934) gedaan; het waren de samenhangende locaal compacte commutatieve groepen, die directe producten van compacte en van eindig-dimensionale vectorruimtegroepen bleken te zijn. Er werden voor of in de oorlog nog enkele minder belangrijke stappen gedaan, maar de samenhangende locaal compacte groepen in het algemeen bleven een open probleem. De weg waarop ze aangepakt zouden moeten worden, lag wel uitgetekend: men moest G als unitaire groep in de oneindig-dimensionale Hilbertruimte der functies op G beschouwen en van deze groep direct de infinitesimale algebra construeren, in de geest zoals men dit met eenledige unitaire groepen (bijv. ten behoeve van de ergodenstelling) pleegt te doen. Er zijn, geloof ik, heel veel wiskundigen rond 1940 met dit probleem bezig geweest; er zijn ook enkele foutieve publicaties omtrent zulke pogingen. In elk geval lukte het niet en men gaf de pogingen toen blijkbaar op, mogelijk te vroeg. Rond het midden van de eeuw leidden successievelijke inspanningen van een aantal wiskundigen (MONTGOMERY, ZIPPIN, KURANISHI) tot het uiteindelijke resultaat (GLEASON, YAMABE): de bevestiging van het vermoeden dat de samenhangende locaal compacte groepen de projectieve limieten van Liegroepen zijn. Precies een kwart eeuw na Von NEUMANN's eerste stap was hiermee, in 1952, het probleem in zijn totaliteit opgelost.

Maar met welk soort methoden? Niet zoals men rond 1940 gehoopt had, met voorstellingen in een Hilbertruimte door groepen van Hermitese operatoren, maar door een topologische koorddanserij, waarvan men wel de finesses, maar nauwelijks de zin begrijpt.

Misschien hebt u zich bij de vermoedens van BIEBERBACH en van BURNSIDE afgevraagd: wat heb je er nu eigenlijk aan of dat waar is of niet? Terecht mag men zich deze vraag stellen, maar wat daar wel telt, zijn de voor velerlei toepassingen bruikbare methoden, die ten behoeve van zulke problemen in feite zijn ontwikkeld. De methoden waarmee het vijfde probleem voor compacte en voor abelse groepen werd opgelost, zijn van enorme betekenis; de methode waarmee uiteindelijk het algemene geval werd aangepakt, is volstrekt ad hoc en voor niets anders te gebruiken. Was het vijfde probleem van HILBERT niet in 1952 opgelost, dan zouden we heel wat stellingen over topologische groepen ingewikkelder moeten formuleren, maar we zouden qua inzicht en methodiek niets missen. Met deze opmerking bedoel ik niet de inspanningen te kleineren, die een aantal wiskundigen zich toen hebben getroost. Wel vind ik dat men nog eens zou moeten proberen de voor compacte groepen succesrijke methoden

der functionaalanalyse tot het algemene geval uit te breiden; als dit lukt, zou het zeker inzicht en methodiek verrijken.

De oplossing van HILBERT's vijfde probleem speelt een rol in de moderne versie van hetgeen men ook het HELMHOLTZ-LIE ruimteprobleem noemt. H. von HELMHOLTZ heeft in 1868, dus lang voor HILBERT's *Grundlagen der Geometrie*, een simultane axiomatiek der euclidische en niet-euclidische meetkunden ontworpen - tegenwoordig zou men zeggen "een karakterisering der euclidische en niet-euclidische groepen", hoewel het begrip "groep" in HELMHOLTZ's werk nog vaag en zonder vaste vorm is. S. LIE (1890) formuleerde en preciseerde HELMHOLTZ's ideeën. Het probleem om uit deze axiomatiek de differentieerbaarheidsveronderstellingen te verwijderen, werd al door HILBERT en BROUWER aangepakt; het werd opnieuw in 1930 door KOLMOGOROV geformuleerd. In kleine stapjes werd er vanaf 1941 naar toe gewerkt. De definitieve oplossing kwam door J. TITS in 1952. Het resultaat kan tegenwoordig als volgt worden samengevat: zij R een samenhangende en locaal compacte metrische ruimte en F de groep der isometrieën van R; stel F is transitief over een congruentieklasse van kleine driehoeken, dan is $\lceil R,F \rceil$ een euclidische of niet-euclidische meetkunde.

Verlangt men alleen transitiviteit over een congruentieklasse van puntenparen (met kleine afstand), dan komen er nog de euclidische en niet-euclidische meetkunden over de complexe getallen, quaternionen en octaven bij (het laatste alleen voor dimensie twee).

Naast het HELMHOLTZ-LIE probleem moet ik hier wel op een ander klassiek denkbeeld wijzen waarop in de laatste tijd met veel succes is voortgeborduurd, het *Erlanger Programm* van F. KLEIN, waaraan echter pas E. CARTAN (1926-1929) zijn volle tegenwoordige inhoud heeft gegeven. Bij F. KLEIN waren de meetkundige structuren het primaire; de invariantiegroepen waren er om tussen zulke meetkunden classificerende verbanden te leggen. E. CARTAN echter stelt de groep primair en leidt er door middel van ondergroepen geometrische structuren, de zogenaamde *homogene ruimten*, uit af. Zodoende werkt bijvoorbeeld die projectieve groep van de n-dimensionale projectieve ruimte evenzeer op de lijnenruimte, op de ruimte der 2-dimensionale vlakken, enz. Zo'n homogene ruimte is gekenmerkt door de ondergroep, die een element van die ruimte vasthoudt. Hoe kan men nu dit hele incidentieverband tussen de diverse ruimten puur groepentheoretisch karakteriseren? Deze vraag is door J. TITS -niet alleen voor de projectieve groep, maar voor alle zogenaamde halfenkelvoudige groepen- beantwoord in de verrukkelijk mooie theorie van, wat men noemt, de *Tits-meetkunden*.

Nu ik eenmaal in de Liegroepen terecht ben gekomen, mag ik de wellicht belangrijkste spruit van deze theorie niet vergeten, CHEVALLEY's algebraische groepen. Was in het vijfde probleem van HILBERT gesteld, dat bij Liegroepen de differentiële structuur door de topologische bepaald is, tussen de beide wereldoorlogen was gebleken dat bij belangrijke Liegroepen de topologische structuur uit de algebraïsche kon worden afgeleid. CHEVALLEY nu vatte het idee op algebraïsche (d.w.z. door algebraïsche vergelijkingen gedefinieerde) lineaire groepen (over willekeurige, meestal algebraïsch afgesloten, lichamen) te bestuderen. Hoewel de infinitesimale methode, die tot de Liealgebra leidt, hier faalde, slaagde CHEVALLEY er toch in in wezen dezelfde resultaten als men van Liegroepen kende, af te leiden. Door de theorie der algebraïsche groepen, speciaal ook over eindige lichamen, is thans ook de theorie der eindige groepen verrijkt.

In de algebra beschouwen we de associatieve wet als een haast vanzelfsprekende eis. De enige ringen en algebra's, die met de associatieve nog een beetje kunnen concurreren, zijn de Lie-algebra's, waar de associatieve wet door de (cyclische) Jacobi-wet

$$(ab)c + (bc)a + (ca)b = 0$$

is vervangen. Naast deze twee wetten heeft een derde in de laatste decennia betekenis verkregen. Het is de alternatieve wet, waarop alleereerst M. ZORN en Ruth MOUFANG in de dertiger jaren de aandacht vestigden: zij in een ring door

$$\{a,b,c\} = (ab)c - a(bc)$$

de *associator* van drie elementen gedefinieerd; de alternatieve wet eist dat de associator een alternerende functie van a,b,c is. Men kende allang zo'n alternatieve algebra: HURWITZ had de algebra's met een van een inproduct afkomstige norm geclassificeerd; ze waren over de reële getallen van de dimensies 1,2,4,8 -de algebra der reële getallen, der complexe getallen, der quaternionen, der octaven, waarvan de eerste twee commutatief waren, de derde nog associatief en de vierde alleen nog alternatief was. Bij algebraisering van een vlakke projectieve meetkunde beantwoordt aan de stelling van PAPPUS-PASCAL de commutatieve wet der vermenigvuldiging, aan DESARGUES de associatieve wet en aan de eis van de uniciteit van het vierde harmonische punt de alternatieve wet; het was deze meetkundige kant van waaruit het zoeklicht op de alternatieve wet werd gericht, met een verstrekkend gevolg voor

het begrip van bepaalde Liegroepen. Ik bedoel de vijf (complexe) "uitzonderingstypen", de $G_2$, $F_4$, $E_6$, $E_7$, $E_8$; vreemde eenden in de bijt temidden van de enkelvoudige Liegroepen, die anders in vier grote klassen waren opgedeeld. Wat de $G_2$ betekent, had E. CARTAN al vastgesteld: het was de automorfismengroep van de octaven. Vanaf 1950 werd de status van de andere uitzonderingstypen (complex en reëel) opgehelderd; ze hadden alle te maken met meetkunden over de Hurwitz algebra's: vlakke elliptische en projectieve meetkunden, symplectische en zogenaamde metasymplectische meetkunden, die van hun kant weer verwant waren aan de Tits-meetkunden.

Als ik me nu in mijn relaas tot de topologie wend en de groepen de laan uitstuur, moet ik u meteen waarschuwen dat ze straks door de achterdeur weer binnen zullen komen.

De algebraïsche topologie, hoewel al door POINCARÉ ontwikkeld, begon pas in het midden van de jaren twintig echt van de grond te komen. U weet waar het om gaat: uit i-dimensionale simplexen vormt men door lineaire combinatie "ketens", die additieve groepen $K_i$ vormen. Daar hoort als homomorfisme de zelfkantoperator $\mathfrak{Z}$ bij; de kern van $\mathfrak{Z}$ in $K_i$ bestaat uit de cyclussen; het beeld van $\mathfrak{Z}$ in $K_i$ is er een ondergroep van; de modulo-groep van beide is de i-de homologiegroep. Als duale van de homologie werd in het midden van de jaren dertig de, meer bruikbare, cohomologie uitgevonden, waarmee men ook nog producten tussen de verschillende dimensies kon vormen. Het vervelende van de algebraïsche topologie is, dat de topologische invariantie van de homologiegroepen en -ringen allesbehalve direct evident is. Dit is geheel anders bij de homotopie, die ook al weer op zijn minst sinds POINCARÉ bekend was: gesloten wegen (of algemenere afbeeldingen) heten homotoop als ze continu in elkaar kunnen worden overgevoerd; het samenstellen van gesloten wegen leidt tot een groep, de fundamentaalgroep. De topologische invariantie van de homotopiebegrippen is direct duidelijk. In 1935 kwam W. HUREWICZ op het idee hogerdimensionale homotopiegroepen door middel van sferenafbeeldingen te definiëren, maar, wat de hoofdzaak was, hij kon deze homotopiegroepen direct in de klinkende munt van nieuwe diepe topologische inzichten omzetten. Het was voor mijn eigen ontwikkeling van verstrekkende betekenis, dat ik na mijn leerjaren bij H. HOPF bij de geboorte van HUREWICZ's ideeën mocht assisteren.

Een van HUREWICZ's belangrijke resultaten was, dat een polytoop met triviale fundamentaalgroep en homologiegroepen ook homotopisch triviaal was; een ander dat bij polytopen met triviale hogere *homotopie*groepen de *homolo-*

*gie*groepen door de fundamentaalgroep uniek bepaald zijn. HUREWICZ wierp toen meteen de vraag op, hòè de fundamentaalgroep G dan de hogere homotopiegroepen bepaalt. Om deze vraag te beantwoorden, hoef je maar één polytoop met de fundamentaalgroep G te onderzoeken. Merkwaardigerwijs zochten we er toen eigenlijk te veel achter. We begrepen niet dat de bij een groep G (als fundamentaalgroep) behorende homologiegroepen nieuwe functoren van zelfstandige betekenis waren en dachten er te veel aan, ze in klassieke groepenfunctoren uit te drukken. Met "wij" bedoel ik dan HUREWICZ en mezelf, maar ook H. HOPF, die desalniettemin met wat hij in de eerste oorlogsjaren hieraan deed, de stoot gaf tot het ontstaan van een nieuw onderdeel van de wiskunde. Ik haakte erop in en hoewel ik in een ander artikel juist de methode van het direct topologisch werken in een discrete groep had ontwikkeld, bleef ik nog te zeer in het algoritmische steken. B. ECKMANN en EILENBERG & Mac LANE hakten toen (1945) de knoop door. Ze gebruikten als polytoop met fundamentaalgroep G een als het ware universeel model: vat G zelf als hoekpuntenverzameling van een polytoop $\tilde{P}$ op en benoem elke eindige deelverzameling tot simplex. Hier is alles homologisch triviaal; de rij der ketens

$$\ldots \xleftarrow{\partial} K_{i-1} \xleftarrow{\partial} K_i \xleftarrow{\partial} \ldots$$

is een exacte rij (dit is de wezenlijke bron van het begrip *exacte rij*). $\tilde{P}$ laat de linksvermenigvuldiging met elementen van G toe; door onder G equivalente punten met elkaar te identificeren, krijg je een polytoop P, die de fundamentaalgroep G bezit en waarvan $\tilde{P}$ de universele ontrolling is. Voor de constructie van P hebben we alleen de kale groep G gebruikt; de cohomologie van P is rechtstreeks in termen van G gedefinieerd en wordt derhalve ook kort cohomologie van G genoemd. Het probleem om te weten te komen, hòè G de homologie van asferische polytopen bepaalt, is hiermee niet opgelost, maar doodgeslagen- zoiets is van ouds in de wiskunde een teken van belangrijke vooruitgang geweest.

Dit is de oorsprong van de hele cohomologische algebra, en wanneer u dit woord verneemt, zult u wel begrijpen waarom mijn aankondiging van een gloednieuw onderdeel van de wiskunde, dat uit HOPF's onderzoekingen in de oorlog zou voortkomen, niet overdreven was.

Toen de kruitdamp van de tweede wereldoorlog was opgetrokken was er uiteraard inmiddels wiskundig meer gebeurd dan hetgeen mij uit Zürich bekend was geworden. Als ik me goed herinner, sloeg het eerste mathematische

nieuws, dat mij bereikte, op WALD's *sequente analyse*, op wat later *cybernetica* werd genoemd, op L. SCHWARTZ's *distributies* en, uiteraard, op *computers*. Met de computergeschiedenis wordt u later nog geconfronteerd *); bij distributies wil ik alleen nog aan locaal convexe ruimten herinneren en de naam van G.W. MACKEY noemen; cybernetica en *mathematische statistiek* geven mij de gelegenheid tot een opmerking omtrent de naoorlogse maatschappelijke implicaties van de wiskundebeoefening. Beide gebieden zijn gekenmerkt door de tegenstelling tussen een "highbrow" theorie en een zeer aardse praktijk. In de statistiek hebben in de afgelopen kwart eeuw de toepassingen een vlucht genomen zoals op geen ander wiskundig gebied, maar het is zeker niet overdreven te stellen dat het overgrote deel van deze toepassingen, vooral in de sector van psychologie en sociologie, een grandioos misbruik is; de opvatting dat men een, op ondeugdelijke theorieën gebaseerd, met ondeugdelijke middelen bijeengeraapt, ondeugdelijk cijfermateriaal met mathematische middelen (die soms ook nog ondeugdelijk zijn) een wetenschappelijke status kan verlenen, heeft wel het gezag van, maar niet het begrip voor de wiskunde doen stijgen. Anders dan de mathematische statistiek beschikt de cybernetica maar over één pasklare formule, die dan echter voor de meest absurde doeleinden wordt gebruikt, bijv. om de informatie van een piano uit zijn toetsental te berekenen. De cybernetica op zijn beurt kan op een schat van krachttermen en slogans bogen, die zich uitstekend tot verbaal misbruik lenen. Zulke misbruiken van de wiskunde zijn er altijd geweest; ze hebben het doordringen van de wiskunde in velerlei toepassingsgebieden misschien vertraagd, maar geenszins blijvend gehinderd.

Langdurige miskenning van belangrijke ontdekkingen is in de wiskunde een zeldzaam verschijnsel, maar als enkeling kan men zich natuurlijk wel eens vergissen. Zo is het mij misschien met de *categorieën* vergaan. Misschien, zeg ik; de geschiedenis heeft nog niet het beslissende woord gesproken. Ik heb de categorieën lang als "general abstract nonsense" in de zin van EILENBERG beschouwd, heb me later geregeld door allerlei grapjes die de categorieën rijk zijn, tot bewondering laten verleiden, heb jarenlang zonder succes geprobeerd een beetje categorieën te onderwijzen, en ben, toen ik er eindelijk toch nog in slaagde, de categorieën dusdanig gaan doorzien, dat ik er -to nader order- niet meer in geloof, maar dan altijd in de stille hoop dat er meer achter zit dan ik thans kan bevroeden.

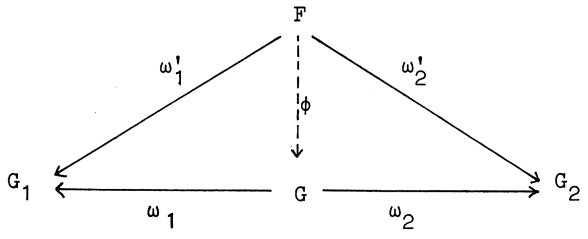
---

*) Zie de voordracht van A. van WIJNGAARDEN (blz. 59 e.v.).

De categorieën hebben zich tot een in zichzelf gesloten gebied ontwikkeld waarin diep onderzoek wordt bedreven en op welk gebied geregeld boeken verschijnen. Maar de opzet van een de wiskunde overkoepelende theorie is, naar mij voorkomt, niet geslaagd.

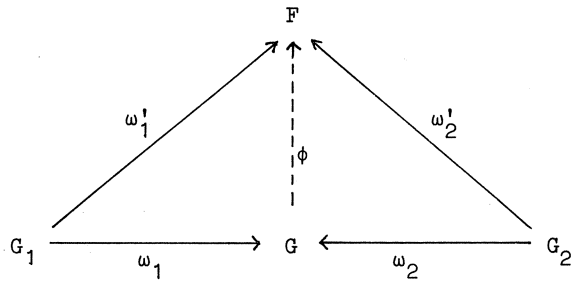
Laat ik beginnen met dat begrip, waaruit de categorieën bij EILENBERG & Mac LANE in 1945 hun bestaan afleiden: de *natuurlijke equivalentie*. Als ik van een eindig-dimensionale lineaire ruimte R de duale $R^*$ en hiervan weer de duale $R^{**}$ neem, dan krijg ik allemaal isomorfe structuren; maar onder de isomorfieën van R en $R^{**}$ is er één gepriviligeerde, "natuurlijke", hetgeen tussen R en $R^*$ en tussen $R^*$ en $R^{**}$ geenszins het geval is. Wat "natuurlijk" hier betekent, is door EILENBERG & Mac LANE's begrip der natuurlijke equivalentie overtuigend uit de doeken gedaan. Ieder, die zin en doel van de categorieën wil uitleggen, begint dan ook met dit voorbeeld. Hij begint ermee, maar hij beperkt er zich ook toe. Alle relaties tot de meer "concrete" wiskunde putten zich in dit ene voorbeeld uit. Natuurlijk kan men er meer bedenken, maar waarvoor? Je voelt direct aan wat een natuurlijke equivalentie is en het kost meestal geen moeite dit gevoel te verifiëren. Het is alleen jammer dat je zo weinig hebt aan de wetenschap dat iets een natuurlijke equivalentie is.

Een andere bron van de categorieën is het definiëren door middel van universele eigenschappen. Men definieert bijvoorbeeld het *directe product* van twee groepen $G_1$ en $G_2$ (of van meer groepen) door zich aan de totaliteit der groepen te refereren: een G samen met homomorfismen (projecties) $\omega_i$ van G op $G_i$ (i=1,2) heet direct product van $G_1$ en $G_2$, als er voor elke groep F met homomorfismen $\omega_i'$ in $G_i$ een uniek homomorfisme $\phi$ van F in G is met $\omega_i' = \omega_i \circ \phi$ (i=1,2):




Het is een wonderbaarlijk mooie definitie, die er nog mooier op wordt doordat dualisering, d.w.z. omkering van de pijlen, het *vrije product* van de groepen $G_1$,$G_2$ uit de hoge hoed tovert: het vrije product van twee groepen $G_1$ en $G_2$ is een groep G met homomorfismen $\omega_i$ van $G_i$ in G, zodanig dat bij elke

groep F met homomorfismen $\omega_i'$ van $G_i$ in F één homomorfisme $\phi$ van G in F bestaat, zodat $\omega_i' = \phi \circ \omega_i$ (i=1,2):




Is dat niet wonderbaarlijk? Ik kom er ook telkens weer van onder de indruk. Het is alleen jammer dat je, als je iets met directe producten wilt doen, de universele definitie meteen weer moet vergeten; in de praktijk is ze onbruikbaar. Sterker, het verband tussen directe en vrije producten, door de dualiteit gelegd, is zinsbedrog, er is geen enkele stelling over groepen die je door middel van dualiteit van vrije naar directe producten of omgekeerd kunt overbrengen. De dualiteit past trouwens helemaal niet bij de categorie der groepen, aangezien wel

$$1 \leftarrow C \leftarrow B$$

steeds tot een exacte rij

$$1 \leftarrow C \leftarrow B \leftarrow A \leftarrow 1$$

kan worden aangevuld, maar niet steeds

$$1 \rightarrow C \rightarrow B$$

tot een exacte rij

$$1 \rightarrow C \rightarrow B \rightarrow A \rightarrow 1.$$

Tot 1957 bestond de categorieënleer voornamelijk uit wat -nuttige- terminologie en een aantal aantrekkelijke grapjes. Diepgang komt er pas in met D. KAN's schepping van het begrip van geadjungeerdheid van functoren (bijv. zijn geadjungeerd de vergeetfunctor die aan een lineaire ruimte de onderliggende verzameling toevoegt, en de functor die uit een verzameling vrij een lineaire ruimte opbouwt). Wie wiskundige schoonheid weet te appre-

ciëren zal zich aan de bekoring van dit begrip moeilijk kunnen onttrekken, maar wie toendertijd hoopte dat nu de weg gebaand was om de wiskunde door de categorieën te overkoepelen, is -voorlopig- bedrogen uitgekomen. Er is buiten de categorieën zelf geen emplooi voor de geadjungeerde functoren.

Ik loochen niet dat categorieën een boeiend onderwerp zijn; ook de categoriale terminologie is waardevol. Er kan geen twijfel over bestaan dat voor sommige axiomatieken de juiste opzet de categoriale is. Van groot belang zijn natuurlijk exacte rijen (een uitvinding van HUREWICZ die, naar ik meen, nimmer door hem gepubliceerd, maar alleen mondeling doorgegeven werd) en diagrammen, maar die zijn veeleer een hulpmiddel dan een onderwerp der categorieënleer. In elk geval rechtvaardigt hetgeen tot nu toe door de categorieën is bereikt, niet de grote verwachtingen die men erin gesteld had. Misschien waren ze te hoog gespannen. De toekomst zal het leren. Een typisch voorbeeld is Mac LANE & BIRKHOFF's *Algebra* met een aantal hoofdstukken over categorieën, die in de rest van het boek niet of nauwelijks worden gebruikt.

In de wondertuin der transfiniete cardinaal- en ordinaalgetallen heb ik me, sinds ik er als student een kijkje in mocht nemen, gaarne verlustigd, maar ik heb dit toch steeds als een ongezond plezier beschouwd. Pathologische topologische ruimten, bijvoorbeeld, heb ik, zoveel ik kon, gemeden; jamaar, wat je pathologisch noemt, wordt ook door de smaak bepaald. Nietseparabele metrische ruimten, bijvoorbeeld, was zo'n pathologie; jamaar, de nette ruimte der bijna-periodieke continue functies was, jammer genoeg, niet-separabel. Transfiniete ordinaalgetallen boven, zeg maar, $\varepsilon$ of $\Omega$ waren pathologisch; jamaar om zo'n stelling als HAHN-BANACH te bewijzen had je ze nodig.

U weet inmiddels dat je het overal in de algebra en analyse, waar vroeger de transfiniete ordinaalgetallen onmisbaar leken, zonder ze kunt stellen. De toverstaf waarmee ze de laan zijn uitgestuurd, heet lemma van ZORN. Om bijvoorbeeld aan te tonen, dat elke commutatieve ring R met één een maximaal echt ideaal bezit, beschouw je de verzameling $\Omega$ van alle echte idealen van R en verifieer je dat de vereniging van een geordend deel van $\Omega$ weer tot $\Omega$ behoort; naar ZORN volgt dan dat $\Omega$ een grootste lid bezit, dus dat er een maximaal ideaal is.

ZORN's lemma dateert al van voor de oorlog -men zou het trouwens ook naar HAUSDORFF of KURATOWSKI kunnen noemen-, maar pas na de oorlog is het echt voor een grote schoonmaak in de wiskunde gebruikt. Cardinaal- en ordinaalgetallen zijn er als hulpmiddel door geëlimineerd. Het resultaat is, kan

men zeggen, een machtigheidsvrije wiskunde. Het is wel grappig, dat parallel (of moet ik zeggen, antiparallel) hiermee het machtigheidsbegrip de schoolwiskunde wordt binnengesleurd -tot het opdienen van SCHRÖDER-BERNSTEIN's equivalentiestelling aan elfjarigen toe. Zij die dit voorstaan, verbeelden zich verschrikkelijk modern te zijn, maar het is nu net een moderniteit van een kwart tot een halve eeuw geleden.

U weet zeker wat een *filter* $F$ op een verzemeling V is: $F$ is een niet-lege familie van niet-lege delen van V zodat $V \supset B \supset A \in F \rightarrow B \in F$ en $(A \in F \wedge B \in F) \rightarrow A \cap B \in F$.

Volgens ZORN kan elk filter op V tot een maximaal filter op V worden uitgebreid. Een maximaal filter op V heeft de eigenschap: voor elke $C \subset V$ is óf $C \in F$ óf $V \setminus C \in F$. De familie van alle delen van V, die een vaste $p \in V$ bevatten, is een maximaal filter. Dit soort maximale filters is echter een uitzondering van de maximale filters met lege doorsnee bijvoorbeeld op de verzameling $\mathbb{N}$ der natuurlijke getallen kan men geen enkel voorbeeld expliciet aangeven, ofschoon het er $2^{2^{\aleph_0}}$ zijn. Maximale filters zijn klaarblijkelijk pathologische monstruositeiten. Wel, de Stone-Čech-compactificatie van $\mathbb{N}$ bestaat juist uit de maximale filters; dus is de Stone-Čech-compactificatie als verzameling van monstruositeiten een monstruositeit.

Als men het directe product van lichamen vormt, krijgt men geen lichaam, maar slechts een ring. Zij V zo'n stel lichamen; deel V op in twee deelverzamelingen V' en V"; beschouw een element a van het directe product $K = \otimes_{L \in V} L$, waarvan de L-coördinaten met $L \in V'$ verdwijnen, en een element b, waarvan juist de L-coördinaten met $L \in V''$ verdwijnen; dan toont $ab = 0$ aan dat K nuldelers heeft. Men kan dit repareren door K door een van zijn maximale idealen te delen. De maximale idealen $I$ van K hebben met de maximale filters $F$ van V te maken: bij elke $I$ hoort een $F$ (en omgekeerd) zodat $I$ bestaat uit dié elementen a van K, waarvan de L-coördinaten verdwijnen voor alle L uit een geschikt lid van $F$. Als men hierbij van maximale filters met lege doorsnee uitgaat, krijgt men vreemdsoortige restklassen-lichamen, zogenaamde ultraproducten van het gegeven stel V van lichamen -uiteraard geheel pathologische constructies.

Welnu, dit soort ultraproducten is gebleken een belangrijk hulpmiddel te zijn voor het verkrijgen van zeer concrete getaltheoretische resultaten, zoals in een andere lezing *) zal worden uiteengezet. Onze opvat-

*) Zie de voordracht van F. van der BLIJ (blz. 24).

tingen omtrent hetgeen schappelijk en hetgeen monstrueus in de wiskunde is, zijn in een kwart eeuw wel gewijzigd.

Wat ook onnoemelijk gewijzigd is -en hier begeef ik me op een zonder veel detailkennis te overzien gebied- is de mathematische stijl. Ik wil dit met een aantal voorbeelden duidelijk maken.

Een kwart eeuw geleden was de thans overwegend gebruikelijke verzamelingentheoretische symboliek nog allesbehalve gebruikelijk. Uit die tijd dateert zelfs een topologisch werk waarin vereniging en doorsnede van verzamelingen zonder symboliek, in omgangstaal, worden aangegeven. Van de functie f(x) i.p.v. f te spreken, was een kwart eeuw geleden nog algemeen gebruikelijk; thans is f aan de winnende hand, hoewel f(x) het nog lang niet heeft opgegeven. Als ik de afbeelding f van A in B bedoelde, schreef ik een 35 jaar geleden: de afbeelding fA $\subset$ B, wat tegenwoordig -terecht- onaanvaardbaar zou zijn. Maar deze ontwikkeling is nog geenszins ten einde; het is tegenwoordig nog goede stijl te schrijven (ik citeer uit boeken die befaamd zijn voor exacte stijl):

$$\text{de som } \mu(f) = \sum_{x \in X} \alpha(x) f(x),$$

$$\text{de integraal } I(f) = \int_{-\infty}^{\infty} f(x)dx,$$

$$\text{de open verzameling } G \subset X,$$

enz., waar achter "som", "integraal", "open verzameling", geen som, geen integraal en geen open verzameling, maar een propositie vermeld staat, want zo hebben we immers tekens van de aard van het "=" teken leren interpreteren. Over nog een kwart eeuw zullen zulke misbruiken stellig verdwenen zijn.

Een groep werd een kwart eeuw geleden nog gedefinieerd als "een verzameling, waarin een vermenigvuldiging is gedefinieerd, zodat ...". Dit soort terminologie raakt snel buiten gebruik. De definitie luidt nu "een paar bestaande uit een verzameling en een vermenigvuldiging zodat ...". Maar het is nog steeds goede stijl om bijv. bij de groep-definitie de existentie van een e te eisen zodat ae = ea = a voor alle a, en achteraf de gebonden variabele e te behandelen alsof hij een constante was. Ook deze gewoonte zal voor het scheiden van deze eeuw uitgeroeid zijn.

Men leze alleen maar HILBERT's *Grundlagen der Geometrie* om te beseffen

hoe de stijl veranderd is. Het begint met: "We denken zekere dingen (punten, rechten, vlakken) in zekere relatie", en dan volgen de axioma's. We zouden tegenwoordig zeggen: "Een (euclidische) meetkunde is een drietal verzamelingen (punten, rechten, vlakken) en een stel relaties (incidentie, tussen, congruent, enz.) zodat ...".

Tenslotte het veld winnen van logische symboliek, niet om er logica mee te bedrijven, maar zoals PEANO het had bedoeld, om mathematische beweringen en misschien zelfs stukjes van bewijzen beknopter en duidelijker dan in de omgangstaal mogelijk zou zijn, neer te schrijven. Een kwart eeuw geleden zou dit nog als aanstellerij zijn beschouwd, maar inmiddels hebben we de voordelen ervan leren appreciëren, vooral waar het op kwantoren en hun volgorde aankomt. Via de logische symboliek hebben we ook geleerd in de omgangstaal meer aandacht te besteden aan kwantoren in gevallen waar wij het vroeger vaak wel geloofden.

Ik beperk me tot deze enkele voorbeelden voor het meer bewust beleven en opzettelijk ordenen van de mathematische taal -voorproefjes van, naar ik meen, wat ons in het resterende kwart van deze eeuw aan taalkundige ontwikkelingen te wachten staat.

MC SYLLABUS 18, 1973, 17-29

# GETALTHEORIE 1946-1971

F. VAN DER BLIJ *)

*Inleiding*

We willen aan de hand van een aantal voorbeelden, gekozen uit verschillende delen van de getaltheorie, iets laten zien van de ontwikkeling van dit onderdeel van de wiskunde in de laatste vijfentwintig jaar.

Getaltheorie is een goed voorbeeld van zuivere wiskunde; zijn beoefenaar stelt zich een probleem, en in het vaak voorkomende geval dat dit niet opgelost kan worden, vervangt hij het probleem door een ander, analoog, gegeneraliseerd, gespecialiseerd probleem dat beter oplosbaar lijkt.

Daarom valt deze voordracht in twee hoofdstukken uiteen. In het eerste spreken wij over klassieke problemen, waarvan enkele werden opgelost en bij andere nauwelijks vooruitgang werd geboekt. In het tweede spreken we over generalisaties en analogieën. Bij de resultaten zullen we enige aandacht proberen te schenken aan de vraag of de oplossing het resultaat was van een lange ontwikkeling (met bijv. steeds betere methoden) of eigenlijk even goed al vòòr 1946 gevonden had kunnen worden, omdat het materiaal voor de oplossing van het probleem al lang gereed lag.

*) Met dank aan D.C. van LEYENHORST, die assistentie verleende bij de opstelling van dit overzicht.

# HOOFDSTUK I. KLASSIEKE PROBLEMEN

## 1. *Analytische getaltheorie*

Deze had een zeer grote bloei vòòr 1946. Een van de vraagstellingen is om arithmetisch gedefinieerde functies met analytische hulpmiddelen te beschrijven, bijv. om asymptotisch gedrag van deze functies te onderzoeken, afwijkingen van benaderende formules te schatten, enz.

a) Als eerste voorbeeld kiezen we het aantal (rationale) priemgetallen kleiner dan of gelijk aan x. We geven dit aantal aan met $\pi(x)$; een klassiek resultaat is

$$(1.1) \qquad \lim_{x\to\infty} \frac{\pi(x)\ \log x}{x} = 1.$$

Meer informatie geeft

$$(1.2) \qquad \pi(x) = \int_2^x \frac{dt}{\log t} + \varepsilon(x),$$

met

$$(1.3) \qquad \varepsilon(x) = O(x\, e^{-\alpha \log^{\frac{1}{2}} x}).$$

Maar er zijn betere resultaten; in LANDAU's *Vorlesungen* vinden we

$$(1.4) \qquad \varepsilon(x) = O(x\, e^{-\alpha \log^{\frac{1}{2}} x\ (\log\log)^{\frac{1}{2}} x}).$$

In 1958 kondigden VINOGRADOV en KOROBOV aan dat

$$(1.5) \qquad \varepsilon(x) = O(x\, e^{-\alpha \log^{3/5} x}),$$

maar een bewijs werd niet gepubliceerd. Het beste, mij bekende resultaat op dit ogenblik is:

$$(1.6) \qquad \varepsilon(x) = O(x\, e^{-\alpha \log^{3/5} x\ (\log\log x)^{-1/5}}).$$

We moeten constateren dat tussen 1946 en 1971 geen grote vooruitgang geboekt

is in de richting van het vermoeden van RIEMANN

$$(1.7) \qquad \varepsilon(x) = O(x^{\frac{1}{2}+\varepsilon}).$$

Toch is er in de periode 1946-1971 wel iets te melden over (1.1). De klassieke bewijzen van (1.1) (en a fortiori ook van (1.2), (1.3) e.v.) gebruikten vrij gecompliceerde methoden uit de complexe functietheorie. De esthetici onder de zuiver wiskundigen zochten al lang naar een "elementair" bewijs, bijv. alleen van combinatoriek gebruik makend. ERDÖS en SELBERG construeerden zo'n elementair bewijs in 1948, gebruik makende van de formule

$$(1.8) \qquad \sum_{p\le x} \log^2 p + \sum_{pq\le x} \log p \log q = 2x \log x + O(x).$$

De constructie van dit elementaire bewijs kan aangemerkt worden als een belangrijk resultaat op het gebied van de klassieke getaltheorie in de laatste vijfentwintig jaar. Alleen is er geen enkele fundamenteel nieuwe theorie bij nodig geweest. Gevaarlijk geformuleerd: dit bewijs had evengoed vòòr 1946 geconstrueerd kunnen worden.

b) De belangrijkste resultaten bij het tweede voorbeeld liggen even vòòr 1946. Toch vermelden we het als voorbeeld van analytische getaltheorie, in verband met analogie met het derde voorbeeld. Laat p(n) het aantal partities van een getal n voorstellen. Dan geldt

$$(1.9) \qquad \sum_{n=0}^{\infty} p(n)\, x^n = \prod_{k=1}^{\infty} (1-x^k)^{-1}.$$

Kan men nu, door middel van analytische methoden, iets zeggen over de coëfficiënten van de in (1.9) gedefinieerde machtreeks? HARDY en RAMANUJAN bewezen in 1918

$$(1.10) \qquad p_n = \frac{1}{2\pi\sqrt{2}} \sum_{k=1}^{\alpha\sqrt{n}} k^{\frac{1}{2}}\, A_k(n)\, g'(n) + O(n^{-\frac{1}{4}})$$

met

$$g(\tau) = (\tau - \tfrac{1}{24})^{-\frac{1}{2}}\, e^{\frac{\pi}{3k}\sqrt{6(\tau-\frac{1}{24})}}, \qquad (0<\alpha<\infty),$$

en $A_k(n)$ is een (met Dedekind-sommen gebouwde) som van eenheidswortels.

RADEMAKER bewees, in 1937, dat een kleine variatie van de functie g de

mogelijkheid gaf p(n) als een oneindige reeks te representeren:

$$(1.11) \qquad g(\tau) = 2(\tau - \tfrac{1}{24})^{-\frac{1}{2}} \sinh \frac{\pi}{3k} \sqrt{6(\tau - \tfrac{1}{24})}$$

en $\alpha = \infty$ in (1.10). Hieruit volgt

$$(1.12) \qquad p(n) \sim \frac{1}{12n} \sqrt{3n}\, e^{(\pi\sqrt{6n})/3}.$$

Na 1946 was er niet veel meer te verbeteren; een arithmetisch gedefinieerde functie was beschreven met analytische middelen. Alleen wil ik een variant, door PETERSON in 1950 gepubliceerd, vermelden omdat deze in veel ruimer verband belangrijk bleek:

$$(1.13) \qquad p(n) = 2\pi i\, (24n-1)^{-\frac{3}{4}} \sum_{m=1}^{\infty} \frac{1}{m} W_m(n)\, J_{3/2}\left(-\frac{\pi i}{6m} \sqrt{6(n-\tfrac{1}{24})}\right),$$

waarbij $W_m(n)$ een gegeneraliseerde Kloosterman-som is en J de Besselfunctie voorstelt. Het blijkt dat een groot aantal arithmetische functies (die samenhangen met de groep van de modulaire transformaties) uitgedrukt kan worden in Besselfuncties. De in de laatste jaren uitgevoerde abstracte analyse op de modulaire groep maakt de rol van de z.g. bolfuncties behorende bij deze modulaire groep, naast Besselfuncties ook meer algemene Whittakerse functies, duidelijk.

c) Als derde voorbeeld kiezen we de representatie van natuurlijke getallen door definiete kwaternaire kwadratische vormen. Laat $r_F(n)$ het aantal representaties van n door F zijn. Dan geldt

$$(1.14) \qquad r_F(n) = S_F(n) + \varepsilon(n),$$

waarbij $S_F(n)$ de som van de zogenaamde singuliere reeks is, een via approximatieve methoden verkregen analytische uitdrukking, die ook algebraïsch te definiëren is (product van "locale" aantallen representaties), en expliciet in functies als sommen van delers e.d. uitgedrukt kan worden. Verder geldt

$$S_F(n) \sim \alpha n \qquad (\alpha \neq 0).$$

In 1927 bewees KLOOSTERMAN

(1.15) $\varepsilon(n) = O(n^{1-\rho+\varepsilon})$ met $\rho = \frac{1}{8}$ .

Men formuleerde al spoedig het vermoeden dat (1.15) moet gelden met $\rho = \frac{1}{2}$. In 1939 bewees RANKIN (1.15) met $\rho = \frac{1}{5}$. In 1948 bewees A. WEIL, gebruik makend van resultaten uit de algebraïsche meetkunde, een schatting voor Kloosterman-sommen (zie boven), die ingevuld in een enigszins analoog aan (1.13) gebouwde som voor $\varepsilon(n)$ voerde tot (1.15) met $\rho = \frac{1}{4}$.

Gebruik makend van geheel andere methoden uit de theorie van de algebraïsche functies bewees EICHLER in 1954 de formule (1.15) met $\rho = \frac{1}{2}$. Dit is een voorbeeld van een bewijs van een oud vermoeden dat gegeven werd met methoden die in de daaraan voorafgaande decennia nieuw ontwikkeld waren.

## 2. *Algebraïsche getaltheorie*

Het onderzoek van de arithmetische structuur van eindige algebraïsche uitbreidingen van de rationale getallen is een centraal onderwerp in de algebraïsche getaltheorie. Daar in het algemeen niet ieder ideaal hoofdideaal is, ligt het onderzoek naar ideaalkassen, geconstrueerd met een op de deelverzameling van de hoofdidealen gebouwde equivalentierelatie, voor de hand. Op natuurlijke wijze vormen deze ideaalklassen een groep. Een typische vraagstelling is, om arithmetisch gedefinieerde groepen op andere wijze te beschrijven.

De klasselichamentheorie legt een verband tussen de groep van de ideaalklassen en bijv. Galoisgroepen van algebraïsche uitbreidingen. Het probleem om voor niet-abelse uitbreidingen een adequate theorie te vinden is in de afgelopen 25 jaar zijn oplossing ogenschijnlijk niet veel naderbij gekomen. Een belangrijk element is de generalisatie naar oneindige algebraïsche uitbreidingen, waarbij de Galoisgroep van een passende topologie werd voorzien. De methoden van de cohomologietheorie bleken zeer bruikbaar om resultaten en problemen uit de klassieke theorie opnieuw te formuleren. In plaats van deze ontwikkelingen te schetsen wil ik twee problemen bespreken waarvoor in de laatste kwart eeuw wel een definitieve oplossing gevonden is.

a) Het "Klassenkörperturm"-probleem handelt over opeenvolgende eindige algebraïsche uitbreidingen van een algebraïsch getallichaam (dat is een eindige algebraïsche uitbreiding van de rationale getallen). Laat k een getallichaam zijn, waarin het klasseaantal groter dan 1 is, d.w.z. niet ieder ideaal is hoofdideaal. Het Hilbert-klasselichaam $k_1$ van dit getallichaam k is een eindige algebraïsche uitbreiding van k (met een Galoisgroep t.o.v. k die isomorf is met de groep van de ideaalklassen van k), waarin ieder ideaal van k

een hoofdideaal wordt, d.w.z. ieder ideaal van k bestaat uit veelvouden van één element van het klasselichaam $k_1$. Maar het klasseaantal van $k_1$ kan weer groter dan 1 zijn. Dan construeert men analoog een lichaam $k_2$, enz.

Zo ontstaat een rij ("Turm") van lichamen $k \subset k_1 \subset k_2 \subset \ldots$ . Het probleem is nu of iedere op deze manier geconstrueerde rij afbreekt, d.w.z. of ieder getallichaam in te bedden is in een getallichaam, waarin ieder ideaal hoofdideaal is. Of zijn er oneindige klasselichamentorens? Voor dit probleem vonden ŠAFEREVICH en GOLOD in 1964 een antwoord. De grondgedachte berust op de constructie van een vrij eenvoudige arithmetische functie, die schattingen levert verband houdende met klasseaantallen.

Een gevolg van deze schattingen is dat een kwadratisch getallichaam, ontstaan uit de rationale getallen door adjunctie van de vierkantswortel uit een getal met voldoende veel verschillende priemfactoren voldoet. Zo zijn $\mathbb{Q}(\sqrt{2.3.5.7.11.13.17.19})$ en $\mathbb{Q}(\sqrt{-2.3.5.7.11.13})$ voorbeelden van startpunten van oneindige klasselichamentorens.

b) Een ander, in de laatste vijfentwintig jaar opgelost probleem is de vraag voor welke imaginair kwadratische getallichamen het klasseaantal 1 is. In de lichamen $\mathbb{Q}(\sqrt{-D})$ met D = 1,2,3,7,11 bestaat het principe van deling met rest, waaruit is af te leiden dat ieder ideaal hoofdideaal is. Ook in $\mathbb{Q}(\sqrt{-D})$ met D = 19,43,67,163 is het klasseaantal 1. Vóór 1946 werd reeds bewezen dat nog ten hoogste één imaginair kwadratisch getallichaam met klasseaantal 1 kan bestaan.

In 1952 gaf HEEGNER een bewijs dat zo'n lichaam niet bestond, maar het bewijs bevatte een lacune. In 1967 gaf STARK een volledig bewijs. Hij gebruikte analytische middelen, o.a. reeksen

$$(2.1) \qquad \sum_{(x,y)\neq(0,0)} \frac{\chi(ax^2+bxy+cy^2)}{(ax^2+bxy+cy^2)^s}$$

met een karakter $\chi$.

Kort daarna gaven o.a. DEURING en SIEGEL bewijzen van het niet bestaan van een tiende imaginair kwadratisch lichaam met klasseaantal 1, volgens de door WEBER en HEEGNER aangeduide methode (met elliptische functies). Merkwaardig is dat deze bewijzen alle voeren tot een diophantische vergelijking:

$$(2.2) \qquad x^2 = 2y(y^3-1)$$

waarvan de (eindig vele) oplossingen lichamen van het gezochte type geven.

Met het feit dat $\mathbb{Q}(\sqrt{-163})$ klasseaantal 1 heeft, hangt samen dat $x^2 + x + 41$ (discriminant -163) voor kleine waarden van x steeds priemgetallen geeft en dat $e^{\pi\sqrt{163}}$ minder dan $10^{-12}$ van een geheel rationaal getal verschilt. Men zou nog kunnen opmerken dat de na 1965 gevonden bewijzen van het bestaan van niet meer dan 9 imaginair kwadratische lichamen met klasseaantal 1 geen wezenlijk nieuwe, recent ontwikkelde methoden gebruiken.

### 3. *Diophantische vergelijkingen*

Laat F een veelterm in n variabelen met rationale coëfficiënten zijn. Heeft F(x) = 0 een rationale oplossing? En zo ja, hoeveel? Heeft F(x) = 0 een gehele oplossing? Een algemene theorie is niet te geven. Voor het geval dat door de vergelijking een kromme in een affien of projectief vlak gedefinieerd wordt, kan iets meer gezegd worden; vooral, omdat de rationale punten op een algebraïsche kromme met genus 1 een groep vormen, terwijl MORDELL bewees dat deze groep slechts eindig veel voortbrengenden heeft. Een klassiek stelling van THUE en SIEGEL leert dat op een kromme met geslacht ≥ 1 slechts eindig veel punten met gehele rationale coördinaten kunnen liggen. Het vermoeden dat op krommen met genus > 1 slechts eindig veel rationale punten liggen, is ook in de afgelopen vijfentwintig jaar nog niet bewezen. Dit zou tot gevolg hebben dat $x^n + y^n = z^n$ voor n > 2 slechts eindig veel oplossingen zou hebben. Wel bewees MUMFORD in 1965 dat het aantal rationale punten P op een kromme met genus > 1 en met "hoogte" h(P) < x, kleiner is dan A log x + B met van x onafhankelijke A en B. Gevolg: het aantal gehele x, y, z met $|z| \leq N$ en $x^n + y^n = z^n$ (n>2) is kleiner dan A log log N + B.

Op één onderdeel van de diophantische vergelijkingen wil ik nader ingaan. Laat F nu een homogene vorm in n variabelen van de graad d voorstellen, met gehele rationale coëfficiënten. Als F(x) = 0 een niet-triviale gehele rationale oplossing heeft, moet ook $F(x) \equiv 0 \pmod{p}$ voor iedere p een niet-triviale oplossing hebben. De stelling dat iedere homogene vorm in meer dan (d+1) variabelen een niet-triviaal nulpunt heeft, is een stapje. De stelling dat, als over een lichaam k iedere vorm in $(d^e+1)$ variabelen een niet-triviaal nulpunt heeft, over k(t), het lichaam van de rationale functies over k, iedere vorm in $(d^{e+1}+1)$ variabelen een niet-triviaal nulpunt heeft, is een ander boeiend resultaat. Dat voor p-adische lichamen bewezen werd dat iedere vorm van de graad d in meer dan $(d^2+1)$ variabelen voor d = 2,3,5,7,11 een niet-triviaal nulpunt heeft, leidde tot het vermoeden dat deze uitspraak voor alle d zou gelden.

In 1965 bewezen AX en KOCHEN dat, bij gegeven d, iedere vorm in $(d^2+1)$ variabelen over alle p-adische lichamen met voldoend grote p een niet-triviaal nulpunt bezit. Dit bewijs gebruikt allerlei recente methoden, o.a. ultraproducten *), formele logica e.a.

Een in 1966 door TERJANIAN gegeven tegenvoorbeeld van de algemene uitspraak, n.l. een vorm van de graad 4, in 18 variabelen, die over het 2-adische lichaam geen niet-triviaal nulpunt heeft, is echter onafhankelijk van recente theorievorming.

## 4. *Diophantische approximaties*

Bij ieder reëel getal $\alpha$ bestaan oneindig veel onvereenvoudigbare breuken $\frac{p}{q}$ zodat

$$(4.1) \qquad \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2} .$$

Als $\alpha$ een algebraïsch getal van de graad $\nu$ is, geldt voor iedere onvereenvoudigbare $\frac{p}{q}$ dat

$$(4.2) \qquad \left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^\nu} .$$

Bij een gegeven getal $\alpha$ kan men zoeken naar het supremum $\bar{\mu}(\alpha)$ van de getallen $\mu$ zodat

$$(4.3) \qquad \left|\alpha - \frac{p}{q}\right| < \frac{c}{q^\mu}$$

oneindig veel oplossingen p,q met (p,q) = 1 heeft.

Als $\alpha$ kwadratisch algebraïsch is, geldt $\bar{\mu}(\alpha) = 2$. Uit (4.2) volgt dat als $\alpha$ algebraïsch van de graad $\nu$ is, geldt $\bar{\mu}(\alpha) \leq \nu$. In 1908 bewees THUE $\bar{\mu}(\alpha) \leq \frac{1}{2}\nu+1$; in 1921 bewees SIEGEL $\bar{\mu}(\alpha) < 2\sqrt{\nu}$; in 1947 bewees DYSON $\bar{\mu}(\alpha) < \sqrt{2\nu}$; in 1955 bewees ROTH $\bar{\mu}(\alpha) = 2$ voor alle algebraïsche getallen.

Het door BAKER in 1968 bereikte resultaat over diophantische approximaties geeft geen verscherping, maar maakt optredende constanten effectief berekenbaar. Daar die diophantische approximatie voor het bewijzen van de eindigheid van aantallen gehele punten op algebraïsche krommen een rol

---

*) Zie het referaat van H. FREUDENTHAL (blz. 13).

speelt, kunnen nu ook bij bepaalde diophantische vergelijkingen expliciet bovengrenzen voor het aantal oplossingen gegeven worden.

Bijvoorbeeld, als (x,y) een gehele oplossing is van

$$y^2 = x^3 + k \tag{4.4}$$

dan geldt

$$\log \max (|x|,|y|) < 10^{10} |k|^{10000}.$$

De methode van BAKER berust op de toepassing van lineaire vormen in de logaritmen van algebraïsche getallen.

## 5. *Diversen*

De ingebruikname van de computer heeft een groot aantal half getaltheoretische, half combinatorische resultaten opgeleverd; niet alleen meer decimalen van $\pi$ en e of verder onderzoek van MERSENNE en FERMAT getallen, maar ook eindige groepen, eindige meetkunden, grieks-latijnse vierkanten e.d.

Een groot aantal vermoedens over gehele of rationale punten op krommen met genus 1 (of op abelse variëteiten) werd gestimuleerd vanuit numeriek onderzoek.

Bij dit overzicht ontbreken enkele onderdelen van de getaltheorie, waaronder transcendentievragen (van belang zijn de resultaten van SPRINDŽUK over MAHLER's klassificatie), additieve getaltheorie i.h.b. de resultaten van MANN over dichtheden, resultaten in de richting van het vermoeden van GOLDBACH.

# HOOFDSTUK II. GENERALISATIES

## 6. *Vraagstelling*

Voortgekomen uit de klassieke getaltheorie zijn vele gebieden van algebraïsch onderzoek.

a) Naast getallichamen (eindige algebraïsche uitbreidingen van de rationale getallen) beschouwt men functielichamen (eindige algebraïsche uitbreidingen van het lichaam van de rationale functies). Daar de algebraïsche theorie een groot deel parallel loopt, ligt het voor de hand problemen over te brengen. De theorie van klasselichamen, van onderzoek naar priemidealen, van diophantische vergelijkingen kon overgebracht worden. In bepaalde gevallen kon een niet bewezen vermoeden voor getallichamen wel bewezen worden voor functielichamen.

Over de voor functielichamen geconstrueerde $\zeta$-functie formuleerde WEIL enkele fundamentele vermoedens, o.a. de rationaliteit als functie van $p^s$ en een analogon van het vermoeden van Riemann. DWORK slaagde er in, met een ingenieuze combinatie van reële en p-adische analyse, de rationaliteit van op analoge wijze gegeneraliseerde $\zeta$-functies te bewijzen. MANIN en GRAUERT bewezen voor functielichamen stellingen over het aantal rationale punten op algebraïsche krommen.

b) In het lichaam van de p-adische getallen laat zich eenvoudig een ring van gehele p-adische getallen aanwijzen. In hoeverre zijn de problemen uit de ring van de gehele rationale getallen over te brengen naar het analogon van de gehele p-adische getallen? Voor diophantische vergelijkingen en voor diophantische approximaties zijn vele stellingen overgebracht. Ook de algebraïsche problemen (bijv. theorie van de klasselichamen) zijn in het p-adische geval opgebouwd.

c) Natuurlijk waren de in paragraaf 1 gemaakte opmerkingen over kwaternaire kwadratische vormen een deelgebied uit de theorie van de kwadratische vormen over vectorruimten van willekeurige dimensie. Bij dit onderwerp heeft de theorie steeds weer een ander aanzien gekregen. Na de klassieke opbouw, en dan denk ik aan MINKOWSKI, komen p-adische methoden (HASSE) naast de analytische (HARDY-LITTLEWOOD). Een meer algebraïsche opbouw komt bij SIEGEL. Het boek van EICHLER (1952) legt duidelijk het verband met de orthogonale

groepen. De ontwikkelingen door TAMAGAWA en KNESER en in 1965 de twee artikelen van A. WEIL in Acta Mathematica wijzen op een steeds meer groepentheoretische behandeling.

Vanuit de topologie is een nieuwe belangstelling voor de gehele kwadratische vormen gegroeid. De recent ontwikkelde K-theorie geeft een zeer ruime generalisatie van de klassieke theorie van de kwadratische vormen.

Aan de andere kant spelen vragen als in paragraaf 1 onder c) gesteld over schattingen van resttermen nog steeds een rol. Voor vormen in 2k variabelen wordt de singuliere reeks van de orde $n^{k-1}$. Voor de restterm wordt de schatting

$$(6.1) \qquad \varepsilon(n) = O(n^{\frac{1}{2}k-\rho+\varepsilon}).$$

De resultaten onder 1c) vermeld voor $\rho = \frac{1}{8}$, $\rho = \frac{1}{5}$ en $\rho = \frac{1}{4}$ laten zich direct generaliseren.

Het resultaat van EICHLER voor $\rho = \frac{1}{2}$ laat zich tot op heden echter *niet* generaliseren. In 1969 publiceerde DE BRANGES een bewijs voor de schatting $\rho = \frac{1}{2}$ in het algemene geval. Dit is echter onjuist en het is naar alle waarschijnlijkheid ook niet te repareren.

Opmerkelijk is dat na voorbereidingen door SATO en IHARA het aan DELIGNE in 1968 gelukte te bewijzen dat als de vermoedens van WEIL over de $\zeta$-functie van algebraïsche variëteiten (generalisaties van de $\zeta$-functies van functielichamen, die bij algebraïsche krommen behoren) juist zijn, voor de formule (6.1) de schatting met $\rho = \frac{1}{2}$ bewezen kan worden.*)

d) Problemen rond de priemgetalstelling en het vermoeden van GOLDBACH hebben gevoerd tot de introductie van pseudo-priemgetallen, rijen getallen $p_1, p_2, p_3, \ldots$ met voorgeschreven dichtheid. Men kan dan de verzameling van de sommen van twee van deze getallen onderzoeken of ook de halfgroep door de vermenigvuldiging van deze getallen voortgebracht. Merkwaardig is een resultaat van BEURLING, DIAMOND e.a.

Als $P = \{p_1, p_2, p_3, \ldots\}$ en N de door P voortgebrachte semigroep is en

$$\#\{n \mid n \in N \text{ en } n < x\} = Ax + O(x \log^{-\gamma} x), \quad \gamma > 1\tfrac{1}{2}$$

dan

$$\#\{p \mid p \in P \text{ en } p < x\} \sim \frac{x}{\log x}.$$

*) In 1973 gelukte het aan DELIGNE om de betreffende vermoedens van WEIL te bewijzen en daarmee de schatting van (6) met $\rho=\frac{1}{2}$ af te leiden.

(Er is een reeks $p_1, p_2, \ldots$ met $\gamma = 1\frac{1}{2}$ waarvoor de analoge uitspraak onjuist is.)

e) De resultaten van statistische en ergodische methoden in de getaltheorie moeten onbesproken blijven. De representatie van getallen door ternaire kwadratische vormen, die zich in verband met convergentieproblemen moeilijk met de analytische methoden laten behandelen, werd nauwkeurig met ergodentheorie behandeld door LINNIK (1968).

## 7. *Samenvatting*

De ontwikkeling van de getaltheorie in de laatste 25 jaar te overzien is niet eenvoudig. Grote sensationele vondsten op het gebied van de klassieke analytische of algebraïsche getaltheorie zijn eigenlijk niet aan te wijzen. Van veel belang is het samengaan van beide. Dit bleek bij de theorie van de kwadratische vormen; eerst samen met orthogonale groepen, later gegeneraliseerd tot algebraïsche groepen. De interpretatie van de singuliere reeks (uit de analytische approximatie verkregen) in termen van algebra en groepentheorie, de interpretatie van Besselfuncties, zoals in de partitieformule, in termen van bolfuncties behorende bij de modulaire groep zijn fundamentele ontdekkingen.

Daarnaast de toepassing van logica in de getaltheorie; we noemden de stelling van AX en KOCHEN over niet-triviale oplossingen van homogene vergelijkingen over p-adische lichamen en nu wijzen we nog op de oplossing van HILBERT's tiende probleem over de oplossingen van diophantische vergelijkingen met logische middelen, waarover in een andere voordracht bericht zal worden. *)

*) Zie de voordracht van J.J. de IONGH (blz. 39 e.v.).

*Literatuur*

We zien af van een literatuurlijst. We vermelden slechts enkele vrij recent verschenen publicaties waarin men alle verwijzingen kan vinden.


Bij paragraaf 1

R. AYOUB, *An introduction to the analytic theory of numbers*, Mathematical Surveys No. 10, Amer. Math. Soc., Providence (R.I.), 1963.

A. WALFISZ, *Weylsche Exponentialsummen in der neuere Zahlentheorie*, Mathematische Forschungsberichte no.15, VEB Deutscher Verlag der Wissenschaften, Berlin, 1963.

K. PRACHAR, *Primzahlverteilung*, Springer-Verlag, Berlin etc., 1957.

Bij paragraaf 2

J.W.S. CASSELS & A. FRÖHLICH (eds.) *Algebraic number theory*, Acad. Press, London, 1967.

M. Deuring *Imaginaire quadratische Zahlkörper mit der Klassenzahl Eins*, Invent. Math., 5 (1968) 169-179.

H.M. STARK, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J., 14 (1967) 1-27

C.L. SIEGEL, *Zum Beweise des Starkschen Satzes*, Invent. Math., 5 (1968) 180-191.

Bij paragraaf 3

L.J. MORDELL, *Diophantine equations*, Acad. Press, London, 1969.

W.J. LE VEQUE, *Studies in number theory*, Prentice-Hall, Englewood Cliffs, 1969.

J.-P. SERRE, *Cours d'arithmétique*, 1970.

Bij paragraaf 6

Yu.V. LINNIK, *Ergodic properties of algebraic fields*, Springer-Verlag, Berlin etc., 1968.

MC SYLLABUS 18, 1973, 31-37

# VAN RECREATIE NAAR TOEPASSING, VAN MEETKUNDE NAAR CODES, GRAFEN EN GROEPEN

J.J. SEIDEL

## 1. *Latijnse vierkanten*

### *1.1. Definitie*

Een Latijns vierkant van de orde n is een vierkante matrix, waarvan elke rij en elke kolom een permutatie is van n symbolen $\{1,2,\ldots,n\}$. Twee Latijnse vierkanten van de orde n zijn orthogonaal, als hun superpositie elk van de $n^2$ geordende paren $(i,j)$, met $i,j \in \{1,2,\ldots,n\}$, precies éénmaal bevat.

*Voorbeeld*

De volgende Latijnse vierkanten zijn orthogonaal:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix} \quad \text{, wegens} \quad \begin{bmatrix} 11 & 22 & 33 & 44 \\ 23 & 14 & 41 & 32 \\ 34 & 43 & 12 & 21 \\ 42 & 31 & 24 & 13 \end{bmatrix}$$

### *1.2. Toepassingen*

*1.2.1.* Uit elk van de landen Engeland, Frankrijk, Rusland en Amerika worden een generaal, een kolonel, een kapitein en een luitenant afgevaardigd. Kunnen deze 16 officieren worden opgesteld in een $4 \times 4$ vierkant, zodat elke rang en elke nationaliteit precies éénmaal voorkomt in elke rij en in elke

kolom? De oplossing wordt gegeven door een paar orthogonale Latijnse vierkanten van de orde 4.

*1.2.2.* Wij wensen de opbrengst van 4 graansoorten te vergelijken. Het proefveld wordt verdeeld in 16 vierkante stukken, gearrangeerd in 4 rijen en 4 kolommen. De 4 graansoorten worden over deze stukken verdeeld volgens een Latijns vierkant, zodat elke graansoort éénmaal in elke rij en in elke kolom wordt geplant. Zo kunnen systematische verschillen in de vruchtbaarheid van de grond worden geëlimineerd. In hetzelfde experiment kunnen ook vier verschillende bemestingsmethoden worden onderzocht, wanneer deze methoden worden toegepast volgens een Latijns vierkant orthogonaal met het vorige, zodat elke methode éénmaal op elke graansoort wordt toegepast.

*1.3. Het vermoeden van Euler weerlegd*

In 1782 formuleerde EULER het volgende vermoeden:

er bestaat geen paar orthogonale Latijnse vierkanten van orde $n \equiv 2 \pmod 4$, $n > 2$.

Dit vermoeden werd in 1900 voor $n = 6$ bevestigd door TARRY. Voor alle andere n werd het echter in 1959 weerlegd door BOSE, SHRIKHANDE en PARKER, die de volgende stelling bewezen:

STELLING. Er bestaat een paar orthogonale Latijnse vierkanten van elke orde $n \neq 6$.

*Voorbeeld*

$$\begin{bmatrix} 0 & 6 & 5 & 4 & 7 & 8 & 9 & 1 & 2 & 3 \\ 9 & 1 & 0 & 6 & 5 & 7 & 8 & 2 & 3 & 4 \\ 8 & 9 & 2 & 1 & 0 & 6 & 7 & 3 & 4 & 5 \\ 7 & 8 & 9 & 3 & 2 & 1 & 0 & 4 & 5 & 6 \\ 1 & 7 & 8 & 9 & 4 & 3 & 2 & 5 & 6 & 0 \\ 3 & 2 & 7 & 8 & 9 & 5 & 4 & 6 & 0 & 1 \\ 5 & 4 & 3 & 7 & 8 & 9 & 6 & 0 & 1 & 2 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & 7 & 8 & 9 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 & 9 & 7 & 8 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 & 8 & 9 & 7 \end{bmatrix} \quad \begin{bmatrix} 0 & 9 & 8 & 7 & 1 & 3 & 5 & 2 & 4 & 6 \\ 6 & 1 & 9 & 8 & 7 & 2 & 4 & 3 & 5 & 0 \\ 5 & 0 & 2 & 9 & 8 & 7 & 3 & 4 & 6 & 1 \\ 4 & 6 & 1 & 3 & 9 & 8 & 7 & 5 & 0 & 2 \\ 7 & 5 & 0 & 2 & 4 & 9 & 8 & 6 & 1 & 3 \\ 8 & 7 & 6 & 1 & 3 & 5 & 9 & 0 & 2 & 4 \\ 9 & 8 & 7 & 0 & 2 & 4 & 6 & 1 & 3 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & 8 & 9 & 7 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 & 9 & 7 & 8 \end{bmatrix}$$

## 2. *Het probleem van Kirkman*

### 2.1. *Voorbeeld*

T.P. KIRKMAN stelde in 1847 het volgende probleem: vijftien schoolmeisjes wandelen op elk van de 7 dagen van de week in 5 rijen van 3. Is het mogelijk dat elk meisje met elk ander meisje slechts éénmaal per week in dezelfde rij loopt?

Dit probleem heeft 7 oplossingen, waarvan wij er één aanduiden:

| zondag | maandag | dinsdag | woensdag | donderdag | vrijdag | zaterdag |
|---|---|---|---|---|---|---|
| 0, 5,10 | 0, 1, 4 | 1, 2, 5 | 4, 5, 8 | 2, 4,10 | 4, 6,12 | 10,12, 3 |
| 1, 6,11 | 2, 3, 6 | 3, 4, 7 | 6, 7,10 | 3, 5,11 | 5, 7,13 | 11,13, 4 |
| 2, 7,12 | 7, 8,11 | 8, 9,12 | 11,12, 0 | 6, 8,14 | 8,10, 1 | 14, 1, 7 |
| 3, 8,13 | 9,10,13 | 10,11,14 | 13,14, 2 | 7, 9, 0 | 9,11, 2 | 0, 2, 8 |
| 4, 9,14 | 12,14, 5 | 13, 0, 6 | 1, 3, 9 | 12,13, 1 | 14, 0, 3 | 5, 6, 9 |

Deze oplossing wordt verkregen uit de binaire projectieve ruimte PG(3,2), waarvan de 15 punten als de meisjes, en de 35 lijnen als de rijen worden geïnterpreteerd. Dan moeten worden gevonden 7 spreads (i.e. 7 verzamelingen van 5 lijnen), waarvan elke alle 15 punten bevat. Daartoe worden de punten van PG(3,2) voorgesteld als de machten van een primitief element x van het Galois lichaam $GF(2^4)$. De vermenigvuldiging met x verdeelt de 35 lijnen in drie klassen, van afmeting 5, 15, 15, namelijk

$$\{x^h, x^{h+5}, x^{h+10}\},\ \{x^i, x^{i+1}, x^{i+4}\},\ \{x^j, x^{j+2}, x^{j+8}\}.$$

Een beetje puzzelen geeft dan bovenstaande oplossing.

### 2.2. *Het algemene probleem*

Arrangeer n schoolmeisjes (n is een oneven veelvoud van 3) op $\frac{1}{2}(n-1)$ dagen in rijen van 3, zodat elk paar meisjes slechts éénmaal in dezelfde rij loopt.

RAY-CHAUDHURI en WILSON bewezen in 1969, dat dit probleem voor elke n kan worden opgelost.

## 3. *De codes van Golay*

### 3.1. *Lineaire codes*

Een lineaire (n,k) code over GF(q) is een lineaire deelruimte van dimensie k van de vectorruimte V(n,q) van dimensie n over het Galois lichaam GF(q). De vectoren van de deelruimte heten codewoorden. De Hamming afstand tussen twee vectoren is het aantal coördinaten waarin zij verschillen. Het gewicht van een vector is het aantal coördinaten $\neq 0$. Wanneer van een code alle codewoorden $\neq 0$ gewicht $\geq 2e+1$ hebben, dan heet de code e-error-correcting.

*Voorbeeld*

Het vlak in V(4,3), opgespannen door

$$\underline{f} = (1,0,1,1), \qquad g = (0,1,1,1)$$

is een ternaire lineaire (4,2) code, die 1-error-correcting is.

### 3.2. *De binaire Golay code*

Zij I de eenheidsmatrix, j de al-één vector van orde 11. Zij

$$Q = \text{circul}\,(0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0).$$

De 12 rijen van de matrix

$$\begin{bmatrix} 0 & 0^T & 1 & j^T \\ j & I & j & Q \end{bmatrix}$$

genereren een lineaire (24,12) code over GF(2). Deze code heeft $2^{12}$ codewoorden met de volgende gewichtsverdeling:

| aantal | 1 | 759 | 2576 | 759 | 1 |
|---|---|---|---|---|---|
| gewicht | 0 | 8 | 12 | 16 | 24 |

Door weglating van één coördinaat wordt verkregen een 3-error-correcting (23,12) code; dit is de binaire Golay code. Deze code is perfect; de disjuncte bollen met straal 3 om de codewoorden vullen V(23,2) geheel wegens

$$2^{23} = 2^{12}\,(1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}).$$

De code houdt verband met de Mathieu groepen $M_{24}$ en $M_{23}$, en met het Steiner systeem (24,8,5).

*3.3. Bolstapeling in $\mathbb{R}_{24}$*

De lineaire (24,12) code geeft aanleiding tot een bolstapeling in de reële 24-dimensionale ruimte, waarin elke bol 98256 andere bollen raakt.

*3.4. De ternaire Golay code*

De ternaire Golay code is een 2-error-correcting lineaire (11,6) code over GF(3). Ook deze code is perfect. Hij houdt verband met $M_{12}$ en $M_{11}$.

*4. De groep van Conway*

*4.1. De Leech lattice*

Er is één rooster $\Gamma$ over $\mathbb{Z}$ in $\mathbb{R}_{24}$ met de eigenschappen

$$\det \Gamma = 1, \quad \forall_{x\in\Gamma}((x,x) \equiv 0 \bmod 2), \quad \min_{0\neq x\in\Gamma} (x,x) \geq 4.$$

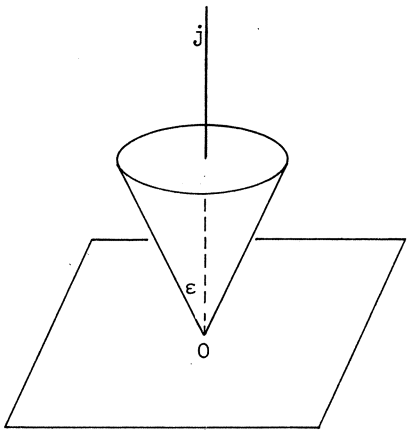
Dit is een Leech lattice. De bijbehorende bolstapeling bevat die van sectie 3.3, en elke bol raakt 196560 andere bollen.

*4.2. De groep van Conway*

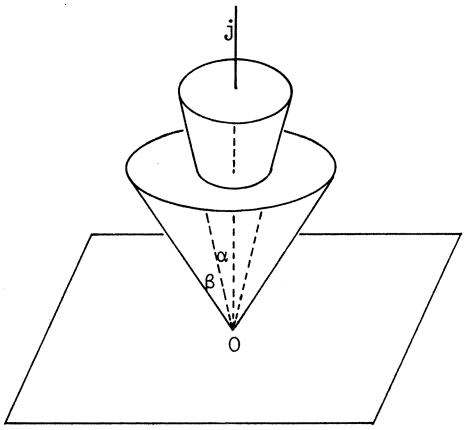
Conway's groep $\cdot 0$ is de automorfisme groep van de Leech lattice. De groep heeft een centrum van de orde 2, en de quotiënt groep $\cdot 1$ is een enkelvoudige groep van de orde $2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$. Haast alle in de afgelopen tien jaar ontdekte enkelvoudige groepen, en ook de Mathieu groepen, zijn ondergroepen van de Conway groep.

*4.3. Lijnenstelsels*

Zowel de lineaire (24,12) code uit sectie 3.2 als de Leech lattice uit sectie 4.1 kunnen worden voorgesteld als een bijzonder stelsel van rechten door de oorsprong in de reële 24-dimensionale ruimte $\mathbb{R}_{24}$.




1+759+1288 rechten,
cos ε = 1/3, volgens Golay code




1+4600+47104+46575 rechten,
cos α = 1/2, cos β = 1/4, volgens Leech lattice

Inderdaad, schrijf de vectoren van de (24,12) code met {+1,-1} in plaats van met {0,1}, en interpreteer de vectoren

$$x = (-1)^8(+1)^{16}, \quad y = (-1)^{12}(+1)^{12}, \quad z = (-1)^{16}(+1)^8,$$

als reële vectoren in $\mathbb{R}_{24}$, dan geldt voor de inproducten $(j,x) = 8$, $(j,y) = 0$, $(j,z) = -8$.

Vervolgens beschouwen wij in de Leech lattice twee vectoren x en y met minimale norm, dus met $(x,x) = (y,y) = 4$. Dan geldt

$$4 \leq (x-y,x-y) = (x,x) + (y,y) - 2(x,y), \quad \text{dus } |(x,y)| \leq 2.$$

Voor de hoek tussen x en y volgt

$$\cos(x,y) = \pm 1/2, \pm 1/4, 0.$$

*Literatuur*

Bij paragraaf 1

R.C.BOSE, S.S. SHRIKHANDE & E.T. PARKER, *Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture,* Canad. Jl. Math., 12 (1960), 189-203.

Bij paragraaf 2

D.K. CHAUDHURI & R.M. WILSON, *Solution of Kirkman's schoolgirl problem,* A.M.S. Proc. Symp. Pure Math., 19 (1971), 187-205.

Bij paragraaf 3

M.J.E. GOLAY, *Notes on digital coding,* Proc. I.R.E., 37 (1949), 657.

J. LEECH, *Some sphere packing in higher space,* Canad. Jl. Math., 16 (1964), 657-682.

J. LEECH, *Notes on sphere packings,* Canad. Jl. Math., 19 (1967), 251-267.

Bij paragraaf 4

J.H. CONWAY, *The perfect group of order 8,315,553,613,086,720,000 and the sporadic simple groups,* Proc. N.A.S., 61 (1968), 398-400.

J.H. CONWAY, *A group of order 8,315,553,613,086,720,000,* Bull. London Math. Soc., 1 (1969), 79-88.

J.H. CONWAY, *A characterization of Leech's lattice,* Inv. Math., 7 (1969), 137-142.

J.M. GOETHALS & J.J. SEIDEL, *Strongly regular graphs derived from combinatorial designs,* Canad. Jl. Math., 22 (1970), 597-614.

MC SYLLABUS 18, 1973, 39-58

# TWEE HOOGTEPUNTEN UIT HET MODERNE GRONDSLAGENONDERZOEK VAN DE WISKUNDE

J.J. DE IONGH
Uitgewerkt door P. VAN EMDE BOAS

*1.*

Toen in 1946 het Mathematisch Centrum gesticht werd, was het grondslagenonderzoek van de wiskunde nog een klein wetenschapsgebied, tamelijk ver van de hoofdstroom van de wiskunde gelegen, in de richting van het land der filosofen, dat door slechts enkele grote wiskundigen voor het eerst ontgonnen werd. Nu, 25 jaren later, is het een samenstel geworden van een zestal uitgebreide en veel kleinere onderzoeksterreinen, die, ieder voor zich, door een groot aantal specialisten volgens eigen, goed ontwikkelde methoden bewerkt worden.

Logica en bewijstheorie, axiomatische verzamelingenleer, modellentheorie, theorie van de recursieve functies en de abstracte rekenmachines, intuïtionistische en, algemener, constructieve wiskunde, algebraïsche logica en algebraïsche bewijstheorie zijn enkele van deze hoofdgebieden. Misschien zal een formele categorieëntheorie zich tot een nieuw dergelijk onderzoeksveld naast de axiomatische verzamelingentheorie gaan ontwikkelen.

De eenheid van het grondslagenonderzoek wordt bij deze groeiende verscheidenheid toch, gedeeltelijk, bewaard, doordat resultaten en methoden van het ene gebied, analoog vervormd op andere gebieden toegepast worden en daar tot nieuwe ontwikkelingen aanleiding geven.

Een duidelijker teken van gezonde groei is het nog, dat het grondslagenonderzoek zijn samenhang met en zijn betekenis voor de andere gebieden

van de wiskunde heeft weten te bewijzen.

De belangrijkste bijdrage van het grondslagenonderzoek tot de ontwikkeling van het geheel van de wiskunde ligt waarschijnlijk in de opbouw van een scherpere taal en van een nauwkeuriger omschreven begrip "formeel bewijs". Deze beide hebben een sterke unificerende invloed op de moderne wiskunde uitgeoefend.*)

Minder belangrijk, maar veel gemakkelijker aan te geven, ja op het eerste gezicht reeds duidelijk indrukwekkend, is de bijdrage, die het grondslagenonderzoek in de laatste 10 jaren geleverd heeft tot het oplossen van grote klassieke problemen uit de centrale gebieden van de wiskunde.

In 1900 heeft David HILBERT op het Internationale Congres van Mathematici te Parijs in een beroemde voordracht met de titel *Mathematische Probleme* betoogd, dat helder en eenvoudig te omschrijven problemen als het ware de sporten zijn van de ladder, waarlangs de wiskunde omhoog klimt. Hij besloot zijn voordracht met het aangeven van 23 dergelijke belangrijke en volgens hem voor de verdere ontwikkeling van de wiskunde vruchtbare problemen en probleemgebieden.

Vele hiervan hebben in de twintigste eeuw als toetssteen gediend voor de vooruitgang van de wiskunde; de meeste zijn in deze 70 jaren geheel of voor een belangrijk gedeelte opgelost.

HILBERT's eerste en HILBERT's tiende probleem hebben in de laatste 10 jaren aanleiding gegeven tot belangrijk en uiterst boeiend werk van grondslagenonderzoekers.

In deze voordracht wil ik enkele hoofdlijnen van dit werk voor u schetsen.

*2.*

Voordat ik echter aan de behandeling van het tiende probleem begin, wil ik even enkele van de eenvoudigste resultaten van de verzamelingenleer met u herhalen.

Verzamelingen V en W zijn gelijkmachtig (in formule: $V \sim W$), indien er een (1,1)-afbeelding van V op W te vinden is; dus: $V \sim W \underset{D}{=} \bigvee_f [f\colon V \rightarrowtail\!\!\!\!\rightarrow W]$.

Het blijkt eenvoudig afbeeldingen aan te geven, waardoor we de volgende stellingen kunnen bewijzen.

---

*) Zie ook de voordracht van H. FREUDENTHAL (blz. 14-15).

STELLING. $\mathbb{N} \sim \mathbb{N}^2$, *namelijk* $f(\langle x,y\rangle) \underset{D}{=} \frac{1}{2}(x+y-1)(x+y-2) + x$.

STELLING. $\bigwedge_{n\in\mathbb{N}} [\mathbb{N} \sim \mathbb{N}^n]$.

STELLING. $\mathbb{N} \sim \bigcup_n \mathbb{N}^n$.

$\bigcup_n \mathbb{N}^n$ is hierbij de verzameling van alle eindige rijtjes van natuurlijke getallen.

Verzamelingen gelijkmachtig met $\mathbb{N}$ noemen we *aftelbaar (oneindig)*. Met de voor het gehele grondslagenonderzoek fundamentele diagonaalmethode van Georg CANTOR kunnen we echter bewijzen:

STELLING. $\mathbb{N} \not\sim \mathbb{N}^{\mathbb{N}}$.

Hierbij is $\mathbb{N}^{\mathbb{N}}$ de verzameling van alle oneindige rijen van natuurlijke getallen.

We bewijzen deze stelling in de vorm: bij iedere afbeelding f van $\mathbb{N}$ in $\mathbb{N}^{\mathbb{N}}$ is er een element $\alpha$ van $\mathbb{N}^{\mathbb{N}}$ te vinden, zó dat voor alle $n \in \mathbb{N}$ $f(n)$ ongelijk is aan $\alpha$.

BEWIJS: Zij $f: \mathbb{N} \in \mathbb{N}^{\mathbb{N}}$ met $f(n) = \langle a_{n1}, a_{n2}, a_{n3}, \ldots\rangle$. We beschouwen de diagonaalrij $\langle a_{11}, a_{22}, a_{33}, \ldots\rangle$; we veranderen deze op iedere plaats en vormen zo bijvoorbeeld de nieuwe rij $\alpha = \langle a_{11}+1, a_{22}+1, a_{33}+1, \ldots\rangle$, $\alpha \in \mathbb{N}^{\mathbb{N}}$, afhankelijk van f. Kies nu een willekeurige $n \in \mathbb{N}$; vorm $f(n)$. Op de $n^{de}$ plaats van $f(n)$ staat $a_{nn}$; op de $n^{de}$ plaats van $\alpha$ staat $a_{nn}+1$. Maar $a_{nn} \neq a_{nn}+1$, dus $f(n) \neq \alpha$. □

*3.*

Het tiende probleem van HILBERT luidt:

"*Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*"

We moeten dus een rekenmethode zoeken om, bij een willekeurige veelterm $P(x_1,\ldots,x_n)$ met gehele getallen als coëfficiënten, te bepalen of er gehele getallen $X_1,\ldots,X_n$ bestaan zó dat $P(X_1,\ldots,X_n) = 0$ is.

Indien we het gemakkelijker vinden, de vraag te beantwoorden of er getallen $X_1,\ldots,X_n \in \mathbb{N}_0$ ($\mathbb{N}_0$ is de verzameling van de natuurlijke getallen, 0 inbegrepen) te vinden zijn, zó dat $P(X_1,\ldots,X_n) = 0$ is, mogen we ons hiertoe beperken. Om dit te laten zien vormen we de $2^n$ veeltermen $P_1(x_1,\ldots,x_n) = P(x_1,\ldots,x_n), P_2(x_1,\ldots,x_n) = P(-x_1,x_2,\ldots,x_n),\ldots,P_{2^n}(x_1,\ldots,x_n) = P(-x_1,-x_2,\ldots,-x_n)$.

Dan geldt

$$\bigvee_{x_1,\ldots,x_n\in\mathbb{Z}} [P(x_1,\ldots,x_n) = 0] \Longleftrightarrow$$

$$\Longleftrightarrow \bigvee_{x_1,\ldots,x_n\in\mathbb{N}_0} [P_1(x_1,\ldots,x_n)\cdot\ldots\cdot P_{2^n}(x_1,\ldots,x_n) = 0].$$

Ook andersom is de vraag naar het bestaan van oplossingen in getallen uit $\mathbb{N}_0$ niet moeilijker dan de vraag naar het bestaan van oplossingen in $\mathbb{Z}$ Omdat, volgens een beroemde stelling van LAGRANGE, ieder getal uit $\mathbb{N}_0$ te schrijven is als een som van vier kwadraten van getallen uit $\mathbb{N}_0$ (of uit $\mathbb{Z}$) geldt immers:

$$\bigvee_{x_1,\ldots,x_n\in\mathbb{N}_0} [P(x_1,\ldots,x_n) = 0] \Longleftrightarrow$$

$$\Longleftrightarrow \bigvee_{x_1,x_1',x_1'',x_1''',x_2,x_2',\ldots,x_n'''\in\mathbb{Z}} [P(x_1^2+x_1'^2+x_1''^2+x_1'''^2, x_2^2+x_2'^2+x_2''^2+x_2'''^2,\ldots$$

$$\ldots, x_n^2+x_n'^2+x_n''^2+x_n'''^2) = 0].$$

De vraag of een vergelijking een oplossing in de natuurlijke getallen met nul erbij bezit, is dus equivalent met de vraag of een andere vergelijking een oplossing heeft in de gehele getallen, en andersom, HILBERT's probleem -een rekenmethode te vinden, die bij *willekeurige* gegeven veelterm met coëfficiënten in de gehele getallen, ons de beslissing levert, of deze veelterm een oplossing in de gehele getallen heeft- blijkt equivalent te zijn met het analoge probleem, waarbij de oplossingen elementen van $\mathbb{N}_0$ moeten zijn. De grondslagenonderzoekers houden meer van de natuurlijke getallen met de nul erbij, zodat wij ons kunnen richten op het probleem: "*Bestaat er een rekenmethode om bij een gegeven willekeurige diophantische vergelijking vast te stellen of deze een oplossing bezit in* $\mathbb{N}_0$?"

Om vat te krijgen op het begrip "willekeurige diophantische vergelijkingen" merken we op dat deze vergelijkingen worden opgeschreven als eindige rijtjes symbolen. De bouwstenen van de vergelijkingen zijn de natuurlijke getallen 0,1,2,3,..., de variabelen $x_1,x_2,x_3,\ldots$ en een aantal operatoren +, -, ×, of relaties =. Deze opmerking stelt ons in staat de bouwstenen af te beelden op de natuurlijke getallen; daarmee wordt de vergelijking afgebeeld op een eindig rijtje natuurlijke getallen. Op deze wijze verkrijgen we zonder moeite een codering van de diophantische vergelijking in de natuur-

lijke getallen.

Deze codering stelt ons in staat de vergelijkingen op een rij te zetten; we kunnen zodoende over de $n^{de}$ vergelijking spreken.

Een probleem hierbij is dat niet ieder rijtje symbolen een vergelijking voorstelt, of dat twee rijtjes een in wezen gelijke vergelijking voorstellen. Dit zijn geen essentiële moeilijkheden.

We hebben hiermee het probleem van HILBERT vertaald tot het volgende probleem: "*Bestaat er een machine (of een rekenmethode) zodanig dat, als ik het getal n erin stop, er een 0 uit komt indien de $n^{de}$ diophantische vergelijking geen oplossing heeft en een 1 indien de $n^{de}$ diophantische vergelijking wel een oplossing heeft?*"

Een dergelijke hypothetische machine zullen we aangeven met $\mathbb{D}$. Sinds 1900 hebben de wiskundigen vergeefs naar deze machine gezocht; meer beperkte machines, die in staat zijn om voor deelklassen van diophantische vergelijkingen de beslissing te leveren, zijn geconstrueerd, maar de hele machine bleef onvindbaar.

De grondslagenonderzoekers zijn toen het probleem van de andere kant gaan aanpakken; zij hebben bewezen dat een machine $\mathbb{D}$ niet kan bestaan.

Hierbij doet zich direct het probleem voor dat een dergelijk bewijs vereist dat we moeten definiëren wat we verstaan onder een rekenmethode. Dit probleem zouden we niet hebben als we het positieve resultaat hadden bewezen; van een eventuele oplossing hadden we wel kunnen zien dat de aangegeven methode een rekenmethode is. Maar om te bewijzen dat er voor een probleem geen rekenmethode bestaat, moet je een overzicht hebben over alle mogelijke rekenmethoden en dit kan alleen als je het begrip rekenmethode definieert.

*4.*

Omstreeks 1936 ontstaan op een aantal verschillende plaatsen tegelijkertijd definities voor begrippen die de intuïtieve notie van effectieve berekenbaarheid zouden moeten bepalen. Deze definities werden ieder opgesteld vanuit totaal verschillende concepties. Opmerkelijk is echter dat al deze definities dezelfde klasse van berekenbare functies leveren: voor een functie die volgens het ene begrip berekenbaar is, bestaat ook in ieder der andere noties een rekenmethode. Dit is een goede reden om te veronderstellen dat hiermee een fundamenteel begrip benaderd is.

De boven vermelde definities zijn afkomstig van K. GÖDEL, A. CHURCH, S. KLEENE, A.M. TURING en E.J. POST. A.A. MARKOV gaf naderhand nog een

nieuwe versie die ook equivalent is met de voorafgaande. De equivalentie van deze verschillende begrippen werd bewezen door KLEENE en TURING.

De hypothese dat deze begrippen precies overeenstemmen met het intuïtieve begrip "effectief berekenbaar" staat bekend als de *these van CHURCH*. Ik wil niet deze definities met u behandelen, maar ik wil het intuïtieve begrip schetsen vanuit het standpunt dat TURING heeft gekozen. TURING dacht, in een periode dat de electronische rekenmachine nog niet was geconstrueerd, aan een abstracte rekenautomaat.

De automaat bevat een band met vierkante vakjes waarop symbolen uit een eindig alfabet geschreven kunnen worden. De band is in principe oneindig, d.w.z. hij is eindig, maar zodra er aan een van beide zijden het gevaar dreigt dat de band opraakt, plakken we er nog een paar kilometer band bij. De band die we erbij plakken is altijd blanco. Er staan dus altijd slechts eindig veel symbolen op de ponsband. De machine is verder zeer eenvoudig. Hij kan in een vast eindig aantal inwendige toestanden verkeren. Hij leest telkens een symbool van de band en schrijft, afhankelijk van zijn inwendige toestand en van het gelezen symbool, al dan niet een nieuw symbool op de plaats van het gelezen symbool; verder gaat hij over in een nieuwe inwendige toestand en tenslotte kan hij een stap naar rechts dan wel een stap naar links gaan. Hierna is de machine klaar voor een volgende zet.

We kunnen dit als volgt aangeven. Laten $S_0,S_1,S_2,\ldots,S_k$ de eindig vele symbolen zijn waarmee de machine werkt. Laten de interne toestanden worden aangegeven met $q_1,\ldots,q_n$. Het gedrag van de machine op het moment dat hij symbool $S_i$ leest in toestand $q_j$, is geheel bepaald door dit paar $\{q_j,S_i\}$. We kunnen het gedrag aangeven met een drietal $\{S_k,q_\ell,X\}$ waarbij X staat voor R, L of Ø. Het is ook mogelijk dat de machine voor een paar $\{q_j,S_i\}$ geen instructie bezit. In dit geval blijft de machine stilstaan en is de berekening afgelopen.

Hoe moeten we ons voorstellen dat de machine een berekening uitvoert. Dit is een kwestie van codering. We gaan ervan uit dat $S_0$ het blanco symbool is, ook wel aangegeven met 0. $S_1$ geven we ook aan met 1. We kunnen een natuurlijk getal k op de band aangeven door een rij van k+1 keer het symbool 1, voorafgegaan en gevolgd door blanco symbolen. Het getal 0 is dus aangegeven door één enkel symbool 1. Dat dit een omslachtige codering is voor grote getallen doet minder terzake, zolang het om een theoretisch model gaat.

We kunnen ons voorstellen dat de op deze wijze geprepareerde band in de machine gestopt wordt en dat de machine wordt gestart. Als de machine tot

stilstand is gekomen, halen we de band uit de machine en tellen we het aantal symbolen 1 op de band. Dit aantal interpreteren we als de berekende waarde.

Op deze wijze kunnen we iedere Turing machine zien als een functie die aan een natuurlijk getal misschien een nieuw natuurlijk getal toevoegt. Het is namelijk in het geheel niet zeker dat de berekening die eenmaal is begonnen, ooit gereed komt. Denk bijvoorbeeld aan de machine die zo geprogrammeerd is dat hij een symbool 1, dat hij ziet, in een symbool 0 verandert en een symbool 0 in een symbool 1; bij deze zetten beweegt de machine niet. Deze machine zal zodra hij een symbool 1 of een blanco symbool tegenkomt nadien alleen nog maar dit symbool heen en terug veranderen, en hij zal daarmee nooit klaar komen. Dit is precies zo als bij een tafelrekenmachine die je door nul laat delen; de machine loopt aan een stuk door en brengt alleen maar gebrom voort.

*5.*

We hebben gezien dat het gedrag van een Turing machine geheel gekarakteriseerd is door zijn programma. Dit programma kunnen we opgebouwd denken uit een eindige rij van vijftallen $\langle q_i, S_j, S_k, q_\ell, X\rangle$ waarbij $q_i$ en $q_\ell$ toestanden zijn, $S_j$ en $S_k$ symbolen uit het eindige alfabet en X voor R, L of $\emptyset$ staat. Op deze wijze coderen we de Turing machines door middel van eindige symbolenrijtjes. Zoals we eerder hebben opgemerkt kunnen we deze symbolenrijtjes in een lijst zetten, wat het mogelijk maakt te spreken over het $n^{de}$ programma uit deze lijst. Deze lijst bevat dan alle mogelijke programma's. Naast programma's die een functie berekenen, komen ook programma's voor die nooit ophouden met brommen, terwijl het voor weer andere programma's afhangt van de invoer of de machine stopt of niet.

Het blijkt dat het opstellen van de instructies van het $n^{de}$ programma uit de lijst zelf weer een berekening is die door een machine kan worden uitgevoerd. Er kan een zogeheten *universeel Turing programma* worden samengesteld dat tot effect heeft dat de machine, gegeven een n en een k, op de band eerst de instructies van de $n^{de}$ Turing machine reconstrueert en vervolgens dit $n^{de}$ Turing programma laat werken op de invoer k. Het resultaat hiervan kan een natuurlijk getal zijn, maar het kan ook een voortdurend gebrom opleveren. We zullen deze universele machine aangeven met $\mathbb{U}$.

Het is maar goed, dat $\mathbb{U}$ niet voor iedere invoer n en k ook echt stopt. Als dit wel gebeurt komen we als volgt op een tegenspraak: door de universele

machine $\mathbb{U}$ te koppelen met enkele veel eenvoudiger Turing machines kunnen we ons voorstellen dat we een machine hebben die het volgende programma uitvoert.

Als op de band het getal k staat geschreven schrijven we eerst ernaast nog eens het getal k. Vervolgens laten we d.m.v. de universele Turing machine $\mathbb{U}$ uitrekenen wat de $k^{de}$ machine uit de lijst doet met invoer k. Als dit tenslotte tot een resultaat heeft geleid, tellen we bij dit resultaat nog 1 op en vervolgens stoppen we.

De boven geschetste machine berekent dus de functie die we kunnen aangeven met

$$\mathbb{U}(k,k) + 1.$$

Omdat de machine zelf weer een Turing machine is, zal zijn programma ergens in de lijst voorkomen, zeg op de $k_0^{de}$ plaats. Bekijk nu wat de machine doet met $k_0$ als argument. Per definitie is het resultaat gelijk aan

$$\mathbb{U}(k_0,k_0) + 1.$$

Volgens de definitie van de universele Turing machine $\mathbb{U}$ kunnen we ook het resultaat van de machine $k_0$ door $\mathbb{U}$ laten uitrekenen. In dit geval vinden we als resultaat van machine $k_0$ op argument $k_0$:

$$\mathbb{U}(k_0,k_0),$$

en zien we dat

$$\mathbb{U}(k_0,k_0) = \mathbb{U}(k_0,k_0) + 1,$$

en dit is een tegenspraak. De universele machine kan dus niet voor iedere invoer stoppen.

Eenzelfde tegenspraak kunnen we afleiden als we aannemen, dat er een lijst bestaat van al die machines die bij iedere invoer stoppen, een lijst van totale Turing machines. Ook dan kunnen we een machine $\mathbb{V}$ construeren die op argument k het $n^{de}$ programma uit de lijst van totale Turing machines laat werken, en deze berekening stopt derhalve voor iedere invoer.

Opnieuw kunnen we een programma samenstellen dat de functie

$$\mathbb{V}(n,n) + 1$$

uitrekent. Dit is zelf een totaal programma en het komt dus voor in de lijst

van totale programma's, zeg op de plaats $k_0$. Opnieuw komen we tot de tegenspraak dat

$$\mathbb{V}(k_0,k_0) = \mathbb{V}(k_0,k_0) + 1.$$

Waarom geeft deze constructie niet een tegenspraak als we de lijst van alle machines nemen die dan niet noodzakelijk altijd stoppen? We bekijken opnieuw het programma $k_0$ dat de functie $\mathbb{U}(n,n) + 1$ berekent; we vinden dan opnieuw de relatie

$$\mathbb{U}(k_0,k_0) = \mathbb{U}(k_0,k_0) + 1.$$

Dit hoeft echter geen tegenspraak te zijn als we niet langer vasthouden aan de eis dat $\mathbb{U}(k_0,k_0)$ een eindig getal is. Als we aanvaarden dat de berekening van $\mathbb{U}(k_0,k_0)$ niet stopt, dan staat er zoveel als

$$\text{gebrom} = \text{gebrom} + 1$$

en dit is geen tegenspraak.

We zijn na dit alles geïnteresseerd in de vraag wat we voor gegeven n en k kunnen zeggen over het gedrag van $\mathbb{U}$: stopt $\mathbb{U}(n,k)$ of stopt $\mathbb{U}(n,k)$ niet? Veronderstel dat het mogelijk zou zijn om een machine $\mathbb{S}$ te maken die dit probleem voor ons oplost. Dat wil zeggen: de machine $\mathbb{S}$ is zo geprogrammeerd, dat $\mathbb{S}(n,k)$ altijd stopt en een antwoord 0 of 1 geeft, en wel zó dat

$\mathbb{S}(n,k) = 1$ indien $\mathbb{U}(n,k)$ stopt

en

$\mathbb{S}(n,k) = 0$ indien $\mathbb{U}(n,k)$ altijd blijft doorlopen.

We kunnen met gebruikmaking van deze machine $\mathbb{S}$ een machine construeren die het volgende programma uitvoert:
Gegeven een getal n; test eerst of $\mathbb{U}(n,n)$ stopt of niet (met $\mathbb{S}$); zo ja, bereken dan $\mathbb{U}(n,n) + 1$ en geef de uitkomst daarvan als antwoord; zo nee, geef dan 0 als antwoord.

Het boven beschreven programma is duidelijk weer een totaal programma. De erdoor berekende functie kunnen we aangeven met

$$f(k) = \begin{cases} \mathbb{U}(k,k) + 1 & \text{indien } \mathbb{U}(k,k) \text{ stopt } (\mathbb{S}(k,k) = 1) \\ 0 & \text{anders } (\mathbb{S}(k,k) = 0). \end{cases}$$

Zij opnieuw $k_0$ de plaats in de lijst van dit programma voor f. Omdat $k_0$ een totaal programma is, zal $\mathbb{S}(k_0,n) = 1$ gelden voor iedere n, dus ook voor $n = k_0$. Als we nagaan wat dit betekent, dan vinden we opnieuw onze contradictie

$$\mathbb{U}(k_0,k_0) = \mathbb{U}(k_0,k_0) + 1.$$

De foute veronderstelling waarvan we zijn uitgegaan is de aanname dat de machine $\mathbb{S}$ bestaat. We hebben hier één van de kernresultaten van het grondslagenonderzoek te pakken: de machine $\mathbb{S}$ bestaat niet. Anders geformuleerd: *het stopprobleem voor de Turing machines kan niet door een Turing machine worden opgelost.*

Tenslotte kunnen we nog wijzen op de analogie die bestaat tussen de hierboven gegeven redeneringen en de diagonaalmethode van CANTOR, die we in het begin van deze voordracht hebben besproken.

*6.*

Bij het tiende probleem van HILBERT ging het om het bestaan van een machine $\mathbb{D}$, die in staat is van een gegeven diophantische vergelijking vast te stellen of er oplossingen bestaan of niet. We kunnen na de verhandeling over de effectieve berekenbaarheid de vraagstelling nader preciseren. De vraag wordt dan: *bestaat er een Turing machine* $\mathbb{D}$ *die in staat is van een (gecodeerde) diophantische vergelijking vast te stellen of er oplossingen zijn of niet?*

We hebben van een specifiek soort machine gezien dat hij niet kan bestaan, nl. de machine $\mathbb{S}$ die het stopprobleem moet oplossen. Indien we er nu in zouden slagen om, aannemende dat de machine $\mathbb{D}$ bestaat, een constructie $\mathbb{F}$ te geven om de machine $\mathbb{D}$ zo om te bouwen dat hij het stopprobleem oplost (d.w.z. we bouwen $\mathbb{D}$ om tot $\mathbb{S}$ door middel van samenstelling met $\mathbb{F}$), dan hebben we aangetoond dat $\mathbb{D}$ niet kan bestaan. Immers $\mathbb{S}$ kan niet bestaan, maar $\mathbb{D}$ en $\mathbb{F}$ samen geven een voorbeeld van machine $\mathbb{S}$.

De Amerikaanse wiskundigen Julia ROBINSON, Martin DAVIS en Hilary PUTNAM zijn er in geslaagd om, uitgaande van een machine $\mathbb{E}$ die machtiger is dan $\mathbb{D}$, een dergelijke constructie $\mathbb{F}$ aan te geven. De machine $\mathbb{E}$ is in zoverre machtiger dan de machine $\mathbb{D}$ dat hij van een grotere klasse van vergelijkingen vaststelt of er oplossingen bestaan. Deze grotere klasse van de exponentieel diophantische vergelijkingen bevat ook die vergelijkingen waar

variabelen in een exponent mogen voorkomen, zoals bijvoorbeeld de vergelijking:

$$3x^z + 3y^t z^7 = 0.$$

Uitgaande van een machine $\mathbb{E}$, die voor dit soort vergelijkingen vaststelt of er oplossingen zijn of niet, slaagden zij er met veel handig programmeerwerk in de transformatie $\mathbb{F}$ te construeren.

Hierna resteerde het gat tussen $\mathbb{D}$ en $\mathbb{E}$. In feite kwam dit neer op het volgende probleem: *is het mogelijk een diophantische vergelijking* $P(u,v,w,x_1,\ldots,x_n)$ *te vinden, zodanig dat deze een oplossing* $x_1,\ldots,x_n$ *bezit dan en slechts dan als* $u^v=w$?

Het construeren van deze vergelijking lukte in 1970. Uitvinder was een jonge student uit Leningrad, Ju.V. MATIJASEVIČ, die dit probleem kon oplossen met behulp van zijn kennis over de Fibonacci getallen en de vergelijking van Pell (dit is de vergelijking $x^2 - (q^2-1)y^2 = 1$), opgestoken van zijn leraar op de middelbare school, gecombineerd met de colleges van A.J. MAL'CEV, over de resultaten van J. ROBINSON, M. DAVIS en H. PUTNAM.

Hiermee is het tiende probleem van HILBERT in negatieve zin opgelost. De existentie van de machine $\mathbb{D}$ stelt ons in staat om eerst $\mathbb{E}$ en daarna $\mathbb{S}$ te construeren. $\mathbb{S}$ bestaat niet, dus $\mathbb{D}$ kan ook niet bestaan.

*7.*

Het tweede gedeelte van de voordracht is gewijd aan het *continuumprobleem*. Dit probleem is niet bij toeval door HILBERT als eerste probleem op zijn lijst gezet. Mijns inziens is dit probleem nog steeds het diepste, grootste en meest veelzijdige probleem der wiskunde. De grondslagentheoretici hebben het gedeeltelijk opgelost, of liever gezegd, ze hebben laten zien hoe het niet op te lossen is met de huidige hulpmiddelen en wat voor geheel nieuwe dingen er bij zouden moeten komen om het probleem op te lossen.

Het continuumprobleem is daarom een goed probleem omdat het zich zeer eenvoudig laat formuleren.

Met behulp van de diagonaalmethode hebben we aangetoond dat de verzameling der natuurlijke getallen $\mathbb{N}$ niet gelijkmachtig is met de verzameling $\{0,1\}^{\mathbb{N}}$, de verzameling van alle aftelbare rijen nullen en enen. Deze laatste verzameling is gelijkmachtig met die der reële getallen die we aangeven met $\mathbb{R}$.

De vraag komt vanzelfsprekend op of er nog een verzameling $V \subset \mathbb{R}$ bestaat, die een machtigheid heeft die groter is dan die van $\mathbb{N}$ en kleiner dan die van $\mathbb{R}$. Dit komt neer op de vraag of de machtigheid van $\mathbb{R}$ de kleinste machtigheid is die groter is dan die van $\mathbb{N}$. In formule: bestaat er een verzameling V met $\mathbb{N} \subseteq V \subseteq \mathbb{R}$ en $\mathbb{N} \not\sim V$ en $V \not\sim \mathbb{R}$?

CANTOR heeft reeds voor 1900 de veronderstelling uitgesproken dat een dergelijke verzameling V niet bestaat. Deze veronderstelling staat bekend als de *continuumhypothese*. De continuumhypothese kan gegeneraliseerd worden voor willekeurige machtigheden. De uitspraak (gegeneraliseerde continuumhypothese) luidt dan:

*tussen* V *en* $\{0,1\}^V$ *zit geen machtigheid.*

We zullen op deze gegeneraliseerde continuumhypothese verder niet ingaan.

U ziet dat in de formulering van het continuumprobleem: "is de continuumhypothese waar?", alleen maar zeer simpele begrippen voorkomen zoals reële getallen, natuurlijke getallen en een-eenduidige afbeeldingen.

*8.*

Een eerste probleem bij de discussie van het continuumprobleem is, dat gebleken is dat het naieve inzicht in de verzamelingen niet toereikend is. In de periode rond 1890 tot 1900 was dit naieve inzicht voldoende om voor iedereen aanvaardbare, keurige bewijzen te construeren. De beroemde paradoxen van RUSSELL en anderen (waar ik niet verder op in kan gaan) toonden evenwel aan dat het rekenen met zomaar gedefinieerde verzamelingen tot contradicties leidde.

De reactie in de wiskunde was er een van puriteinse zuiverheid. Aan het wiskundig redeneren werden zeer precieze regels opgelegd. De uitgangspunten van de verzamelingentheorie werden vastgelegd in een aantal axioma's, waarvan men de waarheid voor een vastgelegde klasse van verzamelingen meende te kunnen inzien. De wiskundige kan daarna op grond van de axioma's met behulp van de logica stellingen gaan afleiden. Het blijkt dat de gewone wiskunde op deze manier uit een axiomastelsel, zoals dat van ZERMELO en FRAENKEL, geheel kan worden afgeleid.

In deze context kan men naast het continuumprobleem de formele vraag stellen of de continuumhypothese afleidbaar is uit de gegeven axioma's voor de verzamelingenleer of dat zij met deze axioma's strijdig is. De stellingname in de filosofie der wiskunde dat met het antwoord op deze twee afleidbaarheidsproblemen ook het antwoord op het continuumprobleem gegeven zou

zijn, of in het algemeen, dat wiskundige waarheid gereduceerd kan worden tot afleidbaarheid in een formeel systeem (het formalisme genaamd) blijkt inadequaat te zijn om als bindende interpretatie te gelden. Wel kan men het formalisme methodisch als eerste stap gebruiken bij de bestudering van problemen.

Dat het formalisme inadequaat is blijkt uit de *onvolledigheidsstelling* van K. GÖDEL uit 1931. Deze stelling spreekt uit dat in ieder axiomastelsel dat rijk genoeg is om de getallentheorie te omvatten, zinnen bestaan zodanig dat noch de zin noch zijn ontkenning afleidbaar is. In notatie:

$$\sim(\vdash A) \quad \text{en} \quad \sim(\vdash \neg A).$$

(Het symbool $\vdash$ wordt gebruikt om aan te geven dat een zin A afleidbaar is uit een verzameling van zinnen $\Gamma$ (denk voor $\Gamma$ aan een axiomastelsel): $\Gamma \vdash A$. Als duidelijk is welk axiomastelsel bedoeld wordt, wordt $\Gamma$ weggelaten.)

Volgens het formalisme kunnen we dus niet zeggen of A waar is of niet. Het blijkt evenwel dat nadenken over het systeem leert dat A wel degelijk waar is. We moeten dan ook concluderen dat het principe: "waar = afleidbaar" niet correspondeert met het intuïtieve waarheidsbegrip.

Naast de mogelijkheid dat $ZF \vdash CH$ en $ZF \vdash \neg CH$, bestaat dus nog de mogelijkheid dat noch CH noch $\neg CH$ uit ZF afleidbaar is. Deze laatste mogelijkheid is inderdaad het geval.

Hoe moeten we ons voorstellen dat men ooit kan vaststellen dat bijv. $\sim(ZF \vdash \neg CH)$? Stel u voor dat we wel hebben, dat de ontkenning van CH afleidbaar is uit ZF. In dit geval krijg ik een inconsistent systeem als ik aan ZF de continuumhypothese als axioma toevoeg:

$$\left.\begin{array}{l} ZF \vdash \neg CH \qquad \text{impliceert } ZF + CH \vdash \neg CH \\ ZF + CH \vdash CH \end{array}\right\} \Longrightarrow$$

$$\text{dus } ZF + CH \vdash CH \wedge \neg CH$$

en dit is een contradictie. Dit zou betekenen dat het onmogelijk is een consistente interpretatie van het axiomastelsel ZF + CH te geven. Als in de praktijk blijkt dat een dergelijke interpretatie toch mogelijk is, moeten we concluderen dat het uitgangspunt $ZF \vdash \neg CH$ onjuist is.

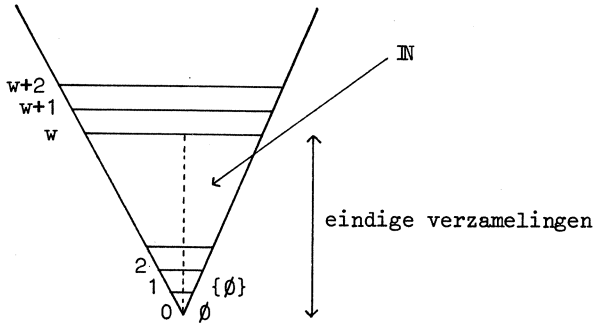
*9.*

Het bewijs dat CH niet in strijd was met de axioma's van ZERMELO en FRAENKEL ($\neg(ZF \vdash \neg CH)$) is gegeven door K. GÖDEL (1938-1940). Zijn bewijsmethode laat zich als volgt schetsen.

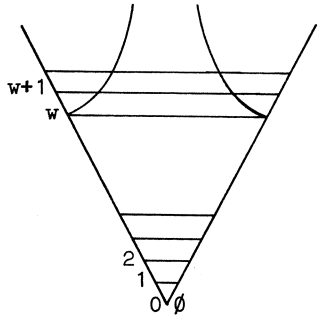
Een formeel systeem bestaat uit eindige zinnen die te coderen zijn met eindige rijtjes symbolen. Zoals we in het eerste deel van de voordracht hebben gezien, kunnen we alle eindige rijtjes in een lijst zetten. We kunnen ook andere dingen in het systeem in een lijst zetten, bijvoorbeeld stukken van zinnen, zoals definities van verzamelingen. Hieruit volgt dus in het bijzonder dat er slechts aftelbaar veel definities zijn.

Intuïtief worden de verzamelingen opgebouwd vanuit de lege verzameling $\emptyset$. Met de lege verzameling heb je ook de verzameling $\{\emptyset\}$, het paar $\{\emptyset,\{\emptyset\}\}$, of de eindige verzameling $\{\emptyset,\{\emptyset\},\{\{\emptyset\}\},\{\emptyset,\{\emptyset\}\}\}$. Iedere keer als we een verzameling A hebben gevonden kunnen we kijken naar de verzameling $P(A)$ van alle deelverzamelingen van A. Doen we dit oneindig vaak dan vinden we uiteindelijk de collectie van alle eindige deelverzamelingen. Daarbinnen zit de verzameling van de natuurlijke getallen $\mathbb{N}$ (er zit in ZF een axioma dat het bestaan van $\mathbb{N}$ impliceert). Als we $\mathbb{N}$ eenmaal hebben, komen we snel tot steeds hogere en grotere verzamelingen.

Deze hiërarchie in de klasse verzamelingen die we zo doorlopen, wordt gesuggereerd door het volgende plaatje.




We merkten echter hierboven op dat het aantal verzamelingen dat in het formele systeem beschreven wordt op zijn hoogst aftelbaar is. Zo bevat $P(\mathbb{N})$ overaftelbaar veel verzamelingen, maar hiervan zitten er slechts aftelbaar veel in het formele systeem. Voor het formele systeem vinden we dus een kleiner domein; het model van de construeerbare verzamelingen:




Hoewel we als buitenstaander direct inzien dat het domein der construeerbare verzamelingen niet "alles" bevat is het onmogelijk om van binnen uit een gat te vinden: iedere verzameling die op grond van de axioma's bestaat zit erin.

Als de verzamelingstheoreticus eenmaal een model heeft gevonden kan hij zijn theorie gaan relativeren voor dat model. Dit houdt in dat hij iedere zin transformeert tot een zin, die alleen nog maar over de elementen van het model spreekt. Dit kan men zich als volgt voorstellen: laat U(x) een zin zijn die uitdrukt, dat x in het model zit; we voegen dan aan een formule F een formule $F^*$ toe door F eerst te ontleden in zijn bouwstenen en daarna deze weer in elkaar te zetten met een kleine wijziging, die eruit bestaat dat de constructie

$$\forall_x\, G(x) \quad \text{wordt getransformeerd tot} \quad \forall_x[U(x) \Rightarrow G(x)]$$

en

$$\exists_x\, H(x) \quad \text{wordt getransformeerd tot} \quad \exists_x[U(x) \wedge H(x)].$$

Deze transformatie is effectief en kan zogezegd door een machine worden uitgevoerd. De getransformeerde formules zijn weer binnen het systeem te herkennen.

De zin U(x) kan nu zo gekozen worden dat het volgende geldt:

1) Als A een axioma van ZF is, is $A^*$ uit ZF afleidbaar.

2) De afleidingsregels in ZF gaan door voor de getransformeerde formules. Bijvoorbeeld, de zin $A \to B$ wordt getransformeerd tot $(A \to B)^* = A^* \to B^*$. Passen we in een bewijs de afleidingsregel

$$\frac{A,\ A \to B}{B}$$

toe, dan is de stap

$$\frac{A^*,\ A^* \to B^*}{B^*}$$

een toepassing van dezelfde afleidingsregel. Een gevolg hiervan is dat stellingen uit de ZF-theorie overgaan in stellingen uit de $(ZF)^*$-theorie. In formule:

$$ZF \vdash S \Rightarrow (ZF)^* \vdash S^*.$$

Maar aangezien $(ZF)^*$ zelf afleidbaar is in ZF (volgens 1)) volgt dan ook

$$ZF \vdash S^*.$$

3) Tenslotte blijkt de keuze van U ook nog te impliceren dat de getransformeerde van de zin die de continuumhypothese uitdrukt afleidbaar is in ZF. In formule:

$$ZF \vdash (CH)^*.$$

Op grond hiervan kunnen we vaststellen dat nooit kan gelden dat $ZF \vdash \neg CH$, indien we er tenminste van uit willen gaan dat ZF zelf consistent is. Het model van de constructieve verzamelingen geeft een interpretatie voor ZF + CH. Anders gesteld: stel $ZF \vdash \neg CH$; dan volgt, zoals we onder 2) gezien hebben, ook $ZF \vdash (\neg CH)^* = \neg(CH)^*$; aangezien ook $ZF \vdash (CH)^*$ geldt, volgt $ZF \vdash (CH)^* \wedge \neg(CH)^*$, dus ZF is inconsistent.

Hiermede heeft men de relatieve consistentie van CH bewezen: als de axioma's van ZERMELO en FRAENKEL consistent zijn, dan is ook dit systeem met de continuumhypothese erbij consistent. Hiermee is dus het eerste van de twee formele vragen die we aan het continuumprobleem hebben toegevoegd opgelost.

*10.*

Het ligt voor de hand dat de verzamelingstheoretici na 1940 hebben geprobeerd de methode die door GÖDEL was gebruikt om de relatieve consistentie van de continuumhypothese aan te tonen, ook te gebruiken om ten aanzien van de resterende vraag over de al dan niet afleidbaarheid van de continuumhypo-

these te beslissen. Men zocht naar een andere methode om uit een model van de verzamelingentheorie een deelmodel te lichten zodat in de gerelativeerde theorie de ontkenning van de continuumhypothese zou gelden.

In 1950 toonde de Britse grondslagenonderzoeker J.C. SHEPHERDSON aan dat een oplossing langs deze weg niet mogelijk was. Het was niet mogelijk een zogeheten inwendig model te construeren waarin de continuumhypothese onwaar was.

Hiermee bleef het probleem een aantal jaren vast zitten, totdat de analyticus P.J. COHEN, die verlegen zat om een echt moeilijk probleem, zich ermee ging bemoeien. Gewapend met de resultaten van GÖDEL en SHEPHERDSON toog hij aan de arbeid en wist in 1963 het probleem op te lossen. Zijn oplossing laat zich ongeveer als volgt schetsen.

Het is mogelijk een aftelbaar model te construeren van de ZF verzamelingentheorie. Dit betekent bijvoorbeeld dat er in dit model een aftelbare verzameling zit die de rol speelt van de verzameling der reële getallen. Van buitenaf gezien is deze verzameling niet groot genoeg, maar vanuit het model gezien is deze "tegenspraak" niet zichtbaar: de afbeelding, die zou moeten aangeven dat de reële getallen aftelbaar zouden zijn, zit eenvoudig niet in het model.

Voor een dergelijk aftelbaar model gelden nog meer curieuze eigenschappen. We weten dat een aftelbare verzameling overaftelbaar veel deelverzamelingen bezit. Om het model aftelbaar te kunnen houden, kunnen er in het model slechts aftelbaar veel deelverzamelingen van $\mathbb{N}$ voorkomen. Ook nu is dit geen tegenspraak, want een aftelling van de deelverzamelingen van $\mathbb{N}$ kan slechts buiten het model gegeven worden.

Een dergelijke uitwendige aftelling stelt ons in staat door een diagonaal proces een verzameling te construeren die niet in het model zit. Dat wil zeggen, de elementen van deze verzameling zitten wel in het model, maar de verzameling als geheel niet. Deze verzameling kunnen we echter ook opvatten als een nieuw predicaat dat we aangeven met Cor. Over Cor kunnen we spreken als we onze formele taal, waarin we over het systeem spreken, uitbreiden met het predicaatsymbool Cor. Verder breiden we het axiomastelsel uit met een aantal axioma's, waarvan we kunnen inzien dat ze over het door ons bedoelde predicaat Cor gelden.

Het gevolg van deze uitbreiding is dat we het model een nieuwe structuur erbij hebben gegeven. Dankzij die extra structuur kunnen we een nieuw deelmodel $M^{**}$ aangeven met een bijbehorende nieuwe interpretatie van alle ZF predicaten en axioma's, dankzij welke de hindernis aangegeven door

SHEPHERDSON kon worden overwonnen.

Laten we de interpretatie van ZF op het bovengenoemde deelmodel $M^{**}$ van het met Cor verrijkte aftelbare model aangeven door de formules van twee sterren te voorzien. Met iedere formule A uit ZF correspondeert weer een formule $A^{**}$, die handelt over $M^{**}$.

De oplossing van COHEN komt er nu op neer dat het predicaat Cor op een zodanige wijze wordt geconstrueerd dat het volgende geldt:

1) als ZF consistent is dan is de theorie $ZF_{Cor}$ die ik krijg door ZF met het predicaat Cor uit te breiden, opnieuw consistent;

2) als de formule A afgeleid kan worden in $ZF_{Cor}$, dan is de interpretatie van A op het deelmodel $A^{**}$ ook afleidbaar uit $ZF_{Cor}$:

$$ZF_{Cor} \vdash A \quad \text{impliceert} \quad ZF_{Cor} \vdash A^{**};$$

3) de interpretatie van de continuumhypothese in het deelmodel kan op grond van $ZF_{Cor}$ weerlegd worden

$$ZF_{Cor} \vdash \neg CH^{**}.$$

Met behulp van een dergelijke constructie kan nu bewezen worden dat de continuumhypothese niet uit ZF afleidbaar is. Stel namelijk dat $ZF \vdash CH$; dan volgt zeker $ZF_{Cor} \vdash CH$, want $ZF_{Cor}$ is een consistente uitbreiding van ZF. Uit 2) volgt dan dat $ZF_{Cor} \vdash CH^{**}$. In 3) zien we echter dat $ZF_{Cor} \vdash \neg CH^{**}$, dus $ZF_{Cor} \vdash CH^{**} \wedge \neg CH^{**}$, dus $ZF_{Cor}$ kan niet consistent zijn. Dit is in strijd met 1) zodat we een tegenspraak vinden. Derhalve is CH niet afleidbaar uit ZF.

*11.*

In het voorafgaande hebben we gezien dat op grond van het ZERMELO-FRAENKEL systeem de continuumhypothese noch zijn ontkenning afleidbaar zijn (analoge resultaten zijn voor andere formele systemen van de verzamelingenleer te bereiken). Dit betekent in feite dat de bestaande formele systemen ons in de steek laten, als het er om gaat het continuumprobleem te beslissen. Uit de onvolledigheidsstelling van GÖDEL volgt dat er altijd zinnen zijn die niet afleidbaar en niet weerlegbaar zijn (in een formeel systeem), maar daarvan kunnen we soms op andere wijze inzien of ze al dan niet waar zijn; ook dit is bij de continuumhypothese nog niet het geval.

Tenslotte zou men kunnen hopen dat een uitbreiding van het axioma-

stelsel ons in staat zou stellen het continuumprobleem te beslissen. Er zijn uitbreidingen geconstrueerd met een veelheid aan krachtige oneindigheidsaxioma's, maar in al deze systemen blijft het continuumprobleem onbeslisbaar.

We komen tot de conclusie dat voor een oplossing van het continuumprobleem wezenlijk nieuwe ideeën nodig zijn. De grondslagentheoretici hebben aangetoond dat de bekende axioma's geen oplossing geven. Men zou kunnen hopen dat deze nieuwe ideeën in wezen reeds aanwezig zijn in de ideeën van BROUWER over de spreiding en de waaier. Deze zouden het inzicht in de structuur van de machtsverzameling zodanig moeten vergroten dat het continuumprobleem beslisbaar wordt.

*Literatuur*


Algemeen overzicht

Andrzej MOSTOWSKI, *Thirty years of foundational studies*, lectures on the development of mathematical logic and the study of the foundations of mathematics in 1930-1964, Basil Blackwell, Oxford, 1966.

Andrzej MOSTOWSKI, *Recent results in set theory*, in: Imre LATAKOS (ed.), *Problems in the philosophy of mathematics*, pp. 82-96, North Holland Publishing Cy., 1967.

Hilbert's problemen

David HILBERT, *Gesammelte Abhandlungen*, dritter Band, pp. 290-329, Chelsea Publishing Company, Bronx, New York, 1965, (herdruk).

Tiende probleem

A.I. MAL'CEV, *Algorithms and recursive functions*, Wolters-Noordhoff, Groningen, 1970.

Julia ROBINSON, *Diophantine decision problems*, in W.J. LeVEQUE (ed.), *Studies in number theory*, pp. 76-117, Prentice Hall Inc., Englewood Cliffs, N.J., 1969.

N.N. VOROB'EV, *Fibonacci numbers*, Blaisdell Publ. Cy., New York - London, (vertaling uit het Russisch).

Ju.V. MATIJASEVIČ, *Enumerable sets are diophantine*, Soviet Mathematics, 11 (1970), 354-359 = Doklady Akad. Nauk SSSR, 191 (1970), 279.

Martin DAVIS, *An explicit diophantine definition of the exponential function*, Communications on pure and applied mathematics, 24 (1971), 137-145.

Hans HERMES(*), *Die Unlösbarkeit des zehnten Hilbertschen Problems*, Enseignement Mathématique (11), 18 (1972), 47-57.

Eerste probleem

Kurt GÖDEL(*), *What is Cantor's continuum problem?* American Mathematical Monthly, 54 (1947), 515-525; herziene herdruk in: P. BENACERRAF and H. PUTNAM, *Philosophy of Mathematics*, Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1964.

Andrzej MOSTOWSKI(*), *Widerspruchsfreiheit und Unabhängigkeit der Kontinuumhypothese*, Elemente der Mathematik, 19 (1964), 121-144.

Kurt GÖDEL, *The consistency of the axiom of choice and of the generalized continuum-hypothesis with the axioms of set theory*, Annals of Mathematics, Study 3, Princeton Univ. Press, Princeton, 1940.

J.C. SHEPHERDSON, *Inner models for set theory I, II and III*, Journal of Symbolic Logic, 16 (1951), 161-190; 17 (1952), 225-237; 18 (1953), 145-167.

Paul J. COHEN, *The independence of the continuum hypothesis, I and II*, Proceedings National Academy of Sciences U.S.A., 50 (1963), 1143-1148; 51 (1964), 105-110.

Paul J. COHEN, *Set theory and the continuum hypothesis*, W.A. Benjamin Inc., New York - Amsterdam, 1966.

Joseph R. SHOENFIELD, *Mathematical logic*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1967.

Andrzej MOSTOWSKI, *Constructible sets with applications*, North Holland Publishing Cy., Amsterdam, 1969.

J. Barkley ROSSER, *Simplified independence proofs, Boolean valued models of set theory*, Academic Press, New York - London, 1969.

De met (*) aangegeven artikelen van HERMES, GÖDEL en MOSTOWSKI zijn uitstekende, relatief eenvoudig gehouden inleidingen tot de in deze voordracht behandelde problemen.

MC SYLLABUS 18, 1973, 59-79

# ONTWIKKELINGEN OP COMPUTERGEBIED

A. VAN WIJNGAARDEN

Honderd jaar geleden stierf een verbitterd mens. Met deze zin hoop ik alvast duidelijk te maken dat het onderwerp van deze voordracht iets met geschiedenis te maken heeft, maar u zult zich wellicht afvragen of die uitspraak waar is en ook of hij zin heeft. Welnu, waar is hij zeker want er sterven zoveel mensen en er zijn zoveel mensen verbitterd. Als ik het hierbij liet dan zou de zin zeker ontbreken, en zelfs als ik erbij zeg dat deze man een wiskundige was, ook dan is het haast een trivialiteit, want er zijn weliswaar relatief niet zoveel wiskundigen onder de mensen, maar toch een heleboel en velen daarvan zijn verbitterd. Maar die man over wie ik het wou hebben, of over wie ik het nu eigenlijk helemaal niet wou hebben, maar die ik even nodig heb om de zaak waarover ik het wel wil hebben, namelijk de ontwikkeling van een computer in de laatste kwart eeuw, in een juister historisch perspectief te plaatsen, was een zeer speciale man. Maar daarover later.

Met een kleine historische inleiding zal ik u wat laten zien van de uitvindingen die zoal door de mensheid gedaan zijn op het gebied van de computer en haar voorlopers. Nu moet ik erbij zeggen dat het woord *computer* eigenlijk een wat vaag woord is. In onze moderne definitie is een computer hetzij een rekenautomaat hetzij een mens. Ik wil het echter niet over de constructie van mensen, maar over de constructie van rekenautomaten hebben. Ik heb een stuk van de geschiedenis alvast op het bord geschreven (tabel 1).

| | |
|---|---|
| -1100 | HAN PIN HO: Rekenstaafjes |
| - 800 | HOMERUS: Odyssee, Boek XVIII, vers 409 etc. |
| 100 | HERON VAN ALEXANDRIË: Pneumatica, Automata |
| 1623 | SCHICKART: Rekenmachine + - × ÷ |
| 1644 | PASCAL: Rekenmachine + - |
| 1674 | LEIBNIZ: Rekenmachine + - × ÷ |
| 1728 | FALCON: Ponskaart |
| 1738 | DE VAUCANSON: Verbetering van de ponskaartbesturing |
| 1808 | JACQUARD: Industriële vormgeving van de ponskaartbesturing |
| 1833 | BABBAGE: Analytical engine |
| 1876 | KELVIN: Integreermachine |
| 1931 | BUSH: Differential analyser |
| 1936 | TURING: Turingmachine |
| 1941 | ZUSE: Z3 |
| 1944 | AIKEN: Mark 1 |
| 1945 | VON NEUMANN: Stored-program computer |
| 1946 | ECKERT & MAUCHLY: ENIAC |
| 1949 | WILKES: EDSAC, invoerprogramma, subroutine |
| 1951 | RUTISHAUSER: Haakjesgebergte |
| 1952 | WILKES: Symbolisch adresseren |
| 1953 | WILKES: Microprogrammering |
| | ADAMS & LANING: Pseudocomputer |
| 1957 | FORTRAN |
| 1959 | BACKUS: Formele syntaxis |
| 1960 | ALGOL 60 |
| 1962 | VAN WIJNGAARDEN: Formele semantiek |
| 1966 | IBM Wien Formele definitie van PL/I |
| 1967 | DE BAKKER: Formele definitie van ALGOL 60 |
| 1968 | ALGOL 68 |

Tabel 1

U ziet daar een aantal jaartallen staan en daarachter één of meer eigennamen. Daar staat allereerst -1100, dat betekent het jaar 1101 voor Christus. De kleine discrepantie komt doordat de mensen na duizenden jaren Chinese, Indische en Arabische beschaving hier in de westerse wereld nog steeds niet tot de ontdekking gekomen zijn dat nul toch eigenlijk een getal is. Het doet er overigens ook helemaal niet toe, want het jaartal is maar een ruwe schatting. In ieder geval is er in die tijd de Chinees HAN PIN HO die de rekenstaafjes, de voorloper van de Chinese abacus, uitdenkt. Hier schuilt ook nog een andere kleine onnauwkeurigheid: die naam heb ik verzonnen, want ik had achter ieder jaartal graag minstens één naam staan. Bovendien is het van wiskundig standpunt aanvaardbaar. Ik kan weliswaar niet bewijzen dat hij HAN PIN HO heette, maar u kunt ook niet bewijzen dat hij niet zo heette. Mogelijk is de abacus trouwens al duizenden jaren daarvoor in Mesopotamië uitgevonden. In ieder geval is eens de gedachte geboren mechanische hulpmiddelen te gebruiken om beter te kunnen rekenen.

Dan krijg ik (zie tabel 1) twee schrijvers, HOMERUS en HERON, twee Grieken die beiden over automaten berichten. De eerste man van wie wij dat weten is HOMERUS. Ik zal u een stukje uit de *Ilias* voorlezen in de vertaling van TIMMERMAN. Het gaat over het bezoek van Thetis aan Hephaistos. U weet: Hephaistos was de god van de onderwereld, een grote knappe smid die alles kon maken en ook alles maakte. Bovendien kon hij niet goed lopen want hij was een keer van de Olympus afgegooid. Ik had het u eigenlijk liever in het Grieks voorgelezen, want dat klinkt mooier, maar mogelijk zou de informatie slecht overkomen.

*Aldus sprak hij, de reus, en stond hijgende op van het aambeeld;*
*Hinkend en strompelend hipten zijn magere schenen beneden!*
*Daarop keerd' hij de balgen van 't vuur af en al zijn gereedschap*
*Waar hij mee werkte, dat bracht hij bijeen in een zilveren werkbak,*
*Wies met een spons zijn gezicht en zijn krachtige nek en zijn handen,*
*Beide, en harige borst af en dook in zijn chiton en nam zijn*
*Stevige stok en manklopend ging hij naar buiten en wieglend*
*Steunden ook gouden slavinnen, als levende meisjes, hun meester.*
*Zij hebben óók in hun borst wel verstand en een stem en ook wilskracht;*
*Kennen ook, door d' onsterflijke Goden geleerd, wel een handwerk!...*
*Zij dan nu zwoegden, terwijl zij hun meester aan twee kanten steunden.*

Dus u ziet, Hephaistos had goed van zijn kunde gebruik gemaakt. Hij had

zich een stel slavinnen gesmeed, van goud notabene, die hem steunden. Ze konden nog denken ook, zegt HOMERUS, de Goden hadden hun dat geleerd, en ook nog praten. Ik moet toegeven dat HOMERUS misschien niet altijd de meest geloofwaardige bron vormt voor wetenschappelijke informatie, maar in ieder geval was de conceptie van de automaat bekend.

HERON daarentegen is een meer geloofwaardige schrijver uit 100 na C., die leefde in Alexandrië. Deze man maakte zelf automaten en heeft daarover bericht. Hij heeft namelijk de constructie van automaten beschreven in twee boeken: het ene heet *Pneumatica* en het andere *Automata*. Nu zijn we midden in de geschiedenis. U ziet, hier is de uitvinding van de automaat. Zijn automaten hebben overigens niets met rekenen te maken, maar met meer praktische zaken als het openen van tempeldeuren. Eerst was er de behoefte om te kunnen rekenen, nog heel primitief, dan de uitvinding van de automaat.

Nu springen we weer een hele tijd over, nl. tot de uitvinding van de rekenmachine, door Wilhelm SCHICKART, een Duitser. Zijn rekenmachine kan optellen en aftrekken, vermenigvuldigen en delen. Hij heeft haar beschreven in een brief aan KEPLER. Zijn machine is niet bewaard gebleven, maar in elk geval weten wij uit zijn beschrijving ongeveer hoe ze eruit gezien moet hebben. In dat jaar, 1623, wordt ook Blaise PASCAL geboren en in 1641 vindt PASCAL ook een rekenmachine uit. Hij kan alleen maar optellen en aftrekken, maar er is meer van bewaard gebleven. Gottfried Wilhelm LEIBNIZ is er al dertig jaar mee bezig geweest om te kijken of hij ook een rekenmachine kon maken, als hij in 1674 zover is. Hij maakt ook een rekenmachine, maar weer eentje die ook kan vermenigvuldigen en delen. Bovendien is de machine van LEIBNIZ zo doordacht dat het ontwerp daarvan doordringt in latere machines en, ik spring nu weer 200 jaar verder, in 1870 kan de industrie ook inderdaad rekenmachines maken. Er verloopt altijd een grote spanne tijds tussen het hebben van de idee en het maken van de eerste modellen tot het in werkelijke technische produktie brengen van de uitvinding. Het duurde hier ongeveer 200 jaar.

De mens kent nu de automaat en hij kent de rekenmachine, maar hij is nog ver van de rekenautomaat, want daar is nog iets anders voor nodig, nl. de automatisering van het lezen, schrijven en onthouden. We kijken naar 1728, als FALCON de ponskaart uitvindt ter besturing van het weefgetouw. Een weefgetouw dient om damast te maken, u weet wel, met die ingewikkelde patronen vol wapens en bloemen voor de lakens van de adel, en dat is een verschrikkelijk werk. In 1728 dan vindt FALCON de Jacquardkaart uit, zoals

ik het nu zeg, maar JACQUARD was nog niet geboren en wist dus nog nergens van. In 1738 verbetert DE VAUCANSON, een groot automatenbouwer, die ponskaartbesturing. Maar in 1808, door de grote economische pressie van de blokkade van Frankrijk door Engeland (het continentale stelsel) gedwongen, wordt het streven naar autonomie steeds groter en JACQUARD maakt van deze oorspronkelijke uitvinding een geheel industrierijp produkt.

De ponskaart is hier ingevoerd als besturingselement voor het weefgetouw, maar u herkent gemakkelijk hierin ook de informatiedrager, het *geheugen*, benodigd om de in het te weven patroon bevatte informatie te onthouden. Ook hier verlopen overigens tussen de oorspronkelijk idee en de technische uitvoering zo'n tachtig jaar. In ieder geval heeft de laatste knaap het zo goed gedaan dat in dit verband die andere twee helemaal vergeten zijn.

Nu zien wij een aantal zaken bij elkaar. De mens wil rekenen. Hij heeft daarvoor een rekenmachine uitgevonden, maar daar moet hij zelf nog aan draaien. Hij heeft automaten uitgevonden, maar die kunnen niet rekenen. Hij heeft apparatuur gevonden, waarmee hij informatie sneller in het systeem kan brengen en waarmee hij ingewikkelde besturing kan regelen, de *ponskaart*, maar weefgetouwen zijn geen rekenmachines, en ook geen automaten. In 1833 is er dan een Engels wiskundige, Charles BABBAGE, die op dat moment het idee heeft om een en ander te combineren en een rekenautomaat te maken, de "analytical engine". Ik moet erbij zeggen, een alleraardigste man die BABBAGE. Als student was hij al lid, met enkele andere knapen, van een vereniging in Cambridge (de Analytical Society), die ten doel had de fluctuties van NEWTON uit het Engelse onderwijs te verdrijven en de notatie van LEIBNIZ erin te krijgen. Hij heeft wel succes daarmee gehad, zoals u weet. Wij hebben hier dus te maken met een man die heel oorspronkelijk was, maar ook één die veel interesse had voor juiste formulering, en dat klopt, want dat hebben computermensen nog steeds. Deze man nu was degene die in 1871 stierf als een verbitterd mens en ik geef hem geen ongelijk. Hij had zijn leven besteed aan het maken van een machine, een fantastische machine, maar alles zat tegen en uiteindelijk liep alles op niets uit. Het had hem niet aan hulp ontbroken, want hij had van de Engelse regering een subsidie gekregen van £ 14.000, wat in die tijd een geweldig kapitaal was. Technisch was het probleem heel moeilijk en voordat het ding een beetje klaar kon komen liep zijn instrumentmaker weg; hij kreeg ruzie met BABBAGE en nam volgens het contract alle gereedschappen mee. BABBAGE heeft geprobeerd wat

hij kon, maar de technische ontwikkeling van die tijd liet eenvoudig niet toe om zoiets te maken. Ik moet zeggen dat ik nog grote schroom zou hebben een project te entameren om een door stoom gedreven automatische rekenmachine in elkaar te zetten. Het is dan ook niet gelukt, maar dat wil niet zeggen dat zijn pogingen geen directe resultaten nagelaten hebben. Het is uit historisch oogpunt goed om te onthouden dat een van zijn instrumentmakers de heer Whitworth was. Deze mijnheer Whitworth ontdekte dat je, om nauwkeurige apparaten te maken, werkmethoden moest ontwikkelen die eenvoudig beter waren dan de bestaande techniek toeliet. Hij moest dus betere technische methoden ontwikkelen en hieruit kwam onder andere het standaardmodel van de schroefdraad voort, de eerste genormaliseerde technische constructie. U ziet hier ook weer dat uit wetenschappelijk onderzoek alle mogelijke resultaten komen, mogelijk niet bedoeld maar toch heel belangrijk.

Het duurde nog driekwart eeuw voor BABBAGE's droom werkelijkheid werd, maar in die tussentijd, in 1876, kreeg lord KELVIN, die helemaal geen KELVIN heette maar THOMSON, zoals u weet, het idee om een machine te maken om differentiaalvergelijkingen automatisch op te lossen. Hij heeft precies beschreven hoe je het doen moet, maar er ontbrak een kleinigheid aan, nl. een energieversterker, want een perpetuum mobile bouwen kon zelfs KELVIN niet. In ieder geval, het ding werkte niet. Logisch werkte het wel, maar niet in werkelijkheid. KELVIN begreep dat ook drommels goed. Dit idee werd later, in 1931, opgenomen door Vannevar BUSH. Deze ontwikkelde de "differential analyser". Dat is een machine die het ontwerp van KELVIN navolgt, maar met die kleinigheid erbij, doordat hij precies dat elementje erin bouwde, de koppelversterker, dat nodig was om het apparaat ook werkelijk te laten werken. Die differential analyser was eigenlijk de eerste rekenautomaat die werkte. Alleen was het niet een rekenautomaat in de zin van een mechanisme dat met cijfers werkt, digitaal, maar het werkte met rotaties van assen en dat soort dingen meer. Deze automaten, analogonrekenautomaten, hebben een belangrijke bijdrage tot de research geleverd, maar zij missen toch het wezenlijk universele dat de digitale rekenautomaten kenmerkt.

Nu komen we tot de oertijd van de computer. In 1936 vindt de Engelse logicus en wiskundige Alan TURING een rekenautomaat uit die niet onderworpen is aan fysische wetten of temperatuurverschillen; hij werkt altijd. Het is namelijk een geesteskind van papier en potlood. Hij kan alles, dat wel, maar het is geen gemakkelijke machine; het is heel lastig om ermee te werken. Die abstracte Turingmachine is een heel belangrijke stap gebleken in

de fundamentele theorie van de rekenautomaten, maar vooralsnog leek het meer een zijspoor in de ontwikkeling. TURING was overigens een groot man, die later ook daadwerkelijk interesse in echte rekenautomaten had en aan hun ontwikkeling heeft bijgedragen.

Nu begint de ontwikkeling van de echte computer. In de veertiger jaren leven Konrad ZUSE in Duitsland en Howard AIKEN in Amerika, ver van elkaar gescheiden. Ze wisten van elkaars bestaan niet af. AIKEN wist van de ideeën van BABBAGE, ZUSE beweert daar nooit van gehoord te hebben, maar in ieder geval begonnen ze onafhankelijk van elkaar automatische rekenmachines te maken, en nu met de toenmalige stand van de techniek, dus met gebruik van electriciteit en relais, zoals die in telefooncentrales gebruikt werden. En beiden slaagden erin; ZUSE in 1941 en AIKEN in 1944. ZUSE woonde in Berlijn. Telkens als hij een machine klaar of driekwart klaar had, werd zij gebombardeerd en moest hij weer een nieuwe bouwen. Maar iedere keer werd zij wel beter, dat moet gezegd worden. De laatste, gedeeltelijk gereedgekomen machine werd aan het eind van de oorlog gauw naar Beieren vervoerd en daar heeft zij de oorlog overleefd. Eigenlijk was het al niet meer helemaal een relaisrekenmachine, want er waren stukken met electronica ingebouwd. Dit was tevens haar ondergang, want gaandeweg werd de machine kleiner en kleiner omdat de radiobuizen bij de boeren tegen boter en aardappelen ingeruild werden. Daarmede is ook voor vele jaren in Duitsland de ontwikkeling van de rekenautomaten op nonactief gesteld.

Meer succes had AIKEN met zijn Mark I, gebouwd op zijn aanwijzingen door IBM met conventionele hulpmiddelen. De machine heeft jarenlang intensief gewerkt en onder andere een serie tabellen van speciale functies berekend, waar tegenwoordig niemand meer naar kijkt, zoals Besselfuncties van orde 65 en zo. De machine was de eerste van de echte rekenautomaten; succesvol, maar tevens als fossiel geboren. Door de conventionele constructie was de snelheid, in onze ogen, gering. Een vermenigvuldiging vergde 6 seconden (van getallen met 23 decimalen weliswaar).

De ontwikkeling van de electronica had evenwel geheel nieuwe mogelijkheden geschapen en in 1946 stelden ECKERT en MAUCHLY de ENIAC in dienst, een volledig electronische rekenautomaat, die voor een vermenigvuldiging nog maar 3 milliseconden nodig had (van getallen met 10 decimalen weliswaar). Dat betekende een snelheidssprong met een factor duizend in één jaar en hier begint, nu dus 25 jaar geleden, het tijdperk van de onbegrijpelijk snelle computer. Die 25 jaar hebben er nog eens een factor tiendui-

zend aan toegevoegd, maar daarnaast zijn er nog veel andere, mogelijk meer fundamentele zaken gevonden.

Een wezenlijke bijdrage tot de rekenautomaat kwam van de wiskundige John Von NEUMANN. Hij had het ENIAC-project begeleid, maar vond in 1945 (dus nog voor de ENIAC in bedrijf werd gesteld) iets geheel nieuws uit. Een rekenautomaat moet rekenen en er moeten dus allerlei getallen in bewaard worden. Maar het is ook een automaat en dus moeten ook allerlei opdrachten onthouden worden. In de opzet van BABBAGE en in die van de Mark I en de ENIAC zijn dit geheel verschillende zaken. In de ENIAC werden bijv. getallen bewaard in een tiental registers, terwijl het programma gegeven werd door een schakeling met snoeren en stekkers. Het idee van Von NEUMANN was nu dat die getallen en opdrachten beide informatie zijn en op gelijke wijze opgeslagen dienden te worden in een geheugen. Daarmee is dan ook de mogelijkheid geboden om op de opdrachten, net als op de getallen, zekere bewerkingen uit te voeren, zoals het modificeren van het adresgedeelte. Het was een revolutionaire gedachte en het is waarlijk het sluitstuk op de reeks van ideeën die nodig waren om tot de rekenautomaat in onze moderne zin te komen. Von NEUMANN gaf zelf een aantal richtlijnen voor de ontwikkeling van rekenautomaten langs deze lijn, maar het duurde nog enkele jaren tot in mei 1949 de eerste "echte" computer gereedkwam, de EDSAC, door Maurice WILKES in Cambridge (Engeland) ontworpen. Het ontwerp en de bouw had drie jaar in beslag genomen, wat lange tijd een record was. Het effect van het ter beschikking komen van een echte computer in een universitair milieu was enorm.

Hiermee is de voortijd van de computer afgesloten. Sinds de EDSAC zijn vele experimentele machines gebouwd en na een aantal jaren werd de ontwikkeling en bouw door de industrie overgenomen. Na veel vallen en opstaan werd het huidige groeipatroon bereikt, waarin bijna elk jaar het aantal computers, de gemiddelde snelheid en de geheugenomvang verdubbelen. Gelukkig gaat de prijs naar verhouding veel langzamer omhoog, zodat men steeds meer waar voor zijn geld krijgt. Dit mag alles weinig met wiskunde te maken schijnen te hebben, maar in werkelijkheid heeft het er alles mee te maken. Meer computers betekent dat meer mensen de mogelijkheid hebben ze te gebruiken, en hogere snelheid en groter geheugen betekenen dat omvangrijker onderzoekingen kunnen worden verricht.

Van principieel belang is het voor de wiskundige of de snelheid nog willekeurig ver kan worden opgevoerd, met andere woorden of hij te zijner tijd in een bepaalde tijdspanne een willekeurig lange keten van gevolgtrek-

kingen en combinaties kan laten uitvoeren. Dit blijkt helaas niet het geval te zijn. Op het ogenblik naderen de tijdseenheden die in een computer een rol spelen de nanoseconde. In een nanoseconde legt het licht een afstand van 30 centimeter af en dus moeten de schakelonderdelen van de computer bijzonder klein gemaakt worden om de signalen in staat te stellen zonder te veel vertraging hun loop door de schakelingen te volbrengen. Dit verkrijgt men door de computerschakelingen als een soort kristal te laten groeien. Wat vroeger bijvoorbeeld een vacuümbuis was, is eerst een transistor geworden en nu nog slechts een microscopisch klein onderdeel van een geïntegreerde schakeling. Dit proces van verkleining kan echter niet onbeperkt doorgaan, want, voorzover de fysica het bij het rechte eind heeft, we komen vroeg of laat bij afstanden waar de onzekerheidsrelatie van HEISENBERG een rol gaat spelen en dan vervalt de basis aan het begrip informatie-overdracht. Voorlopig zijn we daar echter nog niet aan toe. Een goede raad wil ik hieraan toevoegen. Als u werkelijk erg groot rekenwerk hebt, begin er dan niet aan. Immers, als u nu met die berekening begint op een bepaalde machine, dan hebt u na, zeg, 20 jaar het resultaat van de berekening. Stelt u de berekening echter 10 jaar uit, dan zijn de computers 1000 maal zo snel en kost de berekening nog maar een week. Deze redenering is na 10 jaar echter ook nog geldig. Die eerste berekening is dan namelijk niet echt groot meer. Zo moet men zich ook nooit laten overhalen om naar een ster geschoten te worden. De maan dat gaat nog, maar als de ster ver weg is, loopt men het gevaar onderweg ingehaald te worden door een raket die jaren later is ontwikkeld en dus ook veel sneller is!

De ontwikkeling van de computer heeft heel veel te danken aan wiskundigen. Het ontwerp van zo'n ingewikkelde constructie was voor velen een interessante uitdaging. Al spoedig werd het mede dankzij die wiskundigen van een kunst tot een technische wetenschap, de *toegepaste logica*. Al die schakelingen zijn natuurlijk te beschrijven met gewone logische formules en de uitwerking daarvan kan weer met de computer geschieden. Op deze wijze is het ontwerp geautomatiseerd en daarmee was de aardigheid er een beetje af.

De wiskundigen ontdekten echter al spoedig een veel interessanter onderwerp: niet het maken van computers maar het maken van programma's voor computers. We hebben daar tegenwoordig twee woorden voor in het Nederlands: *apparatuur* (dat is het geheel van koper, silicium, vacuüm, en zo) en *programmatuur* (dat is wat men er bij moet schrijven om de zaak aan de gang te krijgen en te houden). De Engelsen zeggen *hardware*, dat is een woord dat

bestond (ijzerwaren en zo), voor apparatuur en *software*, dat niet bestond, voor programmatuur. Goed, in 1949 was er dus een computer waar WILKES mee werkte. Als men een bepaalde berekening correct geprogrammeerd had, dan was het ding ontzaglijk gauw klaar met de berekening. De droeve werkelijkheid voor de meeste niet wonderlijk begaafde programmeurs was, dat ze misschien weken nodig hadden om hun probleem te programmeren om dan van de machine binnen uiterst korte tijd niet het antwoord te ontvangen, maar de mededeling dat het programma fout was. De moeilijkheid van het rekenen was nu niet meer het tijdrovende uitvoeren van de rekenhandelingen (dat deed de computer), maar het tijdrovende programmeren. Het lag voor de hand nu te proberen die programmeervaardigheid op dezelfde manier op te peppen als met de rekenvaardigheid van de mens was gebeurd, nu door het programmeren te automatiseren. De vraag zouden wij nu zo stellen: "Kun je het maken van de programma's ook aan de computer overlaten? Die dingen kunnen toch alles!"

De moeilijkheid van het probleem schuilt er natuurlijk in, dat men de computer toch op een of andere wijze moet vertellen wat men berekend wenst te hebben. Welnu, WILKES maakte niet alleen een computer, maar hij introduceerde tegelijk twee fundamentele programmeerideeën, het *invoerprogramma* en het *subprogramma*.

Men kan nu wel zeggen, dat de opdrachten van een uit te voeren programma zich in het geheugen van de computer moeten bevinden evenals de getallen waarmee gerekend wordt, maar er rijst direct een moeilijkheid. Hoe komen die opdrachten dan in de computer? Blijkbaar moeten die ingelezen worden, maar wie dwingt de computer daar dan toe? Natuurlijk een programma. Maar hoe komt dit programma dan in de computer? Men ziet hier de impasse van de kip en het ei. De oplossing is, dat er een speciaal programma (het invoerprogramma) is dat in staat is elk ander programma in te lezen. Dit invoerprogramma moet dan met speciale hulpmiddelen in het geheugen worden gebracht. De eerste invoerprogramma's waren nog heel primitief, maar naarmate de computers over meer geheugenruimte beschikten kon het invoerprogramma uitgebreider worden, waardoor het de programmeur van allerlei lastige taken kon verlossen. Enkele principiële stappen in dit proces zullen we nog tegenkomen.

Het komt in een berekening vaak voor dat een bepaald stukje programma op een aantal plaatsen nodig is, bijvoorbeeld ter berekening van een vierkantswortel. Het is uit ruimte-overwegingen oneconomisch een dergelijk subprogramma evenzovele malen op te nemen, maar men plaatst het eenmaal in het

geheugen en iedere keer dat de vierkantswortel nodig is, onderbreekt men de reeks opdrachten om dat subprogramma uit te voeren. De moeilijkheid is, dat na afloop de oorspronkelijke reeks opdrachten weer op de juiste plaats hervat moet worden. Het subprogramma moet dus het terugkeeradres onthouden en WILKES vond een sierlijke oplossing voor dit vraagstuk, gebruik makend van de eigenschap dat de computer op opdrachten kan opereren alsof het getallen zijn, wat immers de grondgedachte van Von NEUMANN was.

In 1951 komt Heinz RUTISHAUSER, een Zwitsers mathematicus, met een heel nieuw idee, het *automatisch programmeren*. Hij merkt op dat de opdrachtencode van de machines om technische redenen verschrikkelijk primitief is en dat ze de programmeur dwingt om allerlei zaken, waarvoor hij in de wiskunde eenvoudige uitdrukkingswijzen kent, op moeizame wijze tot uitdrukking te brengen. Een formule als bijv. $a \times (b + c) - d$ moet door de programmeur in elementaire handelingen worden ontleed. RUTISHAUSER vond dat de computer dat dan maar moest gaan leren. Daar komt heel wat bij kijken, want de computer moeten de voorrangsregels van operatoren worden bijgebracht. Dit is echter een logisch, geheel te analyseren proces en een invoerprogramma zou die taak op zich kunnen nemen. Het invoerprogramma fungeert dan als een vertaler van de *taal* waarvan de programmeur zich bedient naar de taal waarvoor de machine is gebouwd. Daarbij komt een hele rij problemen aan de orde. De voorrangsregels noemde ik al, maar veel eenvoudiger problemen, zoals het herkennen van wat wij nu een identificator noemen (als in die formule $a$, $b$, $c$ en $d$) en het omzetten daarvan in machine-adressen, is al niet eenvoudig. RUTISHAUSER had dus enkele heel goede ideeën, maar hij had ook een handicap: hij had zelf nog geen rekenmachine in huis. Hij had er wel eentje, hij had namelijk de Zuse 4 in huis, die uit Duitsland overgebracht was, maar dat ding werkte niet zo best, en hij was met anderen zelf een machine aan het bouwen, maar die was nog niet klaar. RUTISHAUSER kon op dat moment dus nog niet zoveel proberen als wel nodig was.

Ondertussen gaat WILKES door en in 1952 introduceert hij het begrip *symbolisch adresseren*. In de rekenmachine bevinden de getallen en opdrachten zich op zeer bepaalde adressen. WILKES zag, ondanks het feit dat hij in abstracto nog niet zover was als RUTISHAUSER, dat in ieder geval de precieze adressen logisch irrelevant waren en dat alleen over zekere trajecten de volgorde ter zake deed. Tot groot profijt van de programmeur keilde hij de vaste adressen overboord. Dat was een belangrijke stap in de richting die RUTISHAUSER gewezen had.

In 1953 introduceert WILKES weer een nieuw idee, het *microprogrammeren*. Tot dusverre was er een streng onderscheid tussen apparatuur en programmatuur. Als men evenwel de werking van bijv. de opteller in een computer beschouwt, dan ziet men dat zich daar eigenlijk in het klein weer een rekenprocesje afspeelt. Twee cijfers worden opgeteld in een kolom, een overdracht wordt doorgegeven en weer opgeteld bij de twee cijfers in de kolom links ervan, enz. Dat rekenprocesje moet door een of andere schakeling geschieden, maar deze schakeling kan ook gezien en uitgevoerd worden als een heel speciaal computertje met een heel speciale miniopdrachtencode. Daarmee was de grens tussen ontwerp en gebruik van de computer vervaagd. In de eerste plaats stelde de idee van de microprogrammering de constructeurs in staat de computers op een meer systematische wijze op te bouwen. Zelfs is het mogelijk de microprogrammering gedeeltelijk aan de programmeur over te laten, zodat de programmeur de machine aan zijn speciale probleem kan aanpassen.

Daar is allemaal eigenlijk weinig van terecht gekomen. Veeleer is de ontwikkeling de andere kant uitgegaan, doordat het vroeger zo eenvoudige invoerprogramma uitgedijd is tot een ware bureaucratie, het *bedrijfssysteem*, dat de programmeur onder het mom van de helpende hand te bieden, stevig aan banden legt en hem dwingt allerlei irrelevante gegevens te verschaffen. Hoe het ook zij, wat de programmeur ervaart als gegeven apparatuur en vrije programmatuur hoeft geenszins samen te vallen met wat technisch onder de apparatuur of de programmatuur zou horen te vallen.

De tegenhanger van de microprogrammering is de *macroprogrammering*, waarbij men een programma maakt, dat zich als een andere machine gedraagt, dus een nieuw programma inleest dat voor de echte machine volkomen onbegrijpelijk zou zijn, maar voor de pseudomachine wel begrijpelijk is. Dit idee is ook in 1953 ontwikkeld, nl. door ADAMS en LANING. In 1953 was er nl. een Summer School in Cambridge, maar nu aan de andere kant van de oceaan, waar de Whirlwind werkte, de snelste computer van zijn tijd. Op die Summer School wilde men cursisten leren programmeren, maar de code van de Whirlwind was een beetje ingewikkeld en men wilde het wat eenvoudiger doen. Men liet de Whirlwind zich daarom als een eenvoudige computer gedragen. Tegenwoordig vindt men zoiets heel normaal, maar alles wat we tegenwoordig heel normaal vinden moet toch eerst eens zijn uitgevonden. Voor de cursisten was niet de Whirlwind op zichzelf interessant, maar alleen de Whirlwind met dat macroprogramma erin. Die combinatie was dus in feite de machine

waarover het ging, en waarom geef je dat ding dan ook geen andere naam? Goed, de machine zelf heette de Whirlwind, maar met dat stukje extra programmatuur heette zij de "Summer School Computer".

Nu begint een tijdperk van grote activiteit om de toegang tot de computer gemakkelijker te maken. In de eerste jaren, toen er nog maar enkele computers waren, waren de gebruikers enerzijds niet veeleisend en anderzijds ook "geboren" programmeurs die de gebrekkige machinecodes en de handicap van een uiterst kleine omvang van het machinegeheugen meer als een uitdaging dan als handicap beschouwden. Naarmate er meer en meer machines kwamen, werden de gebruikers van lager gemiddeld gehalte en evenredig veeleisender. Aan de andere kant waren de machines sneller en kwam vooral meer geheugen ter beschikking, zodat wat efficiency opgeofferd kon worden ten behoeve van het gerief van de programmeurs. In het voetspoor van de bovengenoemde ontwikkelingen werden nu allerlei codes, z.g. autocodes, ontwikkeld die het programmeren eenvoudiger maakten. Een van de allereerste verbeteringen was daarbij dat de programmeur de beschikking kreeg over z.g. drijvende punt aritmetiek, waardoor de getallen waarmee hij rekende, niet meer beperkt waren tot het bereik van -1 tot 1, maar praktisch van $-\infty$ tot $\infty$. Dit maakte het schalen van grootheden overbodig, een van de moeilijkste en tijdrovendste taken van de programmeur. Spoedig werd trouwens ook de apparatuur hieraan aangepast, doordat de operaties met drijvende punt aan de standaardcode van de machines werden toegevoegd.

De eerste autocodes waren nog maar sterk verbeterde machinecodes. Weliswaar kon men voor een geheel getal wellicht de identificator $i$ gebruiken en voor een drijvende punt getal $x$ in plaats van met adressen te scharrelen, maar de programma's bleven toch typisch machinegebonden. Ver daarboven rees het tot stand komen van FORTRAN in 1957, een echte taal, waarin de programmeur zich kon uitdrukken met een gemak en helderheid als nooit daarvoor bereikt was. FORTRAN veroverde dan ook snel een grote bekendheid en gebruikskring. In de loop van de jaren werd de taal wel een weinig verbeterd, maar niet op essentiële wijze. Ondanks het feit dat er gaandeweg principieel aantrekkelijker en machtiger talen ontwikkeld zijn, blijft FORTRAN hardnekkig doorleven.

In de jaren 1958-1962 is een voor de wiskunde zeer interessante taal ontworpen, nl. ALGOL 60. Doordat het ontwerp een internationale onderneming was waarbij vele programmeurs en wiskundigen uit de hele wereld betrokken waren, was het produkt eenvoudig een orde beter dan FORTRAN en is er bij

wiskundigen dan ook veel beter ingegaan. ALGOL 60 is een taal die door heel Europa gebruikt wordt. Europa reikt in dit geval tot Wladiwostok en aan de andere kant, met wat uitspattingen, in Amerika tot Californië.

Met de ontwikkeling van ALGOL 60 is het moment aangebroken dat formele talen ontwikkeld worden die de mens aanspreken, die niet makkelijk zijn voor de machine, maar die makkelijk zijn voor de mens. Nu moet echter de computer geleerd worden om zulk een taal te verstaan. Een programma dat dat leert, heet een *vertaler*; compiler zeggen de mensen tegenwoordig meestal, wat eigenlijk een rare naam is. De eerst ALGOL 60-compiler is in Amsterdam gemaakt onder leiding van DIJKSTRA.

Met de ontwikkeling van ALGOL 60 is evenwel ook een nieuw gebied van research begonnen, de ontwikkeling van metatalen. In 1959 vindt John BACKUS, wiskundige, vader van FORTRAN en ALGOL 60-auteur, een methode om de syntaxis van een formele taal te beschrijven. Als men nl. een formele taal wil definiëren dan moet die definitie natuurlijk ook weer in een taal geschreven zijn, een *metataal*. Bij FORTRAN werd daarvoor gewoon Engels gebruikt, maar BACKUS vond een formalisme waarmee grote gedeelten van de grammatica van een taal als ALGOL 60 konden worden beschreven op een voor een wiskundige aanvaardbare en sierlijke wijze. Logici kenden dergelijke formalismen al, maar kwamen nooit toe aan het gebruik ervan. Zij waren meer geïnteresseerd in moeilijkheden en onmogelijkheden die zich zouden kunnen voordoen bij het gebruik ervan dan in dat gebruik zelf. Bij de beschrijving van ALGOL 60 bleek echter het formalisme van BACKUS een uitkomst en de publicatie van het ALGOL 60-Rapport maakte het formalisme populair als BNF, de Backus-Naur-Form.

Het formalisme van BACKUS heeft echter maar een beperkt vermogen. Het kan nl. slechts een gedeelte van de syntaxis van een taal definiëren en niets van de semantiek. De syntaxis onderscheidt welke zinnen in een taal kunnen voorkomen. Zo zegt de syntaxis van het Nederlands dat "Het paard loopt op straat" of "Ik loop op straat" wel en "De paard loop op straat" niet een Nederlandse zin is en dit zou ook kunnen worden beschreven in BNF. Men kan echter aantonen dat niet de hele Nederlandse syntaxis zo kan worden beschreven. De semantiek, die leert wat de betekenis van de zin is, valt helemaal buiten het bereik van BNF. Dat is voor het Nederlands niet zo erg, want het is niet recht duidelijk wat de betekenis van "betekenis" is.

Bij een programmeertaal ligt de zaak anders. Daar is de betekenis van een programma volledig gedefinieerd door de acties die de computer op grond

van dat programma uitvoert en omdat de computer zelf een wel gedefinieerd apparaat is, ligt het voor de hand om ook de formalisering van de semantiek te lijf te gaan. Vanaf 1962 zijn methoden ontwikkeld om de semantiek te formaliseren en in de jaren 1966-1968 kwamen formele definities van PL/I, dat is een onecht kind van FORTRAN en ALGOL 60, en van ALGOL 60 tot stand.

In De BAKKER's formele beschrijving van ALGOL 60 wordt een automaat gedefinieerd die een tekst kan lezen bestaande uit een formele definitie van een taal, hier ALGOL 60, en een daarin geschreven programma. Deze automaat zorgt er dan voor dat dat programma geïnterpreteerd wordt volgens die definitie van de taal. Natuurlijk moet de automaat zelf ook worden gedefinieerd. Daarvoor wordt de automaat gedefinieerd door een in ALGOL 60 geschreven programma dat uiteenzet hoe de automaat op een willekeurige invoerband reageert. Wanneer men niet weet wat ALGOL 60 is, kan men dus ook niet begrijpen hoe de automaat werkt en dus de z.g. definitie van ALGOL 60 zal interpreteren. Maar als men uit een informele beschrijving een idee van ALGOL 60 heeft gekregen dan heeft men ook een idee van de werking van de automaat door het definiërend programma te lezen. Dan krijgt men vervolgens een nieuwe en mogelijk betere indruk van ALGOL 60 door na te gaan hoe de automaat op de definitie van ALGOL 60 reageert. Dit spel kan men itereren en er zijn drie mogelijke uitkomsten. De eerste mogelijkheid is dat men na enige tijd twee keer achter elkaar hetzelfde beeld van ALGOL 60 heeft gekregen. Voortgaan heeft dan geen zin meer en men heeft een consistent beeld van ALGOL 60. De tweede mogelijkheid is dat men na een groot aantal iteraties steeds een nieuw beeld van ALGOL 60 krijgt. Het ligt dan aan het uithoudingsvermogen van de lezer of hij nog een keer wil itereren dan wel iets anders gaan doen. De derde mogelijkheid is dat men een beeld van ALGOL 60 krijgt dat niet het beeld was van één iteratie daarvoor, maar van enkele iteraties daarvoor. Deze situatie is kennelijk hopeloos en de lezer wordt aangeraden een ander vak te kiezen. Hierbij moet nog worden opgemerkt dat in het eerste geval nog niet gezegd is dat men het "goede" beeld van ALGOL 60 heeft gekregen. Het enige wat wij kunnen zeggen is dat het een consistent beeld is. Als een ander hetzelfde experiment uithaalt en ook tot zo'n consistent beeld komt, dan volgt daar niet uit dat dit hetzelfde consistente beeld is. Om uit te maken of die twee beelden identiek zijn is een probleem waarvoor geen algoritme bestaat die in een eindig aantal stappen tot een conclusie komt. Het enige wat men zou kunnen proberen is gezamenlijk een aantal programma's bestuderen en zien of de verwachte uitkomsten

van die programma's dezelfde zijn. Treft men een programma waarvan de een meent dat het zus en de ander dat het zo zal aflopen, dan weet men natuurlijk dat de twee beelden wel consistent maar niet gelijk zijn. Zolang men echter zo'n programma niet ontdekt heeft weet men niets. Gelukkig loopt het zo'n vaart niet. Het lezen van zo'n formele beschrijving is zo moeilijk dat men wel nooit tot een dergelijke wedstrijd zal overgaan.

In 1965 tenslotte wordt een poging door de internationale ALGOL-groep ondernomen om gebruikmakend van alle verworven kennis en inzicht te komen tot een opvolger van ALGOL 60. In 1968 komt deze opvolger, ALGOL 68, tot stand. Zowel in de macht van de taal zelf als in de macht van de metataal die voor haar definitie gebruikt is, een z.g. twee-niveau grammatica, verhoudt zij zich tot ALGOL 60 als ALGOL 60 zich verhoudt tot FORTRAN.

Hiermee sluiten wij het ontegenzeglijk eenzijdig belichte historisch overzicht af. Anderen zouden wellicht andere punten in de ontwikkeling belangrijker vinden dan de hier behandelde maar wat werkelijk belangrijk is weet men pas na lange tijd. Wat we wel nog zullen proberen te doen is eens zien wat deze ontwikkeling van de computerwetenschap, tegenwoordig *informatica* genoemd, nu voor de wiskunde in het algemeen betekent. Allereerst merken wij op dat een groot deel van die informatica eenvoudig een stuk wiskunde is. Weliswaar is zij wat anders getint dan de wiskunde zoals wij die vanouds kennen. Stellingen en bewijzen spelen nog maar een kleine rol. Wel ontstaan gaandeweg meer en meer verbindingen met klassieke gedeelten van de wiskunde, speciaal uit de logica en de verzamelingenleer. Bij het ontwerpen van een taal zoals ALGOL 68 heeft men zich afgevraagd: wat moeten wij in die taal allemaal tot uitdrukking kunnen brengen? Natuurlijk moeten wij er berekeningen met gehele of reële getallen in kunnen uitdrukken. Maar ook het werken met abstracte zaken zoals verzamelingen of afbeeldingen van afbeeldingen moet mogelijk zijn. Dit blijkt allemaal heel gemakkelijk als het uitgangspunt van het ontwerp maar abstract genoeg is. Maar er zijn ook begrippen uit de informatica die wij niet zo in de wiskunde herkennen. Een typisch voorbeeld daarvan is de relatie tussen een adres in het geheugen van de computer en de waarde die op dat adres is opgeslagen. Zo'n adres wordt in ALGOL 68 geabstraheerd tot een "naam" en de relatie wordt uitgedrukt door te zeggen dat die naam verwijst naar die waarde. Zo'n naam zelf is in ALGOL 68 dan ook weer een waarde, evenals een geheel getal of een afbeelding, en op deze wijze levert het geheel van grootheden waarover men spreken kan een interessant mathematisch geheel, dat mogelijk hier en daar

tot verdieping van inzicht kan leiden.

Om te weten wat de computer voor de wiskunde heeft betekend deze eerste 25 jaar kunnen wij enerzijds kijken naar behaalde resultaten en anderzijds naar wat wij geleerd hebben over haar mogelijkheden en beperkingen. Laten wij met dat laatste beginnen. Een veel besproken probleem is of de computer kan denken. Dit hele probleem is natuurlijk een schijnvraag zolang wij niet eerst precies gedefinieerd hebben wat denken is. Het vervelende is dat wij door het geven van zo'n precieze definitie ook automatisch het antwoord geven, nl. dat de computer kan denken. Immers, alles wat precies omschreven wordt kan ook vroeger of later voor een automaat worden geprogrammeerd. Gelukkig kan niemand een dergelijke definitie geven, althans niet één die door iedereen aanvaard zal worden. Men zou b.v. kunnen vinden dat als de computer alle ingeklede vierkantsvergelijkingen van de Nederlandse middelbare school-boekjes kon oplossen, zij blijkbaar denkt. Althans, dit is de conclusie die men over de scholier trekt als hij die vraagstukjes goed weet op te lossen. Men meent doorgaans ook dat de scholier door die juiste oplossingen niet alleen toont vierkantsvergelijkingen te kunnen oplossen, maar ook de gegeven teksten te "begrijpen". Nu blijkt het zeer wel mogelijk te zijn de computer deze vaardigheid bij te brengen. Hierbij bedoelen wij natuurlijk niet dat wij haar het antwoord leren op alle nu in de schoolboekjes gedrukte sommetjes, maar dat wij haar een aantal richtlijnen leren waarmee zij deze sommetjes en mogelijk ook die in een nog uit te geven boekje kan oplossen. Het merkwaardige is dat de moeilijkheid er niet in zit om de computer te leren zo'n tekst precies te begrijpen, maar om de computer te leren zorgvuldig nagenoeg de gehele tekst te negeren en er slechts een enkel stukje dat van belang is uit te vissen. Demonstraties met dit soort programma's zijn voor de mens die niet weet wat er precies achter steekt dan ook vaak uitermate verbluffend. Daarom is waarschijnlijk de beste houding tegenover het denkprobleem die welke door TURING, die wij in het begin al tegengekomen zijn, is gegeven. TURING redeneert als volgt. Stel men converseert via het toetsenbord van een telex met een andere partij. Men stelt vragen en geeft antwoorden over en weer en als men na geruime tijd niet heeft kunnen uitmaken of degene aan de andere kant van de lijn een mens dan wel een computer is, mag men de computer het recht tot denken niet ontzeggen. Zo'n definitie is operationeel en van de proefpersoon en de omstandigheden afhankelijk, maar zij is reëel en geeft de computer dezelfde kansen als men aan een medemens geeft, van wie men meent dat hij kan den-

ken, alleen maar omdat men er enige uren of misschien jaren naar tevredenheid mee heeft geconverseerd. Zolang wij niet beter weten kunnen wij dan ook niet uitsluiten dat computers nu en in de toekomst wellicht nog beter kunnen gaan denken en dan ook mogelijk belangrijke bijdragen aan de wiskunde leveren.

Dit is misschien een toekomstfantasie. Als wij ons afvragen wat de computer tot nu toe voor de wiskunde heeft betekend dan is het antwoord: buitengewoon weinig. En het ziet er niet naar uit dat die situatie in de nabije toekomst noemenswaardig zal veranderen.

Laten wij eens naar enkele moeilijke vraagstukjes kijken. Het ligt voor de hand om te zoeken in de elementaire getallentheorie, want daar zijn bekende vraagstukken te over. Eerst een triviaal vraagstukje. Zij gevraagd een driehoek met gehele zijden $a$, $b$ en $c$ te vinden zodanig dat de zwaartelijnen rationaal zijn. Dat is een oud probleem en EULER geeft al een aantal oplossingen waarvan de "kleinste" is (68,85,87). Daarbij noemen wij een driehoek kleiner dan de andere als zijn kleinste zijde kleiner is dan de kleinste zijde van de andere of als de kleinste zijden van beide gelijk zijn en de op een na kleinste van de eerste kleiner is dan de op een na kleinste van de andere, of als de kleinste zijden gelijk zijn en de op een na kleinste zijden gelijk zijn en de derde zijde van de eerste driehoek kleiner is dan die van de andere. Men kan zich nu afvragen of de boven gegeven driehoek inderdaad de kleinste is. Dat is typisch een vraag die in een eindig aantal beslissingen te beantwoorden valt. Men hoeft nl. alleen alle driehoeken die kleiner zijn dan de gegeven op de rationaliteit van hun zwaartelijnen te beproeven. Dat is natuurlijk een heel werk, maar voordat wij computers ter beschikking hadden lukte het ons toch die berekening uit te voeren. Nu zou diezelfde berekening ons met programmeren incluis maar bescheiden tijd kosten. Het antwoord op de vraag is overigens dat de boven gegeven driehoek inderdaad de kleinste is, maar is zoiets een bijdrage tot de wiskunde?

Een interessanter probleem is afkomstig van DIOPHANTOS. Beschouw eens de verzameling getallen $\{0,1,3,8,120\}$. Voor ieder tweetal elementen $a$ en $b$ uit deze verzameling geldt $a \times b + 1$ is een kwadraat. Bijvoorbeeld is $3 \times 120 + 1 = 361 = 19^2$. De vraag is of men nog een element aan die verzameling kan toevoegen zonder dat die eigenschap verloren gaat. Dit vraagstuk kan men natuurlijk niet oplossen door te gaan proberen, want het aantal mogelijkheden van toevoeging is oneindig groot. Toch lukt het hierop een

antwoord te geven. Van LINT heeft bewezen dat zo'n getal in ieder geval beneden een bepaalde zeer grote waarde moet liggen. Daarmee is het probleem eindig geworden en door enerzijds die bovengrens voldoende naar beneden te halen en anderzijds de computer maar lang genoeg te laten rekenen heeft hij aangetoond dat het antwoord op deze vraag is: nee. Bent u er gelukkig mee?

Men zou kunnen menen dat in principe elk "eindig" vraagstuk met behulp van de computer zou kunnen worden opgelost, maar dat is geenszins het geval. Hiervoor heb ik een tegenvoorbeeld waarvoor ik weer eens 25 jaar de geschiedenis inga. Er is een artikel van Van der CORPUT, een van de stichters van het Mathematisch Centrum. Hij schreef een zeer aardig artikel over het wiskundig gezelschap in Nederland in die tijd. In dat artikel belicht hij de belangrijkste Nederlandse wiskundigen, bijv. de onlangs overleden L.E.J. BROUWER, de grondlegger van het intuïtionisme. Om de lezer een idee te geven van dat intuïtionisme geeft Van der CORPUT een voorbeeld.

Beschouw de getallen $9^{9^9}$ en $9^{9^9} + 9$. De uitspraak "$p$ is het aantal priemgetallen in dit traject" is zowel zinvol voor een intuïtionist als voor een formalist. De formalist heeft natuurlijk geen enkel probleem en de intuïtionist kent een proces waarmee in een eindig aantal stappen uitgemaakt kan worden welke van de tussengelegen getallen ondeelbaar zijn. Van der CORPUT voegt er aan toe dat de mensheid misschien nooit zal weten hoe groot $p$ is, maar dat dat er niet toe doet.

Toen ik indertijd dat artikel las heb ik al gauw met behulp van een tafelrekenmachine gevonden dat op het geval $c = 9^{9^9} + 4$ na, alle getallen in dat traject deelbaar zijn. Verder maakte ik uit dat dat getal geen factor kleiner dan 1000 had. Met de hulpmiddelen die ik toen ter beschikking had, kon ik niet veel verder komen en ik maakte melding van dit bescheiden resultaat en vergat het probleem. Jaren later kwam het probleem toevallig weer onder mijn aandacht en omdat ik intussen de electronische rekenmachine ARRA ter beschikking had, schreef ik een programmaatje om uit te maken of $c$ een deler had en ik zette de machine aan het werk. Het was een stille nacht en de ARRA was een nog tamelijk langzame rekenmachine, waaraan een luidspreker verbonden was, zodat men iets van het ritme van de berekening kon horen. De machine zoemde zo gezellig twee uur voort zonder een factor te vinden en toen wist ik dat $c$ geen factor onder 30000 had. Weer vele jaren

later kwam het vraagstuk weer in mijn gedachten omdat ik een lezing moest houden en ik schreef een programma voor de EL X8, wat overigens veel eenvoudiger was dan vroeger omdat ik mij nu in ALGOL 60 kon uitdrukken. De EL X8 zoemde niet, maar zette zich wel druk aan het werk en na twee uur rekenen wist ik dat $c$ geen factor onder 100.000.000 heeft. Nu zou men kunnen menen dat door maar te wachten tot de computers weer wat sneller worden ik wel eens een antwoord op mijn vraag zal krijgen. Maar dat zit niet zo eenvoudig. Voor een formalist en voor een intuïtionist staat vast dat $c$ hetzij ondeelbaar dan wel deelbaar is. Voor mij geldt deze uitspraak niet. Het is nl. zo, dat als in een of andere zin $c$ ondeelbaar zou zijn, ik het nooit met de hulpmiddelen die de computer mij nu of in de toekomst biedt, zal kunnen uitmaken. Immers, de al meer genoemde onzekerheidsrelatie van HEISENBERG stelt een limiet aan de computersnelheid en het schamele aantal machten van 10 dat nog in het vat zit is volledig irrelevant om ooit met het proberen van factoren tot aan de wortel van $c$, dus $3^{99}$, door te gaan. De enige hoop die ik zou kunnen hebben, is het ter beschikking krijgen van geheel nieuwe wiskundige hulpmiddelen, maar zolang die er niet zijn is dit vraagstuk, hoewel eindig, potentieel onoplosbaar.

Een interessantere bijdrage is vermoedelijk het controleren van de niet-triviale nulpunten van de $\zeta$-functie van Riemann. Zoals bekend luidt het beroemde vermoeden van RIEMANN dat afgezien van de z.g. triviale reële nulpunten alle andere complexe nulpunten een reëel deel $\frac{1}{2}$ hebben. Op dit vermoeden zijn vele delen uit de getallentheorie gebaseerd en het zou interessant zijn een tegenvoorbeeld te geven. Welnu, onlangs is "bewezen" door stug te rekenen dat de eerste 3.500.000 nulpunten inderdaad op de kritieke lijn liggen. Wat volgt daar uit? Wel, allereerst nog niets. Immers, wat betekent het woord "bewezen" in dit verband? Allereerst zou een ieder die dat bewijs niet klakkeloos wenst aan te nemen.

a. het gebruikte programma moeten zien en de uitgetypte resultaten verifieren;
b. de programmatuur van de machine moeten onderzoeken;
c. het logisch ontwerp van de machine moeten onderzoeken en verifiëren of de machine inderdaad volgens dit logisch ontwerp is gebouwd;
d. alle transistoren en andere electronische elementen van de machine controleren zoals zij waren ten tijde van de gemaakte berekening.

Dit is natuurlijk ten enen male uitgesloten, maar als wij in een zwakke bui het resultaat zouden geloven dan volgt hieruit de stelling: voor $x \geq 11$

geldt $\pi(2x) < 2\pi(x)$, waarin $\pi(x)$ het aantal priemgetallen $\leq x$ is. Dit is een mager resultaat!

Ik ben nu even heel wantrouwend jegens de computer en haar programmatuur geweest. Maar de vraag is of dat wel eerlijk is. Wie garandeert dat in de "bewijzen" die door wiskundigen geleverd worden niet ook vele fouten schuilen. Eerlijk gezegd is er goede reden om aan te nemen dat de computer veel betrouwbaarder werkt dan de mens en dat daarom het maken van bewijzen misschien beter aan de computer dan aan de mens overgelaten zou kunnen worden. Anderen gaan niet zo ver en prof. DE BRUIJN in Eindhoven heeft een project AUTOMATH lopen waarmee met behulp van de computer bewijzen niet geleverd, maar op hun deugdelijkheid worden gecontroleerd. Dit is wellicht een van de gebieden waar de computer het vruchtbaarst voor de wiskunde zal zijn.

MC SYLLABUS 18, 1973, 81-91.

# OVERZICHT VAN VIJFENTWINTIG VAKANTIECURSUSSEN

In onderstaande lijst is een overzicht opgenomen van de voordrachten die in het kader van de Vakantiecursus in de periode 1946-1971 werden gehouden. Per cursus zijn de sprekers in volgorde van opkomst opgenomen.
De vacantiecursus 1954 zult u in dit overzicht niet aantreffen, omdat in dat jaar vanwege de organisatie door het MC van het International Congress of Mathematicians geen cursus werd gehouden.

1946 - VC 1

Thema: *Didaktiek van de wiskunde*

| | |
|---|---|
| Heyting, A. | Punten in het oneindige |
| IJzeren, J. van | Abstracte meetkunde en haar betekenis voor de schoolmeetkunde |
| Bottema, O. | De prismoïde |
| Kloosterman, H.D. | Ontbinding in factoren |
| Wielenga, G. | Is wiskunde-onderwijs voor alpha's noodzakelijk? |
| Groot, J. de | Het scheppend vermogen van den wiskundige |
| Bunt, L.N.H. | Moeilijkheden van leerlingen bij het meetkunde-onderwijs |

1947 - VC 2

Thema: *Topologie*

| | |
|---|---|
| Freudenthal, H. | Voorbeelden van topologisch onderzoek |
| Groot, J. de | Het dimensiebegrip en de nulde dimensie |

| | |
|---|---|
| Heemert, A. van | Pathologische krommen |
| Dantzig, D. van | Topologisch-algebraïsche verkenning |
| Waerden, B.L. van der | De stelling van Jordan-Brouwer |
| Hirsch, G. | Een verband tussen de projectieve meetkunde en enige problemen uit de topologie |
| Gerretsen, J.C.H. | Enkele voorbeelden van tweebladige driedimensionale overdekkingsruimten |

1948 - VC 3

Thema: *Grondslagenproblemen*

| | |
|---|---|
| Beth, E.W. | Geschiedenis der logica sinds 1847 |
| Freudenthal, H. | De begrippen axioma en axiomatiek in de wis- en natuurkunde |
| Ridder, J. | Formele logica |
| Beth, E.W. | Toepassing der semantische methode op elementaire axioma-stelsels |
| Iongh, J.J. de | Signifische beschouwingen over de grondslagen van de wiskunde |
| Iongh, J.J. de | De recursieve functie als toegangsweg tot de onvolledigheidsstellingen van Gödel en Church |
| Os, C.H. van | De moderne wiskunde en het menselijk denken |

1949 - VC 4

Thema: *Groepentheorie*

| | |
|---|---|
| Visser, C. | Inleiding I |
| Blij, F. van der | Inleiding II |
| Groot, J. de | De fundamentaalgroep in de topologie |
| Freudenthal, H. | De fundamentele begrippen van de theorie der continue groepen |

| | |
|---|---|
| Bouwkamp, C.J. | Groepentheorie en natuurkunde |
| Springer, T.A. | Groepentheorie en getallenleer |
| Loonstra, F. | Geordende groepen |

1950 - VC 5

Thema: *Waarschijnlijkheidsrekening*

| | |
|---|---|
| Veen, S.C. van | Grepen uit de klassieke waarschijnlijkheidsrekening en haar geschiedenis |
| Hemelrijk, J. | Grondslagen van waarschijnlijkheidsrekening en statistiek |
| Freudenthal, H. | Limietstellingen der waarschijnlijkheidsrekening |
| Hemelrijk, J. | Waarschijnlijkheidsrekening en statistiek |
| Drion, E.F. | Waarschijnlijkheidsrekening en biologie |
| Wolff, P. de | Waarschijnlijkheidsrekening en economie |
| Boer, J. de | Waarschijnlijkheidsrekening en natuurkunde |
| Waerden, B.L. van der | De axiomatiek van Kolmogoroff |

1951 - VC 6

Thema: *De wiskunde in haar onderscheidene toepassingen*

| | |
|---|---|
| Bruijn, N.G. de | De lineaire wereld |
| Heemert, A. van | Enige beschouwingen over de theorie der vliegtuigvleugels |
| Koiter, W.T. | De elastische wereld |
| Bouwkamp, C.J. | Over berekeningen betreffende een golfmeter (On the input impedance of a quarter-wave antenna exciting a cylindrical wavemeter) |

| | |
|---|---|
| Wijngaarden, A. van | De numerieke wereld |
| Hazebroek, P. | Ruimte-zeshoeken en isometrie |
| Bremmer, H. | Enkele toepassingen van de Fourier-integraal |
| Veen, S.C. van | De niet-lineaire wereld |

1952 - VC 7

Thema: *Mechanica*

| | |
|---|---|
| Eilander, M. | Een merkwaardige oplossing van het probleem der twee lichamen |
| Zernike, F. | Trillingen van atomen in moleculen |
| Wansink, J. | De plaats van de mechanica in het V.H.M.O. |
| Dantzig, D. van | Het wiskundig model in de ervaringswetenschappen |
| Fokker, A.D. | Over hoepels en tollen |
| Veen, S.C. van | Een historisch misverstand uit de theorie der kleine trillingen |

1953 - VC 8

Thema: *Diverse onderwerpen uit de zuivere en toegepaste wiskunde*

| | |
|---|---|
| Groot, J. de | Het continuum probleem |
| Kuiper, N.H. | Locale structuren in krommen en andere ruimten |
| Heyting, A. | Inleiding tot de intuïtionistische wiskunde |
| Peremans, W. | Quadratische getallenlichamen |
| Gerretsen, J.C.H. | Bundels van driehoeken |
| Veen, S.C. van | Eenvoudige iteratiemethoden ter bepaling van eigenwaarden |
| Blaauw, G.A. | |
| Dijksterhuis, E.J. | |

1955 - VC 9

Thema: *Het ontwerp-leerplan 1954 wiskunde bij het V.H.M.O.*

| | |
|---|---|
| Wansink, J.H. | Het ontwerp-leerplan voor wiskunde 1945-1955 |
| Gerretsen, J.C.H. | De schoolmeetkunde van didactisch en wetenschappelijk standpunt |
| Seidel, J.J. | De betekenis van het leerplan voor de toekomstige student |
| Hemelrijk, J. | Wat is en waarvoor dient de statistiek? |
| Dantzig, D. van | Enkele prolegomena voor een wetenschappelijke didactiek van wiskunde en statistiek |
| Vredenduin, P.G.J. | Statistiek in het V.H.M.O. |
| Bunt, L.N.H. | Samenvattende slotbeschouwing |

1956 - VC 10

Thema: *De wetenschappelijke grondslagen der elementaire wiskunde*

| | |
|---|---|
| Grosheide F.Wzn., G.H.A. | De wetenschappelijke grondslagen der elementaire wiskunde; axiomatica en meetkunde |
| Rootselaar, B. van | Intuïtionisme en rekenkunde |
| Blij, F. van der | Continuum en reëel getal |
| Loonstra, F. | Abstracte algebra en klassieke algebra |
| Est, W.T. van | Groepentheorie en getallenleer |
| Zaanen, A.C. | Moderne opvattingen van oppervlakte en inhoud |
| Fokker, A.D. | Wiskunde en fysische werkelijkheid |

1957 - VC 11

Thema: *Historische en methodische aspecten van de meetkunde*

| | |
|---|---|
| Bruins, E.M. | Voor-Griekse en Griekse meetkunde |
| Veen, S.C. van | Meetkunde en ervaring in de 19e eeuw |
| Freudenthal, H. | Grondslagen der meetkunde na Riemann (Literatuurlijst) |
| Seidel, J.J. | Afstandsmeetkunde |
| Kuiper, N.H. | Differentiaalmeetkunde |
| Groot, J. de | Enkele recente topologische resultaten |

1958 - VC 12

Thema: *Historische en methodische aspecten van de algebra*

| | |
|---|---|
| Bruins, E.M. | De algebra der oudheid en middeleeuwen |
| Veen, S.C. van | De hoofdstelling der klassieke algebra |
| Zaanen, A.C. | Lineaire algebra en lineaire vectorruimten |
| Iongh, J.J. de | Algebraïsche aspecten van de logica |
| Freudenthal, H. | Enkele lijnen in de ontwikkeling van het algebraïsch formalisme |
| Peremans, W. | De axiomatische methode in de algebra |
| Wijngaarden, A. van | Numerieke algebra |

1959 - VC 13

Thema: *Vectoren*

| | |
|---|---|
| Kuiper, N.H. | De Barycentrische calcül en het ontstaan van de vectoren |
| Timman, R. | Concrete behandeling van vectoren en vectorrekening met voorbeelden uit meetkunde, mechanica, physica etc. |

| | |
|---|---|
| Blij, F. van der | Vectoren in de wiskunde |
| Loonstra, F. | Vectoren in het onderwijs |

1960 - VC 14

Thema: *Het wiskunde-onderwijs in het V.H.M.O. van morgen*

| | |
|---|---|
| Peremans, W. | Het doel van het onderwijs in de wiskunde bij het voorbereidend hoger en middelbaar onderwijs |
| Kuiper, N.H. | Welke gevolgen voor het voorbereidend hoger en middelbaar onderwijs brengt de moderne ontwikkeling der wiskundige wetenschappen met zich mede? |
| Duparc, H.J.A. | Welke gevolgen brengt de veranderde plaats der wiskunde in de maatschappij met zich mede? |
| Brinkman, H.G. | Welke verwachtingen en desiderata zijn practisch voor verwezenlijking vatbaar? |

1961 - VC 15

Thema: *De moderne algebra*

| | |
|---|---|
| Loonstra, F. | Zin en methode van de moderne algebra |
| Murre, J.P. | Toepassingen van de algebra in de meetkunde |
| Dwinger, Ph. | Boolese algebra's |
| Baayen, P.C. | Het tensorproduct |

1962 - VC 16

Thema: *Rondom de vernieuwing van het wiskunde-onderwijs bij het V.H.M.O.*

| | |
|---|---|
| Kuiper, N.H. | Lofzang op de meetkunde |
| Blij, F. van der | Problemen bij het onderwijs in de analyse |

| | |
|---|---|
| Beth, E.W. | Logische en denkpsychologische aspecten van de vernieuwing van het wiskunde-onderwijs |
| Freudenthal, H. | Axiomatiek van het wiskunde-onderwijs bij het V.H.M.O. |

1963 - VC 17

Thema: *Topologie*

| | |
|---|---|
| Est, W.T. van | De ontwikkeling van de algebraïsche topologie |
| Aarts, J.M. | Het vierkleurenprobleem |
| Boland, J.C. | Theorie der graphen |
| Baayen, P.C. | Opmerkingen over de verzamelingentheoretische topologie |

1964 - VC 18

Thema: *Toegepaste analyse*

| | |
|---|---|
| Gerretsen, J.C.H. | Inleiding tot de theorie der distributies |
| Jager, E.M. de | Enige toepassingen van de theorie der distributies in de mathematische physica |
| Jager, E.M. de | Distributies en operatoren |
| Timman, R. | Operatoren-rekening |

1965 - VC 19

Thema: *Getallentheorie*

| | |
|---|---|
| Mullender, P. | Iets over meetkunde der getallen: in het bijzonder producten van lineaire vormen |
| Monna, A.F. | P-adische getallen |

| | |
|---|---|
| Veen, S.C. van | De roosterpunten in het platte vlak |
| Popken, J. | De reële getallen van getaltheoretisch standpunt uit bekeken |

1966 - VC 20

Thema: *Zadelpuntsmethoden*

| | |
|---|---|
| Bruijn, N.G. de | De zadelpuntsmethode |

1967 - VC 21

Thema: *Besliskunde*

| | |
|---|---|
| Leve, G. de | Beslissen met wiskunde |
| Folkers, J.S. | Het lesrooster als beslissingsprobleem |
| Benders, J.F. | Enkele aspecten van de wiskundige optimalisering |
| Kriens, J. | De besliskunde en haar toepassingen |

1968 - VC 22

Thema: *De geschiedenis van de wiskunde tot omstreeks 1900*

| | |
|---|---|
| Duparc, H.J.A. | De wiskunde in de oudheid |
| Bos, H.J.M. | Enige onderwerpen uit de geschiedenis der wiskunde in de 16e en 17e eeuw waaraan de naam van Simon Stevin verbonden is |
| Veen, S.C. van | Poincaré en de wiskunde |
| Freudenthal, H. | De ontwikkeling van de wiskunde in de 19e eeuw |

1969 - VC 23

Thema: *Statistiek en waarschijnlijkheidsrekening*

| | |
|---|---|
| Hemelrijk, J. | De invoering van het kansbegrip in de statistiek |

| | |
|---|---|
| Sittig, J. | Statistiek, normalisatie, economie |
| Molenaar, W. | Een voorbeeld van statistische consultatie |

1970 - VC 24

Thema: *Computer en onderwijs*

| | |
|---|---|
| Wolbers, D.H. | Principe en ontwikkeling van de digitale computer |
| Duijvesteijn, A.J.W. | Toepassing van computers |
| Bruijn, P.C. de | Hardware en software van IBM 360/75 |
| Bakker, A.R. | Inleiding over "time sharing" Philips 9200 systeem |
| Klooster, W. van de en Hofman, W.J.H. | Geprogrammeerde C.P.S. (Conversational Programming System) instructie |
| Barneveld-Binkhuysen, C.F.E. | Demonstratie E.C.A.P. (Electronic Circuit Analysis Program) met behulp van het Proost-systeem en een graphical display |
| Suys, J.L.C. | Demonstratie P 9200 "time sharing" systeem |
| Versantvoort, J.A. | Demonstratie C.S.M.M. met behulp van het Proost-systeem |

1971 - VC 25

Thema: *De ontwikkeling van de wiskunde in de afgelopen 25 jaar*

| | |
|---|---|
| Freudenthal, H. | Vijfentwintig jaar wiskundige ideeën en methoden |
| Blij, F. van der | Getaltheorie 1946-1971 |
| Seidel, J.J. | Van recreatie naar toepassing; van meetkune naar codes, grafen en groepen |

| | |
|---|---|
| Iongh, J.J. de | Twee hoogtepunten uit het moderne grondslagenonderzoek van de wiskunde |
| Wijngaarden, A. van | Ontwikkelingen op computergebied |

De teksten van laatstgenoemde cursus zijn in deze syllabus opgenomen.

# OVERIGE UITGAVEN IN DE SERIE MC SYLLABUS

Onderstaande uitgaven zijn verkrijgbaar bij het Mathematisch Centrum, 2e Boerhaavestraat 49 te Amsterdam-1005.

MCS 1.1 F. GÖBEL & J.VAN DE LUNE, *Leergang Besliskunde, deel 1: Wiskundige basiskennis*, 1965.

MCS 1.2 J. HEMELRIJK & J. KRIENS, *Leergang Besliskunde, deel 2: Kansberekening*, 1965.

MCS 1.3 J. HEMELRIJK & J. KRIENS, *Leergang Besliskunde, deel 3: Statistiek*, 1966.

MCS 1.4 G. DE LEVE & W. MOLENAAR, *Leergang Besliskunde, deel 4: Markovketen, en wachttijden*, 1966

MCS 1.5 G. DE LEVE & J. KRIENS, *Leergang Besliskunde, deel 5: Inleiding tot de mathematische besliskunde*, 1966.

MCS 1.6a B. DORHOUT & J. KRIENS, *Leergang Besliskunde, deel 6a: Wiskundige programmering 1*, 1968.

MCS 1.7a G. DE LEVE, *Leergang Besliskunde, deel 7a: Dynamische programmering 1*, 1968.

MCS 1.7b G. DE LEVE & H.C. TIJMS, *Leergang Besliskunde, deel 7b: Dynamische programmering 2*, 1970.

MCS 1.7c G. De LEVE & H.C. TIJMS, *Leergang Besliskunde, deel 7c: Dynamische programmering 3*, 1971.

MCS 1.8 J. KRIENS, F. GÖBEL & W. MOLENAAR, *Leergang Besliskunde, deel 8: Minimaxmethode, netwerkplanning, simulatie*, 1968.

MCS 2.1 G.J.R. FÖRCH, P.J. VAN DER HOUWEN & R.P. VAN DE RIET, *Colloquium stabiliteit van differentieschema's, deel 1*, 1967.

MCS 2.2 L. DEKKER, T.J. DEKKER, P.J. VAN DER HOUWEN & M.N. SPIJKER, *Colloquium stabiliteit van differentieschema's, deel 2*, 1968.

MCS 3.1 H.A. LAUWERIER, *Randwaardeproblemen, deel 1*, 1967.

MCS 3.2 H.A. LAUWERIER, *Randwaardeproblemen, deel 2*, 1968.

MCS 3.3 H.A. LAUWERIER, *Randwaardeproblemen, deel 3*, 1968.

MCS 4 H.A. LAUWERIER, *Representaties van groepen*, 1968.

MCS 5 J.H. VAN LINT, J.J. SEIDEL, P.C. BAAYEN, *Colloquium discrete wiskunde*, 1968.

MCS 6 K.K. KOKSMA, *Cursus ALGOL 60*, 1969.

MCS 7.1 *Collequium moderne rekenmachines, deel 1*, 1969.

MCS 7.2 *Colloquium moderne rekenmachines, deel 2*, 1969.

MCS 8 H. BAVINCK & J. GRASMAN, *Relaxatietrillingen*, 1969.

MCS 9.1 T.M.T. COOLEN, G.J.R. FÖRCH, E.M. DE JAGER & H.G.J. PIJLS, *Colloquium elliptische differentiaalvergelijkingen, deel 1*, 1969.

MCS 9.2 W.P. VAN DE BRINK, T.M.T. COOLEN, B. DIJKHUIS, P.P.N. DE GROEN, P.J. VAN DER HOUWEN, E.M. DE JAGER, N.M. TEMME & R.J. DE VOGELLAERE, *Colloquium elliptische differentiaalvergelijkingen, deel 2*, 1970.

MCS 10 J. FABIUS & W.R. VAN ZWET, *Grondbegrippen van de waarschijnlijkheidsrekening*, 1970.

MCS 11 H. BART, M.A. KAASHOEK, H.G.J. PIJLS, W.J. DE SCHIPPER & J. DE VRIES, *Colloquium halfalgebra's en positieve operatoren*, 1971.

MCS 12 T.J. DEKKER, *Numerieke algebra*, 1971.

MCS 13 F.E.J. KRUSEMAN ARETZ, *Programmeren voor rekenautomaten; De MC ALGOL 60 vertaler voor de EL X8*, 1971.

MCS 14 H. BAVINK, W. GAUTSCHI & G.M. WILLEMS, *Colloquium approximatie-theorie*, 1971.

MCS 15.1 T.J. DEKKER, P.W. HEMKER & P.J. VAN DER HOUWEN, *Colloquium stijve differentiaalvergelijkingen, deel 1*, 1972.

MCS 15.2 P.A. BEENTJES, K. DEKKER, H.C. HEMKER, S.P.N. VAN KAMPEN & G.M. WILLEMS, *Colloquium stijve differentiaalvergelijkingen, deel 2*, 1973.

* MCS 15.3 P.A. BEENTJES e.a., *Colloquium stijve differentiaalvergelijkingen, deel 3.*

MCS 16.1 L. GEURTS, *Cursus programmeren, deel 1: De elementen van het programmeren*, 1973.

MCS 16.2 L. GEURTS, *Cursus programmeren, deel 2: De programmeertaal ALGOL 60*, 1973.

MCS 17.1 P.S. STOBBE, *Lineaire algebra, deel 1*, 1974.

MCS 17.2 P.S. STOBBE, *Lineaire algebra, deel 2*, 1974.

MCS 18 F. VAN DER BLIJ, H. FREUDENTHAL, J.J. DE JONG, J.J. SEIDEL & A. VAN WIJNGAARDEN, *Een kwart eeuw wiskunde, Syllabus van de Vakantiecursus 1971*, 1974.

MCS 19 A. HORDIJK, R. POTHARST & J. TH. RUNNENBURG, *Optimaal stoppen van Markovketens*, 1974.

* MCS 20 T.M.T. COOLEN, P.W. HEMKER, P.J. VAN DER HOUWEN & E. SLACHT, *ALGOL 60 procedures voor begin- en randwaardeproblemen.*

De met een * gemerkte uitgaven moeten nog verschijnen.