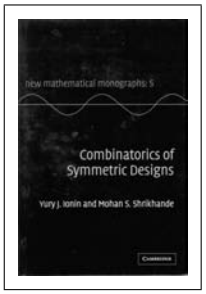
Boekbesprekingen

Book Reviews

Redactie: Hans Cuypers en Hans Sterk

Review Editors NAW - HG 9.93
Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
Postbus 513
5600 MB Eindhoven
reviews@nieuwarchief.nl
www.win.tue.nl/wgreview



Yury J. Ionin, Mohan S. Shrikhande

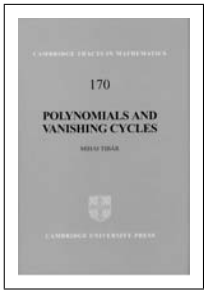
Combinatorics of Symmetric Designs

Cambridge: Cambridge University Press, 2006
New Mathematical Monographs: 5
520 p., prijs £89.00
ISBN 0-521-81833-8

Dit boek geeft een tamelijk compleet en gedetailleerd overzicht van de huidige stand van zaken in de theorie van symmetrische designs. In de eerste twee hoofdstukken komen de bekende resultaten over voorwaarden waaraan de parameters van een symmetrisch design moeten voldoen aan de orde, zoals de ongelijkheid van Fisher en de stelling van Bruck-Ryser-Chowla. Daarna wordt een aantal hoofdstukken gewijd aan de gebruikelijke onderwerpen die men bij een studie van symmetrische designs niet kan vermijden. Zo is er natuurlijk een hoofdstuk over eindige meetkunde, omdat de klassieke voorbeelden van symmetrische designs daar vandaan kommen. Verder zijn er aparte hoofdstukken over de bekende verbanden met zaken als Hadamard matrices, t-designs, (sterk) reguliere grafen, associatieschema's en natuurlijk ook verschilverzamelingen. Hoofdstuk 10 behandelt de theorie van 'balanced generalized weighing matrices', of kortweg BGW-matrices, een specialisme van de auteurs en een onderwerp dat de laatste jaren erg in de belangstelling staat. BGW-matrices zijn een generalisatie van de incidentiematrices van symmetrische designs. Grofweg gezegd zijn BGW-matrices incidentiematrices van symmetrische designs waarbij de 'enen' vervangen zijn door de elementen van een groep. In het bijzondere geval dat de groep de triviale groep is, krijgt men de vertrouwde incidentiematrices weer terug. In de resterende hoofdstukken wordt verder vooral aandacht geschonken aan structurele opbouw van symmetrische designs zoals de decompositie in deeldesigns, de verschillende soorten deeldesigns en de inbedbaarheid van designs in symmetrische designs.

Al met al is dit een goed verzorgd en helder geschreven boek geworden over dit specialistische onderwerp in de beproefde voorbeeld-definitie-stelling-bewijs-traditie, waarbij de auteurs in hun aanpak de nadruk leggen op de combinatorische aspecten van deze materie. Elk hoofdstuk bevat op het einde een serie opgaven, zodat het boek niet alleen geschikt is voor de specialist maar ook te gebruiken is als materiaal voor een college of voor zelfstudie.

Henny Wilbrink



Mihai Tibăr

Polynomials and Vanishing Cycles

Cambridge: Cambridge University Press, 2007
Cambridge Tracts in Mathematics 170
253 p., prijs £50.00
ISBN 0-521-82920-5

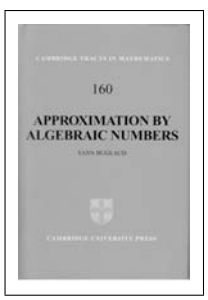
De polynomen die in dit boek besproken worden, zijn voornamelijk complexe veeltermen met veel variabelen. In de algebraïsche

meetkunde gaat het om de bestudering van de nulpuntsverzamelingen van stelsels polynomen. Verdwijnende cykels komen in het spel om hun topologie te onderzoeken. In zijn klassieke boek *L'analysis situs et la géométrie algébrique* (1924) gebruikt Lefschetz waaiers van hypervlaksneden om projectieve variëteiten te bestuderen. De algemene snede van een gladde variëteit is weer glad, maar voor bepaalde waarden treden gewone dubbelpunten als singulariteiten op. Lokaal ziet het eruit als een hyperboloïde, die naar een kegel degenereert. Men ziet nu een homologieklasse, gerepresenteerd door een cykel, hier een cirkel en in het algemeen een n-sfeer, die kleiner en kleiner wordt om tenslotte in het singuliere punt te verdwijnen. Aangezien we complex werken, kunnen we ook volgen wat er gebeurt als we om de kritieke waarde heenlopen. Later zijn verdwijnende cykels en monodromie belangrijke hulpmiddelen in het lokale geval geworden bij de bestudering van geïsoleerde singuliere punten van polynomen.

In het onderhavige boek gaat het nu weer om een meer globaal geval, van polynomen op de hele affiene ruimte. Een polynomiale functie $f\colon \mathbb{C}^{n+1} \to \mathbb{C}$ definieert buiten een verzameling van atypische waarden een lokaal triviale vezeling (dit is de definitie van atypisch). Een nieuw fenomeen is nu dat cykels ook naar oneindig kunnen verdwijnen. Dit manifesteert zich in zogenaamde singulariteiten op oneindig. Nu willen we graag meten hoeveel homologie er verdwijnt. Daartoe wordt een algemene hulpfunctie l gebruikt, die een waaier van hyperoppervlaksneden definieert. In het beeld van (f, l) bevindt zich dan een discriminant, die het beeld is van een kromme van singuliere punten, de polaire kromme, en veel informatie bevat.

Al deze zaken en veel meer komen aan de orde in de eerste twee delen van het boek, *Singularities at infinity of polynomial functions*, en *The impact of global polar varieties*. Het derde deel, *Vanishing cykels of nongeneric pencils*, bevat een vergaande generalisatie. Het boek, dat voornamelijk werk van de auteur en zijn co-auteurs bevat, zegt bedoeld te zijn voor onderzoekers en promovendi. Er is tamelijk veel voorkennis nodig; zo wordt bijvoorbeed niet uitgelegd wat verdwijnende cykels zijn. Resultaten worden meestal in de algemeenste en scherpste vorm gegeven. Al met al bevat dit boek een schat aan informatie voor wie dit onderwerp wil leren.

Jan Stevens



Yann Bugeaud

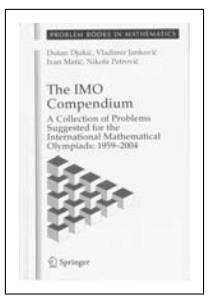
Approximation by Algebraic Numbers

Cambridge: Cambridge University Press, 2004
274 p., prijs £55.00
ISBN 0-521-82329-3

Bugeauds boek over benaderen met algebraïsche getallen is breed opgezet, maar met een duidelijke focus op de theorie van classificatie van reële getallen zoals ingevoerd door Mahler en Koksma en de daarmee samenhangende metrische theorie. In hoofdstuk 3 tot en met 7 krijgt de lezer een goed overzicht van de huidige stand van zaken op dit gebied, waarover eerder in boeken gerapporteerd is door Koksma (1936), Schneider (1957), Harman (1998) en Bernik en Dodson (1999). Bugeauds belangrijkste thema is of voor elk paar dalende rijen $(w_n)_{n\geq 1}$ en $(w_n^*)_{n\geq 1}$ in $[1, \infty)$ er een reëel getal ξ bestaat met Mahler waarden (w_n) en Koksma waarden (w_n^*), in zoverre dat het niet uitgesloten is door de noodzakelijke ongelijkheden $n \leq w_n^* \leq w_n \leq w_n^* + n - 1$ voor alle $n \geq 1$. De auteur vertelt wat bekend is en bewijst de basisstellingen, terwijl hij voor de ingewikkeldere bewijzen verwijzingen geeft. In Hoofdstuk 8 behandelt hij classificaties van Sprindzuk en Mahler voor de complexe getallen. In Hoofdstuk 9 komen benaderingen in andere lichamen (p-adische getallen, formele machtreeksen) aan de orde. Hoofdstuk 10 bevat 55 open problemen, waarbij één sectie gewijd wordt aan het klassieke vermoeden van Littlewood en de problemen in de andere secties samenhangen met het hoofdonderwerp van het boek. Bijna elk hoofdstuk heeft zowel opgaven op een geavanceerd niveau als een uitgebreide opsomming van verwante resultaten in de literatuur. Dit resultereert in een literatuurlijst van 617 publicaties. Dit, met een index, maakt het boek ook geschikt als naslagwerk.

Andere onderwerpen waarop in boeken over diophantische approximaties vaak de nadruk is gelegd, zoals kettingbreuken (Cassels (1957), Schweiger (2000), Hensley (2006)), de stelling van Thue-Siegel-Roth en de Subspace Theorem (W.M. Schmidt (1980), Corvaja en Zannier (2003)), de theorie van lineaire vormen in logaritmen (A. Baker (1975), Feldman (1982), Waldschmidt (1992)), transcendentie (Schneider (1957), Feldman en Nesterenko (1998), Waldschmidt (2000)) en metrische theorie (Sprindzuk (1977), Harman (1998), Bernik en Dodson (1999)), komen kort ter sprake, met name in Hoofdstuk 1 en 2, en voornamelijk in zoverre het relevant is voor het hoofdonderwerp. Daarmee is ook de lezerskring van dit boek aangeduid. Voor wie geïnteresseerd is in de classificatie van getallen is dit boek onmisbaar. Voor anderen is er een ruime keus aan andere boeken.

Rob Tijdeman



Dušan Djukić, Vladimir Janković, Ivan Matić, Nikola Petrović

The IMO Compendium
A collection of problems suggested for the International Mathematical Olympiads: 1959–2004

New York: Springer Verlag, 2006
Problem Books in Mathematics
741 p., prijs € 62,95
ISBN 0-387-24299-6

Dit vuistdikke boek bevat een verzameling problemen van de u waarschijnlijk welbekende Internationale Wiskunde Olympiade (IWO, in het Engels IMO), vanaf de eerste competitie in 1959 tot en met 2004.

Het boek begint met een beknopte geschiedenis van de IWO, daarna volgen twintig bladzijden met resultaten uit de vlakke meetkunde, combinatoriek, getaltheorie, algebra en analyse. Ze dienen als aanvullende kennis om sommige problemen makkelijker op te kunnen lossen en zijn niet triviaal. Ik kan me zelfs voorstellen dat menig middelbare scholier er door afgeschrikt wordt, zeker omdat er weinig uitleg bijstaat. Dit stukje van het boek is daarom hooguit geschikt als vademecum, niet om uit te leren.

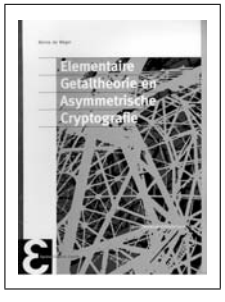
De formidabele probleemverzameling vormt het leeuwendeel van het boek. Niet slechts de competitie-opgaven staan erin (zes per jaar), maar ook de *short list* en/of *long list*, die de basis voor de uiteindelijke selectie vormen (vele tientallen per jaar). Het Compendium beoogt hierin zo volledig mogelijk te zijn, hoewel voor-

in al vermeld staat dat niet al deze lijsten openbaar gemaakt zijn. Hoe dan ook, het aantal problemen komt zo uit op bijna 2000, waarvan een groot aantal waarschijnlijk nooit eerder in druk is verschenen.

Van de problemen in de *short list* worden in het tweede deel van het boek bondige oplossingen gegeven, van die in de *long list* (minus de *short list*) niet. Het resultaat is een prettige mengeling van problemen waarbij je stiekem naar de oplossing kan gluren als het echt niet lukt, en andere waarbij je toch echt op jezelf bent aangewezen. (Zelfs een korte zoektocht op internet leverde mij niet de resterende antwoorden op een presenteerblaadje.)

De doelgroep van het boek beperken de auteurs zelf expliciet tot middelbare scholieren die voor de IWO willen trainen. In Nederland is dat wel een zeer kleine groep beoogde lezers. Is dit boek ook interessant voor de doorsnee NAW-lezer? Jazeker, als die zich tenminste aangesproken voelt door wiskundige problemen die weinig voorkennis vereisen maar desalniettemin ook voor de beroepswiskundige uitdagend kunnen zijn. Perfect voor een regenachtig weekend!

In vergelijking met andere 'probleemboeken' biedt het een grote hoeveelheid problemen, allemaal van hoog niveau. Is het boek voor de doelgroep zelf wel geschikt? Jazeker, maar niet als eerste probleemboek. Wil je je dochter of zoon klaarstomen voor de IWO, begin dan eerst met opgaven van de Nederlandse Wiskunde Olympiade (online op te zoeken) en een boek zoals Arthur Engels *Problem solving strategies*. Daarna is het Compendium een aanrader. *Maxim Hendriks*



Benne de Weger

Elementaire Getaltheorie en Asymmetrische Cryptografie

Utrecht: Epsilon, 2009
192 p., prijs € 21,00
ISBN 90-5041-108-0

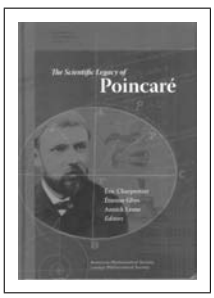
Kies twee priemgetallen p en q, bereken $n = p \cdot q$ en $\phi(n) = (p-1)(q-1)$. Kies daarna een getal e dat relatief priem is met $\phi(n)$. Bereken ten slotte de inverse d van e modulo $\phi(n)$. Je hebt nu een paar sleutels van een RSA cryptosysteem gemaakt. Het paar e en n vormen samen de openbare sleutel, het getal d de geheime privésleutel.

Wat kan ik met RSA? Is RSA een veilig systeem? Kan ik elk paar priemgetallen p en q kiezen of zijn er (on)handige keuzes? Vragen als deze staan centraal in het laatste hoofdstuk van het boek. Dan wordt ook duidelijk dat er wel degelijk handige en onhandige keuzes van p en q zijn. De auteur formuleert een aantal regels die resulteren in een algoritme voor sleutelpaargeneratie, een algoritme dat in de praktijk goed voldoet. Het is overigens niet de eerste keer dat de auteur aandacht besteed aan praktische zaken, al eerder heeft hij de lezer primaliteitstesten en een aantal algoritmes om grote (pseudo)priemgetallen te genereren voorgeschoteld. In de eerdere hoofdstukken is daarnaast ruim aandacht geweest voor zaken als modulo rekenen, de ϕ-functie met daarbij de stelling van Euler, methoden om grote getallen te factoriseren en hun complexiteit.

Het boek biedt echter geen volledige cursus getaltheorie, slechts de getaltheorie die nodig is voor RSA en voor de Diffie-Hellman sleuteluitwisselingsmethode komt aan de orde. Maar die wordt dan wel degelijk en uitgebreid behandeld. Het is ook geen cursus cryptografie: alleen de zojuist genoemde cryptoonderwerpen kun je in het boek vinden. De schrijver heeft willen laten zien hoe het begrip van getaltheorie essentieel is voor het begrijpen en goed kunnen gebruiken van asymmetrische cryptografie. Dat is volgens mij uitstekend gelukt.

Het boek is ontstaan uit een cursus van de Open Universiteit en is dan ook goed geschikt voor zelfstudie. Het bevat veel voorbeelden en opgaven. Van de meeste opgaven is achterin een uitwerking gegeven. Een handig hulpmiddel bij een aantal opgaven waar met grotere getallen moet worden gerekend, is het programma MCR, Modulaire en Cryptografische Rekenmachine, beschikbaar als Java-applet, welke is te vinden op de website bij dit boek.

Samenvattend: voor de doelgroep, studenten Informatica (hbo en universiteit) en ICT-professionals, biedt dit boek een mooi inkijkje in de cryptografie gebaseerd op getaltheorie. *Ernst Lambeck*



Éric Charpentier, Étienne Ghys, Annick Lesne (eds.)

The Scientific Legacy of Poincaré

American Mathematical Society/London Mathematical Society, 2010
History of Mathematics 36
394 p., prijs $ 89.00
ISBN 0-8218-4718-3

Het vele wetenschappelijke werk van Henri Poincaré, zijn veelzijdigheid in de wiskunde en zelfs ook in de natuurkunde en de filosofie, blijft een bron van inspiratie en studie. Deze nieuwe collectie van artikelen, oorspronkelijk in het Frans verschenen in 2006 en, zo te zien, goed vertaald door Joshua Bowman, bevat 19 artikelen over uiteenlopende onderwerpen. Om een idee van de collectie te geven bespreek ik er enkele.

Een prachtig artikel, 'Differential equations with algebraic coefficients over arithmetic manifolds' is van Nicolas Bergeron. Hij laat zien hoe Poincaré het verband legde tussen de analyse van 2de orde lineaire, gewone differentiaalvergelijkingen met zwakke singulariteiten in de coëfficiënten en de hyperbolische meetkunde. Dat begon met het werk van Fuchs die geïnteresseerd was in de analytische voortzetting van de oplossing rondom singuliere punten (monodromie) en de eigenschappen van hun inversen. Poincaré liet zien hoe je deze problemen hanteert met behulp van arithmetische transformatiegroepen, projectieve structuren en automorfe functies.

De artikelen over dynamische systemen en hemelmechanica zijn inhoudelijk minder sterk, behalve het artikel van E. Ghys over de recurrentiestelling voor maatbehoudende systemen. Die heeft tot heel wat discussies geleid, vooral onder fysici. Het bijzondere van het artikel is niet alleen de helderheid waarmee de stelling beschreven wordt, maar ook hoe uitgelegd wordt waarom de recurrentietijd in een aantal gevallen zoveel korter is dan men in het algemeen zou verwachten.

Natuurlijk wordt het Poincaré-vermoeden in deze bundel beschreven, minder bekend zijn echter zijn resultaten voor partiële differentiaalvergelijkingen. Misschien komt dit omdat ze vaak 'verstopt' zijn in de publicaties over fysische onderwerpen. Jean

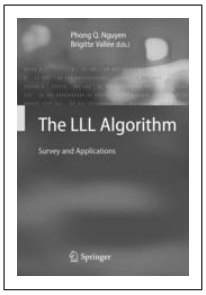
Mawhin beschrijft Poincarés 'sweeping method' voor het Dirichlet probleem van de Laplacevergelijking; deze methode speelt een belangrijke rol in de huidige theorie van elliptische randwaarde problemen. Andere resultaten zoals voor spectraaltheorie en de Poincaré ongelijkheid in de functionaalanalyse en de theorie van PDVs worden uitvoerig besproken.

De filosofische verhandelingen van Poincaré zijn voor een groot deel te vinden in vier boeken. Ze zijn helder geschreven, maar caleidoscopisch van opzet. Het gebrek aan systematiek doet sommige geleerden twijfelen aan de filosofische diepgang, maar dat berust op een vooroordeel. Gerhard Heinzmann licht uit deze boeken het onderwerp 'filosofie van de wetenschap' waar zowel wiskunde, natuurkunde als logica onder valt. Hij laat zien hoe ver Poincarés visie van het axiomatisme van Hilbert staat.

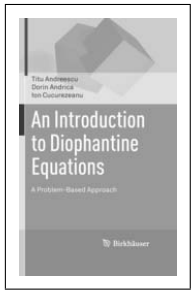
De meeste van de artikelen in deze bundel zouden een mooi uitgangspunt voor een seminarium kunnen zijn, als dan tegelijk de bijbehorende oorsponkelijke artikelen worden gelezen.

Ferdinand Verhulst

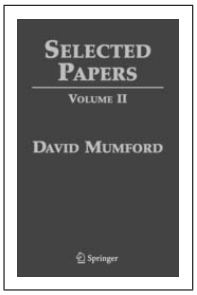
Recent verschenen publicaties. Als u een van deze boeken wilt bespreken of als u suggesties heeft voor andere boeken voor deze rubriek, laat dit dan per e-mail weten aan reviews@nieuwarchief.nl.



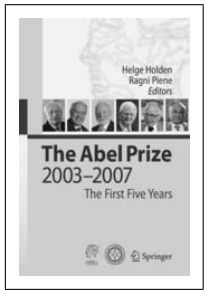
Phong Q. Nguyen, Brigitte Vallée (eds.)
The LLL Algorithm
Survey and Applications
Springer-Verlag, 2010
ISBN: 978-3-642-02294-4
www.springer.com/computer/security+and+cryptology/book/978-3-642-02294-4



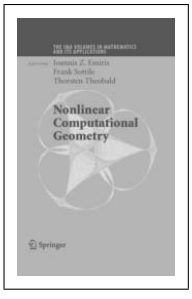
Titu Andreescu, Dorin Andrica, Ion Cucurezeanu
An Introduction to Diophantine Equations
A Problem-Based Approach
Birkhäuser, 2010
ISBN: 978-0-8176-4548-9
www.springer.com/birkhauser/mathematics/book/978-0-8176-4548-9



David Mumford
Amnon Neeman, Ching-Li Chai, Takahiro Shiota (eds.)
Selected Papers
Vol. II: On Algebraic Geometry, including Correspondence with Grothendieck
Springer-Verlag, 2010
ISBN: 978-0-387-72491-1
www.springer.com/mathematics/algebra/book/978-0-387-72491-1



Helge Holden, Ragni Piene (eds.)
The Abel Prize
2003-2007 The First Five Years
Springer-Verlag, 2010
ISBN: 978-3-642-01372-0
www.springer.com/mathematics/history+of+mathematics/book/978-3-642-01372-0



Ioannis Z. Emiris, Frank Sottile, Thorsten Theobald (eds.)
Nonlinear Computational Geometry
Springer-Verlag, 2010
ISBN: 978-1-4419-0998-5
www.springer.com/mathematics/algebra/book/978-1-4419-0998-5