WORTELinDRUK

Het kloppend hart van
de wiskundereünistenkring
De Wortel

nummer 15, september 2005

Deze keer

Redactioneeltje

Meneer Escher was vast een aardige man. Van zijn familie weet ik het niet zo, maar ik hoop maar dat zij ook aardig zijn. Dat is wel te hopen, want we hebben zonder toestemming van hem of zijn erfgenamen een tekening gebruikt in deze WORTELinDRUK.

Dit blaadje kun je moeilijk een publicatie noemen. Die honderd exemplaren die zeer onregelmatig verschijnen... Dat telt toch niet voor zo'n copyright-clausule?

Nee, dit is een boekje voor een select clubje. Met wat interne communicatie over gezellige bijeenkomsten, boeken die je moet lezen en vakkennis. Leuk hoor, maar publiceren, dat doen we eigenlijk helemaal niet.

(En alle lezers hebben de prenten van Escher toch al in de woonkamer hangen)

Jeroen Hendrix

Handgemaakte Sudoku?

> "Sudoku could be your friend for life. I must ask you, therefore, not to touch computer-generated puzzles. Take pleasure in the properly crafted Sudoku puzzles."

Nobuhiko Kanamoto, hoofdredacteur van Nikoli puzzelmagazines, Japan.
Nikoli heeft in Japan het alleenrecht op de naam Sudoku.

Anagram

Wie is deze undercover wiskundige?

Lunar math is not gain

oplossing vorige anagram: *Luitzen E.J. Brouwer*

1 oktober 2005: Linksom of rechtsom

Op 1 oktober aanstaande is er weer een universiteitsbrede alumnidag. De Wortel doet natuurlijk mee. De samenwerking met de kring van psychologie in 2001 was heel goed bevallen, daarom hebben we deze keer weer een gezamenlijk programma opgezet, dit keer met de *kring Taalwetenschap*.

Het algemene programma van de alumnidag staat in het teken van de 2000-ste verjaardag van de plaats Nijmegen. Om half tien bent u welkom in de Aula voor de ochtendlezingen. Meldt u wel even aan, bijvoorbeeld bij alumnizaken op `http://www.ru.nl/er`. De Wortel zal ook een plek reserveren bij de lunch om 12.45 uur.

's Middags nodigen de kringen Taalwetenschap en Wiskunde u dan van harte uit om deel te nemen aan het kringprogramma.

Programma:

13.30 uur:	Ontvangst met koffie en thee
14.00 uur:	**Prof.dr. G. Senft, Max-Planck-Instituut voor Psycholinguïstiek** *Language, culture and cognition, frames of spatial reference*
14.45 uur:	**Mw. dr. H. de Hoop, afdeling Taalwetenschap, faculteit Letteren** *De krokodil om de hoek, oriëntaties in taal*
15.30 - 15.45 uur:	Pauze met koffie en thee
15.45 uur:	**Prof.dr. F. Keune, subfaculteit Wiskunde, faculteit NWI** *Oriëntaties op oppervlakken*
16.30 - 17.00 uur:	Wandeling naar de Refter
17.00 uur:	Gezamenlijke afsluitende borrel in de Refter

Locatie:

Zaal H.00.023, Huygensgebouw (nieuwbouw fac. NWI)
Toernooiveld, Nijmegen

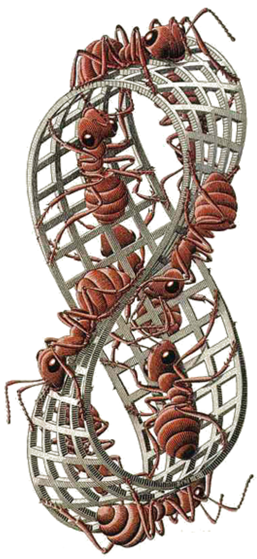
Toelichting:

Als je van A naar B wilt, zul je vaak de kortste weg willen volgen. Maar als dat niet kan, zul je linksom of rechtsom moeten. Als je die weg wilt beschrijven, vereist dat het gebruik van ruimtelijke begrippen. Alle natuurlijke talen bevatten dan ook woorden en constructies die het praten over ruimte en richting mogelijk maken. Helen de Hoop zal enkele Nederlandse uitdrukkingen bespreken, waaronder de voorzetsels 'om' en 'rond'.

Als we naar andere talen kijken, blijkt er nogal wat variatie te zijn in de manieren waarop ze ruimtelijke oriëntatie beschrijven. Gunter Senft zal in zijn bijdrage laten zien dat er talen zijn waarin men niet linksom of rechtsom gaat maar 'via het Oosten of het Westen'.

Ook de wiskunde heeft middelen waarmee we onze positie in de ruimte beschrijven. Frans Keune zal dit aan de hand van oriëntaties in de tweedimensionale ruimte illustreren. Ook zal hij laten zien wat er gebeurt wanneer een tweedimensionale 'platlander' een rondje over een gedraaid oppervlak loopt.

Onze ruimtelijke oriëntatie zal na de drie lezingen wat minder vanzelfsprekend zijn geworden. Tegelijk zullen we zien dat taalkunde en wiskunde oriëntatie kunnen bieden in de wondere wereld van ruimte en richting.



Cijfers en Letters

Wat als mijn vader

[11]r3.1cm 

Peter Esterhazy Weinig mensen weten dat Peter Esterhazy wiskundige is. Doet ook niks ter zake. Peter Esterhazy is een van de belangrijkste Hongaarse schrijvers van dit moment en behoort tot de top van de Europese literatuur. Daar gaat het om. Maar toch. Esterhazy schrijft er zelf over. In zijn laatste, ontluisterende boek, Verbeterde Editie, noteert hij de titel van zijn afstudeerscriptie: Optimum binary search trees. Haast de titel van een roman, peinst hij. Optimum binary search trees, a novel, of Optimum binary search trees, a history. Zo speelt Esterhazy met zijn eigen scriptie. Optimale binaire zoekbomen. Het doet me denken aan Wat-als. Wat zou er gebeurd zijn, als… Wat zou er gebeurd zijn, als mijn vader niet… Wat zou er gebeurd zijn, als mijn vader wel…

Over zijn vader, en over wat er gebeurd zou zijn als zijn vader niet of wel…, daar gaan de laatste twee boeken van Peter Esterhazy, Harmonia Caelestis en het al genoemde Verbeterde Editie, over. Esterhazy is een telg uit een beroemd adellijk geslacht uit de Oostenrijks-Hongaarse dubbelmonarchie. Een van rijkste families uit de zeventiende, achttiende, de negentiende eeuw. Landerijen in wat nu Oostenrijk is, zich uitstrekkend tot in het Oosten van Hongarije. Haydn, om een voorbeeld te noemen, was hofcomponist bij de Esterhazy's en schreef er een aantal van zijn beroemdste werken. Niet bepaald een omgeving waar je veel tekort zult komen als opgroeiende jongen en als de geschiedenis niet zo'n vreselijk lot voor de Hongaren in petto had gehad, hadden we waarschijnlijk nooit van de schrijver Peter Esterhazy gehoord. Maar in de twintigste eeuw was alles anders. Na de Eerste Wereldoorlog hield Oostenrijk-Hongarije op te bestaan. Hongarije werd even, onder Bela Kun, een communistische radenrepubliek, maar in de jaren twintig was de revolutie al weer voorbij en volgde een sterk op Itali gerichte monarchie, met alle fascistische en antisemitische tendensen van dien. Zodoende kwam Hongarije in de Tweede Wereldoorlog aan de verkeerde kant van de geschiedenis terecht. Om daarna onderdeel van het Oostblok te worden. 1956: nog één keer hoop, maar weggeslagen door de Sovjet-tanks in het centrum van Boedapest. De optelsom: een weggegooide eeuw, voor heel Oost-Europa, maar misschien nog het meest voor de Hongaren.

Hoe verging het de Esterhazy's in deze twintigste eeuw? Dat lezen we in Harmonia Caelestis. De roman is geconstrueerd rond de figuur 'Mijn vader', een alias voor allerlei figuren uit het roemruchte verleden van Esterhazy's. Via deze 'Mijn vaders' schieten we als een pingpongbal door de Hongaarse geschiedenis. Allerlei bekende en minder bekende episoden uit die geschiedenis worden door Esterhazy opgehangen aan een of andere voorvader en zo ontstaat een ingewikkeld mozaïek van feit en fictie met de Esterhazy's als steeds terugkerend motief. En daar gaat het de schrijver ook om: Harmonia Caelestis is uiteindelijk één groot eerbetoon aan de familie, ondanks alle nukken en makken die een adellijk geslacht bijna als vanzelfsprekend aankleven en waar Esterhazy ook geen geheim van maakt. Harmonia Caelestis: Harmonie der Sferen. Esterhazy: Huis der Sterren. In de titel van de roman zit het eerbetoon al besloten.

Maar het eerbetoon is vooral aan de echte, de twintigste-eeuwse vader. Want wat die allemaal heeft moeten doorstaan. Even, in het begin van de jaren twintig, is de echte vader nog minister geweest, maar toen de politiek van Horthy de fascistische kant op ging, trad hij terug. Vanaf dat moment was hij outcast, vernederd, geslagen, gevangen gezet, onteigend. Vóór de oorlog, in de oorlog en uiteraard ook in de communistische periode. Een geruïneerd leven, zo schrijft Esterhazy, dat hij doorstond met een bewonderenswaardig incasseringsvermogen en een grote lankmoedigheid.

Hoe kon dat? Vrijwel op hetzelfde moment dat Esterhazy de laatste correcties in de drukproeven van Harmonia Caelestis aanbrengt — we schrijven eind 1999 — wordt hij opgebeld door de Hongaarse binnenlandse veiligheidsdienst. Dat er nog een paar dossiers liggen waarin ook zijn familie voorkomt. En of hij daar interesse in heeft. Nauwelijks heeft hij de dossiers opengeslagen of hij beseft: Mijn vader. Spion. Informant. Voor de communisten. Bespiedde zijn eigen familie. Zijn vrienden. Mij.
Allerlei daden en gebeurtenissen die hij niet begreep of had toegeschreven aan de moed van zijn vader, kregen op eens een heel andere impact. Gewoon een vriendje van de communisten. Een verrader. Een verrader, mijn vader? En Esterhazy zet zich aan het schrijven van de Verbeterde Editie, in een poging om de andere kant van de geschiedenis te begrijpen.

Wat als de vader van Peter Esterhazy. Wat als de vader van Peter Esterhazy geen informant voor de communisten was geweest. Zeker is dat het privilege om te studeren de jonge Peter was onthouden. Peter Esterhazy was geen wiskundige geweest. Geen scriptie over Optimale Zoekbomen. Maar de belangrijkste conclusie is dat Peter Esterhazy niet de schrijver was geweest van twee van de meest aangrijpende romans van de laatste jaren.

- Peter Esterhazy, *Harmonia Caelestis*, ISBN 90-295-1552-X, Arbeiderspers, 787 pp.; idem, Verbeterde Editie, ISBN 90-295-2259-3, Arbeiderspers, 320 pp.

Afgestudeerd: Bart Kirkels

Irreducibiliteitscertificaten voor Polynomen met Gehele Coëfficienten

Eind augustus (2004) ben ik bij Wieb Bosma afgestudeerd in de computeralgebra. Om duidelijk te maken waar de scriptie over gaat zal ik in de rest van dit stuk het polynoom $f \in \mathbb{Z}[X]$ gebruiken. Zeg $f = f_n X^n + f_{n-1} X^{n-1} + \ldots + f_1 X + f_0$. Een bekend irreducibiliteitscriterium is dat van Eisenstein:

Criterium (Eisenstein): Er bestaat een priemgetal p zo dat $p \nmid f_n$, $p^2 \nmid f_0$ en voor alle $0 \leq i \leq n-1 :\ p \mid f_i$.

Als f aan dit criterium voldoet, dan is daarmee bewezen dat f irreducibel is. De eis is dat er een bepaald priemgetal p bestaat; deze p heet nu een irreducibiliteitscertificaat van f dat behoort bij Eisensteins criterium. Dus, voor $f = X^2 + 6X + 3$ hebben we dat f aan het criterium voldoet, namelijk met certificaat 3. Het controleren van een certificaat is hier makkelijk: er hoeft alleen een klein aantal (niet-)delingen nagegaan te worden.

In de scriptie bekijk ik een aantal criteria , waaronder deze van Eisenstein en een generalisatie. Het belangrijkste criterium had te maken met ontbindingen van f over eindige lichamen van priem orde. Het is duidelijk dat als f over een eindig lichaam irreducibel is, het dat dan ook over $\mathbb{Z}$ is. Maar verschillende eindige lichamen gecombineerd kunnen ook irreducibiliteit bewijzen. Een voorbeeld:

> Stel f is een vierdegraads veelterm die over $\mathbb{F}_{p_1}$ splijt in twee irreducibele veeltermen van graad 2. Dan weten we dat áls f splijt over $\mathbb{Z}$, dat in twee veeltermen van graad 2 is.
> Als f ook nog over $\mathbb{F}_{p_2}$ splijt in twee irreducibele veeltermen, van graad 3 en 1, dan weten we daarmee dat f over $\mathbb{Z}$ dus niet in twee veeltermen van graad 2 uiteen kan vallen, en dus dat f irreducibel is.

Een probleem met dit criterium is dat niet elk irreducibel polynoom er aan voldoet, we kunnen dus niet bij elk polynoom een certificaat vinden op deze manier. Om het bestaan van certificaten te bestuderen gebruik ik Galoistheorie. Als de Galoisgroep van f aan bepaalde eisen voldoet, weten we zeker dat er een certificaat bestaat. Zo kunnen we inzien dat alle irreducibele polynomen van priem graad een certificaat hebben, en ook dat bijna elk irreducibel polynoom een certificaat heeft.

Vervolgens beschrijf ik een algoritme dat aan élk irreducibel polynoom een certificaat toevoegt; het liefst met het hierboven beschreven criterium, anders wordt er gebruik gemaakt van Hensel-liften. Dit algoritme en een aantal anderen (bijv. voor het criterium van Eisenstein) test ik en het zojuist beschreven algoritme komt behoorlijk goed uit de bus.

Maar waarom al die moeite doen om certificaten te vinden terwijl er snelle factorisatie-methodes bestaan? Het antwoord is dat we volledig zeker willen zijn van de factorisatie. Er kunnen namelijk foutjes in de implementatie van een factorisatie-methode zitten, en bovendien is het niet uitgesloten dat er iets mis is met de methode zelf. Het is makkelijk om te controleren of een factor correct is: gewoon uitdelen. Maar het bewijzen van irreducibiliteit is toch een andere taak. Hiervoor kunnen zogeheten bewijsassistenten gebruikt worden; programma's die wiskundige bewijzen mechanisch controleren. Dit wil wel zeggen dat de wiskunde in een bepaalde taal geformaliseerd moet worden. De correctheidsbewijzen van de genoemde certificaten zijn makkelijk te controleren, en vandaar dat ze interessant zijn voor ons. In de scriptie geef ik een inleiding over het formaliseren van wiskunde op een computer, en hoe de certificaten nu precies een rol kunnen spelen bij het formeel bewijzen van irreducibiliteit.

De hele scriptie, en ook de geïmplementeerde algoritmes, staan online op `http://www.math.ru.nl/~bosma/students/kirkels`
Voor vragen of opmerkingen kun je me altijd mailen: `B.W.M.Kirkels@tue.nl`

Bart Kirkels

Colofon

WORTELinDRUK is de nieuwsbrief van Wiskunde Reünistenkring **De Wortel**

aan dit nummer werkte mee: bart Kirkels

september 2005
jaargang 7 nummer 15

redactie: Mignon Engel, Jeroen Hendrix, Frans Janssen, Twan Laan

redactieadres:
secretariaat wiskunde
Toernooiveld 1
6525 ED Nijmegen

`dewortel@math.ru.nl`