

PYTHA GORAS

WISKUNDETIJDSCHRIFT VOOR JONGEREN

**Hoe veilig is de
Oosterscheldekering?**

Darten op gemene borden

Vervalste certificaten van DigiNotar

51ste JAARGANG - NUMMER 2 - NOVEMBER 2011

Pythagoras, het vijftigjarige wiskundetijdschrift voor jongeren, zoekt per 1 september 2012 een enthousiaste

HOOFDREDACTEUR (m/v)

Het betreft een betaalde functie voor één dag in de week.

Taken en verantwoordelijkheden

De hoofdredacteur van *Pythagoras*

- werft en redigeert nieuwe kopij
- geeft leiding aan de redactie
- onderhoudt contact met auteurs
- vertegenwoordigt het tijdschrift in wiskundig Nederland en België
- representeert het tijdschrift bij evenementen als de Nationale Wiskunde Dagen
- zorgt ervoor dat *Pythagoras* ook toegankelijk is voor jongere lezers

Gevraagd

- journalistieke ervaring, bij voorkeur op het gebied van de popularisering van wiskunde
- leidinggevende eigenschappen
- creativiteit en een goede pen
- aantoonbare affiniteit met wiskunde

Geboden

- een geolied productieapparaat
- een enthousiaste redactie
- flexibele werktijden

Neem voor meer informatie contact op met een van de leden van de sollicitatiecommissie: Klaas Pieter Hart (K.P.Hart@tudelft.nl), Heiner Wind (hwind@home.nl) of Chris Zaal (chriszaal@uva.nl).

Je sollicitatiebrief (inclusief cv) dient uiterlijk 15 februari 2012 in ons bezit te zijn. Stuur je sollicitatie per e-mail naar vacature@pythagoras.nu.

AANBIEDING: BOEK + DVD

Pythagoras is al sinds 1961 een begrip in Nederland en België. Ter gelegenheid van het vijftigjarig bestaan verscheen in maart van dit jaar *De Pythagoras Code – het beste uit een halve eeuw wiskunde voor liefhebbers*, een selectie uit vijftig jaargangen van het blad.

De Pythagoras Code is verkrijgbaar bij de boekhandel voor € 19,95. Je kunt het boek echter ook rechtstreeks bij de redactie bestellen.

Voor een kleine meerprijs krijg je er dan een DVD bij met de eerste vijftig jaargangen van het tijdschrift (1961-2011)! Deze DVD is niet in de boekhandel te koop.



Voor het boek plus de DVD betaal je slechts € 23,50 plus verzendkosten à € 2,30 (totaal € 25,80). De DVD is ook apart te bestellen voor € 11 + € 1,50 verzendkosten (totaal € 12,50).

Hoe bestellen?

Stuur een e-mail naar arnout@pythagoras.nu met als onderwerp 'bestelling', vermeld het aantal exemplaren ('boek + DVD' of 'DVD') en een postadres. Maak dan het juiste bedrag over op giro 3605919 t.n.v. A. Jaspers, Leiden. De bestelling wordt verstuurd zodra de betaling ontvangen is.

Op www.pythagoras.nu zijn de laatste jaren steeds meer oude nummers online gezet. De complete eerste vijftig jaargangen zullen t.z.t. op de site beschikbaar zijn. De resolutie van de pdf's op de website is echter lager dan de resolutie van de pdf's op de DVD.

INHOUD

8



GEMENE DARTBORDEN

Is darts een sport? Van oudsher is het vooral een spel dat in cafés gespeeld wordt, maar sinds 1978 is er jaarlijks het *World Professional Darts Championship*. Sinds Raymond van Barneveld dit toernooi een keer won, geldt darten ook in Nederland als topsport. De indeling van het dartbord verbergt interessante wiskunde.

16



HOE VEILIG IS DE OOSTERSCHELDEKERING?

Eén van de huzarenstukken van de Deltawerken was het afsluiten van de Oosterschelde. Jan Stout, projectmanager bij Rijkswaterstaat, vertelt over de veiligheid van de Oosterscheldekering.

24



HAMEYE RAMZARO MISHKANAM – DE BREEKBARE VEILIGHEID VAN INTERNETCERTIFICATEN

‘Hameye ramzaro mishkanam’, vrij vertaald betekent dat: ‘ik breek elk geheimschrift’. De Iraanse hackers die in juli dit jaar inbraken bij DigiNotar zetten deze spreuk open en bloot in één van de ruim 500 nepcertificaten die ze uitgaven. Maar wat zijn dat eigenlijk, certificaten, en waarom zou je ze ooit vertrouwen?

EN VERDER

- 2 Kleine nootjes
- 4 Een bizarre voetbalwedstrijd
- 6 Journaal
- 12 Het 3D-A4'tje en andere reptiles
- 20 Sudoku's en drietallen
- 22 Omgekeerde kettinglijnen in de architectuur
- 27 Een bijzondere uitslag
- 30 Pythagoras Olympiade
- 33 Oplossing sudoku en 3d-puzzel nr. 1

■ **NIVEAUBALKJES** Pagina's met één of meer zwarte balkjes (onder de paginanummering) geven de moeilijkheidsgraad aan. Eén balkje: lastig. Twee balkjes: vereist wiskundekennis uit de vijfde of zesde klas. Drie balkjes: net iets moeilijker.

KLEINE NOOTJES

■ door Jan Guichelaar

ZINGENDE SCHAKERS

In een klas van 24 leerlingen zijn er 21 die zwemmen, 18 spelen schaak en 10 zingen in een koor. Eén leerling zit in alle drie de groepen. Hoeveel schakers zingen in het koor?
(Elsy Dewitte, België)



N Y X Σ > $\cap$ $\perp$ S

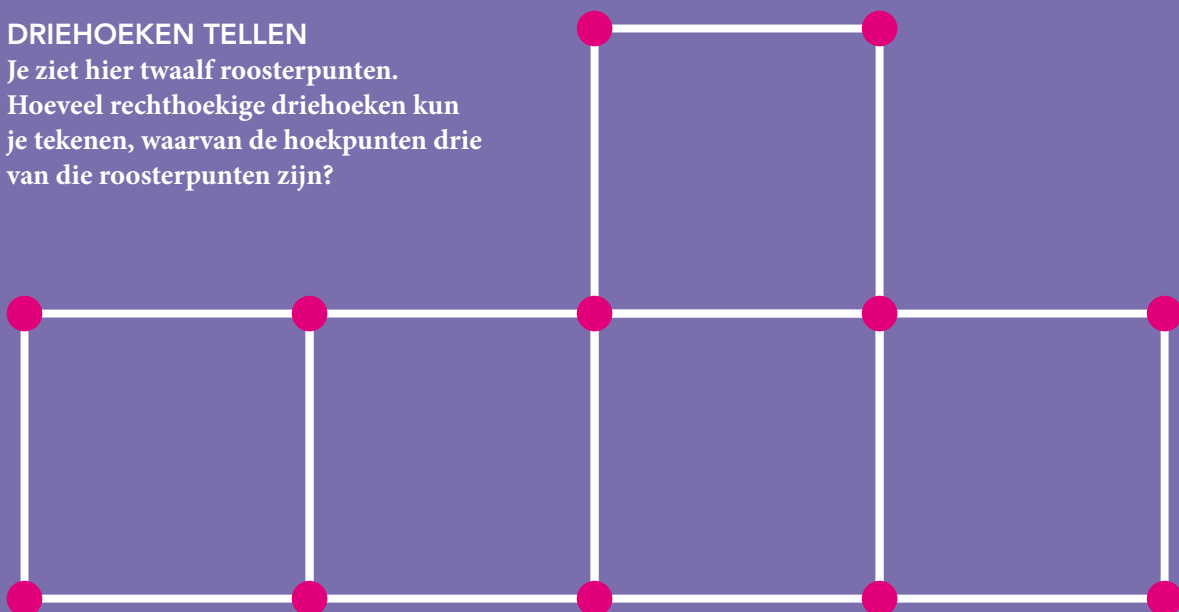
2

TAAL OF WISKUNDE?

Wat is de logica in deze rij tekens?

DRIEHOEKEN TELLEN

Je ziet hier twaalf roosterpunten. Hoeveel rechthoekige driehoeken kun je tekenen, waarvan de hoekpunten drie van die roosterpunten zijn?



Kleine nootjes zijn eenvoudige opgaven die weinig of geen wiskundige voorkennis vereisen om opgelost te kunnen worden. De antwoorden vind je in het volgende nummer van *Pythagoras*.

1961

DUURT DAT NOG LANG?

De cijfers 0, 1, 6, 8 en 9 kun je op hun kop zetten en dan krijg je de cijfers 0, 1, 9, 8 en 6. Het jaar 1961 is het recentste jaar dat op zijn kop hetzelfde jaar geeft. Wanneer doet zich dat voor het eerst weer voor?

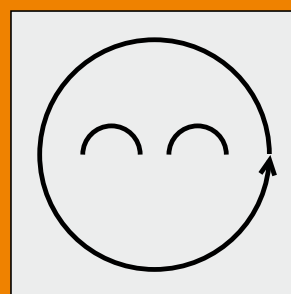
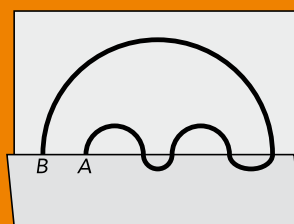


STOELENDANS

Plaats negen stoelen zodanig langs de muren van een rechthoekige kamer, dat langs elke muur even veel stoelen staan.

OPLOSSINGEN KLEINE NOOTJES NR. 1

Door de vierde dimensie? Vouw het blaadje zoals in de linkerfiguur. Begin te tekenen in punt A. Aangekomen in B, vouw je het blaadje terug en maak je de tekening af zoals in de rechterfiguur.

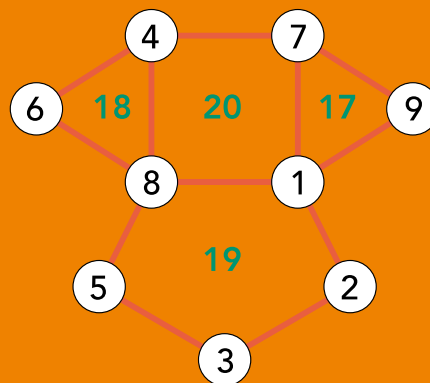


Volkorenbrood. Eén brood kost € 2,63.

Vijf gewichtjes. Nee, niet eenduidig, er zijn meerdere mogelijkheden. De gewichtjes kunnen 3, 4, 5, 6 en 8 gram zijn, dan heb je de evenwichten $8 = 5 + 3$, $8 + 5 = 6 + 4 + 3$, $8 + 3 = 6 + 5$ en $6 + 3 = 5 + 4$. Maar de gewichtjes kunnen bijvoorbeeld ook 1, 2, 3, 4 en 9 gram zijn; daarmee zijn ook vier verschillende evenwichten te maken.

2011 maken. Je wilt natuurlijk zoveel mogelijk negens in het getal hebben. De oplossing is: het getal bestaande uit een 4 gevolgd door 223 negens (want $4 + 223 \cdot 9 = 2011$).

Getallen plaatsen.



Het doel van een voetbalwedstrijd is redelijk duidelijk, zou je denken: je schiet de bal zo vaak mogelijk in het doel van je tegenstander, en het team met de meeste doelpunten wint. Maar bij de fameuze wedstrijd Grenada-Barbados in 1994 was alles anders.

■ door Jeanine Daems

EEN BIZARRE VOETBALWEDSTRIJD

‘Je moet altijd zorgen dat je een doelpunt meer scoort als de tegenstander.’ Deze fameuze uitspraak van Johan Cruyff is meestal waar, maar niet altijd. In toernooien ligt het allemaal net een beetje ingewikkelder, omdat de uitslag en het aantal gescoorde doelpunten in een wedstrijd dan beïnvloeden wat er daarna gebeurt: welk team het toernooi moet verlaten, of tegen wie er in de volgende ronde gespeeld moet worden. Maar toch: je moet winnen om de gunstigste situatie te bereiken, en winnen doe je door te scoren in het doel van de tegenstander.

Als de organisatie van zo’n toernooi niet goed heeft nagedacht, kunnen er echter rare dingen gebeuren. Een bizar voorbeeld is de beroemd geworden wedstrijd tussen twee landen in het Caribisch gebied tijdens de groepsfase van de Shell Caribbean Cup in 1994 (fragmenten zijn te zien op www.youtube.com/watch?v=ThpYsN-4p7w).

Barbados en Grenada speelden tegen elkaar. Samen met Puerto Rico zaten ze in een groep, en dit was de laatste groepswedstrijd. Grenada stond er beter voor, want Barbados – Puerto Rico was geëindigd in 0 – 1 en Grenada – Puerto Rico in 2 – 0.

Om winnaar in de groep te worden en verder te gaan in het toernooi, moest Barbados in ieder geval winnen van Grenada. Bovendien moesten ze een beter doelsaldo hebben dan Grenada. Dat betekende: winnen met minstens twee doelpunten verschil.

SCHIETEN IN EIGEN DOEL Er waren twee regels in het toernooi die tot de bizarre situatie tijdens deze wedstrijd leidden. Ten eerste: de organisatie had besloten dat elke wedstrijd in de groepsfase een winnaar moest hebben, gelijkspel mocht niet voorkomen. Als het na 90 minuten spelen gelijkspel was, dan werd de wedstrijd met maximaal een half uur verlengd, en daarin gold *sudden death*: wie in de extra tijd als eerste scoorde, was de winnaar.

Ten tweede: in het geval van verlenging en *sudden death*, telde de goal van het team dat in de extra tijd scoorde dubbel. Oftewel: de winnaar won dan met twee doelpunten verschil in plaats van één.

Wat gebeurde er nu tijdens deze beruchte wedstrijd? Barbados leidde met 2 – 0 tot de 83ste minuut. Toen scoorde Grenada. De stand was nu dus 2 – 1, wat betekende dat Barbados wel zou winnen, maar dat Grenada toch door zou gaan; Barbados had tenslotte twee doelpunten verschil nodig.

Het team van Barbados realiseerde zich dat in die laatste paar minuten nog een keer scoren misschien wel wat hoog gegrepen zou zijn. Maar nu kwam die tweede, ongebruikelijke regel mooi van pas: in het geval van een verlenging bestond de kans dat Barbados alsnog zou scoren, en dan hadden ze meteen twee punten erbij! Een verlenging eruit slepen was dus het beste dat Barbados op dat moment kon doen. Kortom: Barbados scoorde expres in eigen goal, waardoor de stand 2 – 2 werd.

Grenada had natuurlijk helemaal geen zin in die verlenging, dat zou Barbados een extra half uur ge-



ven om door hun verdediging heen te breken. Eigenlijk was op dat moment zelfs *alles* beter dan een verlenging: als ze zelf een doelpunt zouden scoren, waren ze de winnaars en gingen ze door. En als Barbados nog een doelpunt zou scoren, was Barbados wel de winnaar, maar dan was het verschil slechts één punt, kwam er geen verlenging en was Grenada ook door!

Zo ontstond de situatie dat het voor Grenada beter was om *in welk doel dan ook* te scoren! In de laatste vijf minuten van de wedstrijd probeerde Grenada dus in allebei de goals te scoren, terwijl Barbados de beide doelen stond te verdedigen.

Grenada slaagde er niet in te scoren, dus die ver-

lenging kwam er alsnog. Binnen de eerste vijf minuten scoorde Barbados. De eindstand was nu 4 – 2, en Barbados ging door naar de volgende ronde.

Zo zie je maar: het is belangrijk om van tevoren goed na te denken over de regels van een spel, om dergelijke onbedoelde strategieën te voorzien en te voorkomen. ■

BRONNEN

- John D. Barrow, *100 Essential Things You Didn't Know You Didn't Know*, The Bodley Head, London, 2008
- en.wikipedia.org/wiki/1994_Caribbean_Cup

JOURNAAL

■ door Alex van den Brandhof

Internationale wiskundewedstrijd voor scholieren via internet

Het Duitse wiskunde-instituut MATHEON organiseert al enige jaren een adventskalender. Van 1 tot en met 24 december wordt dagelijks op www.mathekalender.de een vakje 'geopend' waarachter een wiskundeprobleem verschijnt met 10 mogelijke antwoorden.

Die problemen zijn niet gemakkelijk (soms van het niveau van de finale van de Nederlandse Wiskunde Olympiade), maar de oplossing ervan vergt in principe geen geavanceerde wiskunde. De scho-

lier met de beste score wint een laptop. Daarnaast zijn er elke dag kleinere prijzen te winnen.

Net als vorig jaar werken de wiskunde-afdelingen van de Technische Universiteiten van Delft, Eindhoven en Twente, verenigd in 3TU.AMI (Applied Mathematics Institute), ook dit jaar weer samen met het MATHEON. Het is een individuele wedstrijd, maar het kan leuk zijn om met een groep of klas te proberen om samen het goede antwoord van een opgave te vinden.

Zó moeilijk is de Rubikkubus niet!

Informatici van het Massachusetts Institute of Technology (MIT) hebben een methode gevonden om willekeurige grote Rubikkubussen op te lossen. De standaard Rubikkubus heeft het formaat $3 \times 3 \times 3$. De kubus is opgelost als alle kanten eenzelfde kleur hebben. In het Journaal van september 2010 (*Pythagoras* 50-1) meldden we dat het maximale aantal stappen dat nodig is om een Rubikkubus op te lossen ('Gods getal') gelijk is aan 20.

Afgelopen zomer presenteerden de MIT-onderzoekers een algoritme dat gebruikt kan worden voor het oplossen van willekeurige grote Rubikkubussen. Daarmee kunnen ze berekenen van welke orde van grootte Gods getal is voor een $n \times n \times n$ kubus. Zij vonden dat het aantal stappen dat nodig is voor het oplossen van een $n \times n \times n$ kubus voor voldoende grote waarden van n , proportioneel is met $n^2 / \log n$. Dat betekent dat je twee constan-



tes a en b , en een derde getal N kunt vinden, zodanig dat voor elke $n > N$ geldt dat Gods getal voor een $n \times n \times n$ kubus tussen $a \cdot n^2 / \log n$ en $b \cdot n^2 / \log n$ ligt.

Deze onder- en bovengrens van Gods getal lijken behoorlijk grof. Toch geeft het resultaat een heel goed beeld van hoeveel een Rubikkubus moeilijker wordt om op te lossen naarmate het aantal vierkantjes van de kubus toeneemt. En dat blijkt heel erg mee te vallen.

In de *complexiteitstheorie* spreekt men van een moeilijk probleem (in vakjargon *NP-probleem*) indien het aantal stappen

dat nodig is om tot de oplossing te komen, een exponentiële functie is, bijvoorbeeld 2^n . En dat is hier niet het geval. Plot de grafieken van 2^n en van $n^2 / \log n$ maar eens. Je ziet al gauw dat de eerste grafiek een stuk sneller stijgt dan de tweede!

Om de waarde $n^2 / \log n$ te vinden, hebben de informatici een truc bestudeerd die veel kubusoplossers toepassen: het verplaatsen van een enkel vakje naar de juiste positie terwijl alle andere vakjes zo veel mogelijk op hun plaats blijven. Het was al bekend dat het aantal stappen dat nodig is om een kubus met deze techniek op te lossen proportioneel is met n^2 ; dat volgt uit het feit dat een $n \times n \times n$ kubus $6n^2$ vakjes heeft. De onderzoekers hebben de methode effectiever gemaakt door niet naar de verplaatsing van een enkel vakje te kijken, maar door groepen vakjes die dezelfde richting op moeten tegelijk te verplaatsen.

Vol van tetraëders en octaëders

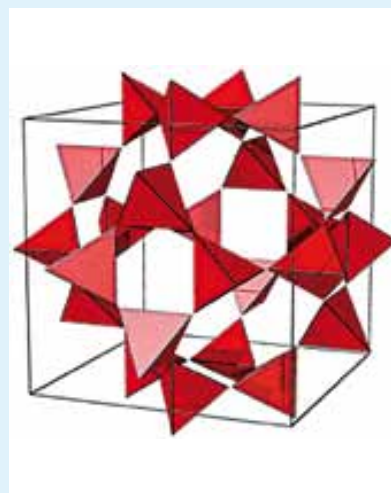
Het vullen van de driedimensionale ruimte met voorwerpen anders dan kubussen is een oud probleem, maar nog altijd onderwerp van hedendaags onderzoek. Yang Jiao, Salvatore Torquato en



Afbeelding: © Salvatore Torquato

John Conway, drie wiskundigen van Princeton University, hebben een nieuwe methode gevonden om de ruimte zonder gaten op te vullen met tetraëders (regelmatige viervlakken) en octaëders (regelmatige achthvlakken). De afbeelding links toont vier mogelijke manieren van vullen, waarop oneindig veel variaties mogelijk zijn. Bij zo'n vulling wordt iedere octaëder vergezeld door zes kleinere tetraëders.

Mogelijke toepassingen van de resultaten liggen op het gebied van materiaalkunde, maar bijvoorbeeld ook bij het verbeteren van transportnetwerken of het opslaan van data.



Hier zijn tetraëders afgebeeld. In de gaten passen precies octaëders. Afbeelding: © Ruggero Gabbrielli

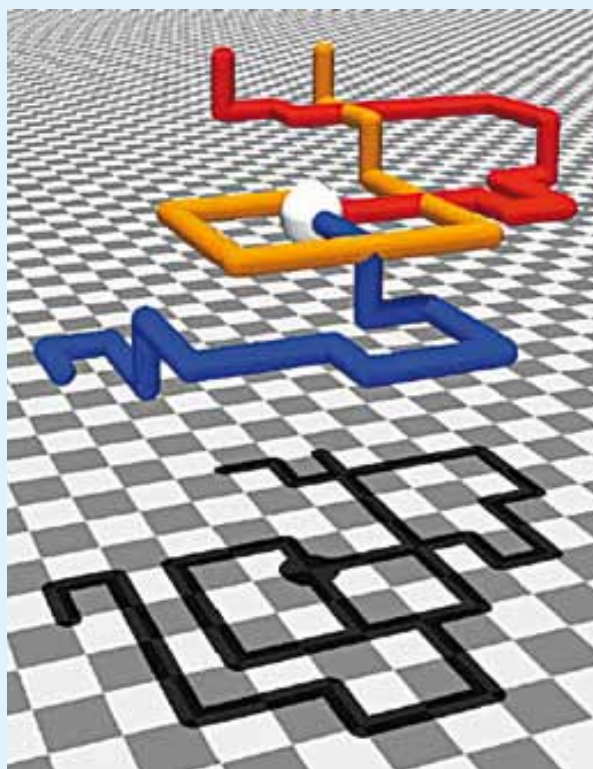
Nieuw wiskundig record zelfmijdende wandelingen

De Utrechtse wiskundestudent Raoul Schram heeft samen met zijn begeleiders een nieuw record neergezet in het rekenen aan zogenaamde zelfmijdende wandelingen: wandelingen in een driedimensionaal rooster die niet twee keer op eenzelfde plek komen.

Schram keek naar zelfmijdende wandelingen van 18 stappen in een driedimensionaal rooster, en door deze wandelingen op een slimme manier te combineren, kon hij berekenen hoeveel zelfmijdende wandelingen van 36 stappen er zijn: 2.941.370.856.334.701.726.560.670, dat is bijna drieduizend triljard.

In de figuur zie je drie zelfmijdende wandelingen van 18 stappen. Die kun je twee-aan-twee combineren tot wandelingen van 36 stappen. Alleen de rood-blauwe wandeling komt niet twee keer op eenzelfde plek; deze is dus zelfmijdend. Rood-oranje en blauw-oranje zijn niet zelfmijdend.

Het onderzoek van Schram kan onder meer gebruikt worden om het gedrag van langwerpige moleculen – zoals polymeren – te beschrijven. Het aantal manieren waarop deze moleculen als een soort kronkelweg kunnen worden opgevouwen, heeft namelijk invloed op eigenschappen als stroperigheid. De hoeveelheid verschillende mogelijkheden neemt echter enorm snel toe wanneer de moleculen langer worden en het aantal stappen groter wordt.



Darts is van oudsher een spel dat in cafés gespeeld wordt, maar sinds 1978 is er jaarlijks het *World Professional Darts Championship*. Sinds Raymond van Barneveld dit toernooi een keer won, geldt darts ook in Nederland als topsport. De indeling van het dartbord verbergt interessante wiskunde.

■ door Alex van den Brandhof en Jeroen Suijs

GEMENE DARTBORDEN

Het dartbord is in 1896 ontworpen door Brian Gamlin, een Engelse timmerman. De nummers 1 tot en met 20 plaatste hij zó, dat elk hoog getal tussen twee lage getallen in zit, zie figuur 1. De reden is duidelijk: hoe groter het getal waarop je mikt, hoe meer je gestraft wordt als de pijl er net naast gaat. Wie op de sector met getal 20 mikt, maar een sector ernaast treft, moet het doen met 1 of 5 punten. Door de grote getallen tussen de kleine te plaatsen, worden er hogere eisen aan de precisie van de spelers gesteld en is het onderscheidend vermogen van het dartbord groter.

De vraag is natuurlijk: heeft Gamlin het dartbord wel zo 'gemeen' mogelijk gemaakt?

Er zijn ongelooflijk veel borden mogelijk. Twintig getallen kunnen we op $20! = 20 \times 19 \times 18 \times \dots \times 1 = 2,43 \times 10^{18}$ manieren achter elkaar zetten. Omdat de getallen in een kring staan, moeten we dit getal nog door 20 delen: twee kringen zijn immers hetzelfde als ze door een draaiing in elkaar over te voeren zijn. Bovendien zijn twee verdelingen die elkaars spiegelbeeld zijn, in feite ook hetzelfde. Dan nog houden we ongeveer $6,08 \times 10^{16}$ (ruim zestig biljard) rangschikkingen over. Welke is het gemeenst?

TRIO'S VAN SECTOREN Wie niet zo goed kan darts, kan beter niet op de sector met 20 mikken: het risico dat de pijl in de 1 of de 5 komt, is te groot. Maar waar dan wel? Bestudering van figuur 1 wijst al snel naar het zuidwesten: wie op de 7 mikt, heeft een aardige kans om de 19 of de 16 te raken.

Als we aannemen dat ook een beginner wel een beetje kan mikken, en dus de bedoelde sector of één van zijn naaste burens raakt, heeft het zin om zulke trio's van sectoren te bekijken. Voor de 7 en

zijn burens is het aantal punten $7 + 19 + 16 = 42$, terwijl de 20 en zijn burens slechts sommeren tot $20 + 1 + 5 = 26$. Als we veronderstellen dat elk van de sectoren in een trio gelijke trefkans heeft, 1 op 3, levert mikken op de 7 dus gemiddeld meer op dan mikken op de 20 (in het kader op pagina 11 kun je lezen hoe het zit als de kansen ongelijk zijn).

Wat is onder deze aanname de 'gemeenste' verdeling van de twintig getallen?

Anders geformuleerd: hoe kunnen we de getallen 1 tot en met 20 rangschikken, zodanig dat de grootste som van de trio's zo klein mogelijk is, en de kleinste som zo groot mogelijk? Vergelijk het



Figuur 1 De indeling van het dartbord is ontworpen door Brian Gamlin.

PUNTENTELLING

Het dartbord is verdeeld in *ringen* en *sectoren*:

- In het midden is de *double bull* of *bull's eye* (rood), 50 punten.
- Daaromheen de *single bull* (groen), 25 punten.
- Daaromheen een brede ring, het *bed* (zwart en wit), waarvoor het aantal punten geldt dat op de rand van het bord staat.
- Daaromheen een smalle ring, de *triple* (of *treble*) *ring* (rood en groen). Deze levert drie maal het puntenaantal op.
- Daaromheen weer een *bed*.
- Daaromheen de *double ring* (rood en groen). Die levert twee keer het puntenaantal op.

Bij professionele wedstrijden starten beide spelers met 501 punten, en alle geworpen punten gaan van het totaal af. De speler moet precies op nul uitkomen, met de laatst geworpen pijl in de *double ring* of de *double bull*.

met een landschap dat zo vlak mogelijk moet zijn: de toppen moeten dan zo laag mogelijk liggen en de dalen zo hoog mogelijk.

Op het gebruikelijke dartbord (figuur 1) is het maximum 42 ($= 16 + 7 + 19$) en het minimum 26 ($= 5 + 20 + 1$). In figuur 2 zie je een verdeling waarbij het maximum omlaag gaat naar 33 en het minimum wordt opgeschroefd tot 30. Een behoorlijke verbetering!

KLEINSTE MAXIMUM We zullen nu laten zien dat het niet nóg beter kan: het is onmogelijk om een dartbord te construeren met een maximum van 32. Dit doen we in vier stappen. Laten we de twintig vakjes van het dartbord aangeven met $a, b, c, d, \dots, s, t$.

Stap 1. Twee opeenvolgende trio's hebben een verschillende som. Immers, de opeenvolgende trio's a, b, c en b, c, d hebben twee getallen gemeen en a en d zijn verschillend.

Stap 2. Een opeenvolgende serie van vijf trio's met respectievelijk som 32, 31, 32, 31, 32 is niet mogelijk. Immers, als het eerste trio a, b, c som 32 heeft en het tweede trio b, c, d som 31, dan geldt $d = a - 1$. Het derde trio c, d, e heeft weer som 32; met $d = a - 1$ volgt dan $a + c + e - 1 = 32$. Uit $a + b + c = 32$ volgt dat $a + c = 32 - b$. Combineren we deze twee vergelijkingen, dan krijgen we $e = b + 1$. Evenzo kun je afleiden uit $d + e + f = 31$ dat $f = c - 1$ en uit $e + f + g = 32$ dat $g = a$. Dit laatste kan echter niet, omdat het dartbord uit twintig verschillende

getallen moet bestaan.

Stap 3. Het gemiddelde van de getallen 1, 2, ..., 20 is 10,5, dus het gemiddelde van de trio's is voor elk dartbord $3 \times 10,5 = 31,5$. Dit betekent dat tegenover elk trio met som 30 er drie trio's met een som van 32 moeten staan om tot een gemiddelde van 31,5 te komen. Omdat er op een dartbord in totaal twintig trio's zijn, kan dit alleen wanneer er drie trio's van 30 zijn, negen trio's van 32 en acht trio's van 31. Bij elk ander aantal trio's van 30 zullen er altijd twee opeenvolgende trio's van 31 zijn of twee opeenvolgende trio's van 32 en dit is niet mogelijk (bijvoorbeeld, bij twee trio's van 30 zijn er zes trio's van 32 en twaalf trio's van 31; deze kun je niet rangschikken zonder twee opeenvolgende trio's van 31). Een serie bestaande uit drie trio's van 30, negen trio's van 32 en acht trio's van 31 kun je niet rangschikken zonder een serie van vijf trio's met respectievelijk som 32, 31, 32, 31, 32 te krijgen. In stap 2 hebben we echter gezien dat zo'n serie niet mogelijk is.

Stap 4. Uit stap 3 volgt nu dat er geen trio van 30 kan zijn. Dat betekent dat de sommen van de trio's afwisselend 31 en 32 moeten zijn. Maar uit stap 2 volgt dat dit niet mogelijk is.



Figuur 2 Van alle trio's is 33 het maximum en 30 het minimum.

getal	20	1	18	4	13	6	10	15	2	17	3	19	7	16	8	11	14	9	12	5	20
verschil	19	17	14	9	7	4	5	13	15	14	16	12	9	8	3	3	5	3	7	15	

Figuur 3 De verschillen bij het dartbord van figuur 1. De som van de verschillen is 198.



Figuur 4 Grote en kleine getallen wisselen elkaar af.

Opgave. In plaats van een verdeling in trio's, kun je het dartbord ook in stukken van vijf sectoren verdelen. Je neemt dan aan dat een pijl maximaal twee sectoren van de miksector inslaat. Onderzoek zelf wat dan de gemeenste verdeling is.

VERSCHIL VAN TWEE SECTOREN Een andere manier om de 'gemeenschap' van het dartbord te meten, is door te kijken naar de (niet-negatieve) verschillen van de getallen op twee naast elkaar gelegen sectoren. In figuur 3 zie je de verschillen bij het bestaande dartbord van figuur 1. De som van de verschillen is gelijk aan 198 en het is duidelijk, dat hoe groter de som van de verschillen is, hoe meer je gestraft wordt voor het missen van een hoog getal.

De vraag is of die waarde van 198 vergroot kan worden. Het antwoord is ja, al is de winst gering: de maximale som van de verschillen is 200. Het is niet moeilijk om een rangschikking te bedenken die

hieraan voldoet. Noem de getallen 1 tot en met 10 *kleine getallen* en de getallen 11 tot en met 20 *grote getallen*. Zet de kleine en de grote getallen afwisselend neer, de som van de verschillen is dan altijd 200. Het doet er niet toe in welke volgorde de kleine en de grote getallen staan, de enige voorwaarde is dat ze elkaar afwisselen. Dat de volgorde er niet toe doet, kun je als volgt inzien. De som van de verschillen is altijd gelijk aan tweemaal de som van de grote getallen min tweemaal de som van de kleine getallen: $2(11 + 12 + 13 + \dots + 20) - 2((1 + 2 + 3 + \dots + 10)) = 2 \times 155 - 2 \times 55 = 200$. Figuur 4 en 5 tonen een voorbeeld.

Heeft Gamlin dit niet bedacht? Waarschijnlijk wel. Maar er is een goede reden om niet te kiezen voor het bord van figuur 4, en al helemaal niet voor het bord van figuur 5, ook al zijn die verdelingen optimaal in de zin dat de som van de verschillen maximaal is.



Figuur 5 Grote en kleine getallen wisselen elkaar af, maar even en oneven helemaal niet!

VERWACHTINGSWAARDE

Ga uit van het dartbord in figuur 1. Veronderstel dat een speler met kans $\frac{3}{4}$ de sector treft waarop hij mikt, en met kans $\frac{1}{4}$ één van de burens (dus elk met kans $\frac{1}{8}$). Op welke sector kan de speler dan het beste mikken, om gemiddeld het beste resultaat te bereiken?

Als de speler altijd op de 20 mikt, zal hij gemiddeld $20 \times \frac{3}{4} + 5 \times \frac{1}{8} + 1 \times \frac{1}{8} = 15,75$ punten scoren. Deze waarde is het *gewogen gemiddelde* van de drie uitkomsten, met de kansen als gewichten. Dit gewogen gemiddelde heet de *verwachtingswaarde* van een worp waarbij op de 20 wordt gemikt. Deze verwachtingswaarde wordt niet beter door op een ander getal te mikken: omdat de succeskans ($\frac{3}{4}$) behoorlijk groot is, is mikken op 20 de beste strategie.

Maar stel nu dat de succeskans iets kleiner is: $\frac{2}{3}$ (en met kans $\frac{1}{3}$ wordt één van de naastgelegen sectoren getroffen). De verwachtingswaarde wordt dan $20 \times \frac{2}{3} + 5 \times \frac{1}{6} + 1 \times \frac{1}{6} = 14\frac{1}{3}$. Het getal 20 is nu niet meer de enige ‘beste keus’, want dezelfde verwachtingswaarde krijg je als je mikt op de 19: $19 \times \frac{2}{3} + 7 \times \frac{1}{6} + 3 \times \frac{1}{6} = 14\frac{1}{3}$. En bij een nog kleinere succeskans, bijvoorbeeld $\frac{3}{5}$, stoot de 19 de 20 van de troon: $19 \times \frac{3}{5} + 7 \times \frac{1}{5} + 3 \times \frac{1}{5} = 13,4$ tegen $20 \times \frac{3}{5} + 5 \times \frac{1}{5} + 1 \times \frac{1}{5} = 13,2$.

Natuurlijk hangt de trefkans af van hoe goed de speler is. Stel, deze kans is p , dus de trefkans van elk van de twee burens is $1 - \frac{1}{2}p$. De verwachte score van een trio a, b, c is dan $\frac{1}{2}(1-p)a + pb + \frac{1}{2}(1-p)c$. Je kunt dit ook schrijven als

$$\frac{1}{2}(1-p)\left(a+b+c+\frac{(3p-1)b}{1-p}\right).$$

De verwachtingswaarde wordt dus bepaald door de som van het trio plus een extra term die afhangt van het middelste getal b en de kans p dat je deze raakt. Wil je de maximale verwachte waarde minimaliseren, dan moet je hogere waardes van b combineren met lagere waardes voor a en c . Dit effect wordt sterker naarmate p groter is.

Opgave. Voor welke waarde van p minimaliseert het bord van Gamlin de maximale verwachtingswaarde?

Een ander aspect dat bij veel varianten van het darts spel van belang is, is namelijk het treffen van een *even* danwel *oneven* getal. Als je graag een oneven getal wilt raken, is het dartbord op zijn gemeentst als even en oneven elkaar afwisselen. En dat laat zich niet combineren met de voorwaarde dat de grote en de kleine getallen elkaar afwisselen. Dat kun je als volgt begrijpen. Begin met 20: dit getal is groot en even. Zijn twee burens zouden klein en oneven moeten zijn. En de burens van die getallen moeten weer groot en even zijn. Het gevolg is dat alle grote getallen even zouden moeten zijn en alle kleine getallen oneven, en dat is natuurlijk onmogelijk.

Bij het dartbord van figuur 5 staan alle even (en dus ook alle oneven) getallen bij elkaar. De dartborden van figuur 2 en 4 vertonen wel een beetje afwisseling tussen even en oneven, maar minder dan het bord van figuur 1. Het beste dartbord is een compromis van verschillende aspecten. De keuze van Gamlin lijkt in dat opzicht niet zo gek.

STRATEGIEËN Bij darts wordt meestal de variant gespeeld waarbij je begint met een aantal

punten en exact op nul moet uitkomen door je laatste pijl in de *double ring* of de *double bull* te gooien. Het is verstandig om eventuele missers in te calculeren. Stel je moet nog 51 punten scoren.

Je kunt nu in één ronde (waarbij je met maximaal drie pijlen mag gooien) uitkomen. Een mogelijkheid is: enkel-17 en (indien raak) dubbel-17. Er is echter een slimmere strategie, die ruimte geeft voor fouten. Mik eerst op enkel-19; als dit raak was, probeer je dubbel-16; als de pijl in enkel-16 belandt, heb je nog altijd een derde pijl waarmee je op dubbel-8 kunt mikken.

Nog een voorbeeld: stel je moet nog 130 punten verzamelen. Dat kan door achtereenvolgens te mikken op triple-16, *double-bull* en dubbel-16, maar deze serie heeft geen ‘terugvalstrategie’. Verstandiger is: triple-20, enkel-20 en *double-bull*. Als de eerste pijl in enkel-20 belandt, probeer je met de tweede pijl dubbel-20, en tot slot *double-bull*. ■

BRONNEN Bij het schrijven van dit artikel is gebruik gemaakt van *FC Algebra – cijfers en sport* van Hans van Maanen (uitgeverij Boom, 1998) en *The hidden mathematics of sport* van Rob Eastaway en John Haigh (uitgeverij Portico, 2011).

Het welbekende A4-papierformaat heeft de eigenschap dat als je twee A4'tjes met de lange zijden tegen elkaar legt, de verhouding tussen de korte en de lange kant van dat dubbel zo grote blad hetzelfde is gebleven. Vanwege deze eigenschap noemen we een A4'tje in dit artikel een '2-reptile'. Welke vormen kunnen reptiles nog meer hebben?

■ door Jaap Klouwen

HET 3D-A4'TJE EN ANDERE REPTILES

Als je een A4'tje dubbel vouwt, blijft de lengte/breedte verhouding van het papier hetzelfde; origineel en 'halvering' zijn gelijkvormig. Hetzelfde geldt voor een verdubbeling: leg twee A4'tjes met de lange zijden naast elkaar. De verhouding tussen de korte en de lange kant van het geheel blijft dan gelijk. Deze verhouding is $1 : \sqrt{2}$, zie figuur 1.

Dit is eenvoudig uit te rekenen als je de verhouding $1 : x$ stelt en verder beseft dat bijvoorbeeld bij verdubbeling de nieuwe verhouding tussen kort en lang $x : 2$ wordt. Gelijkstellen van deze beide verhoudingen levert

$$\frac{1}{x} = \frac{x}{2}$$

en daarmee de kwadratische vergelijking $x^2 = 2$, met de positieve oplossing $x = \sqrt{2}$.

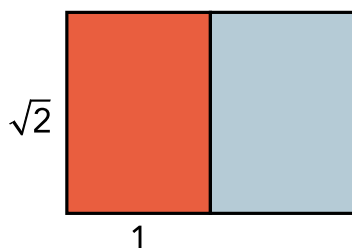
REPTILES In 1923 stelde de Duitse chemicus Wilhelm Ostwald voor om deze verhouding voor papierformaten in te voeren, omdat het met die formaten een rommeltje was geworden. De standaardmaat werd het A0-formaat van 84,1 bij 118,9 centimeter, met een oppervlakte van 1 vierkante

meter (!). De 'dubbelgevouwen' helft van A0 is het A1-formaat, enzovoorts. Zo komen wij aan ons A4'tje van 21,0 bij 29,7 centimeter.

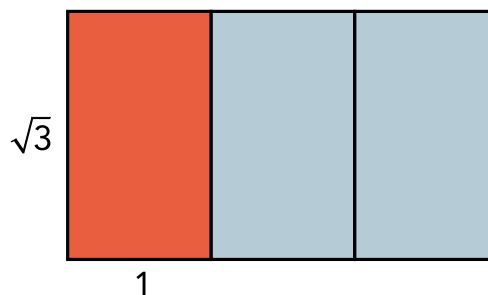
We kunnen een A4'tje een '2-reptile' noemen. Het woord 'reptile' is een samentrekking van de Engelse woorden *repeat* (herhaling) en *tile* (tegel, hier in de betekenis van een vlakverdeling). Twee van zulke vormen kunnen samen weer die vorm opleveren.

Er bestaan ook reptiles van 'hogere' orde. Een rechthoekig stuk papier waarvan de lange zijde $\sqrt{3}$ keer zo groot is als de korte zijde is een 3-reptile, zie figuur 2. Een vierkant is een voorbeeld van een 4-reptile.

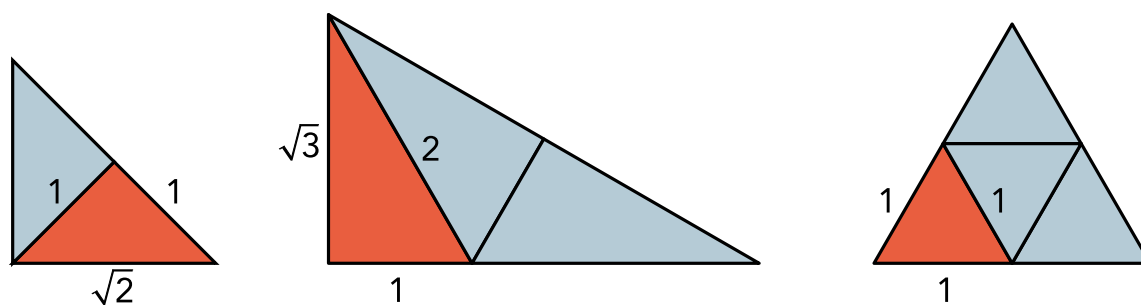
Natuurlijk zijn er ook andere reptiles dan vierkanten en rechthoeken. Figuur 3 toont een 2-, een 3- en een 4-reptile. De driehoekige 2-reptile noem ik voor het gemak de 'geodriehoek', wegens zijn rechthoekigheid en gelijkzijdigheid. De driehoek in de 3-reptile is de bekende 30-, 60- en 90-graden-driehoek met zijden $1 : \sqrt{3} : 2$. In deze 3-reptile is te zien dat reptiles mogen worden gespiegeld. Merk verder op dat bijvoorbeeld met de 4-reptile ook een 16 keer zo grote gelijkzijdige driehoek kan worden



Figuur 1 Een 2-reptile



Figuur 2 Een 3-reptile



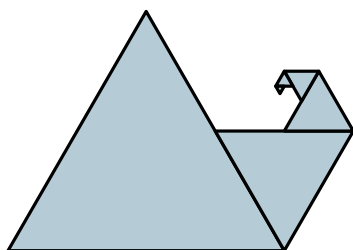
Figuur 3 Een 2-reptile, een 3-reptile en een 4-reptile

gelegd, of een 64 keer zo grote, enzovoorts. We nemen dan steeds de kleinste waarde met die gelijkvormigheidseigenschap.

Opgave 1. Kun je nog andere reptiles vinden?

Met een gelijkzijdige driehoek kan ook nog een andere, bijzondere reptile gemaakt worden, zie figuur 4. Deze figuur bestaat uit oneindig veel gelijkzijdige driehoeken; elke driehoek is vier keer zo klein ten opzichte van de vorige. De vormen die uit een dergelijk proces ontstaan, heten *fractals*. Deze fractal, de *snail*, is tevens een reptile.

Opgave 2. Is deze *snail* een 2-, 3- of hogere orde reptile?



Figuur 4 De *snail*

A4'TJE IN DRIE DIMENSIES Enige tijd geleden bekeek ik een folder van de Hema, met daarin onder andere een set van nagenoeg balkvormige opbergboxen. Als men twee van deze boxen tegen elkaar aanzette, ontstond een (uiteraard) twee keer zo grote box, maar de verhoudingen van de drie zijden bleven nagenoeg behouden. Deze opbergbox toonde bij verdubbeling dus 'vormbehoud'!

Zou er een balk bestaan waarbij dit 'vormbehoud' exact optreedt? Zet je bijvoorbeeld twee kubussen (dobbelstenen) tegen elkaar aan, dan is deze dubbele vorm niet in verhouding met het origineel. Voor twee luciferdoosjes of pakken hagelslag geldt hetzelfde. Op geen enkele manier zijn twee van zulke tegen elkaar gelegde doosjes gelijkvormig met het oorspronkelijke doosje. Er is echter één uitzondering: het '3-dimensionale A4'tje'.

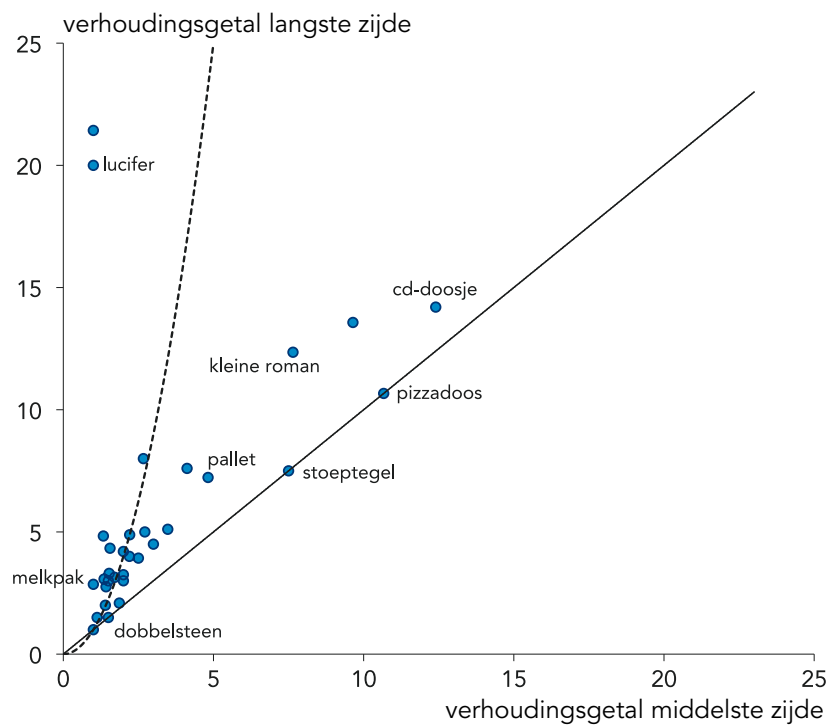
Nadenkend over een mogelijke oplossing voor het 3-dimensionale A4'tje speelden er allerlei blokvormige objecten en verpakkingen door mijn hoofd: een legosteent, een literpak melk, een verhuisdoos, een sigarettendoosje, een luciferdoosje, een pak rijst en nog heel veel meer. Ik maakte een lijst van deze objecten en hun afmetingen, en deelde de afmetingen van al deze objecten steeds door hun *kleinste* lengtezijde. Bijvoorbeeld: een dobbelsteen heeft afmetingen $1,5 \times 1,5 \times 1,5$ cm, dus in verhouding $1 : 1 : 1$; een literpak melk is $7 \times 7 \times 20$ cm, oftewel $1 : 1 : 2,9$; een pakje boter is $3,5 \times 6 \times 11$ cm, dus verhoudingsgewijs $1 : 1,7 : 3,1$. Van een dertigtal objecten zijn in figuur 5 (op de volgende pagina) de verhoudingsgetallen van de middelste en de langste zijde weergegeven, een overstap van drie naar twee dimensies dus. In deze grafiek heeft de dobbelsteen dus 'coördinaten' $(1; 1)$, het melk-pak $(1; 2,9)$, het boterpakje $(1,7; 3,1)$ enzovoorts.

In de figuur liggen op de 45-gradenlijn de dobbelsteen, de fruitella, de stoeptegels en de pizzabezorgdoos. Op de verticale lijn met middelste verhoudingsgetal 1 liggen (wederom) de dobbelsteen, het melk-pak, een tuinpaal en de lucifer. Op de parabool $y = x^2$ liggen objecten met de eigenschap dat de verhouding 'middellang/kort' en 'lang/middellang' constant is ($1 : x : x^2$), bijvoorbeeld de baksteen (waalformaat) $5 \times 10 \times 20$, en het grote pak Venz hagelslag $4,3 \times 9,5 \times 21$, in verhouding $1 : 2,2 : 2,2^2 = 1 : 2,2 : 4,84$.

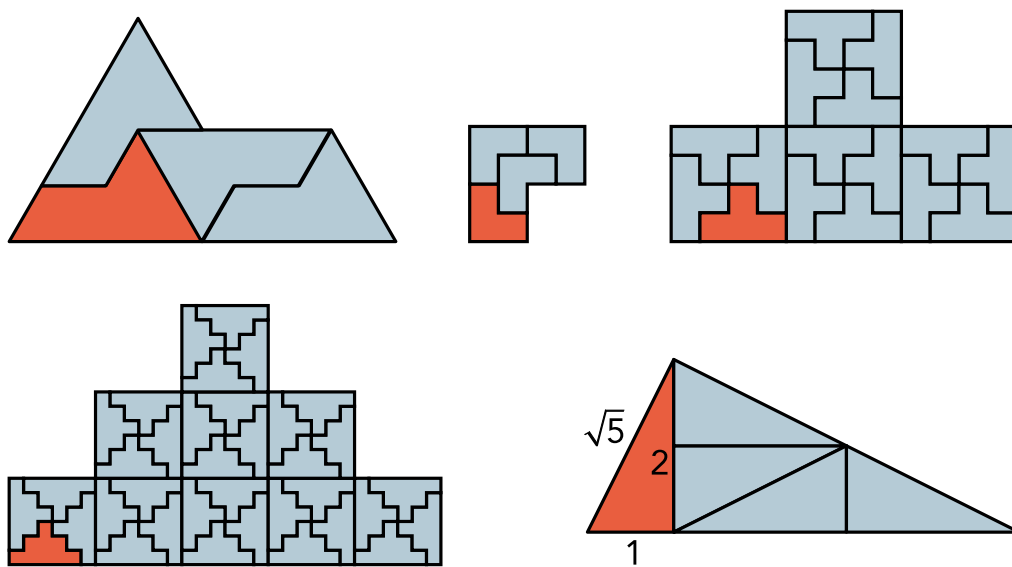
Deze manier van denken over blokvormen geeft ook aanleiding tot leuke beschouwingen als: 'zitten soortgelijke producten in overeenkomstige verpakkingen?' of de ontdekking van de vormgelijkheid van een droptoffee en een pak vacuüm koffie, of die tussen een literpak sap en een legosteent (4 bij 2 noppen).

Opvallend in de grafiek is verder de afwezigheid van objecten rondom het punt $(5; 15)$ (een gat in de verpakkingmarkt?). Ergens in deze puntenwolk van de grafiek zit het 3D-A4'tje.

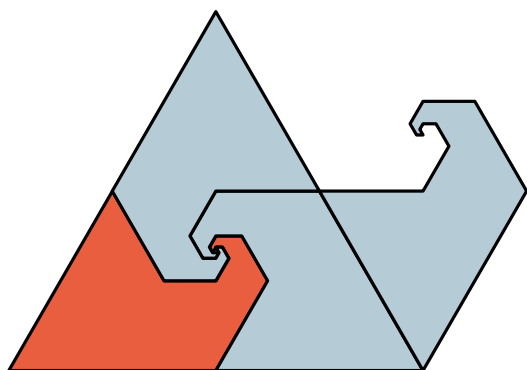
Opgave 3. Wat is de verhouding van korte, middelste en lange zijde van het 3D-A4'tje?



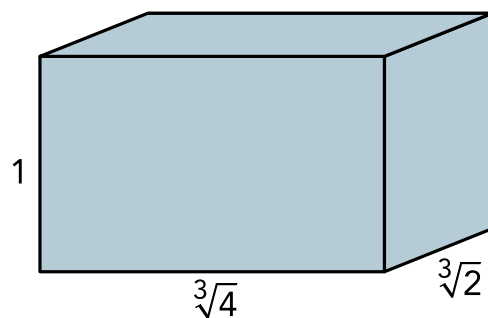
Figuur 5 Verhoudingen van de middelste en langste zijde van diverse balkvormige objecten



Figuur 6 Boven twee 4-reptiles en een 16-reptile, onder een 36-reptile en een 5-reptile



Figuur 7 De snail: een 4-reptile



Figuur 8 Het 3D-A4'tje, oftewel de 'archiefdooos'

ANTWOORDEN

Opgave 1. In figuur 6 zie je twee 4-reptiles, een 16-reptile en een 36-reptile. Een voorbeeld van een 5-reptile is de zogeheten ‘pinwheel tiling’ van John Conway. Merk op dat ook hierin de basisdriehoek met zijden $1 : 2 : \sqrt{5}$ ook gespiegeld gebruikt wordt.

Opgave 2. De *snail* is een 4-reptile, zie figuur 7.

Opgave 3. Het 3D-A4'tje heeft afgerond de verhoudingen $1 : 1,26 : 1,59$. De exacte verhoudingsgetallen zijn $1 : \sqrt[3]{2} : \sqrt[3]{4}$. De getallen zijn te vinden door je te realiseren dat twee overeenkomstige zijden van het drietal afmetingen (a, b, c) nooit tegen zichzelf aan kunnen liggen om vormgelijkheid te behouden bij een verdubbelde inhoud. Het drietal (a, b, c) gaat bijvoorbeeld over in $(b, c, 2a)$. Uit de verhoudingen $a : b = b : c$ en $b : c = c : 2a$ volgt een stelsel van twee vergelijkingen en drie onbekenden:

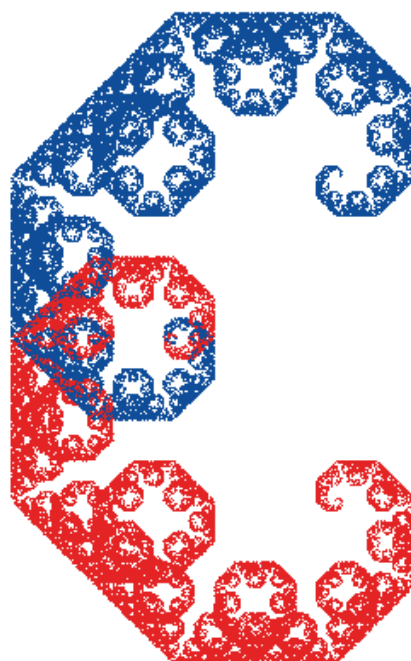
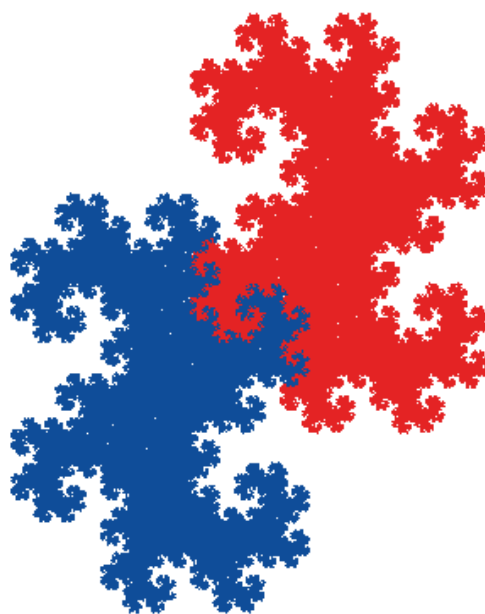
$$\frac{a}{b} = \frac{b}{c} \quad \text{en} \quad \frac{b}{c} = \frac{c}{2a}.$$

Stel je hierin $a = 1$, dan volgt dat $c = b^2$ en $c^2 = 2b$. De variabele c eliminerend vinden we $b^4 = 2b$. Dus $b^3 = 2$, dus $b = \sqrt[3]{2}$ en $c = \sqrt[3]{4}$. Omdat a, b en c willekeurig gekozen zijn, geven alle combinaties van a, b en c die deze drie letters niet op de eigen plaats laten staan deze oplossing. De oplossing is dus uniek.

Ik noem deze vorm de ‘archiefdoos’, omdat ik hem daar het meest op vind lijken; zie figuur 8. Zet twee van deze archiefdozen op elkaar en zet het nieuwe object op zijn grootste zijde, dan ziet men de oorspronkelijke vorm exact terug!

DRAKEN Na dit 3D-uitstapje keren we even terug naar de tweedimensionale 2-reptiles en vragen ons af: zijn er nog andere tweedimensionale 2-reptiles dan het A4'tje en de gelijkbenige, rechthoekige driehoek? Het antwoord is: ja. In 1999 bewezen de wiskundigen S.M. Ngai, V.F. Sirvent, J.J.P. Veerman en Y. Wang dat er precies zes tweedimensionale 2-reptiles zijn. Naast de twee genoemde (rechthoek en driehoek) zijn dat wel andersoortige 2-reptiles. Het zijn vier fractals: de *tweelingdraak*, de *snelwegdraak*, de *Levy-draak* en de *getemde draak*. Er zijn alleen deze zes mogelijkheden, als je eist dat de vormen niet gespiegeld mogen worden. In figuur 9 zie je er twee. Op ingenieuze wijze passen twee van zulke draken ‘in elkaar’ en vormen zo een twee maal zo grote, congruente draak!

Ik eindig in drie dimensies, met een nog intrigerender vraag: zijn er nog andere *driedimensionale* 2-reptiles dan de ‘archiefdoos’? Stuur je bevindingen naar post@pythagoras.nu. ■



Figuur 9 Boven de tweelingdraak, onder de Levy-draak

Dit artikel is gebaseerd op twee puzzels uit het boek *Denkwaar* van Jaap Klouwen, Veen Magazines, 2010.



HOE VEILIG IS DE OOS

Na de watersnoodramp van februari 1953 was iedereen het erover eens: dit mag nooit meer gebeuren! Het was aanleiding om de plannen voor de Deltawerken versneld uit te voeren. De Deltawerken bestaan onder meer uit het afsluiten van zeearmen als de Oosterschelde, de Grevelingen, het Haringvliet en de Nieuwe Waterweg.

■ door Jan Stout

Eén van de huzarenstukken van de Deltawerken was het afsluiten van de Oosterschelde. Eerst zou dit een dam worden, zodat het Oosterscheldebekken stilstaand water zou bevatten. Maar om milieuredenen werd vlak voor de bouw besloten om een open, maar afsluitbare kering te bouwen. Daardoor konden de getijdenstromen nog steeds het bekken in en uit en bleef de unieke natuur in de Oosterschelde behouden. Na ongeveer tien jaar bouwen was de Oosterscheldekering (in dit stuk verder aangeduid als OSK) in 1986 operationeel.

De OSK moet ervoor zorgen dat de waterstanden op het achterliggende Oosterscheldebekken niet te hoog worden, zodat de dijken rond dit bekken (als tweede verdedigingslinie) het achterland voldoende beschermen. Maar hoe veilig is de OSK?

Het is bij wet geregeld dat de OSK niet vaker dan eens in de 4000 jaar mag falen. Met andere woorden: de extreme omstandigheden die statistisch gezien eens per 4000 jaar optreden moeten nog net veilig onder controle gehouden kunnen worden.

De OSK bestaat uit 62 beweegbare schuiven, die bij een te hoge waterstand worden gesloten. Als de te verwachten waterstand aan de zeezijde van de OSK hoger is dan 275 cm boven NAP (Nieuw Amsterdams Peil, de standaard zeewaterhoogte in Nederland), dan wordt automatisch een team van deskundigen opgeroepen; dit team beslist of de kering dicht gaat. Als de verwachte waterstand hoger is dan 300 cm boven NAP, wordt de kering gesloten.

Als om wat voor reden dan ook het team niet bij elkaar kan komen, dan sluit de kering automatisch zodra de waterstand boven de 300 uit komt. Maar de kering kan technisch falen. Tijdens een sluiting kunnen één of meerdere schuiven weigeren – dit noemen we *partieel falen* – of zelfs de hele kering. En hiermee hebben we meteen al een probleem, want door het mogelijk partiële falen kunnen we de faalkans van de kering niet direct in één getal weer geven.

De hamvraag is: wat zijn de gevolgen voor het Oosterscheldebekken als de OSK geheel of gedeeltelijk faalt? Het probleem hebben we bij Rijkswaterstaat in drieën gedeeld, mede omdat per onderdeel verschillende expertise nodig is.

KANSVERDELINGEN Het eerste deel omvat de extreme omstandigheden op de Noordzee, dus aan de buitenkant van de OSK. Dit zijn kansverdelingen voor windrichting, windsnelheid, waterstand, stormduur en het tijdstip van de storm ten opzichte van hoog/laag water (de 'fase'). Een kansverdeling kun je afbeelden als een grafiek met horizontaal, bijvoorbeeld, de windkracht (in meter per seconde) en verticaal de kans dat de wind hoogstens die snelheid heeft, zie de figuur op pagina 17.

Je kunt je voorstellen dat bij een noordwesterstorm de kans op hoge waterstanden groter is dan bij een storm uit het oosten. Sommige kansverdelingen hangen dus van andere af.

Voor de windrichting zijn er 12 klassen, voor de



windsnelheid 21, voor de waterstand 51, 5 voor de stormduur en 3 klassen voor de fase. In totaal zijn dat $12 \times 21 \times 51 \times 5 \times 3 = 192.780$ verschillende mogelijke situaties. De meest extreme situatie waarmee rekening wordt gehouden, is een waterstand van 650 cm boven NAP, windsnelheid 50 m/s (windkracht 12) uit het noordwesten, met een stormduur van 100 uur.

Het in kaart brengen van al deze situaties en hun onderlinge samenhang was een proces van vallen en opstaan. Bij de eerste berekeningen hadden we een veel te grove klassenindeling, wat resulteerde in een veel te hakkerige overschrijdingskromme (je leest later in dit artikel wat dat is).

FAALSCENARIO'S Het *tweede deel* is het bepalen van de faalkans van de kering zelf, en van de bediening. Deze inventarisatie van alles wat er mogelijk mis kan gaan, is een geweldig uitgebreid en ook arbeidsintensief proces.

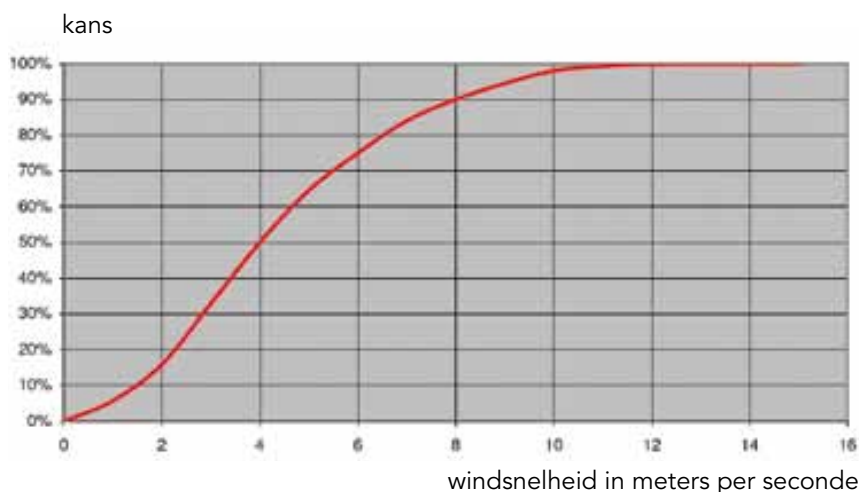
Neem als voorbeeld de energievoorziening. De

OSK heeft eigen dieselgeneratoren die voldoende energie kunnen opwekken om de OSK te sluiten en te openen. In principe hebben we voldoende aan vier generatoren, maar gezien de kans op falen van één of meer generatoren, zijn er twee groepen van ieder vijf stuks neergezet. De kans dat er desondanks niet voldoende energie opgewekt kan worden, is berekend op 1 op de 6000 jaar.

De totale faalkansboom van de OSK bestaat uit 5000 componenten. Van elke component moet bekend zijn wat de kans is dat hij niet beschikbaar is wanneer de kering dicht moet. Dit wordt bepaald door de component zelf, hoe vaak deze geïnspecteerd en getest wordt, de beschikbaarheid van reserveonderdelen en de reparatieduur.

Een voorbeeld van een faalkansboom, met uitleg hoe die werkt, zie je in het kader op pagina 18.

Bij gecertificeerde onderdelen worden de faalkanscijfers aangeleverd door de leverancier. Dit zijn cijfers die gelden bij een standaard gebruik. Een dieselcentrale is normaal gesproken continu in ge-



Voorbeeld van een kansverdeling voor de windsnelheid. De grafiek is *cumulatief*, dat wil zeggen: je leest de kans af op een bepaalde windsnelheid *of lager*. Dus bijvoorbeeld: de helft van de tijd (0,5) waait het 4 m/s of langzamer, 90% (0,9) van de tijd waait het 8 m/s of langzamer. Je kunt de verticale schaalverdeling in gedachten ook omdraaien, dan lees je af: 10% ($1 - 0,9$) van de tijd waait het harder dan 8 m/s.

bruik, maar bij de OSK draait de centrale maar één keer per maand, tijdens testen. Bij een andersoortig gebruik hoort ook een ander faalkanscijfer.

Met 62 schuiven heb je $4,6 \times 10^{18}$ mogelijke combinaties van falen. Dat is zelfs met de huidige computerkracht niet door te rekenen. We hebben ons daarom beperkt tot acht faalscenario's: 1, danwel 2 weigerende schuiven, een blok van 3 tot 5 schuiven, een blok van 6 tot 10 schuiven, een kwart kering, een halve kering, een driekwart kering en ten slotte de hele kering zelf.

Om een indruk te krijgen van de omvang van de faalkansboom: het heeft circa vier mensjaar gekost om deze op te zetten en de uitdraai bedraagt ongeveer 300 pagina's. Naast de acht faalscenario's bestaat natuurlijk ook scenario 9: dat de kering *niet* faalt (gelukkig maar).

De mens heeft uiteraard ook invloed op de faalkans. Meestal een positieve, maar soms een negatieve invloed. De positieve bijdrage start al bij het ge-

controleerd sluiten van de OSK. Daardoor kunnen de waterstanden op het bekken achter de kering op een dusdanige hoogte worden ingesteld, dat de gevolgen van een langdurige golfaanval op de dijken minimaal zijn. Tevens is de mens een hersteller van ongewenste situaties. Als er bijvoorbeeld een schuif weigert, dan kan de mens deze nog handmatig (buiten de computer om) laten zakken.

De negatieve bijdrage kan optreden bij onderhoud. Bijvoorbeeld: een installatie die in onderhoud wordt genomen, maar niet in de oorspronkelijke staat wordt teruggezet. Om dit zo veel mogelijk te voorkomen, zijn voor cruciale handelingen werkprocedures gemaakt en worden de gegevens van het onderhoud in een database gezet voor nadere analyse.

Ook voor het oproepen van het personeel is een faalkansboom gemaakt. De grootste kans dat geen personeel wordt opgeroepen is te wijten aan een fout in de waterstandverwachting. Dit is dus de si-

DE FAALKANSBOOM VAN DE DIESELGENERATOR

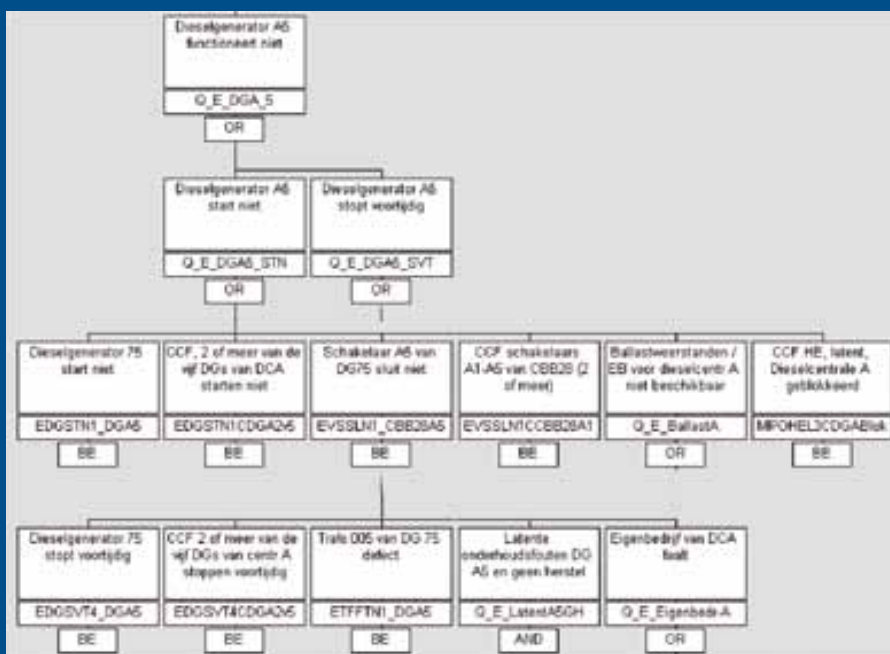
Bij het opstellen van een foutenboom ga je inventariseren wat er allemaal mis kan gaan. In dit voorbeeld nemen we de dieselgenerator. Als deze niet functioneert, dan kan de kering niet gesloten worden.

Er zijn twee mogelijke oorzaken waarom de dieselgenerator niet functioneert: hij start niet OF hij stopt voortijdig. Dit is dus een OF-situatie (in het Engels OR). Dus als één van de oorzaken optreedt, dan functioneert de dieselgenerator niet.

Er bestaat ook een EN-situatie (Engels: AND). Dan moeten beide onderliggende oorzaken optreden.

Elke oorzaak kan weer onderliggende oorzaken hebben en zo splits je de boom steeds verder op totdat je bent uitgekomen op componentniveau, bijvoorbeeld: trafo werkt niet. Dit noemen we een *Basic Event* (BE). Dat is dus het einde van een tak.

Van elke Basic Event weten we de kans van falen. En op die manier kunnen we het falen van de bovenliggende oorzaak uitrekenen totdat we weer helemaal bovenaan zijn en zo de kans van het niet functioneren van een dieselgenerator hebben bepaald.



tuatie dat de verwachte waterstand (op basis van de weersvoorspelling en hoog/laagwater) lager is dan 275 cm boven NAP, maar het water in feite hoger komt dan 300 cm boven NAP. Dan sluit de kering automatisch. Gelukkig is dat de afgelopen 25 jaar niet voorgekomen.

Van elk scenario is bepaald wat de faalkans is als de mens wel of niet aanwezig is, in totaal dus $2 \times 9 = 18$ scenario's. Maar als de kering niet faalt, maakt het niet uit of de mens wel of niet aanwezig is, dus eigenlijk zijn het maar 17 verschillende. Voor de programmatuur is het echter handiger om toch te rekenen met 18 scenario's.

REKENEXERCITIE Het *derde deel* is het doorrekenen welke waterstanden een storm op de Noordzee via de OSK (met de diverse faalscenario's) veroorzaakt in het Oosterscheldebekken. Dit gebeurt met een *hydraulisch model*, als volgt. Een deel van de Noordzee buiten de OSK, de OSK zelf en het Oosterscheldebekken is ingedeeld in vakken. Voor elk vak worden twee vergelijkingen opgesteld, te weten de *gelineariseerde bewegingvergelijking* en de *gelineariseerde continuïteitsvergelijking*, elk met twee onbekenden. Voor de computer heeft elk vak namelijk maar twee eigenschappen: het water heeft er een bepaalde hoogte (de waterstand) en er is in- en uitstroom in een bepaalde richting (het debiet). Gelineariseerd wil zeggen dat slechts een vereenvoudigde versie van de fysisch correcte vergelijkingen wordt gebruikt.

De twee vergelijkingen vormen de wiskundige beschrijving van de eigenschappen van een grote watermassa: water is niet samendrukbaar, vult kuilen en gaten meteen op en er is een bepaalde hoeveelheid energie per kubieke meter nodig om een waterstroom op gang te brengen.

Het gebied wordt ingedeeld in 145 vakken en het model heeft dus 290 vergelijkingen met 290 onbekenden. Gegeven is een van de 192.780 extreme begintoestanden.

Het verloop van een storm wordt nu door de computer opgedeeld in 720 tijdstappen. In elke stap bekijkt de computer wat de waterstand en het debiet in elk vak is, en wat dat betekent voor de aangrenzende vakken. Wiskundig gezien lost de computer 290 vergelijkingen met 290 onbekenden op; fysisch gezien voorspelt dit de toestand in alle vakken gedurende de volgende tijdstap.

Omdat er 192.780 verschillende extreme situaties en 18 faalscenario's zijn, moet deze hele reken-exercitie dus zo'n 3,5 miljoen maal gedaan worden. De eerste berekeningen in 2008 vergden ongeveer vier weken computertijd. Nu, met een clustering van computers, nog maar (!) een weekend.

De berekende waterstanden op 19 belangrijke locaties op het Oosterscheldebekken worden nu opgeslagen in een database.

Anders gezegd: de eerste invoerparameter van het hydraulisch model is een extreme situatie op de Noordzee en daarvan is de kans van optreden bekend. De tweede invoerparameter is een bepaald faalscenario van de OSK met ook daarbij de kans van optreden. Uiteindelijk resulteert dit in een overschrijdingskromme voor elk van de 19 locaties: een kansverdeling die aangeeft hoe groot op deze plek de kans is dat het water tijdens een storm tot een zekere hoogte zal stijgen.

Voor elk van deze locaties op het Oosterscheldebekken wordt door de wet voorgeschreven wat het maatgevend hoogwater (MHW) is. De OSK moet dusdanig goed functioneren dat het MHW hooguit één keer in de 4000 jaar overschreden wordt. Deze kans kunnen we aan de overschrijdingskromme aflezen, en we zien direct of de kering voldoet voor die locatie. De slechtst presterende locatie van de 19 geldt als maat voor de veiligheid van de OSK in elke situatie.

TOEKOMST De eerste uitkomsten waren best spannend. Zijn we slechter of beter dan de geëiste 1 op 4000 jaar? Gelukkig zitten we aan de (zeer) goede dus veilige kant.

Het falen van de kering wordt niet alleen bepaald door het falen van de componenten, maar uiteraard ook door het falen op civiel gebied. Want hoe groot is de kans dat bijvoorbeeld een gedeelte van de OSK wegspoelt of dat de damaansluiting bij het land doorbreekt? Ook deze kansen zijn bekend, maar die zijn minstens duizend keer kleiner dan het falen van de componenten uit de faalkansboom. Ze worden dan ook als constante meegenomen in de totale berekening.

Bij het ontwerp van de OSK (begin jaren '70) was de opwarming van de aarde en de daaraan gekoppeld de zeespiegelrijzing totaal niet in beeld. Het was al een probleem om een kansverdeling te maken van de extreme omstandigheden op de Noordzee. En het is nog veel lastiger om een nieuwe kansverdeling te maken inclusief de zeespiegelrijzing. Hoe groot zal de zeespiegelrijzing zijn in 2070 of in 2100? Gaat het windklimaat veranderen? Aan deze berekeningen en de invloed op de faalkans wordt momenteel gewerkt. We verwachten over twee jaar meer gefundeerde uitspraken te kunnen doen. ■

Jan Stout is projectmanager bij Rijkswaterstaat. Meestal houdt hij zich bezig met projecten waar iets nieuws, wiskunde en organisatie bij elkaar komen.

Je kunt vandaag de dag geen dagblad openslaan, of je vindt er wel een sudoku in. Het oplossen kan behoorlijk verslavend zijn. In deze jaargang van *Pythagoras* schrijven Aad Thoen en Aad van de Wetering in elke aflevering een artikel over sudoku's; niet over het oplossen ervan, maar over de symmetrieën van het ingevulde 9×9 diagram. Pas nadat het puzzelwerk gedaan is begint het hier interessant te worden. Niettemin wordt elke aflevering afgesloten met een puzzel.

■ door Aad Thoen en Aad van de Wetering

SUDOKU'S EN DRIETALLEN

In deze tweede aflevering over voltooide sudoku's spelen *drietallen* de hoofdrol. In elk 3×3 vak staan 3 drietallen in horizontale richting en 3 drietallen in verticale richting. We beschouwen deze drietallen als ongeordend, dat wil zeggen: de volgorde van de cijfers doet er niet toe. Het aantal mogelijke ongeordende drietallen is $(9 \times 8 \times 7)/(3 \times 2 \times 1) = 84$. Dat zijn er 30 meer dan er in totaal (54) in een sudoku kunnen.

Het kleinste aantal drietallen waarmee we een sudoku kunnen opbouwen is 6, namelijk 3 in horizontale en 3 in verticale richting, zie bijvoorbeeld figuur 1. Het andere uiterste (54) is gerealiseerd in figuur 2; sterker, als je de diagonalen meerekent staan er maar liefst 60 verschillende drietallen.

Beide figuren zijn ook puntsymmetrisch, als volgt: kies een willekeurig hokje, en het hokje dat daar ten opzichte van het middelste hokje precies tegenover ligt. Je zult zien dat dan altijd een 1 verandert in een 9, 2 in 8, 3 in 7, 4 in 6, terwijl de 5 onveranderd blijft.

Wat het kijken naar drietallen boeiend maakt, is dat een drietel zowel horizontaal als verticaal kan voorkomen. We gebruiken de volgende notatie: h = aantal horizontale drietallen, v = aantal verticale drietallen, g = aantal gemeenschappelijke drietallen. Het totale aantal verschillende drietallen T is dan gelijk aan $h + v - g$. Figuur 3 toont een eenvoudig voorbeeld met $g = 3$.

In figuur 4 maken we een sprong naar $g = 18$, hier staan de drietallen in de onderste vakken gedraaid ten opzichte van die in de bovenste vakken. Kleuring geeft de correspondentie aan. Elk horizontaal drietel komt ook verticaal voor, maar *niet* andersom.

HV-KETENS Het lijkt bijna onvoorstelbaar, maar het kan zelfs gebeuren dat de horizontale drietallen precies samenvallen met de verticale. Dit is het geval in figuur 5 (dit is de bandsymmetrische sudoku uit de vorige aflevering). Om de fraaiheid van deze figuur uit te leggen, is een notatie voor de vakken nodig: de drie 3×3 vakken in de bovenste rij noemen we (van links naar rechts) A , B en C , de vakken in de middelste rij D , E en F , en die in de onderste rij G , H en I . Als verder weer h en v naar de horizontale en verticale drietallen in een vak verwijzen, dan geldt: $h(A) = v(E)$, $h(E) = v(I)$ en $h(I) = v(A)$; we zijn in een *loop* beland. Op precies dezelfde wijze vormen B , F , G en C , D , H een *hv-cyclus*! Zoveel fraais valt niet te overtreffen. Een langere *hv*-keten van vijf vakken staat weliswaar in figuur 6: $h(I) = v(A)$, $h(A) = v(H)$, $h(H) = v(F)$, $h(F) = v(B)$, maar deze keten is niet gesloten. Het is überhaupt de vraag of een sudoku met een *hv*-cyclus van vier vakken bestaat, waarschijnlijk niet.

Dan nog dit: de 27 drietallen in figuur 5 hebben precies de volgende gedaante: [159][267][348] (het eerste cijfer is 1, 5 of 9, het tweede cijfer is 2, 6 of 7 enzovoorts).

Terug naar figuur 1: het is je misschien opgefallen dat de vakken A , E en I daar *magisch* zijn. Kun je wellicht een sudoku maken waarin liefst vijf magische 3×3 vierkanten staan? Het antwoord geven we in de volgende aflevering; dan is magie het onderwerp.

Ten slotte de puzzel in figuur 7. Behalve in elke rij, kolom en 3×3 vak staan ook op de diagonalen de cijfers 1 tot en met 9. Verdere voorwaarden: de horizontale drietallen komen uit de set [123][456][789], de verticale uit de set [147][258][369]. De oplossing staat op bladzijde 33. ■

2	7	6	1	9	5	3	8	4
9	5	1	8	4	3	7	6	2
4	3	8	6	2	7	5	1	9
3	8	4	2	7	6	1	9	5
7	6	2	9	5	1	8	4	3
5	1	9	4	3	8	6	2	7
1	9	5	3	8	4	2	7	6
8	4	3	7	6	2	9	5	1
6	2	7	5	1	9	4	3	8

Figuur 1 6 drietallen

6	2	9	7	3	4	1	8	5
8	5	3	1	6	9	7	4	2
1	7	4	8	2	5	6	3	9
7	9	8	2	1	3	5	6	4
3	1	2	4	5	6	8	9	7
4	6	5	9	7	8	2	1	3
9	3	6	5	8	2	4	7	1
2	4	7	6	9	1	3	5	8
5	8	1	3	4	7	9	2	6

Figuur 3 $T = 12 + 18 - 3$

1	2	3	9	7	4	5	6	8
4	5	6	8	1	2	3	9	7
7	8	9	6	3	5	2	4	1
5	7	4	1	6	8	9	2	3
8	9	2	3	5	7	4	1	6
6	3	1	2	4	9	7	8	5
9	6	8	5	2	3	1	7	4
3	1	7	4	9	6	8	5	2
2	4	5	7	8	1	6	3	9

Figuur 5 $T = 27 + 27 - 27$

						6	8	
5				2				
		7					1	
			7					
				9				1
				4	2			

Figuur 7 Een drietall-puzzel

1	5	7	9	8	4	2	6	3
4	3	9	2	6	5	7	8	1
2	8	6	1	7	3	9	4	5
3	7	4	8	1	6	5	9	2
6	9	2	3	5	7	8	1	4
8	1	5	4	9	2	6	3	7
5	6	1	7	3	9	4	2	8
9	2	3	5	4	8	1	7	6
7	4	8	6	2	1	3	5	9

Figuur 2 54 (60) drietallen

1	2	3	4	5	6	7	8	9
6	7	8	9	1	2	3	4	5
5	9	4	8	3	7	2	6	1
4	8	9	7	2	3	1	5	6
3	1	5	6	4	8	9	7	2
2	6	7	5	9	1	8	3	4
7	3	2	1	6	5	4	9	8
8	4	6	2	7	9	5	1	3
9	5	1	3	8	4	6	2	7

Figuur 4 $T = 18 + 27 - 18$

1	2	3	5	7	6	8	9	4
4	5	6	9	8	2	7	3	1
7	8	9	4	1	3	2	5	6
9	3	5	6	2	4	1	7	8
8	4	1	7	9	5	6	2	3
2	6	7	8	3	1	9	4	5
3	7	4	1	6	9	5	8	2
5	1	8	2	4	7	3	6	9
6	9	2	3	5	8	4	1	7

Figuur 6 $T = 27 + 27 - 14$

In Barcelona, St. Louis en Ctesiphon (vlak bij het huidige Bagdad) staan architectonische constructies die de vorm van een 'omgekeerde kettinglijn' hebben. Het gaat om achter-eenvolgens de kathedraal Sagrada Família, de Gateway Arch en een bijna tweeduizend jaar oud gewelf.

■ door Jan Guichelaar

OMGEKEERDE KETTINGLIJNEN IN DE ARCHITECTUUR

Als je een lange ketting – of een dun, slap koord – aan twee punten ophangt en vrij laat hangen, gaat die hangen volgens een kromme die we een 'kettinglijn' noemen. Vroeger dacht men dat het een parabool was, maar wetenschappers uit de zeventiende eeuw, waaronder Christiaan Huygens en Galileo Galilei, kwamen erachter dat dat niet zo is. In de formule voor een kettinglijn komt de functie cosinushyperbolicus voor:

$$y = a \cdot \cosh\left(\frac{x}{a}\right).$$

De cosinushyperbolicus is gedefinieerd met e-machten:

$$\cosh(t) = \frac{e^t + e^{-t}}{2}.$$

Het punt $(0, a)$ is het onderste punt van de ketting, waarbij a een getal is dat, losjes gezegd, aangeeft hoe strak de ketting hangt; bij kleine a is er een diepe kuil, bij grote a een ondiepe kuil. Over kettinglijnen schreven we al vaker in dit tijdschrift, zie onder meer 'Waslijnkrommen' (*Pythagoras* 46-4, te vinden in het Archief op www.pythagoras.nu).

POTENTIËLE ENERGIE Een interessante eigenschap van de kettinglijn is dat de ketting zo gaat hangen, dat de potentiële energie zo klein mogelijk is. Voor de natuurkundigen onder ons: de potentiële energie E_p van een massa m op hoogte h is $E_p = mgh$, waarbij g een constante is, de versnelling van de zwaartekracht. Je kunt E_p voor elke schakel van

de ketting bepalen (alleen de hoogte h varieert) en dan alles optellen.

Om de potentiële energie zo laag mogelijk te houden, moeten zoveel mogelijk kettingschakels zo laag mogelijk hangen. In eerste instantie denk je



In Barcelona staat de kathedraal Sagrada Família (gewijd aan de heilige familie en pas door paus Benedictus XVI geconsacreerd in 2010) van architect Antonio Gaudí. De bouw is al 130 jaar aan de gang, omdat alles moet gebeuren van giften. De grote hoeveelheid zuilen in de kerk hebben elk de vorm van een omgekeerde kettinglijn (om de verticaal geroteerd).

ST. LOUIS / CTESIPHON



In de Amerikaanse stad St. Louis staat een enorme poort uit 1965, de Gateway Arch, van 192 meter hoog én 192 meter breed, gebouwd volgens een ontwerp van de architecten Eero Saarinen en Hanns Karl Bandel. De poort staat symbool voor de vele nieuwe Amerikanen die westwaarts gingen.

misschien, dat de ketting dan de vorm van een bijna rechthoekige U aanneemt: er hangen veel schakels lekker laag, in de bodem van de U. Toch is dit niet de beste oplossing.

Stel je namelijk voor, dat je het midden van de bodem nog een klein stukje indeukt. De potentiële energie van vooral de schakels in het midden van de bodem daalt dan verder. De lengte van de ketting kan natuurlijk niet veranderen, dus dit trekt de verticale stukken van de ketting wel iets naar binnen, maar ze komen nauwelijks omhoog als je de bodem niet al te ver indeukt. Je kunt wiskundig aantonen dat de kettinglijn het optimale compromis vormt tussen 'kettingschakels in het midden naar beneden duwen' en 'kettingschakels aan de buitenkanten niet te ver naar binnen en omhoog trekken'.

Een andere manier om de formule af te leiden bekijkt elke schakel van de ketting afzonderlijk (we nemen wel aan dat er veel schakels zijn). De twee spankrachten op de schakel lopen vanwege de kromming niet precies evenwijdig. Als je de drie krachten (er komt ook nog de zwaartekracht op de schakel bij) als vectoren bij elkaar optelt, komt er precies 0 uit, want het stukje staat stil. De twee horizontale componenten van de spankrachten zijn dan natuurlijk even lang (want de zwaartekracht loopt verticaal).

OMGEKEERDE KETTINGLIJN We kunnen nu ook met stenen gaan stapelen en een poort maken. Als we dat zo doen dat elk stukje van een bepaal-

de lengte steeds een even groot gewicht bevat, dan hebben we in plaats van spankrachten tussen de schakels, precies even grote drukkrachten op stukken steen. Samen met de zwaartekracht is er dan ook weer een mooi evenwicht van krachten. Daarom is geen metselspecie nodig om de poort te bouwen: er staan geen schuifkrachten loodrecht op de boog. Zo is de 'omgekeerde kettinglijnpoort' dus niet alleen fraai, maar ook bouwkundig heel efficiënt. Op de foto's zie je dat fraaie aan een paar bouwwerken. ■



Ctesiphon was meer dan tweeduizend jaar geleden de hoofdstad van het rijk van de Parthen. Na de verovering door de Arabieren (begin zevende eeuw) en de stichting van de nieuwe stad Bagdad (ongeveer 850) verhuisden veel inwoners daarheen. Van het oorspronkelijke paleis in Ctesiphon is een gewelf in de vorm van de omgekeerde kettinglijn bewaard gebleven.

'Hameye ramzaro mishkanam', vrij vertaald betekent dat: 'ik breek elk geheimschrift'. De Iraanse hackers die in juli dit jaar inbraken bij DigiNotar zetten deze spreuk open en bloot in één van de ruim 500 nepcertificaten die ze uitgaven. Maar wat zijn dat eigenlijk, certificaten, en waarom zou je ze ooit vertrouwen?

■ door Arnout Jaspers

HAMEYE RAMZARO MISHKANAM

DE BREEKBARE VEILIGHEID VAN INTERNETCERTIFICATEN

Index	Domain	Issued	Expired	Issuer	Subject
1	www.google.com	2015-07-01	2015-07-01	DigiNotar	www.google.com
2	www.facebook.com	2015-07-01	2015-07-01	DigiNotar	www.facebook.com
3	www.twitter.com	2015-07-01	2015-07-01	DigiNotar	www.twitter.com
4	www.linkedin.com	2015-07-01	2015-07-01	DigiNotar	www.linkedin.com
5	www.instagram.com	2015-07-01	2015-07-01	DigiNotar	www.instagram.com
6	www.youtube.com	2015-07-01	2015-07-01	DigiNotar	www.youtube.com
7	www.spotify.com	2015-07-01	2015-07-01	DigiNotar	www.spotify.com
8	www.pinterest.com	2015-07-01	2015-07-01	DigiNotar	www.pinterest.com
9	www.tumblr.com	2015-07-01	2015-07-01	DigiNotar	www.tumblr.com
10	www.reddit.com	2015-07-01	2015-07-01	DigiNotar	www.reddit.com
11	www.500px.com	2015-07-01	2015-07-01	DigiNotar	www.500px.com
12	www.flickr.com	2015-07-01	2015-07-01	DigiNotar	www.flickr.com
13	www.dribbble.com	2015-07-01	2015-07-01	DigiNotar	www.dribbble.com
14	www.behance.net	2015-07-01	2015-07-01	DigiNotar	www.behance.net
15	www.deviantart.com	2015-07-01	2015-07-01	DigiNotar	www.deviantart.com
16	www.artstation.com	2015-07-01	2015-07-01	DigiNotar	www.artstation.com
17	www.polygon.com	2015-07-01	2015-07-01	DigiNotar	www.polygon.com
18	www.gamespot.com	2015-07-01	2015-07-01	DigiNotar	www.gamespot.com
19	www.ign.com	2015-07-01	2015-07-01	DigiNotar	www.ign.com
20	www.eurogamer.com	2015-07-01	2015-07-01	DigiNotar	www.eurogamer.com
21	www.gamesradar.com	2015-07-01	2015-07-01	DigiNotar	www.gamesradar.com
22	www.rockpapershotgun.com	2015-07-01	2015-07-01	DigiNotar	www.rockpapershotgun.com
23	www.pcgamesn.com	2015-07-01	2015-07-01	DigiNotar	www.pcgamesn.com
24	www.gamespot.com	2015-07-01	2015-07-01	DigiNotar	www.gamespot.com
25	www.ign.com	2015-07-01	2015-07-01	DigiNotar	www.ign.com
26	www.eurogamer.com	2015-07-01	2015-07-01	DigiNotar	www.eurogamer.com
27	www.gamesradar.com	2015-07-01	2015-07-01	DigiNotar	www.gamesradar.com
28	www.rockpapershotgun.com	2015-07-01	2015-07-01	DigiNotar	www.rockpapershotgun.com
29	www.pcgamesn.com	2015-07-01	2015-07-01	DigiNotar	www.pcgamesn.com
30	www.gamespot.com	2015-07-01	2015-07-01	DigiNotar	www.gamespot.com
31	www.ign.com	2015-07-01	2015-07-01	DigiNotar	www.ign.com
32	www.eurogamer.com	2015-07-01	2015-07-01	DigiNotar	www.eurogamer.com
33	www.gamesradar.com	2015-07-01	2015-07-01	DigiNotar	www.gamesradar.com
34	www.rockpapershotgun.com	2015-07-01	2015-07-01	DigiNotar	www.rockpapershotgun.com
35	www.pcgamesn.com	2015-07-01	2015-07-01	DigiNotar	www.pcgamesn.com
36	www.gamespot.com	2015-07-01	2015-07-01	DigiNotar	www.gamespot.com
37	www.ign.com	2015-07-01	2015-07-01	DigiNotar	www.ign.com
38	www.eurogamer.com	2015-07-01	2015-07-01	DigiNotar	www.eurogamer.com
39	www.gamesradar.com	2015-07-01	2015-07-01	DigiNotar	www.gamesradar.com
40	www.rockpapershotgun.com	2015-07-01	2015-07-01	DigiNotar	www.rockpapershotgun.com
41	www.pcgamesn.com	2015-07-01	2015-07-01	DigiNotar	www.pcgamesn.com
42	www.gamespot.com	2015-07-01	2015-07-01	DigiNotar	www.gamespot.com
43	www.ign.com	2015-07-01	2015-07-01	DigiNotar	www.ign.com
44	www.eurogamer.com	2015-07-01	2015-07-01	DigiNotar	www.eurogamer.com
45	www.gamesradar.com	2015-07-01	2015-07-01	DigiNotar	www.gamesradar.com
46	www.rockpapershotgun.com	2015-07-01	2015-07-01	DigiNotar	www.rockpapershotgun.com
47	www.pcgamesn.com	2015-07-01	2015-07-01	DigiNotar	www.pcgamesn.com
48	www.gamespot.com	2015-07-01	2015-07-01	DigiNotar	www.gamespot.com
49	www.ign.com	2015-07-01	2015-07-01	DigiNotar	www.ign.com
50	www.eurogamer.com	2015-07-01	2015-07-01	DigiNotar	www.eurogamer.com

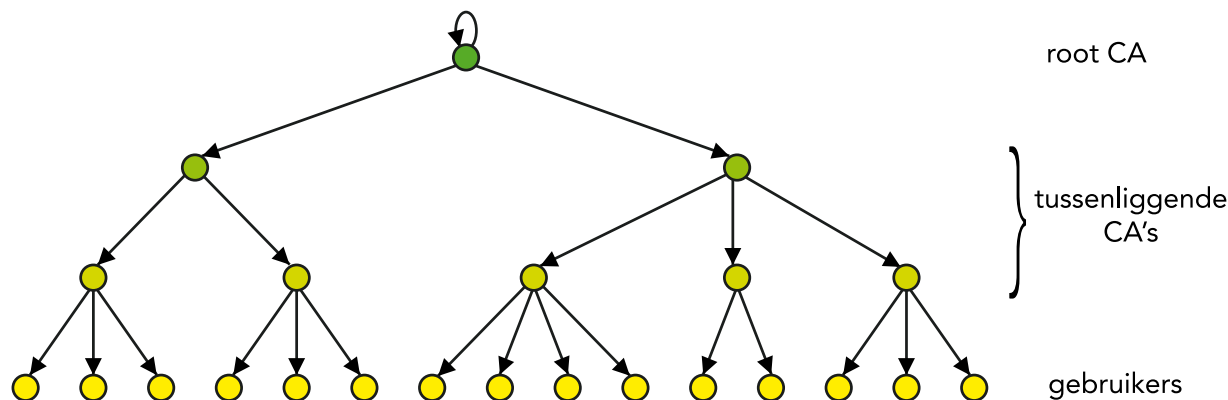
Een deel van de lijst met nepcertificaten van DigiNotar

Het kan je nauwelijks ontgaan zijn: afgelopen zomer raadde de overheid zijn eigen burgers aan om niet in te loggen op de website van de Belastingdienst en andere belangrijke overheidsdiensten. De servers van het bedrijf DigiNotar, dat certificaten uitgaaf om de veiligheid van overheidswebsites te waarborgen, bleken kinderlijk eenvoudig te kraken, en dat was ook gebeurd, waarschijnlijk door een of meer Iraniërs. De hackers konden vervolgens valse veiligheidscertificaten uitgeven en daarmee konden internetgebruikers ongemerkt worden doorverwezen naar onveilige sites.

Elke keer dat je naar een website gaat waarvan de naam met https begint, vraagt jouw brow-

ser (Explorer, Firefox, Chrome, Safari o.i.d.) aan die website om een certificaat, dat moet garanderen dat dit echt de website is die hij beweert te zijn. Stel, je hebt een rekening bij de Bonusbank, logt in op de Bonusbank-website om wat rekeningen te betalen, dan wil je niet dat het een nepsite betreft die er precies hetzelfde uitziet, jouw inloggegevens kaapt en die vervolgens gebruikt om via de echte website van de Bonusbank je rekening leeg te halen.

Op het eerste gezicht verschuift zo'n certificaat het probleem alleen maar: als iemand een perfecte kopie van een website kan maken, kan diegene toch net zo goed een prachtig certificaat maken waarin staat 'dit is echt de website van de Bonusbank'?



Root-CA's, tussenliggende CA's en gebruikers vormen een zogeheten 'hierarchisch vertrouwensnetwerk'

Toch kunnen twee moderne versleutelingstechnieken, *public key cryptografie* en *hash-functies*, dit vrijwel onmogelijk maken – mits bedrijven als DigiNotar en andere *Certificate Authorities* hun eigen beveiliging op orde hebben.

Public key cryptografie houdt in, dat een geheimschrift twee verschillende sleutels heeft, een *publieke sleutel* en een *geheime sleutel*. De publieke dient meestal om berichten te versleutelen, en de geheime om berichten te ontsleutelen, maar het kan ook andersom. De publieke sleutel wordt berekend uit de geheime sleutel, maar andersom is in de praktijk niet mogelijk. RSA is het meest gebruikte public key geheimschrift (zie onder andere de artikelen 'Computer democratiseerde het geheimschrift' in *Pythagoras* 50-5 (april 2011) en 'Hoe werkt RSA?' in *Pythagoras* 37-5 (juni 1998)).

Een hash-functie is een manier om van een bericht met een willekeurige lengte een korte 'samenvatting' (*hash*) te maken met een vaste lengte, bijvoorbeeld 128 bits. Een goede hash-functie zorgt ervoor, dat twee berichten die heel erg op elkaar lijken (bijvoorbeeld maar één letter verschillen) toch een totaal verschillende *hash* hebben. Andersom: als een *hash* (bij toeval) sterk lijkt op een andere *hash*, zullen de berichten toch totaal verschillend zijn. Een hash-functie is openbaar, zodat iedereen kan controleren dat een zekere *hash* inderdaad bij een zeker bestand hoort.

CERTIFICAAT MAKEN Het maken van een certificaat gebeurt via de volgende stappen:

- Bonusbank kiest een geheime RSA-sleutel en berekent hieruit de eigen publieke RSA-sleutel.
- Bonusbank stuurt de eigen naam, domeinnaam (<https://www.bonusbank.com>) en publieke RSA-sleutel naar een Certificate Authority (CA).
- CA controleert de gegevens (op andere manieren dan via internet) en zet er iets bij in de trant van 'wij hebben gecontroleerd dat dit allemaal klopt'. Dit is het certificaat.
- CA maakt een *hash* van het certificaat, en ver-

sleutelt deze met zijn eigen geheime RSA-sleutel (niet het hele certificaat wordt RSA-versleuteld, omdat dit naderhand te veel vertraging in het internetverkeer zou opleveren).

- Bonusbank ontvangt het certificaat en de versleutelde *hash*, en zet deze op zijn website <https://www.bonusbank.com>.

GEBRUIK VAN HET CERTIFICAAT De browser van de klant heeft een lijst met vertrouwde CA's en hun publieke RSA-sleutels. Met de publieke sleutel van de CA ontcijfert hij de *hash*. (In de praktijk is het iets ingewikkelder: er zijn op de wereld een stuk of honderd *root*-CA's waarvan de browser een lijst bijhoudt, die ieder weer andere CA's van een certificaat mogen voorzien waarin staat dat deze firma gerechtigd is om certificaten af te geven. DigiNotar was geen *root*, maar een secundaire CA).

De browser van de klant maakt zelf ook een *hash* van het certificaat op <https://www.bonusbank.com>. Deze moet identiek zijn aan de eerder gevonden *hash*.

Als dit klopt, gebruikt de browser de publieke RSA-sleutel op <https://www.bonusbank.com> om de inlogcodes van de klant te versleutelen. Alleen de

← → C ING BANK N.V. [NL] <https://mijn.ing.nl/internetbankieren/Se>



Voorbeeld van een site die begint met <https://>: zo'n site is beveiligd. Sommige browsers geven dat aan met een hangslotje (helemaal links in de url-balk).

Bonusbank beschikt over de bijbehorende geheime RSA-sleutel waarmee de inlogcodes te lezen zijn.

WAAROP BERUST DE VEILIGHEID? Stel, een bedrieger zet een nepcertificaat van een zekere CA op de eigen website <https://www.bonisbank.com>. Hij beschikt echter niet over de geheime RSA-sleutel van die CA. Hij kan dus de *hash* van het nepcertificaat niet correct versleutelen. Als hij dat met een eigen geheime RSA-sleutel zou doen, levert ont-sleuteling door de klant met de publieke RSA-sleutel van de CA slechts onzin op, een reeks bits die totaal niet met de *hash* van het nepcertificaat overeenkomt.

Een subtielere poging zou zijn: de bedrieger ont-sleutelt de *hash* van een bona fide bank die een echt certificaat van een CA heeft, en probeert een nepcertificaat te maken dat precies dezelfde *hash* oplevert.

In theorie kan dat altijd: er zijn immers maar 2^{128} verschillende hash-codes, terwijl een certificaat veel langer is; alleen al de RSA-sleutel heeft tegenwoordig een lengte van 2048 bits, dus 2^{2048} mogelijkheden. Bij één *hash* horen daarom minstens $2^{2048-128} = 2^{1920}$ verschillende berichten. Toch, als de hash-functie alle bits van het certificaat goed genoeg door elkaar husselt, is dit in de praktijk onmogelijk, het zou duizenden jaren computertijd vergen om zo'n *collision* te vinden.

Helaas bevatten veel certificaten (ook die van DigiNotar) op dit punt een zwakheid: ze gebruiken het hash-algoritme *md5*, dat een paar jaar geleden gekraakt is door een groep Nederlandse, Zwitserse en Amerikaanse cryptografen. Die zijn er inderdaad in geslaagd, met behulp van een netwerk van 200 Playstations die ze als rekenmachines inzetten, om in een paar dagen tijd een vals certificaat te maken met dezelfde md5-hash als een bestaand, echt certificaat.

Echt veilige certificaten gebruiken tegenwoordig een moderner hash-algoritme, zoals *SHA-1*.

De Iraanse hackers hoefden niet de moeite te nemen om md5 te kraken; ze omzeilden de hele beveiliging simpelweg door in te breken op de computers van DigiNotar. Naar verluidt (het rapport van Fox-it is niet openbaar) lukte dit doordat belangrijke wachtwoorden simpel te raden waren. Eenmaal 'binnen' konden ze bij de geheime RSA-sleutel, en konden ze niet van echt te onderscheiden certificaten aanmaken zoveel ze wilden. Met die certificaten hebben ze waarschijnlijk de web-browsers van duizenden Iraanse internetgebruikers misleid, die dachten dat ze naar de websites van Facebook, hun e-mailprovider of zelfs de Mossad (de Israëlische geheime dienst) gingen.

Niemand behalve de hackers zelf weet hoeveel e-mail er is afgeluisterd, en wat de consequenties zullen zijn voor de Iraanse gebruikers. ■

Here's the hexcode of a sample for an MD5 collision:

```
d131dd02c5e6eeca4693d9a0698aff95c 2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a 085125e8f7cdc99fd91dbd280373c5b
d8823e3156348f5bae6d436c919c6 dd53e2b487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1e c69821bcb6a8839396f9652b6ff72a70
```

```
d131dd02c5e6eeca4693d9a0698aff95c 2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a 085125e8f7cdc99fd91dbd280373c5b
d8823e3156348f5bae6d436c919c6 dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1e c69821bcb6a8839396f965ab6ff72a70
```

Both produce the hash value 79054025255fb1a26e4bc422aef54eb4, though they differ in 6 of 1024 bits.^[30]

Gekraakt: voorbeeld van twee berichten met dezelfde md5-hash. Een vals certificaat met dezelfde md5-hash als een echt certificaat is in 2008 gemaakt door een groep cryptografen met onder andere de Nederlandse wiskundigen Arjen Lenstra, Mart Stevens en Benne de Weger.

Op 16 september vond de finale van de 50ste Wiskunde Olympiade plaats op de Technische Universiteit Eindhoven. Aan de eerste ronde, in februari, deden dit jaar maar liefst 5257 leerlingen mee. De beste 799 kregen een uitnodiging voor de tweede ronde op 10 universiteiten in Nederland. De 142 winnaars hiervan gingen in Eindhoven de strijd met elkaar aan. Een van de vragen ging over een toernooi met een opmerkelijke uitslag.

■ door Quintijn Puite

EEN BIJZONDERE UITSLAG



OPGAVE 3 (NWO FINALE 2011)

Bij een toernooi met zes teams speelt ieder team eenmaal tegen elk ander team. Als een team een wedstrijd wint, krijgt het daarvoor 3 punten en krijgt de verliezer 0 punten. Als er gelijk wordt gespeeld, krijgen beide teams 1 punt.

Kunnen de eindscores van de teams precies zes opeenvolgende getallen $a, a + 1, \dots, a + 5$ zijn? Zo ja, bepaal alle waarden van a waarvoor dat kan.

Vaak gaat het bij wiskundige problemen om het bewijzen van bepaalde beweringen. Zo ook bij opgave 3 van de finale van de Nederlandse Wiskunde Olympiade, zie het kader hierboven. Maar deze opgave vraagt nog méér van ons: we moeten eerst nog zelf bedenken wat het antwoord op de vraag eigenlijk is. En pas als we ervan overtuigd zijn dat het antwoord 'ja' of juist 'nee' is, kunnen we gaan proberen om dat waterdicht te bewijzen.

De vraag is dus in eerste instantie: zijn er nou wel of niet zulke opeenvolgende eindscores mogelijk bij een halve competitie tussen zes teams?

UITSLAGENTABELLEN Laten we ons eerst eens verdiepen in zo'n toernooi. Ieder team speelt tegen elk ander team, dus elk team speelt 5 wedstrijden. Dat zijn er dus $6 \times 5 = 30$ in totaal, maar daarbij tellen we elke wedstrijd dubbel. In totaal worden er dus 15 wedstrijden gespeeld.

We kunnen de uitslagen van de 15 wedstrijden in een uitslagentabel zetten. In tabel 1 (op de volgende pagina) zie je daar een voorbeeld van. Team A heeft in totaal 4 punten gehaald: 0 tegen B, 0 te-

gen C, 1 tegen D, 0 tegen E en 3 tegen F. En omdat team A 0 punten tegen team B heeft gehaald, heeft omgekeerd team B juist 3 punten tegen team A gehaald. Elke uitslagentabel moet aan deze regel voldoen: bij lijnspiegelen in de diagonaal gaan 0'en in 3'en over en vice versa, terwijl 1'en in 1'en overgaan.

We zien dat de behaalde scores in dit voorbeeld 4, 4, 6, 8, 8, 9 zijn: nog geen zes opeenvolgende getallen. Maar als we er in zouden slagen zo'n uitslagentabel op correcte wijze te vullen en wel zodanig dat er zes opeenvolgende getallen uitkomen, dan hebben we in ieder geval een a gevonden die voldoet.

Wat voor scores kunnen er überhaupt uit zo'n uitslagentabel komen? Elk team behaalt een score tussen de 0 en 15 punten, dus wat dat betreft ligt de som van alle scores tussen de 0 en de 90. Maar als er een team echt de volle 15 punten haalt, kan geen ander team meer 15 punten halen, want de andere teams hebben dan in ieder geval allemaal één wedstrijd verloren. We bekijken het daarom niet per team maar *per wedstrijd*.

Voor elk van de 15 wedstrijden worden er 2

punten uitgedeeld in geval van gelijkspel, of 3 punten als er een van de teams wint. De som van alle uitslagen ligt dus ergens tussen de 30 en de 45. In het voorbeeld hierboven was dat $4 + 4 + 6 + 8 + 8 + 9 = 39$. Omdat dit op 6 punten na de maximale somscore van 45 is, kunnen we hier meteen iets uit afleiden: er zijn blijkbaar zes wedstrijden geweest waar 2 punten ($1 + 1$) in plaats van 3 punten ($0 + 3$) zijn uitgedeeld. Inderdaad zien we in onze uitslagentabel zes wedstrijden die in gelijkspel zijn geëindigd.

Nu is de vraag of hier zes opeenvolgende scores mogelijk zijn. Bijvoorbeeld 1, 2, 3, 4, 5, 6. Dat is samen 21, dus dat is nooit mogelijk; de somscore ligt immers tussen de 30 en de 45. Ook 2, 3, 4, 5, 6, 7 werkt nog niet (dat is in totaal 27), maar $3 + 4 + 5 + 6 + 7 + 8 (= 33)$, $4 + 5 + 6 + 7 + 8 + 9 (= 39)$ en $5 + 6 + 7 + 8 + 9 + 10 (= 45)$ lijken wel degelijk mogelijk. Kortom, de gevallen $a = 3$, $a = 4$ en $a = 5$ zijn de enige waarden voor a die eventueel mogelijk zijn; andere waarden van a zijn onmogelijk, want voor lagere a is de somscore te laag, terwijl voor hogere a de somscore juist te hoog is. Nu nog kijken of we een daadwerkelijk toernooi kunnen vinden, met deze punten als teamuitkomsten!

ANALYSE PER GEVAL Eerst kijken we naar het geval $a = 5$ met uitslagen $5 + 6 + 7 + 8 + 9 + 10 = 45$. We hebben hierboven al gezien dat de somscore dan maximaal is. Dus elke wedstrijd zijn er 3 punten uitgedeeld en elk team krijgt steeds 0 of 3 punten. Dan heeft dus elk team ook een uitslag die deelbaar is door 3. Maar dan komen nooit de uitsla-

gen 5, 7, 8 en 10 voor. Dit geval is dus niet mogelijk.

In het geval $a = 3$ met uitslagen $3 + 4 + 5 + 6 + 7 + 8 = 33$ zijn er maar 3 punten meer gehaald dan het absolute minimum van 30 waarbij alle wedstrijden in gelijkspel eindigen. Er is dus drie keer een winnaar uit de strijd gekomen, tegenover twaalf wedstrijden die in gelijkspel eindigden. Elk team speelt vijf wedstrijden. Dus het team met 5 punten zou die score nog behaald kunnen hebben met vijf maal 1 punt. Maar het team met 6 punten moet minstens één keer 3 punten hebben behaald. En net zo voor het team met 7 punten. Met één keer 3 punten en vier keer 1 punt haal je maar 7 punten, dus het team met 8 punten moet wel minstens twee keer 3 punten hebben behaald. In totaal zou er dus minstens vier keer 3 punten moeten zijn behaald. Maar dat is in regelrechte tegenspraak met het feit dat er maar drie keer een wedstrijd met een winnaar is geëindigd. Dit geval kan dus ook niet voorkomen.

We hebben nu nog één geval over: $a = 4$. De uitslagen zijn dan $4 + 5 + 6 + 7 + 8 + 9 = 39$. Net als in het voorbeeld hierboven weten we dat er zes wedstrijden zijn die in gelijkspel zijn geëindigd. Dan zijn er dus negen wedstrijden met een winnaar geëindigd. De vraag is nu eigenlijk heel simpel: kunnen we zesmaal de scores 1–1 en negenmaal de scores 3–0 in de uitslagentabel kwijt op zo'n manier dat de eindscores 4, 5, 6, 7, 8, 9 zijn?

Het team met 4 punten heeft ofwel 3, 1, 0, 0, 0 gehaald, danwel 1, 1, 1, 1, 0; iets anders is niet mogelijk. Voor de andere vijf teams kunnen we ook op deze manier kijken welke punten ze hebben ge-

	A	B	C	D	E	F	score
A	–	0	0	1	0	3	4
B	3	–	1	1	0	3	8
C	3	1	–	3	1	0	8
D	1	1	0	–	1	3	6
E	3	3	1	1	–	1	9
F	0	0	3	0	1	–	4

Tabel 1

score		
4	3, 1, 0, 0, 0	1, 1, 1, 1, 0
5	3, 1, 1, 0, 0	1, 1, 1, 1, 1
6	3, 3, 0, 0, 0	3, 1, 1, 1, 0
7	3, 3, 1, 0, 0	3, 1, 1, 1, 1
8	3, 3, 1, 1, 0	
9	3, 3, 3, 0, 0	3, 3, 1, 1, 1

Tabel 2

haald. Dat leidt tot tabel 2.

Omdat we eerder al zagen dat er maar negen maal de score 3 is gevallen, terwijl er elf maal de score 3 voorkomt in de linkerkolom van deze tabel, moeten we twee teams uitkiezen die uitslagen gehaald hebben volgens de rechterkolom. Dat kan op zich op $\binom{5}{2} = 10$ manieren. We kiezen nu eerst maar eens één van die 10 manieren en gaan proberen de uitslagentabel op die manier te vullen. Als dat niet direct lukt, kunnen we natuurlijk ook nog de andere manieren proberen. Pas als dat ons allemaal niet zou lukken, zouden we voor het antwoord ‘nee’ gaan als antwoord op de oorspronkelijke vraag. Maar dan zouden we natuurlijk nog wel echt moeten bewijzen dat het vullen van de tabel daadwerkelijk onmogelijk is (wat nog niet bewezen is als het ons alleen maar een paar keer niet is gelukt).

Hoe dan ook, het blijkt op de manier die in tabel 2 vet is aangegeven mogelijk te zijn een daadwerkelijk spelverloop te vinden dat de eindscores 4, 5, 6, 7, 8, 9 oplevert. Met een beetje proberen vind je al gauw een oplossing, zie tabel 3.

	A	B	C	D	E	F	score
A	–	0	0	0	3	1	4
B	3	–	1	0	0	1	5
C	3	1	–	1	1	0	6
D	3	3	1	–	0	0	7
E	0	3	1	3	–	1	8
F	1	1	3	3	1	–	9

Tabel 3

OP TWEE SPOREN We hebben al met al gezien dat $a = 4$ de enige waarde van a is die voldoet. Maar het bleek helemaal nog niet zo simpel om dat direct in te zien. Zo leek het eerst dat $a = 3$ en $a = 5$ ook wel zouden kunnen voldoen. We hadden daar wat extra argumenten voor nodig om die gevallen uit te sluiten.

Het mooie van deze opgave is dat je net als bij echt onderzoek constant op twee sporen zit. Er is steeds de wisselwerking tussen proberen een toernooi te vinden (voor $a = 3$ bijvoorbeeld) en als dat je niet lukt, heel goed proberen te analyseren waarom het niet lukt en daarmee proberen te bewijzen dat het inderdaad onmogelijk is. Het eindantwoord bestaat uit precies die waarden van a waarvoor er een toernooi met opeenvolgende eindscores is. En bij zo’n eindantwoord hoort een overtuigende onderbouwing: we moeten voor alle genoemde waarden van a een voorbeeld van een scoreverloop laten zien, terwijl we voor de overige waarden van a juist moeten bewijzen waarom er niet een scoreverloop met die einduitslag kan zijn.

Lijkt het jou ook leuk om je tanden in zulke uitdagende opgaven te zetten? Geef je dan bij je wiskundedocent op voor de eerste ronde van de Nederlandse Wiskunde Olympiade 2012, die op vrijdagmiddag 27 januari weer plaatsvindt op alle deelnemende scholen. ■

PYTHAGORAS OLYMPIADE

■ door Matthijs Coster, Alexander van Hoorn en Eddie Nijholt

30 Doe mee met de Pythagoras Olympiade! Elke aflevering bevat vier opgaven. De eerste twee zijn wat eenvoudiger; onder de goede inzendingen van leerlingen uit de klassen 1, 2 en 3 wordt een Irisbon van 20 euro verloot. De laatste twee zijn echte breinbrekers; onder de goede inzendingen van leerlingen (tot en met klas 6) wordt een Irisbon van 20 euro verloot. Bovendien kun je je via deze breinbrekers plaatsen voor de finale van de Nederlandse Wiskunde Olympiade, mocht het via de voorronden niet lukken. Aan het eind van elke jaargang worden de vijf leerlingen die de meeste breinbrekers hebben opgelost, uitgenodigd voor de NWO-finale. Niet-leerlingen kunnen met de Pythagoras Olympiade meedoen voor de eer.



DE GOEDE INZENDERS VAN JUNI 2011

214: Ben De Bondt (klas 5), Koninklijk Atheneum, Grimbergen; Peter Diks; Michelle Sweering (klas 4), Erasmiaans Gymnasium, Rotterdam.

215: Ben De Bondt (klas 5), Koninklijk Atheneum, Grimbergen; Peter Diks; Michelle Sweering (klas 4), Erasmiaans Gymnasium, Rotterdam.

216: Kees Boersma, Vlissingen; Ben De Bondt (klas 5),

HOE IN TE ZENDEN? Inzendingen ontvangen we bij voorkeur per e-mail (getypt of een scan van een handgeschreven oplossing): pytholym@pythagoras.nu.

Eventueel kun je je oplossing sturen naar
Pythagoras Olympiade
Korteweg-de Vries Instituut
Universiteit van Amsterdam,
Postbus 94248
1090 GE Amsterdam.

Voorzie het antwoord van een duidelijke toelichting (dat wil zeggen: een berekening of een bewijs). Vermeld je naam en adres; leerlingen moeten ook hun klas en de naam van hun school vermelden.

Je inzending moet bij ons binnen zijn vóór 31 december 2011.

Koninklijk Atheneum, Grimbergen; Michelle Sweering (klas 4), Erasmiaans Gymnasium, Rotterdam; Dick Veldkamp, Houten.

217: Kees Boersma, Vlissingen; Michelle Sweering (klas 4), Erasmiaans Gymnasium, Rotterdam.

De Irisbonnen gaan naar Ben De Bondt en Michelle Sweering.

OPGAVE 222

Een klas van 25 leerlingen gaat op kamp. Van deze 25 leerlingen nemen er 15 een zonnebril mee. Verder nemen 12 leerlingen een pet mee, en nemen 10 leerlingen een paar handschoenen mee. Er zijn er acht die zowel een zonnebril als een pet mee hebben. Vijf hebben zowel een zonnebril als handschoenen mee. En vier hebben een pet en handschoenen mee. Hoeveel leerlingen hebben een zonnebril, een pet én een paar handschoenen mee?

OPGAVE 223

Matilde heeft op een blaadje papier een vierkant getekend. Ook heeft zij ergens op het blaadje een punt getekend met onzichtbare inkt. Jij mag rechte lijnen trekken en Matilde (die een speciale bril op heeft) vertelt je dan aan welke kant van de lijn het punt ligt (of op de lijn). Hoe kun je er met zo weinig mogelijk lijnen achter komen of het punt binnen, buiten of op het vierkant ligt?

OPGAVE 224

Vind alle getallen a , b , c en d zodanig dat

$$a + b + c + d = 0$$

$$ab + ac + ad + bc + bd + cd = -50$$

$$abc + abd + acd + bcd = 0$$

$$abcd = 49$$

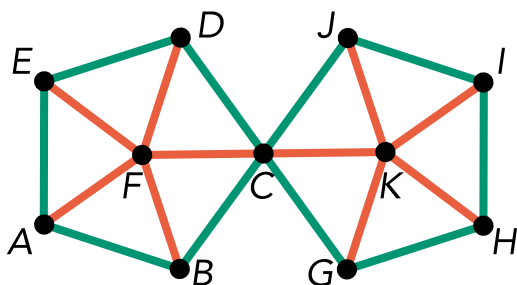
OPGAVE 225

In een openluchtmuseum staat een miniatuur-grachtenpand met een trapgevel. De hele voorgevel heeft een oppervlakte van 79 dm^2 . De breedte van het pand is een oneven aantal decimeter (minimaal 3). De hoogte is een geheel aantal decimeter (minimaal 1). Het dak van het huis bestaat uit een trap, dus geheel bovenaan is de breedte 1, dan 3, dan 5 enzovoorts (deze trappen zijn steeds 1 dm hoog). Wat zijn de mogelijke afmetingen van een dergelijk grachtenpand?



OPLOSSING 214

In een park hebben de paden de vorm van de plattegrond die je hier ziet. Elk groen pad is 116 meter lang, elk rood pad is 100 meter lang. Jolanda wandelt door het park. Wat is de lengte van de kortst mogelijke wandeling, als Jolanda elk van de twintig paden minimaal één keer wil doorlopen? Ze hoeft niet bij hetzelfde punt te eindigen als waar ze begint.



Oplossing. De kortste wandeling gaat over 12 groene en 12 rode paden, en is dus 2592 meter lang. Bijvoorbeeld: BFAFEDEDCFBGKGHKKIHIJKJ.

OPLOSSING 215

Van een getal zet je het laatste cijfer vooraan. Het nieuwe getal is dan anderhalf keer zo groot als het oude. Zoek het kleinst mogelijke getal waarvoor dit geldt.

Oplossing. Noem het gezochte getal x en noem het laatste cijfer daarvan b . Dan is $x = 10a + b$ voor een zeker geheel getal a . De eis is dus te schrijven als $b \cdot 10^n + a = 1\frac{1}{2} \cdot (10a + b)$, ofwel $(2 \cdot 10^n - 3) \cdot b = 28a$, waar n het aantal cijfers van a is. Omdat de rechterkant van deze vergelijking deelbaar is door 4 en $2 \cdot 10^n - 3$ oneven is, moet gelden $b = 4$ of $b = 8$. De rechterkant is ook deelbaar door 7 dus moet $2 \cdot 10^n - 3$ deelbaar zijn door 7. De kleinste waarde van n zodat dit geldt is $n = 5$. Met $b = 4$ vinden we $a = (2 \cdot 10^5 - 3) \cdot 4 / 28 = 28571$, zodat $x = 285714$.

OPLOSSING 216

In deze opgave gebruiken we de notatie $a \uparrow\uparrow b$ voor

$a^{a^{a^{\dots a}}}$ (hierin komen b a 's voor).

Merk op dat $a^{b^c} = a^{(b^c)}$.

Welk getal is groter: $4 \uparrow\uparrow 6$ of $10 \uparrow\uparrow 5$?

Oplossing. We bewijzen met inductie een sterkere stelling, namelijk $4 \uparrow\uparrow (n+1) > 2 \cdot (10 \uparrow\uparrow n)$.

Omdat $256 > 20$ is de stelling waar voor $n = 1$.

Stel dat de stelling waar is voor $n = k$; dan volgt

$$4 \uparrow\uparrow (k+2) = 4^{4 \uparrow\uparrow (k+1)} > 4^{2 \cdot 10 \uparrow\uparrow k} = (4^2)^{10 \uparrow\uparrow k} = (1,6 \cdot 10)^{10 \uparrow\uparrow k} = (1,6^{10 \uparrow\uparrow k}) \cdot (10^{10 \uparrow\uparrow k}) >$$

$2 \cdot (10 \uparrow\uparrow (k+1))$, waar de eerste ongelijkheid volgt uit de inductiehypothese. De stelling is dus ook waar voor $n = k + 1$. Wegens het principe van inductie is de stelling nu voor alle $n \geq 1$ bewezen.

Hieruit volgt $4 \uparrow\uparrow 6 > 10 \uparrow\uparrow 5$.

OPLOSSING 217

Na de vijftigste jaargang van het tijdschrift *Pythagoras* wordt er een verkiezing gehouden welke jaargang tot nu toe de beste was. Iedereen die meedoet aan de stemming kiest een aantal, zeg k , jaargangen ($k \geq 1$). Deze k jaargangen krijgen dan elk $\frac{1}{L}$ punt.

Na de stemming blijkt dat elke jaargang een verschillende score heeft! Hoeveel mensen hebben er minstens gestemd?

Oplossing. Zij n het aantal mensen dat meedoet aan de verkiezing. Een jaargang kan van een persoon wel óf niet een stem krijgen. Het aantal verschillende scores is dus hooguit 2^n . Omdat $2^5 = 32 < 50$, kunnen voor $n \leq 5$ de 50 jaargangen niet allemaal een verschillende score hebben. Voor $n = 6$ kan het wel, bijvoorbeeld als er als volgt gestemd wordt:

```

1111111111111111111111111111111111000000000000000000000000000000
1111111111111000000000000000011111111111100000000000000000000000
1111110000000111111100000001111100000001111110000
11100011100001110000111000011100011100001110001110
1101001101100100110010011001001100110011001101001100
10101010110101101010010101001001001010101000101000

```

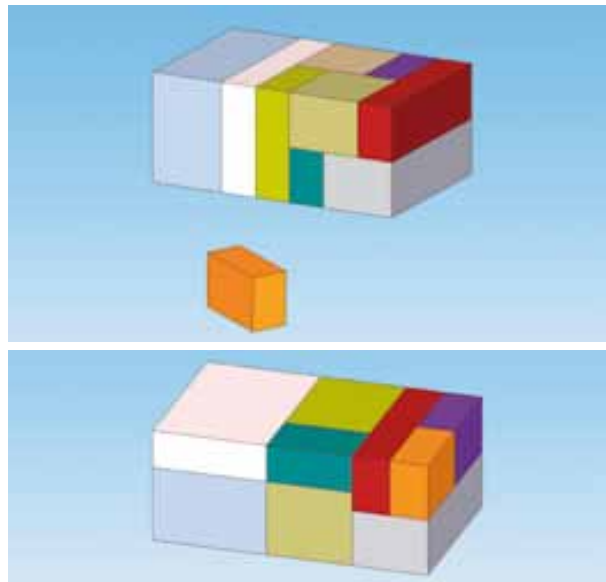
Hierbij betekent de eerste rij dat persoon 1 stemt op: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27; de tweede rij betekent dat persoon 2 stemt op: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40; et cetera.

De verschillende deelnemers stemmen hier op respectievelijk 27, 26, 25, 24, 23 en 22 jaargangen.

OPLOSSING SUDOKU EN 3D-PUZZEL NR. 1

3	7	6	1	8	4	5	9	2
8	5	2	9	6	3	1	4	7
1	9	4	2	7	5	6	8	3
5	1	8	6	2	9	7	3	4
6	3	9	4	1	7	8	2	5
4	2	7	5	3	8	9	1	6
9	4	3	7	5	1	2	6	8
2	8	5	3	9	6	4	7	1
7	6	1	8	4	2	3	5	9

Links zie je de oplossing van figuur 7 op pagina 21.
Rechts zie je de oplossingen van de 3d-puzzel uit het septembernummer.



51ste jaargang nummer 2
november 2011
ISSN 0033 4766

Pythagoras stelt zich ten doel jongeren kennis te laten maken met de leuke en uitdagende kanten van wiskunde. *Pythagoras* richt zich tot leerlingen van vwo en havo en alle anderen die jong van geest zijn.

Internet www.pythagoras.nu

Hoofdredacteur Arnout Jaspers

Eindredacteur Alex van den Brandhof

Redactie Matthijs Coster,
Jeanine Daems, Jan Guichelaar,
Klaas Pieter Hart, Paul Levrie

Vormgeving Grafisch Team
Digipage BV, Leidschendam

Druk Drukkerij Ten Brink, Meppel

Uitgever Koninklijk Wiskundig
Genootschap

Verantwoordelijk uitgever Chris Zaal

Lezersreacties en kopij

Bij voorkeur per e-mail; lezersreacties naar Jan Guichelaar, jan@pythagoras.nu en kopij naar Arnout Jaspers, arnout@pythagoras.nu. Eventueel per post naar Jan Guichelaar, Pedro de Medinalaan 162, 1086 XR Amsterdam.

Abonnementen, bestellingen en mutaties

Drukkerij Ten Brink
Abonnementenadministratie
Postbus 41
7940 AA Meppel
Telefoon: 0522 855 175
E-mail:
abonnementen@pythagoras.nu

Abonnementsprijs

(6 nummers per jaargang)
€ 26,00 (Nederland),
€ 29,00 (België),
€ 32,00 (overig buitenland),
€ 17,00 (groepsabonnement
Nederland),
€ 18,00 (groepsabonnement België).
Zie www.pythagoras.nu voor toelichtingen.

Aan dit nummer werkten mee

Alex van den Brandhof
(alex@pythagoras.nu),
Matthijs Coster
(matthijs@pythagoras.nu),
Jeanine Daems
(jeanine@pythagoras.nu),
Jan Guichelaar
(jan@pythagoras.nu),
Klaas Pieter Hart
(kp@pythagoras.nu),
Alexander van Hoorn
(alexander@pythagoras.nu),
Arnout Jaspers
(arnout@pythagoras.nu),
Jaap Klouwen
(j.klouwen@hva.nl),
Paul Levrie
(paul@pythagoras.nu),
Eddie Nijholt
(eddie@pythagoras.nu),
Quintijn Puite
(g.w.q.puite@tue.nl),
Jan Stout (jwhstout@xs4all.nl),
Jeroen Suijs (jeroen.suijs@uvt.nl),
Aad Thoen
(thoenaad37@gmail.com),
Aad van de Wetering
(avdw3b@wxs.nl).

Pythagoras wordt mede mogelijk gemaakt door de bijdragen van de onderstaande instituten en instellingen.



3D-PUZZEL

■ door Paul Levrie



Benodigdheden: 30 houten kralen en een aantal houten stokjes met dezelfde diameter als de opening in de kralen. Verder heb je een houtboor met deze diameter nodig. Neem drie kralen en verbind die met behulp van de houten stokjes met elkaar zoals in de figuur hier-naast. Je zal nu en dan wel een gat moeten bijboren. Je hebt dan een rechte hoek bestaande uit drie kralen. Maak in totaal tien van die rechte hoeken.



Opdracht. Maak met de tien rechte hoeken een piramide zoals je hierboven ziet: vier lagen waarvan het aantal kralen van beneden naar boven gelijk is aan 16, 9, 4 en 1.

De oplossing vind je in het volgende nummer van *Pythagoras*.