APRIL wiskundemaand

$(\sqrt{\partial S})^2$

In de VS is april wiskundemaand, Heverlee ontvangt de finale van de Vlaamse Wiskunde Olympiade en in Dordrecht strijden vijf Vlaamse leerlingen mee in de Benelux Wiskunde Olympiade. Elke donderdag van april wijdt 'De Standaard' daarom zijn wetenschapspagina's aan de wiskunde.

INTERVIEW
PIERRE DELIGNE

Wiskundige van de week

Welk personage uit de literatuur zou u aanwerven als onderzoeker in uw groep, en waarom?

'Ik zie wiskunde niet als een groepsactiviteit. Contacten kunnen hun nut hebben, zolang je maar niet in een vast kringetje blijft ronddraaien. Antwoord dus: niemand, want er is geen groep.'

Bij welke beroemde wiskundige (levend of dood) had u in de leer willen gaan, en waarom?

'Bij Euler, "ons aller leermeester". Vanwege de uitgebreidheid van zijn interesses, vanwege zijn buitengewone lef, getemperd door zijn uiterst zorgvuldig becijferde bewijzen, en omdat hij zich altijd verre heeft gehouden van de in zijn tijd zo vaak voorkomende ruzies over wie het eerst een bepaald resultaat had uitgedacht.'

Welke studierichting zou u hebben gekozen, als u geen wiskundige was geworden?

'Studierichting: geen enkele. Maar het idee om boer te worden had me wel aangesproken.'

Waarom is wiskunde zo moeilijk?

'Is ze dat? Het is de enige wetenschap waarin datgene wat we aan de Babyloniërs en de oude Grieken te danken hebben, van belang blijft, en waarin artikels die tweehonderd jaar geleden werden gepubliceerd, nog altijd relevant zijn. Dat cumulatieve aspect betekent ook dat je, als je op school de stof van een jaar verwaarloost, achteraf nog maar heel moeilijk weer kunt inpikken.'

Door een hapering in de aardrotatie duurt een dag voortaan vijfentwintig uur. Waaraan besteedt u de extra tijd?

'Normaal moet ik moeite doen om niet elke dag later te gaan slapen en dus ook later op te staan. Een uur erbij zou kunnen helpen om het evenwicht te herstellen.'

U bent de enige wetenschapper op een feestje. Hoe legt u uit wat u doet voor de kost?

'Ik leg uit dat ik het voorrecht geniet om mijn kost te verdienen door mijn lievelingsspel te spelen.'

Men heeft u net (in vertrouwen) verteld dat morgen de wereld vergaat. Wat doet u nog?

'Ik maak een wandeling om de schoonheid van de wereld te bewonderen.'

Welk boek ligt momenteel op uw nachtkastje?

'"Saints in art", een beschrijving van de attributen, kenmerken en eigenschappen van de heiligen. Vroeger konden mensen die niet hadden leren lezen wel beelden en schilderijen uit de gewijde kunst "lezen". Op hun niveau zou ik willen uitkomen.'

Welke muziek speelt er in uw werkkamer?

© imageglobe

Onze landgenoot Pierre Deligne (68) won de Fields Medal en de Abelprijs, allebei bekend als 'Nobelprijs voor de Wiskunde'. Hij werkt vooral aan getaltheorie.

'Geen. Ik kan alleen werken als ik alleen ben en als het stil is.'

Wat is uw grootste frustratie?

'Dat ik, nadat ik een nieuwe theorie heb begrepen of een nieuwe stelling heb aangetoond, een artikel moet schrijven waarin de overvloed aan beelden en argumenten moet worden omgezet in een wiskundig bewijs, waarin al deze elementen in een lineaire volgorde moeten worden gerangschikt, en waarbij elk intuïtief aanvoelen moet worden vertaald in een rigoureus argument. Het is frustrerend werk, maar het is niettemin noodzakelijk. Het levert nieuw begrip dat onontbeerlijk is om op voort te bouwen.'

Hoe komt u van uw frustratie af?

'*Je cultive mon jardin*. Ik onderhoud mijn tuin, In de letterlijke betekenis.'

De gastvrouw van een etentje heeft u een plaats toebedeeld naast God. Waarover zou u het hebben?

'Ik zou een boel vragen voor hem hebben. Zoals: klopt de Riemann-hypothese? En is ze te bewijzen? Er zijn veel vragen waarop we het antwoord met zekerheid kennen, zonder dat we een idee hebben hoe we het moeten bewijzen. Bijvoorbeeld: "de cijfers 0 tot en met 9 komen elk met een frequentie van 1/10 voor in de decimalen van pi."

'Bestaat hiervoor een bewijs? Of kunnen wiskundigen alleen hopen "simpele" problemen op te lossen, in tegenstelling tot de hoop van Hilbert: *Wir müssen wissen. Wir werden wissen. (David Hilbert was een Duitse wiskundige, wiens grafschrift luidt: 'We moeten weten. We zullen weten.' red.)* (hvde)

Criminelen vang je met wiskundigen

In deze dagen van cybercriminaliteit dringt het tot steeds meer mensen door dat ze hun informatie maar beter beveiligen. Dat is deels een kwestie van gezond verstand (geen enkele bank vraagt u om vertrouwelijke gegevens in een onbeveiligd mailtje te stoppen), van technische hulpmiddelen (virusscanners en firewalls), en van wiskunde. **Pieter Van Dooren**

Van cryptografie heeft iedereen wel eens gehoord, maar kent u steganografie? Dat is het verbergen van boodschappen. In sommige gedichten vormen de eerste letters van elk vers samen een woord. Dat woord is niet veranderd, zoals bij cryptografie, het is gewoon slim verstopt. 'Een bekende manier van verstoppen is in een watermerk', zegt professor Ann Dooms (VUB en Jonge Academie). 'Dan ga je de kleur van een reeks pixels of beeldpunten lichtjes veranderen. Moderne digitale beelden kunnen miljoenen kleuren bevatten, en het valt echt niet op als in een blauwe hemel van kleur 14752 er hier en daar een 14751 zit.'

Je kunt perfect een foto in een andere verstoppen, zonder dat het opvalt. Wie er echt naar zoekt, zal zien dat er aan de foto geprutst is, maar dat wil nog niet zeggen dat hij weet hoe.

Dooms: 'Wij gebruiken de wiskunde van de wavelet-transformaties – waarmee onze landgenote Ingrid Daubechies beroemd geworden is – om onze wijzigingen aan te brengen. Die breken het beeld op in grove informatie, midden en details. Wijzig je in de grove frequenties, dan is dat al snel zichtbaar. Stop je de informatie in de fijne frequenties, dan gaat ze misschien verloren als het beeld nadien gecomprimeerd wordt. Daarom werken we op de middenfrequenties, op groepjes van pixels tegelijk. Als iemand nadien een deel van die pixels uitschakelt, komt onze boodschap toch nog steeds door. Pixels uitschakelen kan je tegenstander doen door bijvoorbeeld een stuk van het beeld weg te knippen, of het te comprimeren, of door de kleuren te veranderen.'

Maar watermerken zijn vooral handig om de authenticiteit van een beeld te bewijzen, of aan te tonen wie het gestolen heeft, en in welke versie. Elke wijziging aan het beeld zal immers ook het watermerk wijzigen. Ooit lekte de zoon van een Oscar-jurylid informatie. Hij werd gepakt doordat de DVD's

Sprinkhanen in de file

Hoe kan een volledige zwerm sprinkhanen als één organisme bewegen, terwijl elke afzonderlijke sprinkhaan alleen rekening houdt met zijn directe buren? Als we dat wisten, weten we misschien ook hoe we de files moeten aanpakken, of de veiligheid van massa-ontmoetingen zoals de Love Parade. Een zwerm werkt niet zo handig in een lab, maar biologen kunnen daar wel makkelijk een kleine groep sprinkhanen observeren. Het gedrag van een enkele sprinkhaan kan dan vertaald worden in een wiskundige formule, waarmee vervolgens de beweging van een hele zwerm van die virtuele sprinkhanen kan doorgerekend worden. Dat vraagt veel tijd en geld, en grote computers.

Daarom ontwikkelt Giovanni Samaey (KU Leuven en Jonge Academie) wiskundige technieken om het 'emergente' groepsgedrag van de zwerm te extraheren uit korte simulaties met beperkte aantallen sprinkhanen. Een verrassend resultaat dat met deze technieken aan Oxford en Princeton is bekomen, toont aan dat een sprinkhanenzwerm zijn samenhang sneller herstelt als de aparte sprinkhanen zich willekeuriger gaan bewegen wanneer hun buren alle kanten lijken op te gaan. Dat kan nuttig inzicht geven in filevorming.

In tegenstelling tot automobilisten, die reageren op de remlichten van hun voorganger, letten sprinkhanen vooral op het gedrag van de individuen achter hen (want die eten alles op wat ze te pakken krijgen, ook hun voorliggers). Of daar ook een les voor automobilisten inzit, moet nog blijken. Er is nog werk voor jonge wiskundigen.

© Photo News

Geloof het of niet: de kat komt uit de foto ernaast. Ze zat er als watermerk in verstopt. Of juister, ze zit er nog steeds in, en dat valt niet meteen op. © Ann Dooms

Ann Dooms: ons tv-systeem is marktrijp. © put

die elk jurylid ontvangen hadden, een ander watermerk droegen. Acrobat biedt al een watermerk-functie aan voor wie zijn pdf's wil beveiligen.
Dooms: 'Wij doen aan fundamenteel onderzoek, om te begrijpen hoe groepjes pixels wijzigen. Maar we doen ook toegepast onderzoek. Bijvoorbeeld naar de kwaliteit van televisiebeelden. We stoppen een watermerk in het uit te zenden beeld, en kijken dan naar het watermerk van het ontvangen beeld, en dat leert ons hoeveel kwaliteitsverlies er onderweg is opgetreden. Maar al is het toegepast, je hebt er nog steeds wiskundigen voor nodig. Die voelen zich tenminste op hun gemak in een acht-dimensionele ruimte. Veel mensen zijn bang dat je met een opleiding pure wiskunde nadien alleen maar saaie jobs zult vinden. Vergeet het.'

Caesar

Behalve boodschappen verbergen, kun je ze ook onleesbaar maken. Julius Caesar gebruikte al rekenkunde om zijn boodschappen te beveiligen: hij schoof alle letters drie plaatsen in het alfabet op, zodat de a een d werd, en de d een g. Dat werkte prima, al was het waarschijnlijk eerder omdat de Galliërs niet konden lezen dan omdat ze niet tot drie konden tellen. Maar er zijn ook moeilijker kraakbare manieren om een tekst te 'versleutelen'. 'Meestal gebruikt men voor het omzetten een valkuilfunctie: een wiskundige bewerking die gemakkelijk gaat in de ene richting, maar heel moeilijk in de andere. Zo is het gemakkelijker om een getal met zichzelf te vermenigvuldigen, dan om uit het resultaat een vierkantswortel te trekken', zegt algebra-onderzoeker Johannes Nicaise (KU Leuven en Jonge Academie). 'En met priemgetallen wordt het nog veel leuker: het is relatief gemakkelijk om een computer twee priemgetallen van een paar honderd cijfers te laten zoeken en ze dan met elkaar te vermenigvuldigen, maar zelfs de beste computers doen er maanden of jaren over om dat getal terug te ontbinden in twee priemgetallen. Zo lang, dat het te veel moeite is voor een misdadiger, of zelfs een geheime dienst.'
Maar al is een versleutelde boodschap bestand tegen nieuwsgierige blikken, zender en ontvanger moeten nog steeds de sleutel uitwisselen, en als die onderschept wordt, ben je even ver van huis.
Pas in de jaren zeventig ontwikkelden wiskundigen een oplossing: de bestemmeling stelt een doos ter beschikking die iedereen vrij mag komen ophalen, met een hangslot dat iedereen kan sluiten door het 'dicht te klikken', maar alleen de bestemmeling heeft de sleutel om het hangslot weer te openen. Iets technischer: je versleutelt je boodschap met een 'publieke sleutel' die iedereen mag kennen, maar het resultaat is alleen te decoderen met de sleutel die enkel de ontvanger bezit. Nu moeten er geen sleutels meer uitgewisseld worden.
Wouter Castryck, wiskundige aan de KU Leuven, die ooit een zomerschool over cryptografie gaf : 'Het beste dergelijke systeem van het moment, ECC, werkt met wat we elliptische krommen noemen. Je kunt met minder informatieverkeer dezelfde veiligheid garanderen als concurrerende systemen. Dat is belangrijk bij chipkaarten of RFID-tags, de beveiligingskaartjes die het alarm doen afgaan als je de winkel verlaat met onbetaalde goederen.' Thuisbankieren of documenten ondertekenen met je identiteitskaart zijn andere voorbeelden. Jij geeft daarbij informatie door die alleen van jou kan komen (of juister, alleen van de chip in jouw kaart) en die niemand kan nabootsen, bij gebrek aan de sleutel.
Leuk om weten: de Amerikaanse overheid, maar ook Windows en Java versleutelen hun informatie met een systeem dat ontwikkeld werd door twee Leuvense wiskundigen, Joan Daemen en Vincent Rijmen. Die hadden hun systeem oorspronkelijk Rijndael genoemd, gewoon om te horen hoe de Amerikanen dát zouden uitspreken. Heel eenvoudig: ze doopten het om tot Advanced Encryption Standard, AES.

> **'Veel mensen zijn bang dat je met een opleiding pure wiskunde nadien alleen maar saaie jobs zult vinden. Vergeet het'**
>
> **ANN DOOMS**
> Professor VUB

Tellen is niet simpel

Niemand van ons heeft last met de nul of met negatieve getallen. En toch hebben de wiskundigen er honderden jaren mee geworsteld.

Is de mens de jongste eeuwen zoveel slimmer geworden, dat wij met nul en negatief omgaan alsof het niets is? Nee hoor, ook wij lopen geregeld vast. Denk maar aan het gedoe rond het jaar 2000: hele volksstammen wilden maar niet begrijpen dat de eenentwintigste eeuw in 2001 begon, gewoon omdat onze jaartelling geen jaar nul heeft. En ook wie het wel begreep, heeft toch 2000 gevierd.
En gegarandeerd, in 2100 is het weer van dattum.
Was het u al opgevallen dat er twee nullen bestaan? De ene dient als vuller in ons notatiesysteem, waar de waarde van een cijfer afhangt van zijn plaats in het getal. Er is verschil tussen 3045 en 345. In de tweede betekenis is de nul zelf een getal.
Reeds bij de Babyloniërs hing de waarde van een cijfer af van zijn plaats in het getal, maar toch gebruikten zij eeuwenlang geen teken voor een lege positie: 3045 en 345 werden hetzelfde geschreven; het verschil moest je maar afleiden uit de context.
Gek? Gek is dat wij dat vandaag nog steeds doen. Als de busschauffeur 'twee vijftig' zegt, betaal je hem 2,50 euro, als de verkoopster in de kledingboetiek 'twee vijftig' zegt, weet je dat je eraan hangt voor 250 euro.
Zeker tot in de achttiende eeuw zaten de wiskundigen ook met de negatieve getallen in hun maag. D'Alembert (1717 – 1783), zei ooit: "Als een probleem leidt tot een negatieve oplossing, betekent dit dat een deel van de hypothese vals was'.
En een eeuw voordien zei de grote wiskundige Pascal: 'Een positief getal aftrekken van nul is pure nonsens.'
Of nog: 'Ik heb mensen gekend die maar niet konden begrijpen dat als je vier van nul aftrekt, het resultaat nul is.' (pvd)

WISKUNDEGRAP

Bezoeker gezocht

Een biologe, een fysicus en een wiskundige zitten op een bankje voor een huis. Terwijl ze daar van het zonnetje genieten, gaan er een man en een vrouw in het huis naar binnen. Even later komen ze weer naar buiten, vergezeld van een derde persoon.
De biologe zegt: 'Ze hebben zich voortgeplant!'
De natuurkundige zegt: 'Dat moet een meetfout zijn.'
Waarop de wiskundige bedachtzaam zegt: 'Als er nu iemand naar binnen gaat, is het huis weer leeg!'

QUIZ

15.882

Liefst 15.882 lezers namen vorige week deel aan onze eerste online wiskundequiz. Gemiddeld haalden zij een score van 6,2 op tien.
De grootste 'instinker' was de negende vraag, over de goedkoopste manier om een ketting te maken uit losse stukken. 16 euro, dacht 55 procent van de deelnemers. Maar het kon ook voor 12 euro, door drie schakels los te maken en daarmee de rest aaneen te klinken. Dat antwoord werd door ongeveer een kwart van de deelnemers aangeduid.
Vanaf vandaag staat de tweede aflevering van de quiz online, met nieuwe vragen. Succes! (kdr)
www.standaard.be/wiskundemaand