Nieuws

| News

Deze rubriek is een kroniek van wiskundige activiteiten in Nederland. Toekomstige activiteiten worden aangekondigd en van voorbije activiteiten wordt verslag gedaan.
Wilt u uw aankondiging of verslag in deze rubriek geplaatst zien? Stuur dan uw bijdrage (± 350 woorden, zo mogelijk met illustratie) naar nieuws@nieuwarchief.nl. De redactie behoudt zich het recht voor berichten te weigeren of in te korten.

Redacteur: Charlene Kalle

Een langdurig lemma

Wiskunde heeft de top tien gehaald van belangrijkste wetenschappelijke ontdekkingen in 2009 volgens het Amerikaanse tijdschrift *Time*. Op de zevende plaats staat het Fundamentele Lemma.

Het Fundamentele Lemma komt uit het Langlandsprogramma. Robert Langlands, een Canadese wiskundige, begon in 1967 met het opschrijven van een serie vermoedens, die nu samen bekend staan als het Langlandsprogramma. De vermoedens leggen allerlei verbanden tussen verschillende gebieden binnen de wiskunde, als getaltheorie, analyse, algebraïsche meetkunde en groepentheorie. Toen hij zijn vermoedens formuleerde, vermoedde Langlands ook al dat het hem niet zou lukken om alles zelf uit te werken.

Eén van de onderdelen van het programma is het Fundamentele Lemma. Aanvankelijk dacht Langlands dat het bewijzen daarvan niet al te moeilijk zou zijn en het lukte hem en een aantal van zijn studenten dan ook vrij snel om een paar speciale gevallen te bewijzen. Het algemene geval bleek echter veel lastiger dan gedacht. Pas in 2006 slaagde de Vietnamese wiskundige Ngô Bao Châu, werkzaam aan de Université Paris-Sud en het Institute for Advanced Studies in Princeton, erin het bewijs te leveren en in 2009 waren de experts het erover eens dat het bewijs klopt. *Bron: www.kennislink.nl*

Goede prestaties 6vwo-leerlingen

Nederlandse bètaleerlingen hebben goed gepresteerd op een internationale test naar het niveau van vwo-leerlingen op de gebieden wiskunde en natuurkunde. Dat is gebleken uit de resultaten van de TIMSS-Advanced 2008 naar het niveau van leerlingen in de laatste klas van het voortgezet onderwijs, die op 9 december 2009 bekend gemaakt werden.

Voor de test werden bijna veertig duizend leerlingen uit tien landen onderzocht die op pre-universitair niveau wiskunde en natuurkunde volgen. In Nederland zijn leerlingen getest uit 6 vwo met wiskunde B1,2 en/of natuurkunde 1,2 in hun pakket. In Nederland werd het onderzoek uitgevoerd door de Universiteit Twente, er deden in totaal 228 scholen mee.

De Nederlandse leerlingen deden het vooral goed bij de natuurkundetoets en haalden daar een gemiddelde score van 582, wat ver boven het schaalgemiddelde van de TIMSS van 500 was. Een vijfde van de leerlingen haalde zelfs het hoogst haalbare aantal punten, 625. Nederland stond dan ook bovenaan de natuurkunderanglijst. De gemiddelde score bij wiskunde was 552 punten en hier haalde zes procent van de leerlingen het hoogste niveau. Zeven van de tien landen zat onder dit schaalgemiddelde.

Wel moet opgemerkt worden dat in Nederland slechts een kleine groep leerlingen getest is, omdat slechts 3,5 procent van alle 18-jarigen eindexamen doet in wiskunde en/of natuurkunde op pre-universitair niveau. In de meeste andere landen is dit aandeel flink hoger. In Slovenië is dit voor wiskunde zelfs veertig procent. Hierdoor zijn in de meeste landen de verschillen tussen de leerlingen groter.

Buiten het niveau, werden ook het zelfvertrouwen van de leerlingen op het gebied van wiskunde en natuurkunde en hun interesse voor deze vakken onderzocht. Hieruit bleek dat de Nederlandse meisjes die meededen aan de test net zo veel vertrouwen hebben in hun wiskundevaardigheden als de Nederlandse jongens en het vak ook net zo aantrekkelijk vinden. Wel valt op dat er veel minder meisjes dan jongens wiskunde op dit niveau volgen. Het aandeel meisjes is minder dan een kwart. Samen met Libanon heeft Nederland ook het laagste

percentage vrouwelijke wiskundedocenten dat aan deze leerlingen les geeft, vijftien procent van alle wiskunde B2-docenten.

Bij natuurkunde liggen deze percentages ook lager dan in de andere landen. Negentien procent van de natuurkunde 2 leerlingen is een meisje en het aandeel vrouwelijke docenten is vijf procent. Bovendien hebben deze meisjes bij natuurkunde slechter gepresteerd dan de jongens, vinden ze het vak minder aantrekkelijk en hebben ze minder vertrouwen in hun eigen kunnen. Wel hebben de Nederlandse meisjes het voor natuurkunde gemiddeld beter gedaan dan jongens en meisjes uit andere landen.

Als laatste viel op dat de Nederlandse bètameisjes minder geïnteresseerd zijn in een bètastudie dan de bètajongens. Minder dan de helft van de onderzochte wiskunde B2-meisjes wil een bètatechnische studie gaan doen, 37 procent geeft de voorkeur aan een medische studie. Van de natuurkunde 2-meisjes is dit 26 procent. Van de jongens kiest bijna driekwart voor een bètatechnische studie.

Tijdens het onderzoek zijn ook de docenten ondervraagd. Hieruit bleek dat de Nederlandse docenten zich goed toegerust voelen om de vakken te geven en weinig belemmeringen ervaren in hun werk. Alleen het ontbreken van een eigen werkplek was een serieus probleem voor veertig procent van de docenten. *Bron: www.nwo.nl*

Hoe je een slimme meid op haar toekomst voorbereidt

Er is haast geen verschil tussen hoe goed jongens en meisjes in wiskunde zijn. Dit is de conclusie van Nicole Else-Quest en haar collega's van de University of Villanova na het bestuderen van testdata uit 2003.

De resultaten van twee onderzoeken werden gebruikt: de Trends in International Mathematics and Science Study (TIMSS) en het Programme for International Student Assessment (PISA). Hierin zijn totaal 493.495 leerlingen in de leeftijd van veertien tot zestien jaar getest uit 69 verschillende landen. De TIMSS onderzoekt vooral wiskundige basisvaardigheden en de PISA onderzoekt of leerlingen in staat zijn om hun wiskundevaardigheden toe te passen in het dagelijks leven.

De belangrijkste conclusie uit hun onderzoek was dat jongens en meisjes op het zelfde niveau kunnen presteren, mits gebruik gemaakt wordt van de juiste educatieve middelen en er voor de leerlingen zichtbare vrouwelijke rolmodellen zijn die goed zijn in wiskunde. Het grote verschil tussen jongens en meisjes op het gebied van wiskunde is dat meisjes minder zelfvertrouwen hebben op dit gebied. De onderzoekers stelden vast dat in landen waar meer vrouwen onderzoekachtig werk doen, meisjes vaak beter presteerden op het gebied van wiskunde en ook meer zelfvertrouwen hadden.

Deze resultaten zijn begin dit jaar in de *Psychological Bulletin* van de American Psychological Association verschenen.

Bron: www.sciencedaily.com

Hard van stapel

In het decembernummer van het Nieuw Archief berichtten we al over een nieuw record tetraëders stapelen van Salvatore Torquato en Yang Jiao. Het is hierbij de bedoeling om de ruimte zo ver mogelijk op te vullen met tetraëders. Sinds toen zijn er nieuwe vorderingen gemaakt op verschillende plaatsen.

Ten eerste door Elizabeth Chen, een promovenda aan de University of Michigan. Haar promotor, Jeffrey Lagarias, daagde haar uit om de stapeling van Torquato en Conway uit 2006, met een dichtheid van 72 procent, te verslaan. Chen vond een stapeling van 78 procent, wat betekent dat deze stapeling de ruimte beter opvult dan de bekende optimale bolstapeling, waarbij bollen als kanonskogels gestapeld worden. Chen maakte haar resultaten vorig jaar augustus bekend.

Ondertussen ging ook Sharon Glotzer van University of Michigan aan de slag. Op zoek naar een nieuwe materialen voor de luchtmacht met bijzondere optische eigenschappen vond ze een tetraëderstapeling van maar liefst 85 procent. Eigenlijk was ze op zoek naar een periodieke stapeling, maar de stapeling die ze vond had de complexe structuur van een quasikristal. En net nadat dit resultaat klaar was om gepubliceerd te worden in het tijdschrift *Nature* in december vond een groep onderzoekers aan Cornell University met andere methodes een even dichte stapeling. Verrassend was dat deze stapeling een veel eenvoudigere structuur heeft dan die van Glotzer.

En ook hier bleef het niet bij, want een paar dagen voor de Kerst maakten Torquato en Jiao bekend dat ze de stapeling van de groep in Cornell een beetje hadden aangepast en zo een stapeling hadden gekregen van 85,55 procent. In een interview eind december zei Torquato dat het hem zou verbazen als dit de dichtst mogelijke stapeling zou zijn. En inderdaad, begin januari zette Chen nieuwe artikel op het internet waarin ze een familie van stapelingen omschrijft die de stapeling van Cornell bevat, maar ook een nog betere stapeling. Het record voor tetraëderstapelen staat nu weer op naam van Elizabeth Chen en is 85,63 procent. *Bron: www.nytimes.com*

Niet sporen?

Een groep theoretische natuurkundigen en scheikundigen uit de Verenigde Staten en Israël hebben het gedrag van bacteriën onder moeilijke levensomstandigheden onderzocht. Ze zeggen daardoor meer inzicht te hebben gekregen over hoe mensen beslissingen zouden moeten nemen die te maken hebben met hun gezondheid, welzijn en het lot van anderen. De onderzoekers in kwestie zijn José Onuchic, Peter Wolynes en Daniel Schultz van de University of California en Eschel Ben Jacob van de University of Tel Aviv in Israël. Hun resultaten zijn begin december in het tijdschrift *Proceedings of the National Academy of Sciences* verschenen.

Eén bacteriekolonie kan meer dan honderd keer het aantal mensen op aarde bevatten. Als bacteriën zich in een levensbedreigende situatie bevinden, hebben ze twee belangrijke strategieën voor handen. Ten eerste kunnen ze een endospore maken: deze bevat een kopie van het DNA van de moedercel en bevindt zich in slapende toestand om beter bestand te zijn tegen temperatuurschommelingen en voedseltekort. Onder betere omstandigheden kan deze spore ontkiemen tot volwaardige bacterie. Het nadeel is dat de moedercel sterft als deze een spore produceert. In plaats van een spore te produceren, kunnen bacteriën er tijdens het overgangsproces ook voor kiezen om te ontsnappen en in een andere toestand over te gaan, zogenaamde competentie, waarbij de bacterie zijn membraan aanpast om makkelijker materiaal van de stervende cellen uit zijn omgeving op te kunnen nemen en zo te kunnen blijven leven in de onvriendelijke omstandigheden. De cel zelf blijft zo in leven en keert terug tot zijn normale toestand als omstandigheden verbeteren. Het nadeel is dat de bacterie zeer waarschijnlijk sterft als de omstandigheden verder verslechteren en dat het overgaan in deze toestand alleen helpt als de meeste andere bacteriën dit niet doen. In een dergelijke situatie staat een bacterie dus voor een keuze en onder tijdsdruk om deze keuze te maken. Bovendien hangt de keuze van één bacterie af van de beslissing van alle andere bacteriën in de kolonie.

Bacteriën gebruiken chemische boodschappen om met elkaar te communiceren en zijn op ieder moment op de hoogte van de intenties van alle andere leden van de kolonie. Ze nemen beslissingen op ba-

sis van een gespecialiseerd netwerk van genen en proteïnen. In hun artikel beschrijven de onderzoekers in een model hoe bacteriën dit gen-proteïne netwerk gebruiken om risico's te berekenen. Ook kijken ze naar de speltheorie die bacteriën gebruiken bij het maken van hun uiteindelijke beslissing.

Het dilemma van de bacteriën is enigszins te vergelijken met het bekende prisoner's dilemma. Hierin krijgen twee personen die zijn opgepakt voor dezelfde misdaad door de politie het volgende voorstel. Als ze allebei niet bekennen, dan worden ze bij gebrek aan bewijs vrijgelaten. Als één van beiden bekent, dan wordt deze persoon vrijgelaten en de ander krijgt tien jaar gevangenisstraf. Als ze allebei bekennen, dan krijgen ze allebei vijf jaar gevangenisstraf. In het algemeen zijn bacteriën eerlijk tegenover elkaar over hun bedoelingen. Daardoor is hun dilemma een zeer ingewikkelde versie van het prisoner's dilemma. Het is voor iedere afzonderlijke bacterie alleen aantrekkelijk om te ontsnappen aan het maken van een spore als de meeste andere bacteriëen dat niet doen. Maar als dat zo is, dan is het niet verstandig om deze gok te nemen, omdat de andere bacteriën waarschijnlijk tot dezelfde conclusie zijn gekomen.

Een belangrijk verschil tussen het prisoner's dilemma en het dilemma van de bacteriën is dat de bacteriën maar beperkt de tijd hebben om een beslissing te nemen. Ben Jacob zegt dat ze tijdens het onderzoek ontdekt hebben dat iedere bacterie een interne klok heeft, die sneller gaat tikken naar mate het beslissingsproces langer duurt. En, iedere bacterie stelt de beslissing zo lang mogelijk uit, probeert zo veel mogelijk informatie te verzamelen voordat het de levensbelangrijke beslissing neemt.

Volgens de onderzoekers zijn er directe relaties tussen dit onderzoek en menselijke beslissingen. Bijvoorbeeld als we beslissen om ons ergens voor te laten inenten. Vanwege eventuele risico's zou het voor ieder individu beter zijn om zich niet te laten inenten, maar alleen als de meeste anderen zich wel laten inenten. Ook zouden er toepassingen zijn in de economie en politieke wetenschappen, waarin menselijke beslissingen een grote rol spelen. *Bron: www.sciencedaily.com*

Bacteriën

Fermat Prize voor Lindenstrauss en Villani

Elon Lindenstrauss en Cédric Villani hebben de Fermat Prize 2009 uitgereikt gekregen.

De Franse prijs is vernoemd naar de legendarische wiskundige Pierre de Fermat, vooral bekend om zijn beroemde 'Laatste Stelling' waarvan het bewijs niet in de kantlijn paste. De prijs wordt elke twee jaar uitgereikt door het Institut de Mathematiques van de Université Paul Sabatier in Toulouse en bedraagt 20.000 euro. Het is de bedoeling om onderzoek uit gebieden waar Fermat zelf actief in was in het zonnetje te zetten en dan vooral onderzoek dat toegankelijk is voor veel wiskundigen die werkzaam zijn in deze gebieden.

Elon Lindenstrauss is hoogleraar in de wiskunde aan Princeton University en heeft aanzienlijke bijdragen geleverd in de getaltheorie. Hij doet veel onderzoek op het gebied van ergodentheorie en dynamische systemen en de toepassingen hiervan op het gebied van getaltheorie.

Cédric Villani is directeur van het Institut Henri Poincaré aan de Université Pierre et Marie Curie in Parijs. Hij doet onderzoek naar onder andere beweging en optimaal transport en de toepassingen hiervan.

De prijswinnaars krijgen de gelegenheid om in Toulouse over hun onderzoek te komen praten en hun resultaten te publiceren in het wiskundetijdschrift van de universiteit. *Bron: math.suite101.com*

Een kleurtje krijgen

Onderzoeker Fernando de Oliveira Filho van het Centrum Wiskunde & Informatica (CWI) in Amsterdam verbeterde de ondergrenzen van het chromatisch getal. Hij promoveerde op 1 december op zijn proefschrift 'New Bounds for Geometric Packing and Coloring via Harmonic Analysis and Optimization'.

Het probleem dat De Oliveira Filho bestudeerde, werd in 1950 door de wiskundige Nelson geformuleerd. Die vroeg zich af hoeveel kleuren er nodig zijn om alle punten in het vlak te kleuren, op zo'n manier dat punten die op afstand 1 van elkaar liggen niet dezelfde kleur krijgen. Het minimale aantal kleuren dat hiervoor nodig is wordt het 'chromatisch getal' van het vlak genoemd. Hoewel het eenvoudig klinkt, is het probleem onopgelost en zeer moeilijk. Men weet dat het getal tussen vier en zeven ligt.

Voor hoger dimensionale ruimtes kan dezelfde vraag gesteld worden. De Oliveira Filho verbeterde met nieuwe optimalisatiemethodes de ondergrenzen van de chromatische getallen voor ruimtes van dimensie drie en hoger. Hiervoor gebruikte hij Lebesgue meetbare verzamelingen. Hoe hoger de dimensie, hoe groter de verbetering is die de methodes van De Oliveira Filho opleveren. De optimalisatiemethodes van De Oliveira Filho kunnen waarschijnlijk toegepast worden op tal van andere gebieden. Dit soort kleurproblemen wordt bijvoorbeeld gebruikt bij het toewijzen van frequenties aan mobiele telefoons. *Bron: www.cwi.nl*

Stuk voor stuk

In december verscheen op de website van NewScientist een artikel over de 15 jaar durende zoektocht van Rick Mabry en Paul Deiermann naar het bewijs van de Pizzastelling. In mei 2009 verscheen het artikel van Mabry en Deiermann hierover in de American Mathematical Monthly.

Mabry en Deiermann beantwoordden de volgende vraag. Stel dat je met zijn tweeën een pizza besteld en die pizza verschijnt voorgesneden op tafel. De pizza wordt door een aantal rechte lijnen die van kant tot kant lopen in stukken gedeeld. Deze lijnen hebben allemaal één punt gemeenschappelijk, maar dat punt is niet het middelpunt van de pizza. Verder zijn de hoeken tussen de lijnen hetzelfde. Stel dat je om en om een stuk pakt. Krijg je dan allebei evenveel en zo niet, wie krijgt er meer pizza?

Het is makkelijk te zien dat als één van de lijnen door het midden van de pizza gaat, je dan allebei evenveel pizza krijgt, ongeacht het aantal keer dat gesneden is. Maar wat als dit niet gebeurt? Bij één keer snijden is het antwoord ook duidelijk. Degene die het stuk eet waar het midden van de pizza op ligt, eet het meest. Hetzelfde geldt voor twee keer snijden, maar dat blijkt een uitzondering op de regel te zijn. In artikelen uit 1967 en 1968 in het *Mathematical Magazine* over dit probleem werd namelijk bewezen dat als de pizza een even aantal

keer en meer dan twee keer gesneden is, dat dan beide eters evenveel pizza krijgen.

In 1994 gaf Deiermann een herziene versie van één van deze artikelen aan Mabry. Het vermoeden was dat voor een oneven aantal keer snijden het volgende geldt. Als het aantal keer snijden 'e'en van de volgende getallen is: 3, 7, 11, 15, ... , dan eet de persoon die het midden van de pizza krijgt het meest. Als het aantal keer snijden 5, 9, 13, 17, ... is, dan geldt het omgekeerde. In de herziene versie van het artikel werden de lezers uitgedaagd om een bewijs te geven voor drie en voor vijf keer snijden.

Deiermann en Mabry begonnen enthousiast en hadden al snel de twee vragen uit het artikel beantwoord. Ze dachten een manier te hebben die zou werken voor alle oneven aantallen. Helaas leverde hun methode ingewikkelde reeksen op met goniometrische functies. En hoewel ze alleen maar hoefden te weten of het uiteindelijke resultaat positief of negatief was om te bepalen wie het grootste deel van de pizza kreeg, lukte het hen niet om deze laatste stap te zetten.

Meer dan elf jaar later was Mabry op vakantie in het zuiden van Duitsland, toen hij ineens zag hoe hij de formules kon versimpelen. Terug thuis zette hij de computer aan het werk en dook in de archieven om te kijken of er al resultaten bekend waren over de formules die hij nu had gekregen. In een artikel uit 1999 vond hij wat hij zocht en daarna was hij met Deiermann in staat om het bewijs af te ronden.

Natuurlijk zijn er veel manieren om dit onderzoek voort te zetten. Bijvoorbeeld door te kijken naar wie de meeste korst eet of naar vierkante pizza's. Of naar hogere dimensies. Een calzone zou bijvoorbeeld opgevat kunnen worden als een driedimensionale pizza. Mabry en Deiermann hebben een hoop vragen in deze richtingen ondertussen ook al opgelost, maar er blijft nog genoeg te doen. *Bron: www.newscientist.com*

Meer wiskunde-rekenonderwijs op pabo

In december werd bekend dat pabo-studenten meer uren per week les zullen krijgen in taal en wiskunde-rekenen. Het aantal lesuren zal flink opgekrikt worden, tot vijf uur per week per vak. Op sommige pabo's is het nu minder dan een uur per week.

Deze nieuwe eisen staan in de *Kennisbasis*, een document waarin vastgelegd is wat een leraar moet kennen en kunnen en dat op 7 december werd gepresenteerd door de hbo-raad. Deze basis werd vastgelegd naar aanleiding van de aanhoudende kritiek op de lerarenopleidingen.

Pabo-studenten zullen in de toekomst op taal- en wiskunde-rekenvaardigheid getoetst worden na de propedeuse en aan het einde van de opleiding. Uiteindelijk is het de bedoeling dat de instaptoets zal worden afgeschaft, ook omdat de verscherpte exameneisen vanaf 2014 ervoor zullen zorgen dat studenten met een hoger ingangsniveau van de middelbare school zullen komen.

Door de nieuwe eisen zal het curriculum aangepast moeten worden. Er worden nu verschillende mogelijkheden overwogen, zoals het verlengen van de opleiding met een jaar, het schrappen van vakken of een specialisatie van onder- en bovenbouw op de pabo. *Bron: www.nrc.nl*

Meer π

Op 31 december 2009 heeft Fabrice Bellard het wereldrecord bekende decimalen van π verbroken en nog verrassender: hij heeft dit gedaan op een doodgewone pc. Er zijn nu bijna 2,7 biljoen decimalen van π bekend, om precies te zijn 2699999990000. Om het resultaat op te slaan is 1137 GB aan opslagruimte nodig.

Om de decimalen te vinden heeft Bellard de computer eerst een boel binaire cijfers achter de komma laten berekenen. Dat duurde 103 dagen en daarna nog dertien dagen om het resultaat te controleren. Voor de omzetting van binair naar decimaal waren twaalf dagen nodig en daarna nog eens drie dagen voor de controle. In totaal is de computer van Bellard, die minder dan twee duizend euro heeft gekost, dus 131 dagen aan het rekenen geweest.

Het vorige record stond op ongeveer 2,577 biljoen decimalen. Ze werden berekend door Daisuke Takahashi, die ze op 17 augustus 2009 bekend maakte. *Bron: bellard.org/pi/pi2700e9*

Anderhalf miljoen voor focus en massa in stochastische wiskunde

NWO trekt de komende twee jaar 1,5 miljoen euro uit voor de stochastiek, de tak van de wiskunde die zich bezighoudt met kansrekening, statistiek en stochastische besliskunde. Van het geld worden hoofdzakelijk posities gecreëerd voor aio's, postdocs en universitair docenten. NWO steunt hiermee het wiskundecluster *Stochastics - Theoretical and Applied Research* (STAR), dat op 15 mei 2009 werd opgericht als vierde loot aan de stam van wiskundeclusters. De clusters zijn vijf jaar geleden ontstaan om tegenwicht te bieden aan de teruglopende aantallen studenten en staf aan de wiskundeopleidingen.

Het wiskundecluster STAR wil de samenwerking tussen Nederlandse onderzoekers in de stochastiek bevorderen en hen internationaal beter op de kaart zetten. De zo belangrijke financiële stochastiek en de biostochastiek, die beide nu te weinig massa hebben, zullen ook een impuls krijgen uit de nieuwe financiële ondersteuning. Een speciale commissie zal het onderwijs regionaal en landelijk beter op elkaar afstemmen.

De drie andere clusters zijn *Discrete, Interactive and Algorithmic Mathematics, Algebra and Number Theory* (DIAMANT), *Nonlinear Dynamics of Natural Systems* (NDNS), en *Fellowship of Geometry and Quantum Theory* (FGQT). In het Masterplan Toekomst Wiskunde is voor de vier clusters tezamen een jaarlijks bedrag van 4,5 miljoen euro beoogd. *Bron: Annemarijke Jolmers, NWO*

De sleutel tot succes

Onderzoekers van de Cryptology and Information Security groep van het Centrum Wiskunde en Informatica (CWI) in Amsterdam hebben in samenwerking met groepen uit Duitsland (BSI en de Universität Bonn), Frankrijk (INRIA Nancy), Japan (NTT) en Zwitserland (EPFL) een RSA-sleutel van 232 decimale cijfers gebroken door de priemfactoren hiervan te vinden.

Het cryptosysteem RSA wordt onder andere gebruikt om gegevens te versleutelen die over het internet worden verstuurd. Het idee erachter

is dat het heel moeilijk is om een groot getal in zijn priemfactoren te ontbinden. Daarom wordt voor dit grote getal het product genomen van twee grote priemgetallen. Als je erachter kunt komen wat deze twee priemgetallen zijn, dan kun je de gegevens die met dit getal zijn versleuteld ontcijferen.

Het getal dat werd gekraakt heet RSA-768 en kwam uit de lijst van de RSA Factoring Challenge. In 1991 publiceerde de RSA Laboratories een lijst met getallen en loofde een geldprijs uit voor de factorisatie van deze getallen in priemfactoren. Het doel was om het onderzoek in computationele getaltheorie en het factoriseren van grote getallen in priemfactoren te stimuleren. Het kleinste getal uit deze lijst werd al in april 1991 gefactoriseerd, maar veel getallen uit de lijst zijn nog steeds niet gekraakt. In 2007 besloot de RSA Laboratories met de uitdaging te stoppen.

Om RSA-768 te factoriseren werd gedurende 2,5 jaar gerekend op vele duizenden computers op verschillende locaties. Het CWI heeft een lange traditie in dit soort rekenprojecten. In 1999 speelde het een belangrijke rol bij het voor het eerst breken van een 512-bits RSA-sleutel en in 2008 werd het MD5 internet-beveiligingssysteem 'gekraakt' waarmee de kwetsbaarheid in de infrastructuur van digitale certificaten werd aangetoond. *Bron: www.cwi.nl*

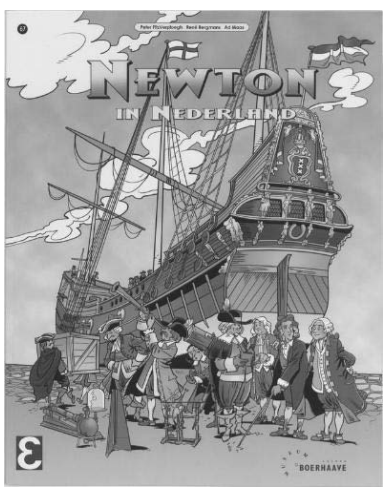
Newton aan het werk

Dit jaar staat Museum Boerhaave in Leiden in het teken van Sir Isaac Newton met een grote tentoonstelling genaamd *NewtonMania*. In een aantal zalen is een tentoonstelling opgezet over de invloed van Newton in de Nederlanden van de zeventiende eeuw. Het topstuk hiervan is zijn beroemde boek *Principia Mathematica* uit 1687. In een aantal andere zalen kun je zelf aan de slag met allerlei experimenten die laten zien hoe de wetten van de natuur werken.

Bij de tentoonstelling zijn onderwijsprogramma's gemaakt voor zowel het basisonderwijs als het voortgezet onderwijs. Ook staat er een quiz online met vragen over 10 van de 22 experimenten.

Ter gelegenheid van deze tentoonstelling geeft Epsilon Uitgaven een stripboek uit, getiteld *Newton in Nederland*.

Bron: www.museumboerhaave.nl/newtonmania



Kwadrateren en parkeren

Afgelopen november werd Simon Blackburn, wiskundeprofessor aan de University of London benaderd door Vauxhall Motors met de vraag of hij een rapport wilde schrijven over de wiskunde achter parkeren. Blackburn besloot dat dit een mooie gelegenheid was om te laten zien wat je met simpele wiskunde kunt doen en ging aan de slag.

Blackburn besloot zich te richten op fileparkeren. Hij bedacht een definitie voor perfect parkeren, namelijk in 1 keer achteruit insteken en dan op de juiste plek terecht komen zonder eindeloos heen en weer te moeten manoeuvreren. Hij berekende hoe lang de parkeerplaats dan moet zijn en het resultaat was de volgende formule:

$$\sqrt{(r^2 - l^2) + (l^2 + k^2) - (\sqrt{r^2 - l^2} - w)^2} - l - k.$$

Hierin is r de straal van de draaicirkel van de auto, l is de afstand tussen het middelpunt van een voorwiel en het middelpunt van het achterwiel aan dezelfde kant, k is de afstand van het middelpunt van een voorwiel tot aan de voorkant van de auto en w is de breedte van de auto die voor je staat als je eenmaal ingeparkeerd bent. De lengte van de parkeerplaats is de som van het getal dat uit de formule komt en de lengte van je auto. *Bron: news.cnet.com*

Onvoldoende voor vmbo-t

Een kwart van de vmbo-t scholen van Nederland presteert onder de maat volgens het dagblad *Trouw*, dat ieder jaar een onderzoek uitvoert naar de prestaties van middelbare scholen. Trouw gebruikte dit jaar een nieuwe manier om de prestaties van scholen te meten. De methode is ontwikkeld door Jaap Donkers, hoogleraar aan de Universiteit Maastricht, en maakt vooral gebruik van de prestaties van de geslaagde leerlingen in de kernvakken Nederlands, Engels en wiskunde.

Uit het onderzoek bleek dat bijna vijftig van de bijna achthonderd vmbo-t scholen die ons land rijk is, gemiddeld voor minstens twee van de drie kernvakken een cijfer haalde dat lager is dan een zes. Voor tien scholen gold dat zelfs voor alle drie de vakken. In veel gevallen compenseren leerlingen van deze scholen een onvoldoende voor hun eindexamen met een veel hoger cijfer voor hun eerder gemaakte schoolonderzoeken.

Hetzelfde onderzoek wees uit dat havo's juist goed scoren. Veertig procent van de scholen blonk uit met een score van een zeven of meer voor minstens één van de kernvakken. *Bron: www.trouw.nl*