Twee pythagoras

wiskundetijdschrift voor jongeren

37 ste jaargang nr. 2 december 1997

Inhoud

1 **Nul . . . of tien?**

2 - 3 **Kleine nootjes**

Varia Historica
4 **Maria Agnesi**

Wiskunde en Internet
5 t/m 7 **Spinnen op het Web**

Wiskundige notaties
8 - 9 **Nul**

Priemgetallen
10 t/m 13 **Delen met rest**

14 - 15 **Pythagoras Olympiade**

16 t/m 19 **De magie van π**

20 - 21 **Twee Sinterklaasproblemen**

22 - 23 **Twee records**

Priemgetallen met de computer
24 - 25 **Modulair rekenen**

26 - 27 **Tweede ronde Nederlandse Wiskunde Olympiade**

28 **Problemen**

29 **Oplossingen nr. 1**

30 **Agenda**

32 **Oplossingen p. 2 & 3**

COLOFON

uitgave
Pythagoras is een uitgave van het NIAM en verschijnt zes keer per jaar.
Een jaargang loopt van september tot en met augustus.
ISSN: 0033-4766

redactieadres
Erjen Lefeber
Faculteit der toegepaste wiskunde
Universiteit Twente
Postbus 217
7500 AE Enschede

email
pythagoras@wins.uva.nl

WWW
www.wins.uva.nl/misc/pythagoras

redactie
Klaas Pieter Hart
Erjen Lefeber
René Swarttouw
Chris Zaal

eindredactie
Chris Zaal

grafisch ontwerp
Joke Mestdagh, Amsterdam
Kitty Molenaar, Amsterdam

zet- en drukwerk
Koninklijke van de Garde, Zaltbommel

Nul ... of tien?

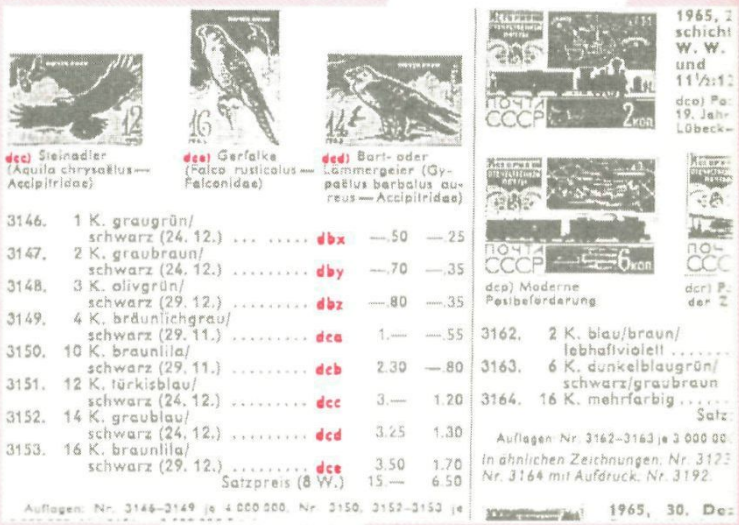
Hessel Pot

In dit nummer van Pythagoras vind je op p. 8 een artikel over de herkomst van het getal nul. De manier waarop wij onze getallen noteren is door de Arabieren naar Europa gebracht. Inclusief de nul, die door velen als essentieel wordt beschouwd in ons rekensysteem. Maar hebben we die nul ook werkelijk nodig?

Normaal schrijven we de natuurlijke getallen met behulp van tien symbolen: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0. Echter, als we voor nul géén symbool invoeren en voor tien het symbool gebruiken, kunnen we de natuurlijke getallen ook noteren als

1	2	3	4	5	6	7	8	9	X
11	12	13	14	15	16	17	18	19	1X
21	22	23	24	25	26	27	28	29	2X
31	32	33	34	35	36	37	38	39	3X
41	42	enzovoort.							

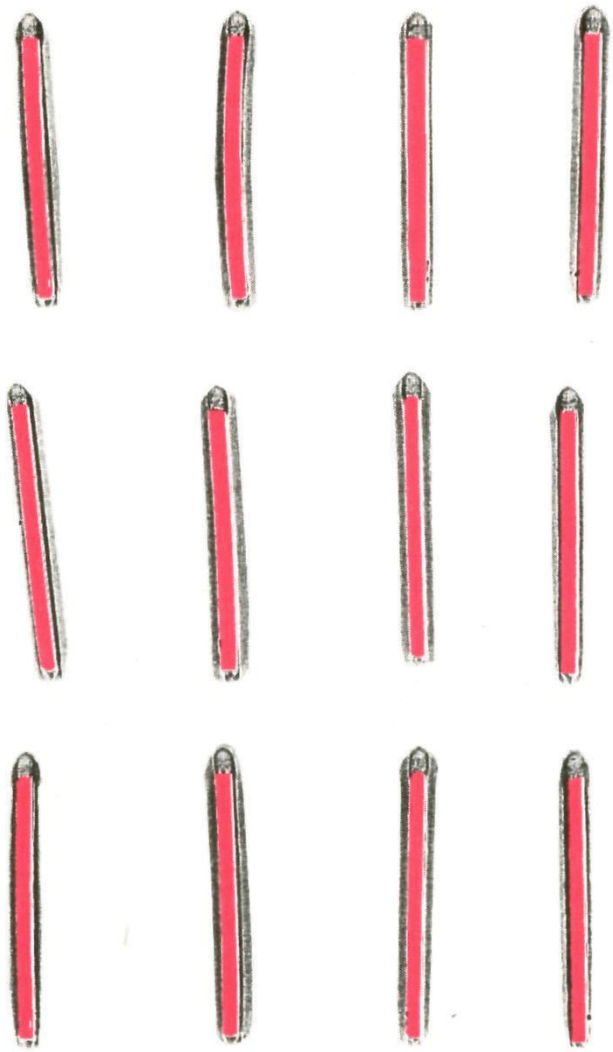
Als je in het gewone systeem $9 + 1$ uitrekent, dan komt op de plaats van de negen een nul te staan en worden tien eenheden overgeboekt naar de volgende cijferpositie. Dit heet met een Engels woord 'overflow'. Het resultaat van $9 + 1$ is dus een getal van twee cijfers: 10. In het systeem met de is $9 + 1$ nog steeds een getal van één cijfer, namelijk X. Pas bij $X + 1$ vindt er overflow plaats: tien eenheden worden overgeboekt naar de volgende cijferpositie en op de plaats van de X komt een 1 te staan. De overflow vindt dus niet plaats bij negen-plus-één, maar bij tien-plus-één. Na de X komt dus het getal 11. Alle getallen zonder een X stellen hetzelfde getal voor als gewoonlijk. Verder stelt $1X$ twintig voor, $2X$ dertig en $9X$ honderd. Honderd-en-een is $X1$. Honderdtien is XX, nog steeds een getal van twee cijfers. Pas bij honderdelf zijn voor het eerst drie cijfers nodig. En pas bij elfhonderdelf vier cijfers. Deze nulloze code komt in de praktijk daadwerkelijk voor. Alleen dan niet met het getal *tien* als basis van het positiestelsel, maar met *zesentwintig*. Voor de 26 benodigde verschillende symbolen voor de getallen 1 tot en met 26 worden dan de 26 letters van ons alfabet gebruikt. Postzegelverzamelaars zullen deze nulloze a-z-code wel kennen. Hij wordt (met kleine variaties) gebruikt in de grote postzegelcatalogussen van MICHEL en van IVERT/TELLIER om de volgnummers van de afgebeelde postzegels aan te geven (zie afbeelding).



Ik ben benieuwd of iemand nog andere praktische toepassingen kent van dergelijke nulloze notatiesytemen voor de natuurlijke getallen.

kleine

Kleine nootjes zijn eenvoudige vraagstukken die door iedereen 'gekraakt' kunnen worden, zonder enige wiskundige voorkennis. De oplossingen staan op p. 32 van dit nummer.



Lucifers

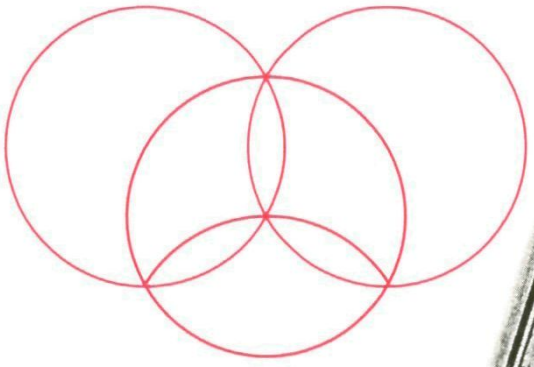
Neem twaalf lucifers en leg ze in drie rijtjes van vier. Kun je nu drie lucifers verplaatsen zodanig dat elke horizontale en elke vertikale rij uit vier lucifers bestaat?

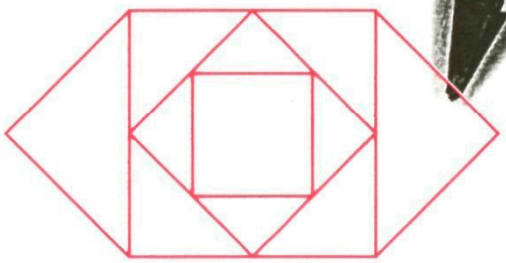
Indianen

Twee indianen lopen door het struikgewas. De ene indiaan is de zoon van de ander maar de ander is niet zijn vader. Hoe is dat mogelijk?

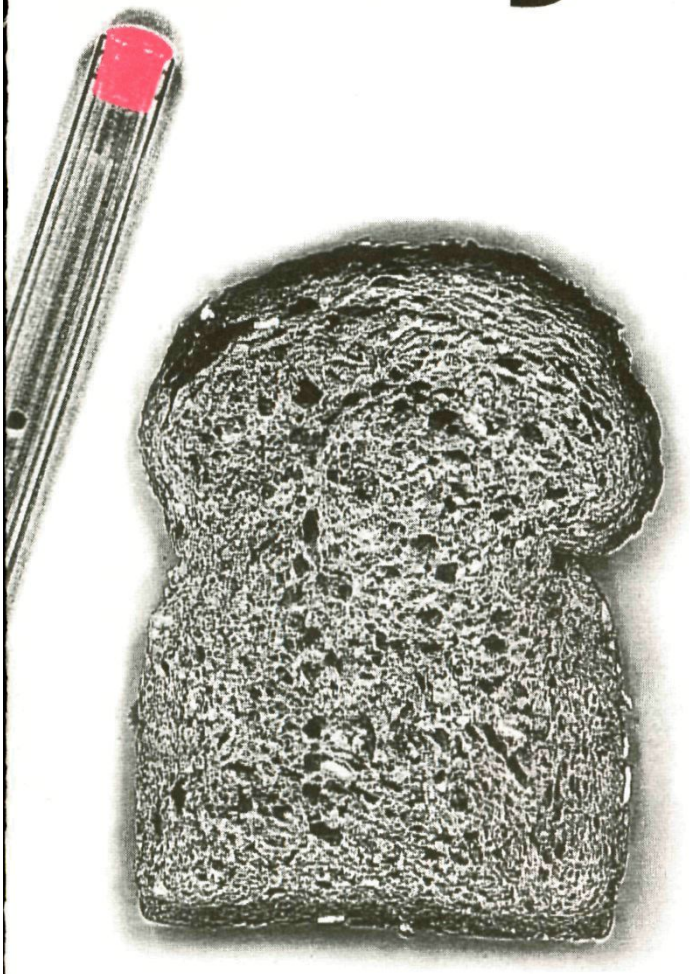
Overtrekken

Kun je uitvinden of het mogelijk is de onderstaande figuren met een pen over te trekken zonder een lijn twee keer te tekenen? Je mag je pen niet van het papier optillen.





nootjes

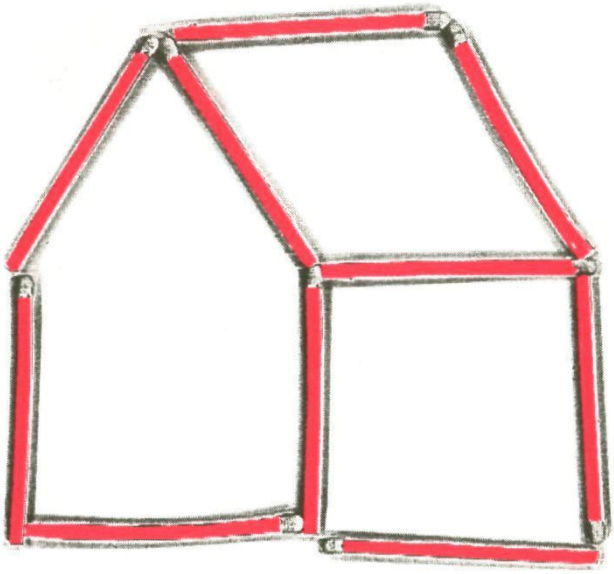


Twintig
Kun je uit het onderstaande rijtje getallen er vijf kiezen zodat de som ervan gelijk aan 20 is?

1, 1, 1, 3, 3, 3, 5, 5, 5, 7, 7, 7.

Jokkebrokken
Pietje zegt dat Jantje liegt en Jantje zegt dat Willem liegt. Willem zegt dat Jantje en Pietje allebei liegen. Wie liegt er nu eigenlijk?

Huisje
Met tien lucifers kun je een eenvoudig huisje maken:



Deze tekening geeft het zuidoost-aanzicht van het huisje weer. Kun je door slechts *twee* lucifers te verleggen het zuidwest-aanzicht krijgen?

Toast
In het vakantiehuisje is geen broodrooster aanwezig, alleen een grill. Onder de grill passen precies twee sneetjes brood. Het roosteren van één kant van een snee brood duurt drie minuten. Om drie sneetjes te roosteren zouden de meeste mensen eerst twee sneetjes onder de grill leggen, ze na drie minuten omkeren, na weer drie minuten het derde sneetje erin doen en omkeren. Dit neemt in zijn geheel twaalf minuten in beslag. Er is echter een snellere manier om drie sneetjes brood onder de grill te roosteren — hoe?

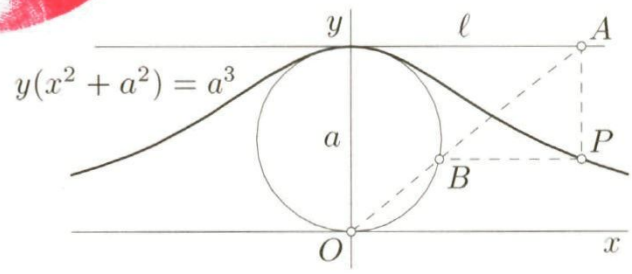
Maria Agnesi

Teun Koetsier

In de eerste helft van de 18e eeuw organiseerde de welgestelde Milaneseprofessor Pietro Agnesi bij hem thuis wetenschappelijke bijeenkomsten. Al als kind nam zijn dochter Maria Gaetana Agnesi daaraan actief deel. De gesprekken, die wetenschappelijke onderwerpen betroffen, werden altijd gevoerd in het Latijn, maar Maria sprak met vrijwel alle buitenlandse bezoekers in hun eigen taal. Op haar elfde beheerste ze niet alleen Duits, Spaans en Frans, maar ook Grieks en Hebreeuws. Aan het eind van de 17e eeuw was de differentiaal- en integraalrekening ontdekt en die had de weg geopend naar nieuwe theorieën in de wiskunde en talloze nieuwe toepassingen. De beweging van een satelliet om de aarde wordt in wezen nog steeds met behulp van uit die tijd stammende theorie beschreven. In 1748 verscheen van Maria Agnesi een belangrijk boek over die differentiaal- en integraalrekening. Maria Agnesi (1718-1799) is echter vooral bekend door de wiskundige kromme die de 'heks van Agnesi' wordt genoemd. In xy-coördinaten kunnen we de kromme beschrijven door $y(x^2+a^2)=a^3$ met $a>0$ een willekeurige constante. Op het hieronder vermelde WWW-adres kun je de kromme met een Java-applet zelf tekenen. Deze kromme ontstaat wanneer je een rechte lijn over een cirkel laat ronddraaien (zie tekening). De kromme heette daarom oorspronkelijk een 'versiera' (afgeleid van het Latijnse vertere = draaien). Het woord 'versiera' was echter ook een afkorting van 'avversiera' of 'vrouw van de duivel'. De Engelsman Colson die het boek van Agnesi in het Engels vertaalde, zou de twee betekenissen door elkaar hebben gehaald. Maria Agnesi was in het geheel geen heks, eerder een engel. Hoewel ze zich ongetwijfeld graag met wetenschap bezig hield, lijkt het erop alsof ze het ook deed om haar vader een genoegen te doen. Bij zijn overlijden in 1752 trok ze zich terug uit het wetenschappelijke leven en wijdde zich verder tot aan haar dood in 1799 aan armenzorg en religieuze studies.

URL's

www-groups.dcs.st-and.ae.uk/~history/Java/Witch.html



De heks van Agnesi. Als je de stippellijn door O laat ronddraaien en A op ℓ en B op de cirkel laat meebewegen, dan snijden de vertikale stippellijn door A en de horizontale stippellijn door B elkaar in een punt P op de kromme.

Dag en nacht wandelen spinnen over World Wide Web op zoek naar documenten. Zodra ze een prooi bemachtigen, slepen ze die mee naar huis en ontleden die in losse woorden en plaatjes. Waarom doen die spinnen dat? Waar komen ze vandaan?

Spinnen op het Web

Leendert van Gastel

Een spin is een klein programma dat contact kan maken met Web-servers en daar documenten van opvraagt. Als zo'n document hyperlinks naar andere documenten bevat, worden die ook opgevraagd. Het maakt daarbij geen verschil of die andere documenten op dezelfde Web-server staan of op een andere. Web-sites zijn voortdurend aan verandering onderhevig, dus moeten deze regelmatig opnieuw bezocht worden. In de praktijk zijn er altijd spinnen bezig, met name als het in Amerika nacht is.

Zoekmachines

Spinnen werken alleen in opdracht. Zij worden erop uitgestuurd om informatie op te halen, bijvoorbeeld voor zoekmachines. Bekende zoekmachines zijn Yahoo, Infoseek en Altavista. Deze bieden je de mogelijkheid om een woord op te geven, waarmee ze voor jou een lijst maken met alle documenten op het Web die dit woord bevatten. Zo hebben we in een eerder nummer met succes op het woord Pythagoras gezocht. Zoekmachines geven onmiddellijk antwoord. Het is dus niet zo dat pas als je een trefwoord opgeeft, er een spin op uitgestuurd wordt om alle documenten af te lopen. Er zijn nu naar schatting zo'n 80 miljoen algemeen toegankelijke Web documenten op zo'n 300.000 Web servers. Als het zoeken van een woord in een document gemiddeld 0,1 seconde zou duren, zit je al snel op een responstijd van drie maanden. Alle Web-documenten worden regelmatig door spinnen bezocht. De resultaten van hun rooftochten worden verwerkt in databases. In zo'n database vind je alle woorden samen met een URL (Internetadres) waar dat woord voorkomt. Alle woorden worden zo verwerkt, behalve lidwoorden en dergelijke. Dit zijn geen kinderachtige databases, miljarden van zulke combinaties van woorden en adressen zijn er in opgeslagen. Om het zoeken toch redelijk snel te laten verlopen, is zo'n database voorzien van een *index*. Dit is een lijst waarin de paren gerangschikt zijn op alfabetische volgorde van het woord. Net zoals wij in een woordenboek snel kunnen zoeken, kan zo'n database met die index snel bij een woord de desbetreffende URL's vinden. Op deze manier is een snelle responstijd van een zoekmachine mogelijk. Desalniettemin worden zeer krachtige computers ingezet

voor die zoekmachines. Sommige zoekmachines werken bovendien alleen voor documenten waarvan de web-site is aangemeld. Wie deze gratis toegankelijke machines betaalt? Op zoekmachines zie je altijd Internet-advertenties en de adverteerders betalen daarvoor. De Gouden Gids hanteert dezelfde formule.

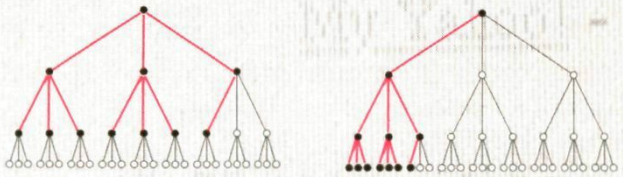
Stropers

Spinnen voorzien zoekmachines dus van materiaal. Maar spinnen hebben meer toepassingen. Off-line browsers zijn webbrowsers waarmee je kunt werken zonder dat je op dat moment een Internetverbinding hebt. Je geeft van te voren zo'n browser een plek op waarin je geïnteresseerd bent. Een spin zal voor jou alle hyperlinks volgen en alvast documenten ophalen. Later kun je dan op je gemak en zonder verbinding deze documenten bekijken. Als je zelf de telefoonrekening moet betalen kan zo'n off-line browser je vele guldens besparen, met name als je de spin zijn werk 's nachts laat doen. Sommige Internet-gebruikers willen graag collecties van plaatjes of van video-beelden aanleggen. Je kunt dan een spin op pad sturen die alleen documenten van een bepaald type ophaalt, zoals gif-plaatjes. Dit soort spinnen zijn echte stropers.

Hoe zoekt een spin?

Het is duidelijk dat spinnen een bepaalde strategie moeten hebben op het Web te zoeken. Anders verdwaalt de spin net zo als een argeloze Web-surfer die zo maar wat hyperlinks aanklikt. Voor het bepalen van zo'n zoekstrategie kunnen we alle Web-documenten wiskundig voorstellen door een graaf: de documenten zijn de knopen en de hyperlinks zijn de verbindingen daartussen. Voor alle strategieën geldt dat bijgehouden moet worden welke knopen reeds bezocht zijn om dubbel werk of het rondlopen in cirkels te voorkomen. Een spin krijgt altijd een startpunt mee, vaak een homepage van een Web-site. Er zijn twee standaard zoekstrategieën:

- *Zoeken in de breedte.* Ga vanuit een startpunt na welke knopen er zijn, die hebben afstand 1. Houd ondertussen bij welke nieuwe knopen je tegenkomt, die hebben afstand 2. Zodra alle knopen van afstand 1 geweest zijn, komen die van afstand 2 aan de beurt. Enzovoort.
- *Zoeken in de diepte.* Ga vanuit een startpunt naar de eerste knoop op afstand 1. Als deze een link naar een nieuwe knoop bevat, ga naar die knoop. Zo niet, ga een stap terug en naar de tweede knoop vanuit het startpunt. Vanuit een knoop gaan we dus eerst de diepte in en keren daarna pas op onze schreden terug naar een eerder alternatief. Bij Internet-spinnen zien we over het algemeen de eerste aanpak. Met dien verstande dat vaak eerst een hele Web-site of een deelboom afgezocht wordt voordat naar een andere Web-site wordt overgegaan. Deze andere Web-sites worden ook weer op dezelfde manier afgelopen.



Figuur 1: Twee verschillende zoekstrategieën: 'breedte-eerst' (links) en diepte-eerst (rechts)

Middelen tegen spinnen

Niet overal zijn spinnen welkom. Op een Web-site kan een bestand `robots.txt` neergezet worden waarin aangegeven staat op welke plekken spinnen (ook wel robots genoemd) niet horen te komen. Dat de spinnen zich hieraan houden, is een kwestie van etiquette, er is geen mogelijkheid om dit af te dwingen. Andere documenten waar spinnen niet bij kunnen komen zijn diegene die pas opgestuurd worden als een formulier wordt ingevuld. Er is dus geen normale link naar zo'n document. Dit geldt nog sterker voor dynamische documenten, die pas opgesteld worden op het moment van het verzoek van de browser, vaak aan de hand van gegevens van de aanvrager.

Je eigen spinnen

Voor het geval dat je zelf eens wat spinnen aan het werk wil zetten, hebben we Internet Marauder uitgetest (marauder is Engels voor plunderaar). Het is een shareware programma voor Windows 95. Je kunt het bijvoorbeeld krijgen bij www.shareware.com (zoek op `Marauder`). Een aardige off-line browser is NetBrief Light (zoek op `nbl32`). Internet Marauder kent aan de verschillende zoekstrategieën persoonlijkheden toe: 'Atilla de Hun' volgt alleen hyperlinks binnen een deelboom van de directorystructuur van de web-site, maar is hierbij zeer vasthoudend. Als een document de eerste keer niet goed doorkomt, dan vraagt hij het opnieuw en opnieuw. 'Napoleon' is meer voor de grote lijn: een hele web-site gaat hij af, echter minder vasthoudend. Spinnen volgen in het algemeen alleen hyperlinks binnende start-site. Desalniettemin kunnen ze een behoorlijke netwerkbelasting geven. Napoleon had voor de auteur binnen een half uur zo'n vierduizend bestanden van de Pythagoras homepage afgehaald. Met het hele Internet zou deze stroper meer dan een heel jaar bezig zijn.

URL's

www.yahoo.com
www.infoseek.com
www.altavista.digital.com
www.shareware.com

Internet-jargon

Web-browser Het computerprogramma waarmee je over het Web 'surft'.

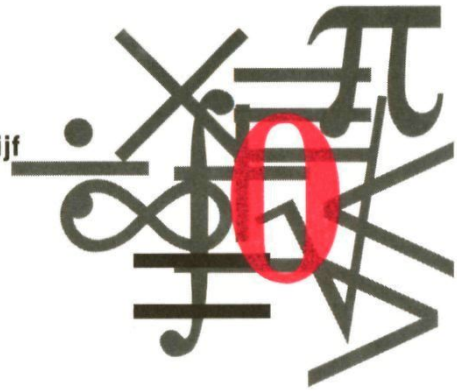
Web-site Een stel bij elkaar horende Web-documenten over één bepaald onderwerp

Web-server Een computer die voor de verbinding met het Internet zorgt.

Hyperlink Een verwijzing naar een ander document met een tekst of plaatje. Door erop te klikken surf je naar dit document.

URL Het Internetadres van een Web-document.

Een symbool voor 'niets' lijkt niet erg veel om het lijf te hebben. Maar zonder de nul zou het leven een stuk lastiger zijn.



Nul

Klaas Pieter Hart

Stel je eens voor dat je met het leger van Alexander de Grote naar het oude Babylon getrokken bent. Je loopt door de straten van de oude stad en hoort twee Babyloniërs ruzie maken over geld. De één beweert bij hoog en bij laag dat de ander hem nog eenenzestig goudstukken moet betalen; de ander vindt dat hij er maar twee hoeft te betalen. Je gaat er bij staan en je ziet de rekening: 𒁹𒁹goudstukken. Je denkt misschien dat daar twee goudstukken gevraagd worden, maar de ontvanger legt je uit dat de Babyloniërs met een zestigtallig stelsel werken en dat de 𒁹 voor één staat en de 𒁹 (die wat groter is) voor zestig. Als je opmerkt dat dat niet zo handig is omdat het lastig is met de hand elke 𒁹 even groot te houden, vraagt je nieuwe kennis of je een beter idee hebt. Je stelt hem voor om wat ruimte tussen de 'cijfers' open te laten zodat duidelijk te zien is dat de 𒁹 en 𒁹 niet samen als twee fungeren. Nu weten de Babyloniërs dat je echt van ver komt want die ruimte gebruiken ze al om machten van zestig over te slaan: 𒁹𒁹 staat namelijk voor $60^2 + 1 = 3601$. "Misschien wordt het tijd dat jullie daar een apart tekentje voor bedenken," zeg je dan, "dan zijn jullie van alle problemen af." Dat vinden je nieuwe vrienden niet eens zo'n slecht idee en na een tijdje gaan ze 𒌋 gebruiken om 'machten over te slaan': 𒁹𒁹 is twee; 𒁹𒁹 is eenenzestig en 𒁹𒌋𒁹 is zesendertighonderd-en-een.

Wat we hiervoor beschreven hebben is de uitvinding van een nieuw Babylonisch cijfer: de nul. Maar deze ontdekking ge-

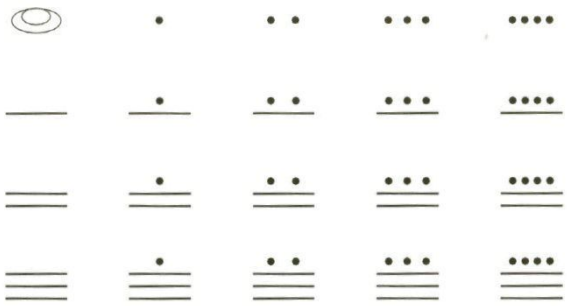
beurde relatief laat; de Babyloniërs hebben duizenden jaren gerekend zonder een teken voor de nul te gebruiken. Ook daarna nog gebruikten de Babyloniërs vreemd genoeg het ‹-teken niet aan het eind van hun getallen, uit de context van het document moest blijken of met ▼ één, zestig of zesendertighonderd bedoeld werd.
Uit het verhaaltje blijkt dat de Babyloniërs een positionele schrijfwijze voor hun getallen hanteerden: de plaats van een cijfer in een getal was van belang voor de grootte van dat getal. Dit in tegenstelling tot bijvoorbeeld het Egyptische systeem waarin voor elke macht van tien een andere hiëroglief gebruikt werd — het symbool voor miljoen was bijvoorbeeld een mannetje dat vol verbazing z'n armen ten hemel heft. Door herhaling van deze symbolen werd dan een getal weergegeven: drie mannetjes voor drie miljoen.

In zo'n systeem is geen nul nodig en de volgorde van de symbolen doet er ook niet toe; door gewoon te tellen weet je welk getal bedoeld wordt.

Onze cijfers worden vaak Arabisch genoemd. Dat zou Hindoe-Arabisch moeten zijn, want die cijfers komen via de Arabieren uit het tegenwoordige India. De Hindoes gebruikten net als de Babyloniërs een positionele schrijfwijze. In het begin hadden ze negen cijfers; ze lieten een plaats open om een macht van tien aan te geven. Zo rond de 7e eeuw voor Christus gingen ze een puntje op die lege plek zetten en dat puntje heette sunya wat 'leeg' betekent. In het Arabisch werd dat cifr en dat werd in het Italiaans 'zero' (nul) en 'ziffero' (cijfer). Het puntje werd langzamerhand een rondje en zo zijn we aan ons symbool voor nul gekomen.
Overigens hebben de Hindoes als eersten 'nul' als een getal beschouwd waar je gewoon mee kunt rekenen en dat verklaart weer ons woord voor dat getal: nul komt van het Latijnse 'nullus' dat 'geen enkele' betekent. ◢

De Maya's

Aan de andere kant van de wereld, in Zuid-Amerika, ontwikkelden de Maya's ook een positioneel getallenstelsel met twintig cijfers, waaronder een nul. Hun nul lijkt erg veel op onze nul: ⬭. Hier is een tabel van de twintig Maya-cijfers:

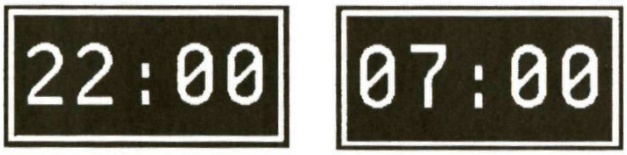


Het merkwaardige van het getallenstelsel van de Maya's was het feit dat .⬭⬭ niet voor 400 stond maar voor 18 ×20 = 360. De reden was dat het Maya-jaar 360 dagen had (plus nog 5 'slechte' dagen en op deze manier werd het aantal dagen in het jaar een mooi rond getal.

Voor het cryptosysteem dat we in de latere artikelen gaan behandelen, moeten we de grootste gemene deler van zeer grote getallen kunnen berekenen. Dit kan met een snelle methode die al bij de oude Grieken bekend was.

Delen met

Met de trein duurt de reis van Amsterdam naar Berlijn 9 uur. Wie om 22 uur uit Amsterdam vertrekt komt niet om 31 uur in Berlijn aan maar om $31 - 24 = 7$ uur. Voor de klok zijn 31 en 7 hetzelfde.



Algemener zijn twee getallen voor de klok gelijk als ze een veelvoud van 24 van elkaar verschillen. We noteren dit met drie streepjes als volgt:

$$31 \equiv 7 \bmod 24.$$

We zeggen dat 31 en 7 congruent zijn modulo 24. Het congruentieteken $\equiv$ is 200 jaar geleden al door Gauss bedacht. Met de klokgetallen 0 tot en met 23 kun je rekenen zoals met gewone gehele getallen. Je telt ze op als gewone getallen, en als de som 24 of meer is trek je er 24 af om onder de 24 te raken. Bijvoorbeeld:

$$22 + 9 \equiv 7 \bmod 24.$$

Je kunt ook vermenigvuldigen. Als de klok 0 uur aangeeft en je 11 keer achter elkaar de klok 15 uur doordraait ben je 165 uur verder. Trek daar 6 keer 24 vanaf en je houdt 21 over. Dit betekent dat de klok op 21 uur staat. Dus:

$$11 \cdot 15 \equiv 21 \bmod 24.$$

In plaats van 24 kunnen we natuurlijk elk ander getal n nemen. Net als bij 24 werken we dan nog alleen maar met de getallen $0, 1, \ldots, n-1$. Je hebt als het ware dan een klok met postities van 0 tot en met $n-1$, na de $n-1$ komt weer de 0. De getallen $0, 1, 2, \ldots, n-1$ modulo n kun je optellen en vermenigvuldigen zoals bij het 'klokrekenen' modulo 24. Dit heet 'rekenen modulo n'.

De negenproef

De rest van een getal modulo 9 kan je snel bepalen door de cijfers op te tellen. Immers, alle machten van 10 hebben rest 1 bij deling door 9. Daarom is het getal $1001 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4$ congruent met $1 + 2 + 3 + 4 = 10$ modulo 9. Om de vermenigvuldiging $1001 \cdot 858 = 7005652$ te controleren kan men snel even 'modulo 9 kijken'.
We hebben $858 \equiv 5 + 6 + 7 + 8 = 26 \equiv 8 \bmod 9$ en $7005652 \equiv 7 + 5 + 6 + 5 = 25 \equiv 7 \bmod 9$. Wegens $1 \cdot 8 \not\equiv 7 \bmod 9$ hebben we ons kennelijk in het antwoord vergist: de linkerkant heeft rest 8 bij deling door 9, en de rechterkant rest 7.

rest°

Vergelijkingen modulo n

Het oplossen van vergelijkingen modulo n gaat een beetje anders dan wat je gewend bent. Op school leer je hoe je eenvoudige vergelijkingen als

$$12x = 0, \quad 12x = 1 \quad \text{en} \quad x^2 = 1$$

moet oplossen. In de eerste twee vergelijkingen deel je door 12 en vind je $x = 0$ en $x = \frac{1}{12}$. In het tweede geval schrijf je $x^2 - 1 = 0$ als $(x+1)(x-1) = 0$ en vind je de oplossingen $x = -1$ en $x = 1$. Laten we deze vergelijkingen nu eens modulo 24 proberen op te lossen. De eerste vergelijking wordt

$$12x \equiv 0 \bmod 24.$$

Als je in $12x$ de getallen 0, 1, 2, $\cdots$, 23 voor x invult, krijg je modulo 24 de getallen 0, 12, 0, 12, enzovoort: afwisselend 0 en 12. Van de 24 getallen modulo 24 geven er dus twaalf een oplossing van de vergelijking $12x \equiv 0$. In plaats van één oplossing vinden we er nu twaalf! Bovendien geeft geen enkele x een oplossing voor de vergelijking $12x \equiv 1 \bmod 24$. De vergelijking $x^2 - 1 \equiv 0 \bmod 24$ kun je ook door te proberen oplossen. Je ziet dan dat de getallen 1, 5, 7, 11, 13, 17, 19 en 23 allemaal oplossingen zijn. In plaats van twee oplossingen vinden we er nu acht. Je kunt vergelijkingen modulo n dus niet oplossen door ze eerst 'gewoon' op te lossen en dan het antwoord modulo n te nemen.

Inversen modulo n

In de cryptografische toepassingen die we in Pythagoras nr. 5 gaan behandelen moeten wij de vergelijking

$$ax \equiv 1 \bmod n$$

voor grote waarden van a en n oplossen. Zo'n x heet de inverse van a modulo n. Je moet hierbij denken aan getallen van zo'n tweehonderd cijfers. Anders dan voor $n = 24$ kunnen we dan niet meer alle mogelijkheden proberen, dat zou langer duren dan de leeftijd van het universum. De volgende stelling zegt wanneer er oplossingen zijn: dit hangt af van de grootste gemene deler d van a en n, dat is het grootste getal dat zowel a als n deelt. Notatie: $d = \text{ggd}(a, n)$.

STELLING. Als $d > 1$ dan heeft de vergelijking $ax \equiv 1 \bmod n$ geen oplossingen. Als $d = 1$, dan heeft de vergelijking $ax \equiv 1 \bmod n$ precies één oplossing.

Wat is er aan de hand als d groter dan 1 is? Dan n is een d-voud: $n = kd$. Maar ook a is een d-voud en dus neemt ax modulo n één van de waarden $d, 2d, \ldots, kd$ aan. Omdat $d > 1$ is geen van die waarden gelijk aan 1 en dus heeft de vergelijking $ax \equiv 1 \bmod n$ dan geen oplossingen.
In het voorbeeld $12x \equiv 1 \bmod 24$ hadden we $\text{ggd}(12, 24) = 12$. Inderdaad waren er geen oplossingen. Om de oplossing te vinden als $d = 1$ moeten we eerst wat meer weten over de ggd.

De Euclidische algoritme

De grootste gemene deler van twee getallen kun je berekenen door die getallen te ontbinden (zie Pythagoras nr. 1). Bijvoorbeeld: $60 = 2^2 \cdot 3 \cdot 5$ en $75 = 3 \cdot 5^2$, zodat

$$\text{ggd}(60, 75) = 3 \cdot 5.$$

Maar voor grotere getallen is het vinden van de ontbindingen een lastig karwei. Er is echter een snellere methode die altijd werkt. Als voorbeeld nemen we de getallen 1001 en 85. De ggd van 1001 en 85 is een deler van hun verschil 916, maar ook van $1001 - 2 \cdot 85 = 831$, van $1001 - 3 \cdot 85 = 746$ en zo verder. Door 85 net zo lang van 1001 af te trekken tot dat niet meer kan zonder negatieve uitkomst, krijg je de *rest* van 1001 bij deling door 85. Als je 85 op 1001 deelt gaat dat 11 keer, en je houdt 66 over: $1001 = 11 \cdot 85 + 66$. We zagen dat ieder getal dat zowel 1001 als 85 deelt, ook de rest $66 = 1001 - 11 \cdot 85$ deelt. Andersom zie je gemakkelijk dat iedere gemeenschappelijke deler van 85 en 66 ook een deler is van $66 + 11 \cdot 85 = 1001$. De paren $(1001, 85)$ en $(85, 66)$ hebben dus precies dezelfde gemeenschappelijk delers. De grootste hiervan is de ggd en dus zien we

$$\text{ggd}(1001, 85) = \text{ggd}(85, 66).$$

In een ggd-berekening mogen we kennelijk steeds het eerste getal vervangen door zijn rest bij deling door het tweede getal. Als we zorgen dat het eerste getal het grootste van de twee is betekent dit dat we ons ggd-probleem door een eenvoudiger ggd-probleem kunnen vervangen. De methode om de grootste gemene deler niet via ontbindingen maar door herhaalddeling met rest nemen te bepalen heet de *Euclidische algoritme*.

VOORBEELD. Voor 1001 en 85 vinden we achtereenvolgens dat $\text{ggd}(1001, 85)$ gelijk is aan $\text{ggd}(85, 66)$, aan $\text{ggd}(66, 19)$ en zoverder. Als we alle delingen netjes onder elkaar opschrijven krijgen we:

$$\begin{aligned}
1001 - 11 \cdot 85 &= 66 \\
85 - 1 \cdot 66 &= 19 \\
66 - 3 \cdot 19 &= 9 \\
19 - 2 \cdot 9 &= 1 \\
9 - 9 \cdot 1 &= 0.
\end{aligned}$$

In de laatste deling wordt de rest 0, en daar kunnen we niet verder door delen. We vinden dus dat $\text{ggd}(1001, 85)$ gelijk is $\text{ggd}(1, 0) = 1$. Het voordeel van Euclides' methode is dat er nooit een getal ontbonden hoeft te worden. Hij is daarom voor de meeste getallen veel sneller dan de methode via ontbindingen. Een ander voordeel van de methode is dat je daarmee de ggd van a en b uit kunt drukken in a en b. Dit gaat als volgt met de uitgebreide Euclidische algoritme.

$$\begin{aligned}
0 \cdot 1001 + 1 \cdot 85 &= 85 \\
1 \cdot 1001 - 11 \cdot 85 &= 66 \\
-1 \cdot 1001 + 12 \cdot 85 &= 19 \\
4 \cdot 1001 - 47 \cdot 85 &= 9 \\
-9 \cdot 1001 + 106 \cdot 85 &= 1
\end{aligned}$$

Hier is de eerste vergelijking een 'flauwe vergelijking', de tweede de gewone deling met rest voor 1001 en 85. In de volgende stap doe je niet alleen deling met rest voor 85 en 66 (gaat 1 keer, rest 19), maar trek je de hele tweede vergelijking 1 keer van de eerste af.

CONCLUSIE. Voor ieder tweetal getallen a en b bestaan er gehele getallen x en y die voldoen aan $xa + yb = \text{ggd}(a, b)$. [Anders dan a en b zijn de getallen x en y niet allebei positief.]

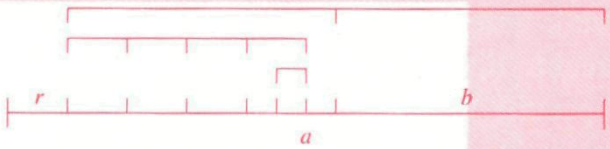
Besluit

We keren terug naar onze vergelijking $ax \equiv 1 \bmod n$. Volgens de stelling is er precies één oplossing als $\text{ggd}(a, n) = 1$. Deze oplossing vind je, net als de ggd zelf, met de Euclidische algoritme. Immers, om een vergelijking als $85x \equiv 1 \bmod 1001$ op te lossen is het voldoende om een geheel getal x te vinden waarvoor $85x + 1001y = 1$ geldt. Modulo 1001 staat hier namelijk niets anders dan $85x \equiv 1$. Zo'n getal vonden we al: $x = 106$. Het getal 106 is dus de inverse van 85 modulo 1001.

OPGAVE. Bereken de inverse van 1997 modulo 1000. Heeft 15 een inverse modulo 1000?

De ggd bij Euclides

In de Griekse wiskunde werden getallen als lengtes van lijnstukken gezien. De rest r van a bij deling door b is dan wat er overblijft als je b net zo vaak afpast op a als mogelijk is. In de Euclidische algoritme passen we vervolgens deze rest weer een geheel aantal keren op b af, en we gaan zo door tot we uiteindelijk een keer rest 0 krijgen. De rest waarmee de deling precies opging is dan de ggd van a en b. Dit is het grootste lijnstuk dat een geheel aantal keren in zowel a als b past, en dus de grootste 'gemeenschappelijke maat' van a en b.



De Grieken ontdekten tot hun verbazing dat in veel 'meetkundige situaties', bijvoorbeeld wanneer a de diagonaal van een vierkant met zijden b is, er *geen enkel* lijnstuk bestaat dat een geheel aantal keren in zowel a als b past. Begrijp je waarom?

De priemeigenschap

Hoe bewijs je dat als een priemgetal p een produkt van twee getallen ab deelt, hij tenminste één van de getallen deelt? Stel maar dat p geen deler van b is. Dan geldt $\text{ggd}(b, p) = 1$,dus er bestaan gehele getallen x en y met $xb + yp = 1$. Vermenigvuldiging met a geeft $xab + yap = a$. Omdat p zowel xab (een veelvoud van ab) als yap deelt, deelt hij nu ook a: einde bewijs.

Kun jij de onderstaande opgaven oplossen? Stuur dan je oplossing naar het onderstaande adres en maak kans op een boekenbon van 25 gulden!

Pythagoras

Opgave 29
Hoeveel deelverzamelingen van de verzameling $\{1, 2, \ldots, 1997\}$ hebben een even aantal elementen?

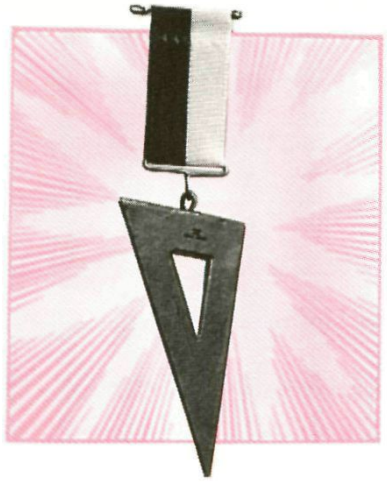
Opgave 30
Suzanne heeft in het vlak een vierkant getekend. Ook heeft zij een punt in het vlak gezet met onzichtbare inkt. Jij mag rechte lijnen trekken en Suzanne (die een speciale bril op heeft) vertelt je dan aan welke kant van de lijn het punt ligt (of op de lijn). Hoeveel vragen heb je nodig om uit te zoeken of het punt binnen, buiten of op het vierkant ligt? [Let op: Als je denkt dat er 18 vragen nodig zijn moet je bewijzen dat je met 18 vragen er altijd uit komt, maar ook dat het met 17 vragen niet altijd lukt.]

Winnaars 1996-1997
De Pythagoras Olympiade van de jaargang 1996-1997 heeft twee winnaars opgeleverd: Jeanine Daems van het **Bouwens van der Boijecollege** te Panningen en Gertjan Kok van het **Sint-Maartens college** te Voorburg. Zij ontvangen beide een boekenbon van 100,-. Bovendien heeft Jeanine op deze manier toegang gekregen tot de tweede ronde van de Nederlandse Wiskunde Olympiade.

Stuur je oplossing naar:

Pythagoras Olympiade
TU Eindhoven
Faculteit Wiskunde
Hoofdgebouw kamer 9.50
Postbus 513
5600 MB Eindhoven
email: sander@win.tue.nl

Vermeld bij de oplossing je *naam, adres, school en klas*. Stuur bij de antwoorden ook een toelichting, waarin uitgelegd wordt hoe je aan het antwoord gekomen bent (een berekening of een bewijs). Insturen is mogelijk tot en met 5 januari 1998. Onder de inzenders van goede oplossingen wordt per opgave een boekenbon van 25 gulden verloot. De oplossingen van deze opgaven verschijnen te zijner tijd op de homepage en in het aprilnummer van Pythagoras. Op de volgende bladzijde staan de oplossingen van opgave 25 en 26 uit het augustusnummer.



Olympiade

Opgave 25

Op elke strippenkaart staat een getal van 6 cijfers (van 000000 tot en met 999999). Als de som van de eerste drie cijfers gelijk is aan de som van de laatste drie cijfers, dan heb je mazzel en krijg je drie kwartjes korting op de strippenkaart. Bewijs dat het aantal 'mazzelstrippenkaarten' gelijk is aan het aantal strippenkaarten waarvan de som van de cijfers 27 is.

OPLOSSING. Noem een strippenkaart waarvan de som van de cijfers 27 is, een 27-strippenkaart. We laten zien dat we bij elke mazzelstrippenkaart een andere 27-strippenkaart kunnen maken. Als de zes cijfers op een mazzelstrippenkaart a, b, c, d, e, en f zijn, geldt $a+b+c=d+e+f$, dus geldt $(9-a)+(9-b)+(9-c)+d+e+f=27$. We kunnen een 27-strippenkaart maken met de cijfers $(9-a)$, $(9-b)$, $(9-c)$, d, e en f. Als je dit andersom doet, zie je dat je bij elke 27-strippenkaart een mazzel-strippenkaart hoort. Dus zijn er precies evenveel mazzelstrippenkaarten als er 27-strippenkaarten zijn.

Deze opgave werd opgelost door: Marianne van Putten van het **Lorentz-Casimir Lyceum** te Eindhoven, H. Verdonk uit 's Gravenhage, Jeanine Daems van het **Bouwens van der Boijecollege** te Panningen, Gertjan Kok van het **Sint-Maartenscollege** te Voorburg en David de Koet van het **Fons Vitæ Lyceum** te Amsterdam. De boekenbon gaat naar David de Koet.

Opgave 26

Gegeven zijn 32 stenen die allemaal een ander gewicht hebben. Laat zien dat 35 keer wegen met een balans voldoende is om de zwaarste en de een-na-zwaarste steen te vinden. Je mag geen andere gewichten gebruiken, alleen de 32 stenen.

OPLOSSING. We gaan in een 'toernooi' van 5 rondes de zwaarste steen bepalen. In de eerste ronde wegen we 16 keer twee stenen tegen elkaar. De 16 'winnaars' gaan naar de volgende ronde, dan wegen we 8 keer twee stenen tegen elkaar. De winnaars gaan weer door naar de volgende ronde. Dit doen we tot er maar een steen overblijft. We hebben dan $16+8+4+2+1=31$ wegingen gedaan. Nu moeten we nog de een na zwaarste steen vinden. Ergens in het toernooi is die steen 'uitgeschakeld' en dat kan alleen door de zwaarste steen gebeurd zijn. We hoeven dus alleen nog maar de zwaarste steen te vinden van de 5 stenen, die bij een weging lichter bleken dan de steen die uiteindelijk de zwaarste bleek te zijn. Dat kan in 4 wegingen door bij elke weging tussen twee stenen de lichtste weg te gooien. Dan blijft precies de zwaarste van de 5 stenen over.

Deze opgave werd opgelost door: Marianne van Putten van het **Lorentz-Casimir Lyceum** te Eindhoven, H. Verdonk uit 's Gravenhage, Menno Dobber van **De Meergronden** te Almere, Gertjan Kok van het **Sint-Maartenscollege** te Voorburg en David de Koet van het **Fons Vitæ Lyceum** te Amsterdam. De boekenbon gaat naar Marianne van Putten.

Het getal π heeft op Internet talrijke fans. Allemaal worden ze geobsedeerd door de willekeurigheid van de decimalen in het getal 3.14159265358979323846264338327950288\ldots

De

Jaap Top en Chris Zaal

Op Internet kan iedereen vrijelijk informatie neerzetten. Maar wat beweegt iemand om dat te doen? Waarom zet iemand zijn hele CD-collectie op Internet? De verbazing over al dit soort nutteloze informatie bracht Paul Philips er toe om de 'Useless Pages' te maken. Hij licht toe: "Nutteloos betekent niet slecht gemaakt of zonder enige waarde, maar dat er geen reden is om deze dingen op het Net te zetten". Voorbeelden: 'Driveways of the Rich & Famous' (foto's van opritten van huizen van vele beroemdheden) en de 'Guide to sleeping in airports'. Maar ook de 'Uselessness of Pi and friends'. En inderdaad, het is verbazend hoeveel informatie er over het getal π te vinden is. Bijvoorbeeld over de decimale ontwikkeling van π. Je rekenmachine geeft voor π de waarde 3.14159265, maar π is tot op vele miljoenen decimalen berekend. Het huidige record is van het Japanse Kanada laboratorium met 51.539.600.000 decimalen. Iedereen kan daar de eerste 200 miljoendecimalen van π downloaden (215 Mb). Maar er zijn vele tientallen andere sites waar je eveneens de decimale ontwikkelingvan π kunt vinden. Tot overmaat van ramp is niet alle informatie foutloos. Volgens de UCLA is de 15094ste decimaal van π gelijk aan 4, terwijl deze volgens alle andere sites 3 is.

De decimalen van π

Om de decimalen van π te berekenen zijn er verschillende methoden. Elke decimaal van π kun je in principe berekenen. Maar dat de decimalen berekenbaar zijn wil nog niet zeggen dat er een gemakkelijk te achterhalen regelmaat in zit. In de decimale ontwikkeling van π valt geen patroon te bekennen. Deze willekeur in de decimale ontwikkeling van π is wat veel mensen intrigeert. Op Internet zijn er allerlei sites waarop de decimale ontwikkeling van π op de een of andere manier bestudeerd wordt. Zo is er de 'Pi-search' site. Hier kun je een aantal cijfers intikken. Als antwoord krijg je de eerste plaats in de decimale ontwikkeling van π waar dat rijtje cijfers voorkomt. Indien gewenst ook de tweede plaats, enzovoort. Probeer het maar eens met je geboortedatum: www.aros.net/~angio/pistuff/piquery.html De decimale ontwikkeling van π is zo willekeurig dat wiskundigen geloven dat de decimale ontwikkeling van π niet te onderscheiden is van een willekeurige rij cijfers. Een eindig rijtje cijfers komt op den duur even vaak in π voor als dat je zou verwachten in een willekeurige rij. Zeker weten doen we dit niet, want niemand heeft dit tot nu toe kunnen bewijzen.

π onthouden

Het onthouden van de eerste zoveel decimalen van π is een sport op zich. Maar

magie van π

in ons computertijdperk is dit een nogal nutteloze bezigheid geworden. Tegenwoordig tover je met een simpele druk op de knop vele duizenden decimalen op je scherm tevoorschijn. Op de Useless Pages over π vind je verschillende π-clubs. De leden van de 1000-club beweren 1000 decimalen van π uit hun hoofd te kennen. Maar als bewijs hoeven ze slechts duizend of meer decimalen per email op te sturen. De tegenhanger van de 1000-club is de -2club, die bestaat uit mensen die beweren niet eens twee decimalen van π te kunnen onthouden! Als je lid wil worden van zo'n π-club, dan kan de volgende zin je op weg helpen (tel de letters in de woorden).

How I want a drink, alcoholic of course, after the heavy lectures involving quantum mechanics!

De vrienden van π

In de Useless Pages over π kom je behalve π ook andere getallen tegen. Zo vind je $\sqrt{2}$ in een miljoen decimalen, maar ook de eerste 500.000 decimalen van $\sqrt{4}$. Ook de getallen 17, 23, 27, 37, 42, 47 en 69 blijken elk een eigen fanclub te hebben.

Computeralgebra$^{\circ\circ}$

Het moderne equivalent van de zakrekenmachine is de grafische rekenmachine. Nog geavanceerder zijn computeralgebra pakketten. Dit zijn grote computerprogramma's waarmee vele ingewikkelde wiskundige berekeningen een fluitje van een cent worden. Bekende pakketten zijn Derive, Mathematica en Maple. In zulke programma's zitten een paar duizend decimalen van π voorgeprogrammeerd. Maar ook meer decimalen zijn geen probleem, deze worden desgevraagd ter plekke berekend. Het getal π komt voor in veel formules, maar duikt soms ook onverwacht op in berekingen. We geven een voorbeeld van een berekening met Maple waarbij π opeens om de hoek komt kijken. We bekijken op het interval $[0, 1]$ de functies

$$f_n(x) = \frac{4 + x^{4n}(1-x)^4}{x^2+1}.$$

Voor elke waarde van $n = 1, 2, 3, \ldots$ staat hier een andere functie. Met Maple kun je de grafiek van deze functies eenvoudig plotten, zie figuur 1. We berekenen de oppervlakte onder de grafieken. Dit zijn integralen die Maple voor ons berekent. Voor $n = 1, 2, 3, 4, 5$ krijgen we achtereenvolgens

$$\tfrac{22}{7} = 3.14285714\ldots$$

$$\tfrac{10886}{3465} = 3.14170274\ldots$$

$$\tfrac{141514}{45045} = 3.14161394\ldots$$

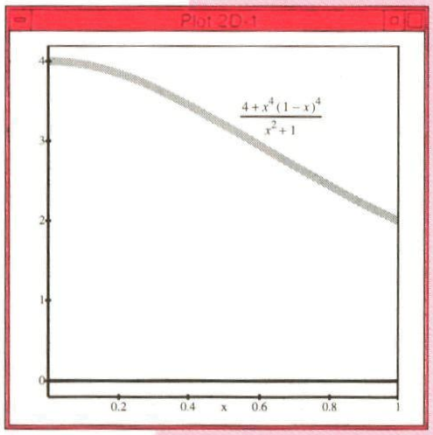
Het getal π

```
> evalf(Pi,215);
```

3.14159265358979323846264338327950288419716939937510582097494459230781640
6286208998628034825342117067982148086513282306647093844609550582231725359
4081284811174502841027019385211055596446229489549303819644288109756659

```
> f := x -> (4+x^(4*n)*(1-x)^4)/(x^2+1);
```

$$f := x \rightarrow \frac{4 + x^{(4\,n)}\,(1-x)^4}{x^2+1}$$




```
> for n from 1 to 5 do int(f(x),x=0..1) od;
```

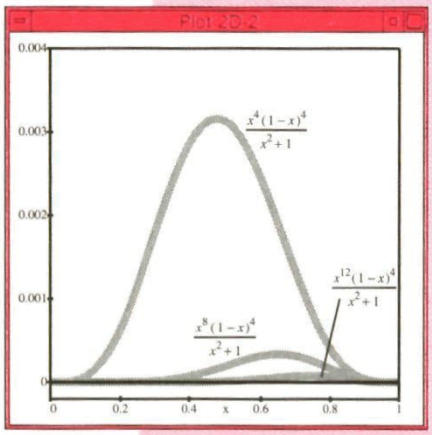
$$\frac{22}{7}$$

$$\frac{10886}{3465}$$

$$\frac{141514}{45045}$$

$$\frac{45708802}{14549535}$$

$$\frac{150185878}{805615}$$




```
> int(4/(x^2+1),x=0..1);
```

$$\pi$$

```
> for n from 1 to 5 do simplify(f(x)) od;
```

$$x^6 - 4\,x^5 + 5\,x^4 - 4\,x^2 + 4$$

$$x^{10} - 4\,x^9 + 5\,x^8 - 4\,x^6 + 4\,x^4 - 4\,x^2 + 4$$

$$x^{14} - 4\,x^{13} + 5\,x^{12} - 4\,x^{10} + 4\,x^8 - 4\,x^6 + 4\,x^4 - 4\,x^2 + 4$$

$$x^{18} - 4\,x^{17} + 5\,x^{16} - 4\,x^{14} + 4\,x^{12} - 4\,x^{10} + 4\,x^8 - 4\,x^6 + 4\,x^4 - 4\,x^2 + 4$$

$$x^{22} - 4\,x^{21} + 5\,x^{20} - 4\,x^{18} + 4\,x^{16} - 4\,x^{14} + 4\,x^{12} - 4\,x^{10} + 4\,x^8 - 4\,x^6 + 4\,x^4 - 4\,x^2 + 4$$

Figuur 1. Maple berekeningen en grafieken

$$\frac{45708802}{14549535} = 3.14159882\ldots$$

$$\frac{150185878}{47805615} = 3.14159493\ldots$$

Alle oppervlaktes zijn breuken die Maple kennelijk exact kan berekenen. Dat is verrassend, want er is geen reden om te denken dat de oppervlakte onder de grafiek een gewone breuk is. Je zou eigenlijk logaritmes verwachten.Een nog grotere verrassing is dat de eerste breuk $\frac{22}{7}$ een veelgebruikte benadering van π was in het tijdperk vóór de rekenmachine. Bovendien zijn de daaropvolgende breuken nog betere benaderingen van π. Hoe komt dit? Kunnen we op de een of andere manier verklaren waarom al deze breuken zo weinig van π verschillen? We gaan eens kijken.We splitsen $f_n(x)$ in twee stukken:

$$f_n(x) = \frac{4}{x^2+1} + \frac{x^{4n}(1-x)^4}{x^2+1}.$$

In het eerste stuk komt n niet meer voor, in het tweede wel. In figuur 1 is voor $n = 1, 2, 3$ ook de grafiek van het tweede stuk geplot. We zien dat de oppervlakte onder deze grafiek heel erg klein is vergeleken met de oppervlakte onder de grafiek van $f_n(x)$ (let op de schaalverdeling). Voor toenemende n wordt deze bovendien steeds kleiner. De oppervlakte die we berekend hebben is dus praktisch gelijk aan de oppervlakte onder de grafiek van $4/(x^2+1)$. Deze berekenen we met Maple. We typen in: `int(4/(1+x^2), x=0..1);` Als antwoord geeft Maple: π. Dat wil zeggen, volgens Maple is de integraal $\int_0^1 4/(x^2+1)\,dx$ exact gelijk aan π. Je kunt het antwoord zelf narekenen zodra je weet dat $1/(x^2+1)$ de afgeleide is van $\arctan(x)$:

$$\int_0^1 \frac{4}{x^2+1}\,dx = \left[4\arctan(\mathrm{x})\right]_0^1$$
$$= 4 \times \tfrac{1}{4}\pi = \pi.$$

Dit verklaart waarom onze uitkomsten allemaal benaderingen van π zijn. Blijft nog over de vraag waarom er uit de oppervlaktes onder de grafiekvan $f_n(x)$ steeds een breuk als antwoord komt. We proberen of Maple iets kan met de functie $f_n(x)$ door er het commando `simplify` op los te laten. Voor $n = 1$ krijgen we:

$$x^6 - 4x^5 + 5x^4 - 4x^2 + 4.$$

Ook voor grotere n blijkt $f_n(x)$ een veelterm te zijn (zie fgiuur 1). De noemer x^2+1 kan blijkbaar steeds weggedeeld worden. Zo'n veelterm kunnen we rechttoe-rechtaan integreren en de uitkomst van zo'n integraal is natuurlijk een breuk. Zo is de integraal van 0 tot 1 van de bovenstaande veelterm gelijk aan $17 - 46 + 55 - 43 + 4$, dus aan 227.

Je kunt zelf verder experimenteren door te zoeken naar functies $t(x)$ die klein zijn op het interval $[0, 1]$ en waarvoor $(4 + t(x))/(x^2+1)$ een veelterm is. Hiermee vind je dan benaderingen van π die breuken zijn. Wij gebruikten $t(x) = x^{4n}(1-x)^4$, dit gaf voor $n = 1$ de benadering $\frac{22}{7}$. Een andere bekende benadering van π is 355/113. Kun je een functie $t(x)$ vinden die deze benadering oplevert? We zijn benieuwd!

URL's

www.go2net.com/internet/useless
www.cc.u-tokyo.ac.jp/kenkai/kanada-lab

In honderdduizenden gezinnen, families, schoolklassen en sportclubs zijn weer lootjes getrokken voor de viering van Sinterklaas. Dat kan verschillende problemen geven: lootjes kunnen zoek raken of iemand kan zichzelf trekken.

Jan Brinkhuis en Erjen Lefeber

Twee S

Lootjes trekken voor Sinterklaas geeft elk jaar problemen. Ook dit jaar weer bij de familie Lootsma. Hun oudste zoon Pieter was wiskunde gaan studeren en kon wegens zijn tentamens de weken voor Sinterklaas niet thuiskomen. Hoe konden er nu lootjes getrokken worden? Mevrouw Lootsma belde haar oudste zoon op en vroeg hem om zijn verlanglijstje. Vervolgens riep ze de rest van het gezin bij elkaar. Iedereen deed zijn eigen verlanglijstje in een envelop en mevrouw Lootsma deed hetzelfde met Pieter's lijstje. Alle enveloppen, behalve die met Pieter's verlanglijstje werden op tafel gelegd en door elkaar geschud. Toen niemand meer wist welke envelop welk lijstje bevatte, pakte moeder er een envelop uit: die was voor Pieter. Omdat zijn lijstje apart gehouden werd, kon Pieter zichzelf niet getrokken hebben. Daarna werd de envelop met Pieters verlanglijstje bij de andere enveloppen gevoegd en werden de enveloppen weer flink door elkaar gehusseld. Vervolgens trok de rest van de familie een envelop en gelukkig trok niemand zichzelf. Mevrouw Lootsma was zeer tevreden. Ze kon die ene envelop naar Pieter sturen en iedereen kon beginnen aan de surprises. In haar enthousiasme stuurde mevrouw Lootsma de envelop echter naar het verkeerde adres. Omdat sommige familieleden al cadeautjes gekocht hadden, kon er niet opnieuw getrokken worden. Wat te doen? Weliswaar wist mevrouw Lootsma waar ze de envelop heen gestuurd had, maar die mensen waren voor een lange tijd op vakantie.

PROBLEEM NR. 1. Hoe kan mevrouw Lootsma er voor zorgen dat Pieter te weten komt wie hij heeft getrokken en wat het verlanglijstje van diegene is? De oplossing moet tot stand komen zonder hulp van buitenstaanders. Bovendien moet de verdeling van de lootjes geheim blijven; niemand mag door de oplossing extra informatie krijgen over wie wie heeft getrokken. Een oplossing van dit probleem kun je vinden op de homepage van Pythagoras.

Jezelf trekken

Zelfs als iedereen aanwezig is bij de trekking van de lootjes kan er van alles mis gaan. Want wat gebeurt er als iemand zichzelf trekt? Dan moet de trekking opnieuw. De kans dat zoiets gebeurt is vrij groot (zie inzet). Dit overkwam de familie Lootsma vorig jaar. Tot drie keer toe

interklaasproblemen

moest er opnieuw getrokken worden. Op het laatst werden er lootjes herkend aan de manier waarop ze gevouwen waren. Zoiets wil je natuurlijk liever voorkomen. Zou er geen oplossing te bedenken zijn voor dit probleem? Is het mogelijk om de trekking zo te organiseren dat niemand zichzelftrekt? Alexander Rinnooy Kan, lid van de Raad van Bestuur van de ING-Bank, stelde deze vraag zich ook. Menig ledig kwartiertje besteedde hij aan deze puzzel. Vorig jaar zag hij in Eclaire, een tijdschrift voor economen, een artikel van Fransje Akveld over het trekken van lootjes staan. Daarop legde hij de schrijfster per brief het volgende probleem voor.

PROBLEEM NR. 2. Kun je een manier bedenken om het lootjes trekken zo te organiseren dat niemand zichzelf trekt? Een correcte oplossing moet aan de volgende drie eisen voldoen:

1. Hulp van buitenstaanders is niet toegestaan.
2. Geen van de deelnemers mag aan het eind van de trekkinginformatie verkregen hebben over de uitslag.
3. De trekking moet voldoende snel zijn. Steeds opnieuw trekken is daarom niet toegestaan, want dat kan in principe eindeloos duren.

Jan Brinkhuis heeft twee oplossingen van dit probleem bedacht. Het zou teveel ruimte in beslag nemen om ze hier af te drukken. Je kunt ze vinden op de homepage van Pythagoras. Bij oplossingen van dit soort problemen kun je je altijd afvragen of ze de best mogelijke oplossingen zijn. Wie heeft een beter idee?

De kans dat je jezelf trekt

De kans dat tijdens het lootjes trekken iemand zichzelf trekt kun je berekenen door de mogelijkheden na te gaan. Met twee personen is het aantal mogelijkheden beperkt. Nummer 1 trekt 1 en nummer 2 trekt 2, of 1 trekt 2 en 2 trekt 1. Deze mogelijkheden kun je weergeven met: 12 en 21. De kans dat iemand zichzelf trekt is dus 12. Bij drie personen zijn er zes mogelijkheden: **123**, 21**3**, 31**2**, **1**3**2**, 2**3**1, 3**2**1. Vetgedrukt zijn de nummers die zichzelf getrokken hebben. De kans dat niemand zichzelf trekt is dus $\frac{2}{6}$. Bij 4 personen zijn 24 mogelijkheden, bij vijf al 120. In het algemeen zijn er voor n personen $n!$ mogelijkheden en de kans dat niemand zichzelf trekt is gelijk aan

$$\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} + \cdots + (-1)^n \frac{1}{n!}.$$

Als je n laat toenemen dan verandert vanaf $n = 6$ de kans bijna niet meer. Dat is toch verrassend! De kans dat een trekking in één keer goed gaat hangt dan nauwelijks van de groepsgrootte af en is praktisch gelijk aan $1/e = 0.36677\ldots$

Afgelopen zomer werd de wiskundige wereld verrast met twee records. In Amerika ontdekte het GIMPS-project een nieuw grootste priemgetal van 895.932 cijfers. In Amsterdam werd een getal van 180 cijfers ontbonden in twee priemfactoren.

Twee records

Op woensdag 3 september 1997 produceerde een computer op het Centrum voor Wiskunde en Informatica (CWI) in Amsterdam de twee priemfactoren van het getal $(12^{167} + 1)/13$. Dit is een getal van 180 cijfers (zie inzet). De factoren werden gevonden na slechts twaalf dagen rekenen op vijfentachtig SGI computers van het CWI. Eén speciale stap in de berekening die zeer veel geheugenruimte vereiste, werd uitgevoerd op het Amsterdamse rekencentrum SARA. De gebruikte factorisatie-methode is de zogenaamde 'Special Number Field Sieve'. Het getal van 180 cijfers is het grootste getal dat ooit met deze methode ontbonden is. Het vorige record, de factorisatie van een getal van 167 cijfers, werd afgelopen februari uitgevoerd door een internationale groep van onderzoekers die hun krachten via Internet gebundeld hadden. Deze factorisatie verbruikte evenwel twee maanden rekentijd. Met het nieuwe record gebruikte het CWI alleen eigen computers. De recordtijd, een factor vijf sneller dan het oude record, was een gevolg van recente verbeteringen in de software. Bovendien waren de gebruikte computers sneller dan hun voorgangers. Het gebruikte programma is oorspronkelijk ontwikkeld aan de Oregon State University en door de Nederlandse wiskundige Arjen Lenstra (nu werkzaam bij Citibank, New York). Gedurende de laatste paar jaar heeft het CWI het programma voortdurend verbeterd, hetgeen tot verschillende wereldrecords geleid heeft. De Amerikaanse firma Microsoft verwerft binnenkort het recht dit programma te gebruiken, om meer kennis op te doen over de nieuwste factorisatie-methoden. Met een vergelijkbare methode, de zogenaamde 'General Number Field Sieve', wordt de betrouwbaarheid van het veelgebruikte RSA cryptosysteem getest.

De record-ontbinding

Het getal dat op 3 september 1997 op het CWI te Amsterdam ontbonden werd is $(12^{167} + 1)/13$,een getal van 180 cijfers:

1286248074529200641089027285847866504705224464171357804194346814698101043793016009864587782936724194244003676117518184671309490252184868543062502487621047944788065325791142443946 93.

Dit getal heeft twee priemfactoren. Een factor van 75 cijfers:

788539152479959923583473870729725158796647538883718863262181413347391236469

en een factor van 105 cijfers:

163117845256502920687558543656697020247411364462120385893160945804553250187472604743326476435522680378897.

36-ste Mersenne-priem

Het getal $2^{2976221} - 1$ heeft 895.932 cijfers. Deze getallengigant vult gemakkelijk een paperback van 400 bladzijden. Op 24 augustus 1997 ontdekte de Amerikaan Gordon Spence op zijn 100 MHz Pentium PC dat dit getal een priemgetal is. Voor het complete bewijs waren vijftien dagen rekenen nodig met een uiterst efficient programma, geschreven door George Woltman, leider van de 'Great Internet Mersenne Prime Search' (GIMPS). Dit getal is het 36ste bekende Mersenne priemgetal en het grootste bekende priemgetal. Een priemgetal is een getal dat alleen 1 en zichzelf als delers heeft. De eerste paar priemgetallen zijn 2, 3, 5, 7 en 11. Kleine getallen kun je controleren of ze priem zijn door te testen of ze deelbaar zijn door kleinere getallen. Maar dit kun je niet doen met een getal van deze enorme afmetingen, want dat zou langer duren dan de leeftijd van het universum. De getallenreus is gekraakt met de zogenaamde Lucas-Lehmer test, een methode waarmee je snel na kunt gaan of een Mersenne-getal, dat is een getal van de vorm $2^n - 1$, een priemgetal is. De test wordt uitgevoerd door computerprogramma's die slimme methoden gebruiken om snel te kunnen vermenigvuldigen. Een snel programma is nog niet genoeg. Op één computer zou een systematische speurtocht naar Mersenne-priemen met exponent $n < 5.260.000$ meer dan 1000 jaar duren. De GIMPS coördineert de inspanningen van nu al meer dan 2000 computers, door gratis software te verstrekken en door de getallen die getest moeten worden te verdelen over individuele personen. De eer van deze ontdekking moeten Gordon Spence en George Woltman dus delen met alle andere deelnemers aan dit project. Duizenden andere getallenreuzen wachten om geveld te worden. Surf daarom naar de GIMPS-site en doe mee aan de zoektocht naar het volgende record-priemgetal!

BRONNEN
www.cwi.nl/cwi/Latest_News.html
www.mersenne.org/2976221.htm

De Lucas-Lehmer test

Mersenne-getallen zijn getallen van de vorm $2^n - 1$. Met de volgende stelling kun je testen of een Mersenne-getal een priemgetal is.

LUCAS-LEHMER TEST. Voor oneven p is het Mersennegetal $2^p - 1$ priem dan en alleen dan als $2^p - 1$ een deler is van $S(p-1)$, waar $S(n+1) = S(n)^2 - 2$ en $S(1) = 4$.
In pseudocode ziet deze test er als volgt uit. Door steeds modulo $2^p - 1$ te rekenen (zie de artikelen op p. 10 en p. 24) wordt enorm veel tijd bespaard.

```
s := 4;
voor i van 2 tot p − 1
    s := s² − 2 mod 2^p − 1;
als s = 0 dan
    print priem
anders
    print niet priem;
```

Voorbeeld. Voor $p = 5$ hebben we, modulo 31 rekenend: $S(1) = 4$, $S(2) = 14$, $S(3) \equiv 8$, $S(4) \equiv 0$. Dus is $2^5 - 1$ priem.

Razendsnel berekent een computer grootste gemene delers van enorme getallen. En als je modulo n rekent, kun je ook gigantisch grote machten supersnel berekenen.

Mod

Wieb Bosma

In Pythagoras 5 zullen we een cryptosysteem behandelen waarvoor het essentieel is dat je snel kunt rekenen modulo grote n. Vooral het berekenen van grote machten en van inversen modulo n is belangrijk. Dat laatste betekent dat je bij een getal a een x wilt vinden zodat $ax \equiv 1 \bmod n$. In 'Deling met rest' op p. 10 kun je lezen hoe je dat doet door de grootste gemene deler van a en n te berekenen.

Grootste gemene delers

Hoe bepaal je de ggd van $11111\cdots111$ en $12345678901234\cdots78901$ (beide getallen van 10001 cijfers)? Het computeralgebra pakket op mijn PC geeft vrijwel onmiddellijk het antwoord 1. Al wat het nodig heeft is het volgende korte programma, dat met behulp van de Euclidische algoritme (zie p. 12) de ggd van a en b berekent.

```
zolang b ≠ 0
    r := a mod b
    a := b; b := r;
print a;
```

De operatie `mod` zit standaard in veel programmeertalen: a `mod` b geeft de rest r van a bij deling door b. In formulevorm: $r = a - \lfloor a/b \rfloor \cdot b$. Hier is $\lfloor a/b \rfloor$ het getal dat je krijgt door a/b naar beneden af te ronden. Met een beetje extra boekhouden programmeer je een *uitgebreide* versie van het Euclidische algoritme. Daarmee vind je dan inversen modulo n.

Modulair rekenen

Modulair optellen en vermenigvuldigen is ook makkelijk met `mod`. Optellen modulo n doe je met $(a+b)$ `mod` n: tel a en b op pas `mod` n toe. Net zo om te vermenigvuldigen: $(a * b)$ `mod` n. Door de rest te nemen bij deling door n zorg je er voor dat je *uitkomsten* steeds kleiner zijn dan n. Het tussenresultaat $a * b$ kan zo groot worden als n^2. Met machtsverheffen moet je oppassen. Je weet dat 347^{1096} modulo 41687 hooguit 5 cijfers zal hebben. Maar als je als eerst 347^{1096} uitrekent dan heeft dat tussenresultaat een paar duizend cijfers. Het rekenen met zulke grote getallen kost veel tijd en misschien past het tussenresultaat niet in het geheugen van de computer!

Modulair machtsverheffen

Om de tussenresultaten klein te houden moet je voortdurend `mod` toepassen. Voor 347^{1096} modulo 41687 rekenen we niet in één keer 347^{1096} uit, maar beginnen met 347^2 en nemen dit modulo 41687. Zo vermenigvuldigen we steeds met 347 en nemen het resultaat modulo 41687:

$$347^2 = 120409 \equiv 37035$$
$$347^3 \equiv 347 \cdot 37035 \equiv 11549$$
$$347^4 \equiv 347 \cdot 11549 \equiv 5551$$

enzovoorts. De tussenresultaten worden nooit groter dan 41687^2. Dan vind je $347^{1096} \equiv 30154 \bmod 41687$ zelfs met een zakrekenmachine.

priemgetallen
met de computer

ulair rekenen°

Herhaald kwadrateren

Voor deze berekening moet je zo 1095 vermenigvuldigingen uitvoeren. Om 347^{10} uit te rekenen hoef je echter niet negen keer met 347 te vermenigvuldigen. Door te kwadrateren vind je 347^2, 347^4 en 347^8. Je krijgt 347^{10} dan door 347^8 en 347^2 met elkaar te vermenigvuldigen. Hier gebruiken we dat 10 de som van twee machten van 2 is: $10 = 2^3 + 2$. Dit werkt altijd, omdat je elk natuurlijk getal als som van machten van 2 kunt schrijven, dit heet de *binaire* schrijfwijze. Dit korte programma bepaalt de binaire schrijfwijze van k:

```
zolang k > 0
  indien k oneven
    k := k - 1; print 1;
  anders
    print 0;
  k := k/2;
```

Voor $k = 10$ krijg je 0101 en het resultaat is 00010010001 voor $k = 1096$. Het programma drukt alleen de binaire schrijfwijze net andersom af dan gebruikelijk is: gewoonlijk schrijven we tien binair als 1010. Het voordeel van herhaald kwadrateren blijkt uit de berekening van de 1096-ste macht. Aan de binaire schrijfwijze van 1096 zie je dat $2^3 + 2^6 + 2^{10} = 1096$. Een 1096-ste macht kun je dan uitrekenen door 10 keer te kwadrateren en nog 2 extra vermenigvuldigingen te doen. Bereken $A_1 = 347^2$, $A_2 = A_1^2$, ... , $A_{10} = A_9^2$, en bepaal $A_3 \cdot A_6 \cdot A_{10}$. Voor het resultaat modulo 41687 neem je na elke kwadratering of vermenigvuldiging de uitkomst modulo 41687. Je hebt zo niet 1095 maar slechts 12 vermenigvuldigingen nodig, en geen getallen groter dan 41687^2. Dit programma bepaalt zo a^k modulo n:

```
t := 1; A := a;
zolang k > 0
  indien k oneven
    k := k - 1; t := t*A mod n;
  k := k/2; A := A^2 mod n;
print t;
```

In plaats van een 0 af te drukken wordt A gekwadrateerd, en in plaats van een 1 af te drukken eerst ook nog het tussenresultaat t met A vermenigvuldigd.

Grote getallen

Met een zakrekenmachine kun je hooguit getallen van 10 cijfers aan. Ook in programmeertalen zoals BASIC en C is het niet eenvoudig om met grote getallen te rekenen. Maar er zijn speciale programma's waarmee je wel met heel grote getallen kunt rekenen. Op de priemgetallenpagina van Pythagoras vind je sites waar je deze gratis software kunt downloaden. De meer geavanceerde computeralgebra systemen (Derive, Mathematica) kunnen nog veel meer. Allerhande wiskundige funkties zijn daar al standaard voorgeprogrammeerd.

Op 19 september 1997 is in Eindhoven de tweede ronde van de Nederlandse Wiskunde Olympiade gehouden. De 116 deelnemers hadden drie uur om de onderstaande vijf opgaven op te lossen.

Neder

Tweede ronde

De eerste ronde van de Nederlandse Wiskunde Olympiade 1997 is gehouden op 11 april 1997. Daaraan namen 2605 leerlingen deel, verdeeld over 247 scholen. De 117 leerlingen die bij de eerste ronde een score van 26 punten of meer haalden, werden uitgenodigd om deel te nemen aan de tweede ronde die op vrijdag 19 september in Eindhoven gehouden is. Het bestuur van de Stichting Nederlandse Wiskunde Olympiade heeft daarnaast nog 6 andere leerlingen uitgenodigd, één van hen op grond van haar prestaties in de Pythagoras Olympiade. Uiteindelijk hebben 116 leerlingen meegedaan. Zij kregen drie uur de tijd om vijf opgaven op te lossen. De maximale score per opgave bedroeg 10 punten. De prijswinnaars vind je in de tabel. Op 14 november jl. was de prijsuitreiking. Aansluitend was het eerste trainingsweekend voor de beste 20 deelnemers van de tweede ronde. Daarmee werd een begin gemaakt met de voorbereiding op de Internationale Olympiade van 1998 in Taiwan, waar ons land met een ploeg van 6 leerlingen vertegenwoordigd zal zijn. Hieronder vind je de vijf opgaven van de tweede ronde. De oplossingen worden gepubliceerd in het februarinummer.

Opgave 1

Bij elk positief geheel getal n definiëren we $f(n)$ als het product van de som van de cijfers van n met n zelf. Voorbeelden:
$f(19) = (1+9) \times 19 = 190$,
$f(97) = (9+7) \times 97 = 1552$.
Toon aan dat er geen getal n bestaat met $f(n) = 19091997$.

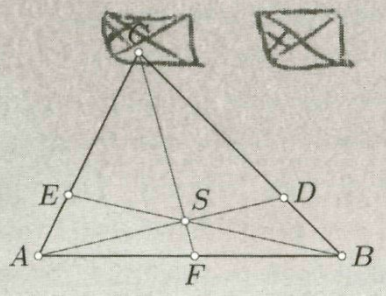
EINDRANGSCHIKKING

	Naam	Plaats	punten 2e ronde	punten 1e ronde
1	Fokko van der Bult	Oegstgeest	48	36
2	Willem Jan Palenstein	Oegstgeest	31	30
3	Herbert Beltman	Markelo	27	31
4	Wouter van der Bilt	Leusden	26	29
4	Maxim Hendrix	Oegstgeest	26	29
6	Guido Schmeits	Heeze	26	28
7	Hugo Buddelmeijer	Delft	25	35
8	Gert-Jan Kok	Rijswijk	25	33
9	Art Willems	Vierlingsbeek	25	27
10	Rink Hallmann	Silvolde	24	33

Wiskundige Olympiade
landse

Opgave 2

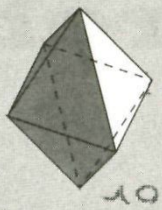
Binnen een driehoek ABC snijden de lijnen AD, BE en CF elkaarin S. Gegeven is dat $AS : DS = 3 : 2$ en $BS : ES = 4 : 3$. Bepaal de verhouding $CS : FS$.



Opgave 3

a. Bekijk de tweedegraadsvergelijking $x^2 + ?x + ? = 0$. Twee spelers zetten achtereenvolgens elk op de plaats van een vraagteken een geheel getal. Toon aan dat de tweede speler er altijd voor kan zorgen dat de vergelijking twee gehele oplossingen krijgt. NB: we zeggen dat de vergelijking $x^2 - 6x + 9 = 0$ ook twee gehele oplossingen heeft, en wel twee gelijke (allebei gelijk aan 3).

b. Bekijk de derdegraadsvergelijking $x^3 + ?x^2 + ?x + ? = 0$. Drie spelers zetten achtereenvolgens elk op de plaats van een vraagteken een geheel getal. De vergelijking blijkt drie gehele (weer eventueel gelijke) oplossingen te hebben. Gegeven is dat twee spelers elk een 3 op de plaats van een vraagteken gezet hebben. Welk getal heeft de derde speler gezet? Bepaal dat getal en de plaats waar het gezet is en bewijs dat er maar één getal mogelijk is.



Opgave 4

We bekijken een octaëder, een regelmatig achtvlak, waarvan één vande zijvlakken rood is geverfd en de zeven andere zijvlakken blauw.

We werpen de octaëder als een dobbelsteen. Het vlak dat boven komt wordt geverfd: als het rood is wordt het blauw geverfd en als het blauw is wordt het rood geverfd. Vervolgens werpen we de octaëder nog eens en verven het weer volgens de bovenstaande regel. In totaal werpen we de octaëder 10 keer. Hoeveel verschillende octaëders kunnen we krijgen na afloop van de 10e keer verven? [Twee octaëders zijn verschillend als ze niet door draaiing in elkaar zijn over te voeren.]

Opgave 5

Gegeven is een driehoek ABC en een punt K binnen de driehoek. Het punt K wordt gespiegeld in de zijden van de driehoek: P, Q en R zijn de gespiegeld en van K in respectievelijk AB, BC en CA. Het middelpunt van de cirkel door de hoekpunten van driehoek PQR is M. Het punt M wordt weer gespiegeld in de zijden van driehoek ABC. De punten P', Q' enR' zijn de gespiegelden van M in respectievelijk AB, BC en CA.

a. Bewijs dat K het middelpunt van de cirkel door de hoekpunten van driehoek $P'Q'R'$ is.

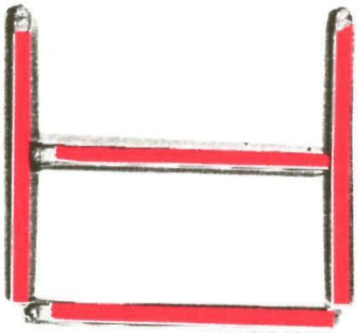
b. Waar moet je K kiezen binnen driehoek ABC zodat M en K samenvallen? Bewijs je antwoord.

Problemen

redactie: Dion Gijswijt

Vormvast

Van lucifers van gelijke lengte maken we figuren door ze tegen elkaar aan te leggen. In deze puzzel mag een lucifer op drie plaatsen tegen een andere lucifer aan worden gelegd: aan één van beide uiteinden en precies in het midden.



Op elk van deze drie plaatsen mag ook niet meer dan één andere lucifer worden aangelegd. Bovendien mogen lucifers niet over elkaar heen liggen. Sommige lucifer-figuren kunnen 'bewegen'. Je kunt bijvoorbeeld het bovenstaande luciferfiguurtje vervormen:

Andere figuren kunnen niet bewegen en heten 'vormvast', zoals bijvoorbeeld een gelijkzijdige driehoek. Probeer vormvaste figuren te maken van 3, 5, 6, 7 en 8 lucifers.

Opeenvolgende kwadraten

15 516 190 096 en 15 516 439 225 zijn kwadraten van twee opeenvolgende gehele getallen. Wat is het kwadraat van het volgende gehele getal? Deze getallen zijn te groot voor de meeste rekenmachines, maar het probleem kan opgelost worden zonder een wortel te trekken.

Het tientje

Christel gaat naar het postkantoor. Ze geeft de beambte een tientje en zegt: "Kunt u me hiervoor een aantal postzegels van 80 cent geven, driemaal zoveel van 90 cent en voor de rest postzegels van 100 cent?" Kon de beambte hieraan zó voldoen dat het tientje precies op ging?

Paardesprongen

Een paard staat op een naar alle richtingen onbegrensd schaakbord. Beredeneer dat het paard elk veld kan bereiken.

Wijn schenken

We hebben drie vaten met als inhoud respectievelijk 12, 7 en 5 liter. Het vat van 12 liter is geheel gevuld met wijn; de twee andere vaten zijn leeg. Kun je de wijn in twee gelijke delen verdelen met behulp van alleen deze drie vaten?

Oplossingen nr. 1

Op deze pagina worden de oplossingen van problemen uit het vorige nummer van Pythagoras besproken. Een volledige bespreking van alle vragen en problemen is te vinden op de homepage.

Dion Gijswijt

Kruiswoordraadsel

7	5	7	■	5	3
5	3	■	■	3	7
2	3	7	5	3	■
3	3	7	■	3	7
■	■	5	3	■	5
■	■	7	7	2	7

De tovercursus

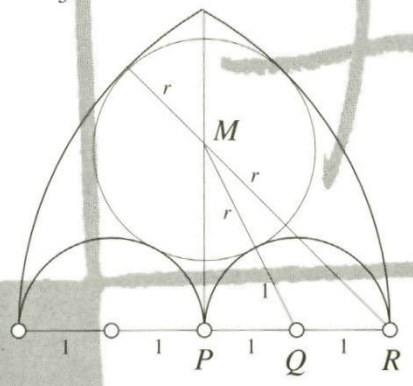
Het probleem kan stap voor stap worden opgelost. Als op de eerste dag een tovenaarsleerling helemaal geen strikken ziet, weet hij dat hij een strik om zijn muts draagt (want er was minstens één strik) en moet hij dus naar voren stappen. Gebeurt er op de eerste dag niets, dan zijn er dus minstens twee leerlingen met strikken en een leerling die in de kring maar één strik ontwaart weet daarom dat hij ook een strik heeft en op de tweede dag naar voren moet stappen. Zo gaat het verder. Elke leerling telt het aantal strikken a bij zijn mede-leerlingen. Als er op cursusdag a niemand naar voren stapt, dan heeft hij zelf ook een strik om en moet hij de volgende dag naar voren stappen.

Verdeel en heers

Je kunt de positieve gehele getallen op maar één manier in twee groepen verdelen zodat twee getallen uit dezelfde groep nooit een priemgetal als som hebben: in de even getallen en de oneven getallen. Zie de homepage voor een bewijs.

Gotiek

Als de straal van de kleine cirkelbogen 1 is, dan is de straal van de grote cirkelbogen gelijk aan 4. Het middelpunt van de cirkel die aan alle cirkelbogen raakt ligt op de vertikale symmetrieas. Noem het middelpunt van deze cirkel M en de straal r. De lijn door M en Q gaat door het raakpunt aan de kleine cirkelbogen. De stelling van Pythagoras toegepast op ΔPQM geeft $MP^2 = (1+r)^2 - 1$. De lijn door M en R gaat door het raakpunt aan de grote cirkelboog. De stelling van Pythagoras toegepast op ΔPRM levert $MR^2 = (1+r)^2 + 3$. Maar $MR + r = 4$, zodat $(4-r)^2 = (1+r)^2 + 3$. Oplossen levert $r = \frac{6}{5}$.



Hieronder volgt een overzicht van de verschillende wiskundige activiteiten die in de komende periode voor middelbare scholieren georganiseerd worden. Ook komen bepaalde activiteiten voor wiskundedocenten op de lijst voor.

Agenda

Data voor deze agenda aanmelden bij pythagoras@wins.uva.nl

za 3 januari '98
De wiskunde van de sociale keuze (076) 5273267
Wintersymposium WG, Amersfoort (076) 5419757

do 22, vr 23 januari '98
Van afbeeldingen naar fractals (071) 5277100
RUL masterclass voor 4, 5 en 6 VWO-ers

vr 30 januari '98
Algebra en meetkunde op de computer (020) 5255074
UvA mastercourse voor VWO-docenten wiskunde

vr 30, za 31 januari '98
Nationale Wiskundedagen (030) 2611611

za 31 januari '98
Mathematische modelleercompetitie, Maastricht

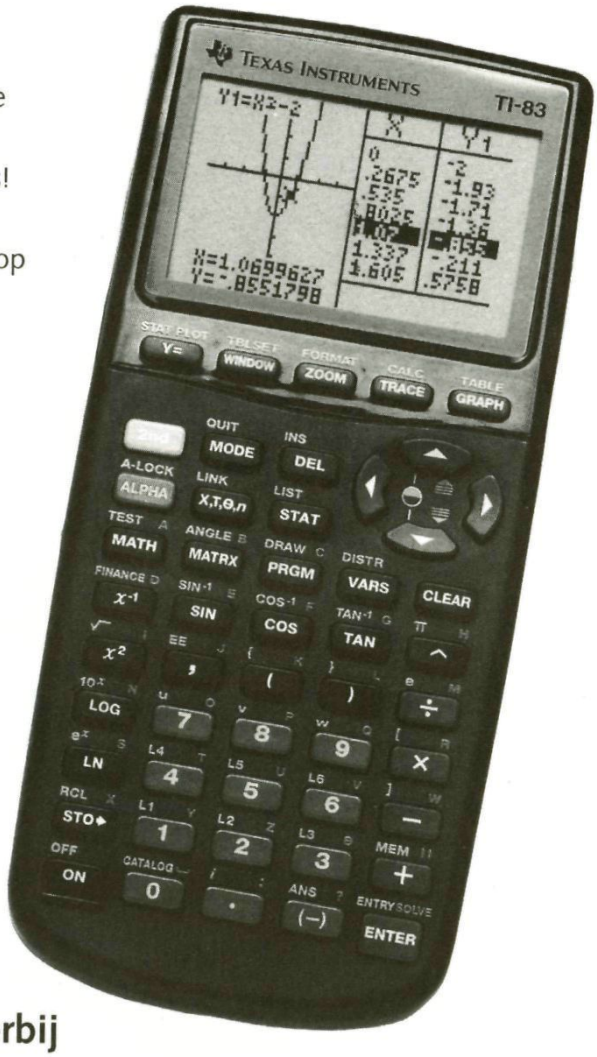
vr 6, 13 en 20 februari '98
Wiskunde en Computer (020) 4447700
VU masterclass voor 5 en 6 VWO-ers

vr 6, 13 en 20 maart '98
Wiskunde en Computer (020) 4447700
VU masterclass voor 5 en 6 VWO-ers

TI-83: veelzijdig en krachtig

De TI-83 is een veelzijdige grafische rekenmachine voor de tweede fase van het voortgezet onderwijs. Terecht is deze machine door het Freudenthal instituut gekozen als 'standaard' in het experiment voor de nieuwe bovenbouwprogramma's wiskunde (PROFI).

Ervaringen met de bekende TI-82 zijn in de TI-83 verwerkt; een eigentijdse machine dus! Zo is de **interface** sterk verbeterd en kan er volop worden gewerkt met **matrices.**
Ook de **grafische presentaties** en de mogelijkheden om **vergelijkingen** op te lossen zijn uitgebreid. Daarnaast kunnen uw leerlingen **gegevens uitwisselen** via de I/O-poort terwijl met TI-graph-link-software **aansluiting op een PC** mogelijk is.



Met name de veelzijdigheid van de TI-83 maakt, dat deze machine naast **wiskunde**, ook voor diverse andere vakken zeer geschikt is. Doordat de machine gekoppeld kan worden aan de CBL en CBR is hij uitermate geschikt voor **natuurkunde**.
Door de financiële functies is de machine een uitkomst bij **financiële** en **economische vakken**, maar ook bij vakken als **aardrijkskunde**, **biologie** en **informatica** kan de TI-83 zeer behulpzaam zijn.

Wilt u meer weten over dit rekenwonder, bel of schrijf naar Texas Instruments.
Tel.: 020 - 5469825,
fax: 020 - 6463136

Wiskunde dichterbij

TI-83: dé machine voor de tweede fase!

Texas Instruments Nederland, Postbus 74781, 1070 BT Amsterdam

TEXAS INSTRUMENTS

Over de medewerkers

dr W. Bosma
is docent computer-algebra aan de KUN

dr J. Brinkhuis
is docent wiskunde aan de EUR

prof.dr J. van de Craats
is hoogleraar wiskunde aan de UvA, de Open Universiteit en de KMA

dr L.J. van Gastel
is werkzaam bij het Expertisecentrum Computer Algebra Nederland

D.C. Gijswijt
is student wiskunde aan de UvA

dr K.P. Hart
is docent topologie aan de TU Delft

drs A. Heck
is werkzaam bij het Expertisecentrum Computer Algebra Nederland

B. de Jongste
is recreatief wiskundige te Den Haag

dr ir T. Koetsier
is docent geschiedenis van de wiskunde aan de VU

prof.dr H.A. Lauwerier
is emiritus hoogleraar toegepaste wiskunde aan de UvA

ir A.A.J. Lefeber
is AIO systeem- en besturingstheorie aan de UT

R. van Luijk
is student wiskunde aan de UU

drs W.R. Oudshoorn
is AIO algebra en meetkunde aan de RUG

drs H.N. Pot
is gewezen leraar wiskunde te Woerden

ir S.M. van Rijnswou
is OIO computeralgebra aan de TUE

dr P. Stevenhagen
is docent algebraïsche getaltheorie aan de UvA

dr ir R.F. Swarttouw
is docent wiskunde aan de VU

dr J. Top
is docent algebra en meetkunde aan de RUG

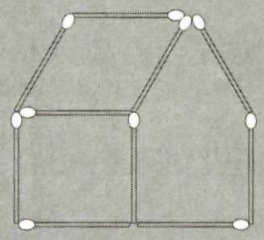
drs C.A.M. Wildhagen
is leraar wiskunde aan het Erasmiaans Gymnasium te Rotterdam

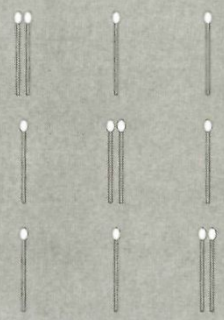
drs C.G. Zaal
is OIO algebraïsche meetkunde aan de UvA

Oplossingen p. 2 en 3

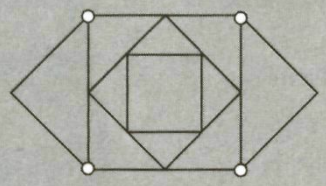
Indianen
Het is de moeder.

Lucifers/Huisje





Overtrekken
De eerste figuur lukt altijd, waar je ook begint. De tweede figuur kan niet, want er zijn vier punten waarin een oneven aantal lijnen samenkomt:



Toast
Het rooster kan in 9 minuten door steeds twee sneetjes tegelijk te roosteren. Je moet dan wel na 3 minuten één van beide sneetjes eruit halen en vervangen door een vers sneetje.

Jokkebrokken
Willem kan niet de waarheid spreken, want dan zou Jantje volgens Willem liegen en de waarheid spreken volgens Pietje. Kortom, Willem liegt en Jantje en Pietje kunnen niet allebei liegen. Als Pietje de waarheid spreekt, dan liegt Jantje en spreekt Willem de waarheid. Maar dat kan niet. Dus liegt Pietje en spreekt Jantje de waarheid.

Twintig
Het kan niet, want de som van vijf oneven getallen is altijd oneven.

Herziene kerndoelen basisvorming,
Tweede Fase havo/vwo, Leerwegen vmbo

Wolters-Noordhoff nodigt u uit

U bent van harte welkom op een of meer van de volgende bijeenkomsten. U kunt daar uitgebreid kennismaken met de herziene delen voor de basisvorming en de nieuwe delen voor de Tweede Fase van

Moderne wiskunde zevende editie
en
Netwerk tweede editie

Gebruikersbijeenkomsten
Eind januari 1998 organiseren wij exclusieve bijeenkomsten voor de gebruikers van onze methoden. U gebruikt *Moderne wiskunde, Netwerk* of *WiskundeLijn* en u hebt geen aanmeldings-kaart ontvangen? Meldt u zich dan telefonisch aan bij Wolters-Noordhoff: (050) 522 63 11.

- maandag 26 januari 1998 Moderne wiskunde
- dinsdag 27 januari 1998 Netwerk
- donderdag 29 januari 1998 WiskundeLijn

Nationale Wiskunde Dagen
Tijdens de Nationale Wiskunde Dagen zijn wij met de nieuwe edities aanwezig op de informatie-markt. Ook nodigen wij u van harte uit deel te nemen aan onze workshop op vrijdagavond, van 21.30 tot 22.30 uur.

U kunt zich nog aanmelden voor de NWD bij het Freudenthal Instituut, telefoon (030) 253 86 11, fax (030) 253 53 53.

- vrijdag 30 en zaterdag 31 januari 1998 te Noordwijkerhout.

Methodekeuzebijeenkomsten
De LPC's organiseren in samenwerking met de uitgevers door het gehele land Methodekeuze-bijeenkomsten. U kunt zich daar laten informeren over alle nieuwe en herziene methodes.

- woensdag 4 en donderdag 5 februari 1998
- woensdag 11 en donderdag 12 februari 1998
- woensdag 18 en donderdag 19 februari 1998

Voor inhoudelijke informatie en inschrijf-formulieren kunt u terecht bij Roel Gordijn (LPC), tel. (033) 453 43 53 of Freke Bosscha, tel. (020) 430 91 63.

Wolters-Noordhoff
Postbus 58
9700 MB Groningen
Telefoon (050) 522 63 11

419/7335 [Euclides]
419/7378 [Pythagoras]

Wolters Noordhoff

419/7335

Pythagoras

Pythagoras wordt uitgegeven onder auspiciën van de Nederlandse Onderwijscommissie voor Wiskunde en richt zich tot alle leerlingen van HAVO en VWO.
Pythagoras stelt zich ten doel jongeren kennis te laten maken met de leuke en uitdagende kanten van wiskunde.

Abonnementen

Abonnees kunnen zich op één van de volgende manieren aanmelden.
Telefonisch: (070) 314 35 00, per fax: (070) 314 35 88,
via Internet: www.wins. uva.nl/misc/pythagoras/abonnee.html
of schriftelijk (een postzegel is niet nodig):
NIAM, Antwoordtnummer 97007, 2509 VH Den Haag

Tarieven '97-'98

Een jaarabonnement op Pythagoras kost *f* 37,50
Losse nummers *f* 8,-- of BF 160
Overige prijzen (per jaar):
Pythagoras België BF 950
Pythagoras buitenland *f* 52,50
Pythagoras/Archimedes *f* 67,50
Pythagoras/Archimedes België BF 1570
Pythagoras/Archimedes buitenland *f* 83,50

Schoolabonnementen

Voor leerlingen in het voortgezet onderwijs en studenten aan lerarenopleidingen zijn er speciale schoolabonnementen.
Voor *f* 25,00 per jaar ontvangen zij één heel jaar lang Pythagoras, op voorwaarde dat de docent wiskunde zorgt voor de aanmelding en verspreiding. Abonnees krijgen een acceptgiro thuisgestuurd.
Bij aanmelding van 5 of meer abonnees, 1 jaarabonnement gratis.

Uitgever/advertenties

NIAM, Neuhuyskade 94, 2596 XM Den Haag
Telefoon (070) 314 35 00, Fax (070) 314 35 88, Giro 5513796
Bankrekening België: ING Brussel
reknr. 627-7064242-48 t.n.v. TMS

Pythagoras wordt gesponsord
door de Universiteit van Amsterdam