PYTHAGORAS

50 jaar

WISKUNDETIJDSCHRIFT VOOR JONGEREN

Codemakers winnen van codebrekers

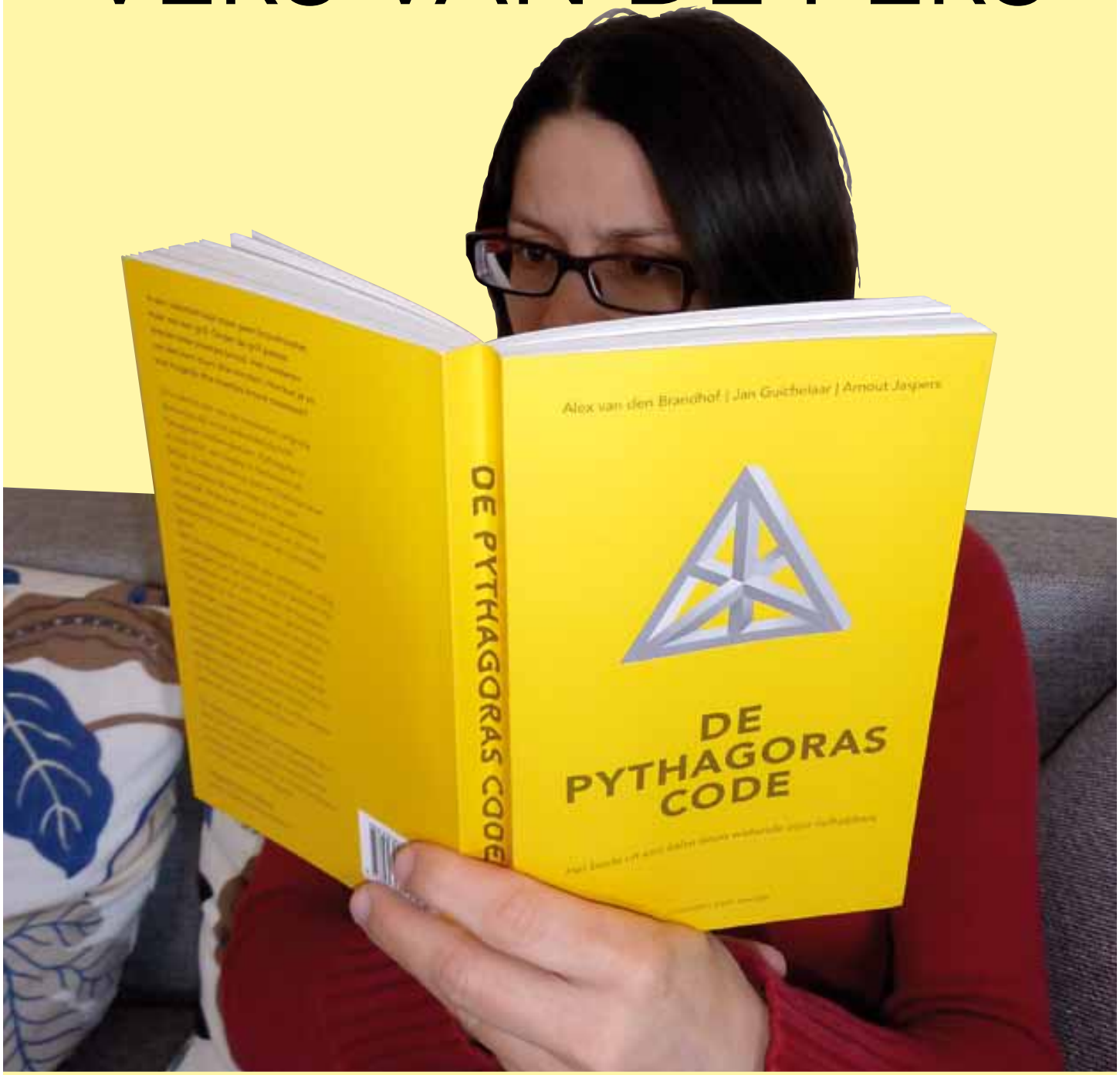
De mooiste formule ooit

Jubileumprijsvraag:

creatief met polyomino's

50ste JAARGANG - NUMMER 5 - APRIL 2011

VERS VAN DE PERS



Pythagoras pakt uit: omdat het wiskundetijdschrift voor jongeren vijftig jaar bestaat, is er nu De Pythagoras Code, een boek met de beste puzzels en artikelen uit vijftig jaargangen. Een greep uit de onderwerpen: geomagische vierkanten, superdoku's, sangaku's, onmogelijke figuren, platonische lichamen, Penrosetegels, kettingbreuken, wiskunst en uiteraard heel veel puzzels, van verrassend simpele raadsels tot breinbrekers die je een weekend of langer niet meer loslaten. Het boek is vanaf deze maand te koop in de boekhandel.

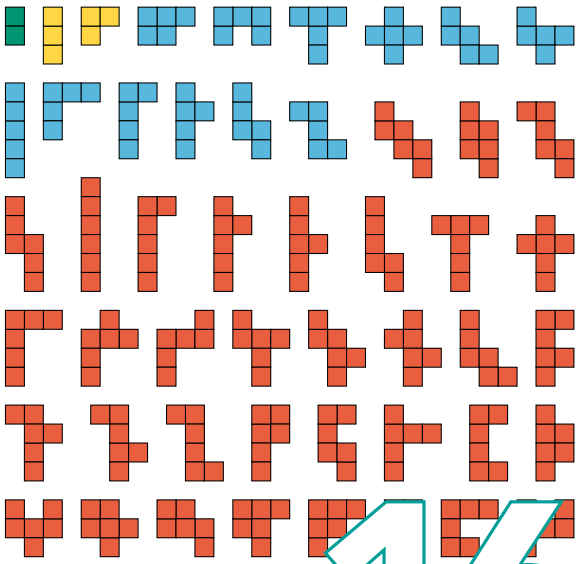
De Pythagoras Code – het beste uit een halve eeuw wiskunde voor liefhebbers.
Samenstelling Alex van den Brandhof, Jan Guichelaar en Arnout Jaspers.
Bert Bakker, 271 pagina's, € 19,95.

INHOUD

4

COMPUTER DEMOCRATISEERDE HET GEHEIMSCHRIFT

In zijn vijftigste jaargang gaat *Pythagoras* na, welke vooruitgang er sinds de eerste jaargang geboekt is op onderwerpen waarbij wiskunde een sleutelrol speelt. De vijfde aflevering van deze serie behandelt *cryptografie*. Totnogtoe winnen de codemakers het van de codebrekers.



16

50 POLYOMINO'S

Jakob Jørgensen is een Deense meubelontwerper. De bijzondere kast op het omslag is gebaseerd op drie *polyomino's*. Zelf kun je ook creatief aan de slag met polyomino's in de laatste aflevering van de jubileumprijsvraag.

20

EEN LELIJK SCHILDERIJ

Aan een schilderij zit een koord bevestigd. Hoe hang je dat koord om meerdere spijkers op zo'n manier, dat het schilderij naar beneden valt als je één spijker verwijdert? Een mooie puzzel die je niet gauw zal loslaten!

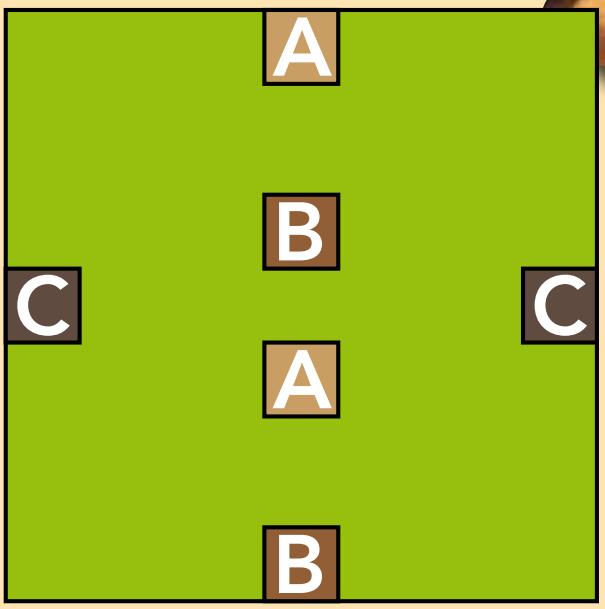
EN VERDER

Beeld omslag:
'IO' door Jakob Jørgensen (www.jjoergensen.dk)

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

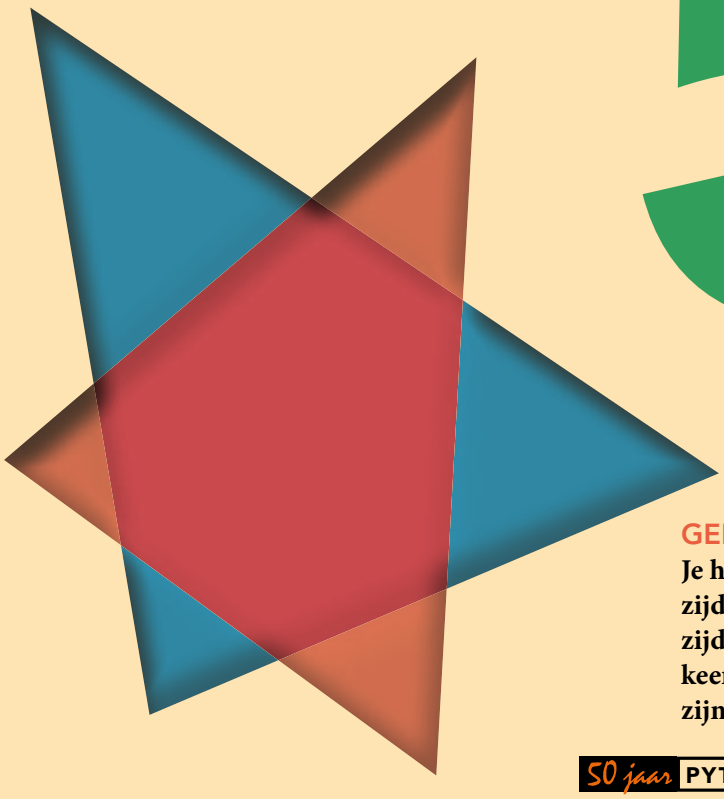
KLEINE NOOTJES

door Dick Beekman en Jan Guichelaar



VERBINDINGSWEGEN

Arjan, Bart en Carel hebben op een afgesloten vierkant terrein ieder twee huizen, zie bovenstaande plattegrond. Ze willen alle drie een weg aanleggen tussen hun twee huizen, maar zonder een andere weg te kruisen. Kan dat?



JUBELJAAR MET DRIE ZEVENS EN EEN ÉÉN

Maak met de vier cijfers 7, 7, 7 en 1 het getal 50. Je mag alleen optellen, aftrekken, vermenigvuldigen en delen. Haakjes mag je gebruiken zoveel je wilt. Cijfers plakken (bijvoorbeeld van 1 en 7 het getal 17 maken) is niet toegestaan.

GELIJKVORMIGE DRIEHOEKEN

Je hebt twee gelijkvormige driehoeken, die twee zijden exact gelijk hebben. De kleinste van de zes zijden is 1. De oppervlakte van de grootste is vier keer zo groot als die van de kleinste. Hoe groot zijn de andere zijden?

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

2 7	→	18
7 2	→	63
8 4	→	96
9 7	→	?
x x	→	50

GETALLENDOOS

In een doos zit een kabouter. Als je in de doos een briefje gooit met daarop twee getallen, één links en één rechts, gooit de kabouter een briefje uit de doos met daarop het *resultaat* van de twee getallen.
Het resultaat van 2 en 7 is 18, van 7 en 2 is 63, en van 8 en 4 is 96.
Finn noteert de getallen 9 en 7. Welk resultaat krijgt Finn van de kabouter?
Alida noteert twee gelijke getallen. Welk getal is dit, als zij 50 als resultaat krijgt?

NABORRELEN

Na een concert in het Concertgebouw in Amsterdam zitten Ria, Ellen, Jan en Henk in café Keyzer. Henk, wijzend op de laatste bitterbal: 'Noem eens een getal onder de tien.' Hij krijgt de antwoorden 2, 7 en 6. 'Fout, dan is de laatste voor mij.' Ervan uitgaande dat Henk eerlijk speelt, hoe groot was de kans dat Henk zou winnen?

Dick Beekman heeft vele jaren zijn bijdragen geleverd bij het bedenken van de *Kleine nootjes*. Hij heeft besloten ermee te stoppen. In dit nummer staan nog zijn bijdragen: 'Verbindingswegen', 'Gelijkvormige driehoeken' en 'Getallendoos'. De redactie dankt Dick hartelijk voor zijn jarenlange inspanningen!

Tot eind jaren '60 van de vorige eeuw waren geheimschriften niet wezenlijk beter dan wat al vóór de Tweede Wereldoorlog ontwikkeld was. Maar door de ontwikkeling van de computer en de revolutionaire vinding van 'public key'-cryptografie raakte het vak in de jaren '70 in een stroomversnelling – mooi op tijd om internetbetalingen, mobiel bellen en talloze andere digitale toepassingen te beveiligen. De codemakers staan voor op de codebrekers. Pas de volgende revolutie, de nog hypothetische kwantumcomputer, kan daar verandering in brengen.

door Arnout Jaspers en Matthijs Coster

COMPUTER DEMOCRATISEERDE HET GEHEIMSCHRIFT

Tot een eeuw geleden werden berichten handmatig vercijferd. De machines die een eeuw geleden werden gebouwd, konden berichten vercijferen en ontcijferen. De Enigma die de Duitsers in de Tweede Wereldoorlog gebruikten, was zo'n machine, waarin voor elke aangeslagen letter één van de 26 codeletters oplichtte.

De dringende behoefte om Enigma te kraken, leverde de eerste voorlopers van de computer op. De Britse *Bombes* waren machines die niets anders konden dan deze code kraken, dus geen echte computers, maar na 1945 kwam er veel geld los om de technologie verder te ontwikkelen. De computer, op zijn beurt, heeft de cryptografie totaal veranderd. Eeuwenlang waren vercijferen (naar het Engelse woord voor geheimschrift, *cipher*) en ontcijferen handwerk. Dat gaat tergend langzaam – zeg met één teken per seconde – en daarom werd alleen tekst gecodeerd.

Moderne computers kunnen duizenden bits per seconde onderwerpen aan uiterst gecompliceerde bewerkingen, zodat ook spraak, beeld en andere datastromen te vercijferen zijn. De computer 'democratiseerde' de cryptografie ook: niet alleen koeriers, spionnen en militairen, maar iedereen kon zijn privacy beschermen, zelfs zonder iets van cryptografie af te weten.

DES Een van de eerste, algemeen gebruikte computergeheimschriften was de *Data Encryption Standard* (DES), ontworpen door IBM. Het is een zogeheten *blokvercijfering*, er worden telkens blokjes van 64 bits als één geheel vercijferd. De uitkomst is opnieuw een blokje van 64 bits. De sleutel telt 56 bits.

DES is een mooi voorbeeld van een traditioneel geheimschrift, maar dan opgepimpt voor het computertijdperk. Al eeuwenlang ontwerpen mensen geheimschriften die letters of cijfers met een een combinatie van *transpositie* en *substitutie* vercijferen.

Transpositie wil zeggen dat een geheime regel de volgorde van de tekens verandert. Een erg simpel voorbeeld: achterstevoren schrijven. Substitutie wil zeggen dat elk teken volgens een geheime regel wordt vervangen door een ander teken. Een heel simpel voorbeeld: A → B, B → C, …, Z → A.

Bovenstaande regels zijn natuurlijk veel te simpel om geheim te blijven. Bovendien moet elke gebruiker zijn eigen geheime regel kunnen kiezen. Daarom bestaat elk goed geheimschrift uit een algoritme en is er een astronomisch groot aantal sleutels waaruit de gebruiker één kan kiezen.

We kunnen de substitutie wat ingewikkelder maken door uit te gaan van een substitutiesleutel. Stel dat PYTHAGORAS als sleutel dient. Haal eerst je de dubbele letters eruit: PYTHAGORS. Dit definieert de volgende substitutie: A → P, B → Y, C → T, D → H, E → A, F → G, G → O, H → R, I → S, J → B, … (je gaat verder met de letters van het alfabet die je nog niet gebruikt hebt). Het aantal mogelijke sleutels is gelijk aan het aantal volgordes van het alfabet: $26! \approx 4 \times 10^{26}$. Als sleutel voor een ingewikkelde transpositie kan een diagram dienen zoals je in het kader hiernaast ziet. Ook het aantal mogelijke diagrammen is natuurlijk erg groot.

Bij een gedegen geheimschrift hangt de veiligheid niet af van het geheimhouden van het algoritme, maar wordt de veiligheid gegarandeerd door het kiezen van de sleutel en is het algoritme gewoon

Blokvercijfering

Klare tekst:

MIJN PINCODE IS NEGEN ZES ZES NUL

Horizontaal invullen, van boven naar beneden:

M		I	J	N	P
I	N			C	O
D	E		I	S	N
E	G		E		
N	Z	E	S	Z	E
S		N		U	L

per kolom opschuiven in het alfabet +2 +1 +1 +3 +1 +0

O		J	M	O	P
K	O			D	O
F	F		L	T	N
G	H		H		
P	A	F	V	A	E
U		O		V	L

Verticaal aflezen, van rechts naar links:

Vercijferde tekst:

PONEL ODTAV MLHVJ FOOFH AOKFG PUPOM

Hier zie je een voorbeeld van blokvercijfering die met pen en papier nog te doen is. Bij blokvercijfering wordt telkens een blokje data met een vaste omvang vercijferd. Het algoritme gooit de volgorde van de letters grondig door elkaar (transpositie) en vervangt systematisch bepaalde letters door andere (substitutie). In de vercijferde tekst zijn op het eind drie 'nullen', ofwel loze letters, toegevoegd om een blokje van vijf vol te maken. Zo verhul je de ware lengte van het blok, omdat dit nuttige informatie kan zijn voor een codebreker.

Opdracht: Hoe ziet een blok*ont*cijfering eruit?

openbaar. IBM publiceerde DES in 1976, met het doel dat veel mensen het zouden gaan gebruiken.

Toen coderen en decoderen nog met de hand ging, moest een vercijferingsalgoritme vooral niet te ingewikkeld zijn, en je moest er redelijk snel mee kunnen werken zonder al te veel kans op fouten. De computer heeft geen last van zulke beperkingen, en daarom worden in geheimschriften als DES de bits aan een enorme lijst van sleutelafhankelijke transposities en substituties onderworpen, net zo lang totdat het bericht voor een buitenstaander niet meer van een puur toevallige reeks bits te onderscheiden is.

DES vercijfert blokjes van 64 bits in 16 rondes. Eén ronde is vergelijkbaar met de blokvercijfering, zie bovenstaand kader. Het resultaat van ronde 1 wordt opnieuw vercijferd, maar dan met een ander diagram en andere substitutieregels, en zo nog 14 keer. Het aantal bewerkingen is zo enorm, waardoor DES alleen met een computer te doen is.

Toch is DES in 1997 gekraakt, door domweg alle $2^{56} \approx 7 \times 10^{16}$ mogelijke sleutels van een testbericht uit te proberen. De gigantische rekenklus werd verdeeld over tienduizenden computers van vrijwilligers over de hele wereld, en na 96 dagen was het testbericht ontcijferd.

In de jaren '70 en '80 was zoiets onmogelijk, doordat het internet niet bestond en computers veel trager waren. DES is dus niet veilig meer, maar het leeft nog voort als triple-DES, een systeem waarbij een bericht met drie sleutels drie keer geDESd wordt. Ook is er sinds 2001 de *Advanced Encryption Standard* (AES), een van origine Belgische blokvercijfering. In grote lijnen werkt dit hetzelfde als DES, maar de blokgrootte is 128 bits en de sleutel naar keuze 128, 192 of 256 bits. Het uitproberen van $2^{128} \approx 3 \times 10^{38}$ sleutels zal voor computers nog geruime tijd te veel zijn.

PUBLIC KEY Pas in 1997 werd bekend dat James H. Ellis, Clifford Cocks en Malcolm Williamson van de Britse geheime overheidsdienst GCHQ al in 1973 een cryptografische doorbraak hadden bereikt die niet voor mogelijk werd gehouden: *Public Key* sleuteluitwisseling. Alle geheimschriften tot dan toe, ook DES en AES, gebruiken een sleutel voor ver- en ontcijfering die de gebruikers angstvallig geheim moeten houden. Probleem is dan altijd: hoe bezorg ik degene die ik een bericht wil sturen veilig mijn geheime sleutel? Landen die hun ambassades van geheime berichten willen voorzien, moeten koeriers over de wereld laten reizen om de geheime sleutels te bezorgen. Voor eenmalige contacten geldt zelfs: als je een veilig kanaal hebt om die sleutel te versturen, kan je net zo goed meteen het niet-vercijferde bericht versturen. Internetbetalingen zijn daarvan een voorbeeld – al dacht toen niemand daar nog aan.

De eer voor de public key sleuteluitwisseling is gegaan naar Whitfield Diffie en Martin Hellman, die hun methode in 1976 meteen konden publiceren omdat ze bij een universiteit werkten. Hun methode was identiek aan die van de Britten, en gebaseerd op de eigenschappen van de *discrete logaritme*. Met dit Diffie-Hellmanprotocol kunnen twee partijen samen een geheime sleutel creëren via een onveilig kanaal, waarbij het niets uitmaakt dat dit eventueel wordt afgeluisterd. Deze geheime sleutel is vervolgens te gebruiken om elkaar berichten te sturen die zijn vercijferd met triple-DES of AES. Met een kleine aanpassing kan het protocol ook rechtstreeks worden gebruikt om boodschappen vercijferd te versturen. Het algoritme staat in detail beschreven in het kader op pagina 7.

RSA Korte tijd later, in 1977, ontwikkelden Ron Rivest, Adi Shamir en Len Adleman een vergelijkbaar algoritme. Kern van het algoritme is het feit, dat het makkelijk is om het product m van twee grote priemgetallen p en q uit te rekenen, maar uiterst moeilijk om m te factoriseren, dat wil zeggen uit een gegeven m de p en q terug te vinden. Hoe RSA werkt, staat in het kader hieronder.

Iedereen kan met RSA een publieke en een geheime sleutel aanmaken. De publieke sleutel zet je op je website, en iedereen kan je zonder voorafgaand contact een vercijferde boodschap sturen, die alleen jij, dankzij je geheime sleutel, kunt ontcijferen. In theorie is er wel een 1-op-1 verband tussen de publieke en de geheime sleutel (anders zou het systeem niet werken), maar als de sleutel lang genoeg is, is het in de praktijk onmogelijk om uit de publieke sleutel de geheime sleutel af te leiden.

Maar welke sleutel is 'lang genoeg'? De veilige grens is sinds de introductie van RSA al flink opgerekt. Het RSA-systeem werd nota bene voor het eerst gepresenteerd in de beroemde column van Martin Gardner in het populair-wetenschappelijke blad *Scientific American*. Daar zat toen een uitda-

HOE WERKT RSA?

In het kort luidt het recept om RSA-sleutels te maken als volgt:

1. Kies grote priemgetallen p en q (minstens 100 cijfers elk).
2. Bepaal de modulus $m = p \times q$.
3. Bereken $n = \text{kgv}(p - 1, q - 1)$.
4. Kies een vercijferexponent e waarvoor geldt $\text{ggd}(e, n) = 1$.
5. Bereken d zo, dat $e \times d \equiv 1 \pmod{n}$.
6. Maak de getallen m en e bekend. Samen vormen die de *openbare sleutel*.
7. Houd d geheim. Dat is de *geheime sleutel*.
8. Vercijferen: $E(x) \equiv x^e \pmod{m}$.
9. Ontcijferen: $D(y) \equiv y^d \pmod{m}$.

In *Pythagoras* 37-5 (juni 1998) schreven Jan van de Craats en Wieb Bosma een uitgebreid artikel over de werking van RSA. Dat artikel is in pdf te vinden op onze website www.pythagoras.nu (klik in het linkermenu op 'Archief').

PUBLIEKE SLEUTEL UITWISSELING VOLGENS DIFFIE EN HELLMAN Om de Diffie-Hellman sleuteluitwisseling te begrijpen, is wat basiskennis van *modulorekenen* en machtsverheffen nodig. Modulo n rekenen houdt in dat je veelvouden van n niet meerekent. Als je modulo 100 rekent, houd je alleen rekening met de laatste twee cijfers van de getallen. $11 \times 41 = 451$, maar modulo 100 geldt $11 \times 41 \equiv 51 \pmod{100}$.

Bij 'Diffie-Hellman' kiezen we eerst een priemgetal als modulus. Als voorbeeld nemen we een klein priemgetal, namelijk 31, zodat je alles met pen en papier kunt narekenen. Voor echte toepassingen zijn de priemgetallen veel groter.

Nu het machtsverheffen. We nemen *grondtal* 3 en berekenen 3^0, 3^1, 3^2, 3^3, ... (mod 31), totdat een patroon opduikt (links staat steeds de exponent van grondtal 3, rechts de uitkomst modulo 31):

0	1	5	26	10	25	15	30	20	5	25	6	30	1
1	3	6	16	11	13	16	28	21	15	26	18	31	3
2	9	7	17	12	8	17	22	22	14	27	23	32	9
3	27	8	20	13	24	18	4	23	11	28	7	33	27
4	19	9	29	14	10	19	12	24	2	29	21	34	…

Je ziet vanaf $3^{30} \equiv 1 \pmod{31}$ herhaling optreden, dus $3^{30} \equiv 3^0$, $3^{31} \equiv 3^1$, $3^{32} \equiv 3^2$, enzovoort. Als je modulo een priemgetal $p > 2$ rekent, dan geldt dat $g^{p-1} \equiv 1$ (zoals we al zagen bij het priemgetal 31). Dit is de *Kleine Stelling van Fermat*. Bovendien is er altijd een g te vinden waarvoor $g^k \not\equiv 1$, voor alle $0 < k < p - 1$. Een dergelijke g heet een *voortbrenger* van de verzameling $\{1, 2, 3, \ldots, p - 1\}$. Een gevolg is dat $\{g^0, g^1, g^2, \ldots, g^{p-2}\} = \{1, 2, 3, ..., p - 1\}$. Met andere woorden, de uitkomsten $g^0 \pmod{31}$, …, $g^{p-2} \pmod{31}$ nemen alle waarden van 1 tot en met $p - 1$ aan. Dus elke waarde komt precies één keer aan bod, en geen enkele wordt overgeslagen. Iets algemener geformuleerd: de functie $f(k) = g^k \pmod{p}$ $(k = 0, 1, \ldots, p - 2)$ husselt de getallen $\{0, 1, \ldots, p - 2\}$ door elkaar, en wel op een manier waar schijnbaar geen enkel patroon in zit.

De waarde van $f(k)$ is voor een gegeven k simpel uit te rekenen (al kan het flink wat rekentijd vergen als k groot is). Maar omgekeerd, als een uitkomst $g^k \pmod{p}$ gegeven is, is het heel moeilijk om de bijbehorende k te vinden. Dat lukt eigenlijk alleen als je een complete lijst van alle $f(k)$'s maakt (net als hierboven met de machten van 3) en de juiste waarde terugzoekt.

Voor priemgetal 31 is dat nog best te doen, maar in echte cryptografische toepassingen gebruikt men priemgetallen van minstens 150 cijfers. Een volledige lijst van de functiewaarden $f(k)$ zou dan 10^{150} getallen omvatten. Het heelal bevat maar iets als 10^{80} atomen, dus je snapt dat dit in de praktijk een probleem is.

Het berekenen van $f(k)$ vergt het tot de macht k verheffen van een grondtal. Het vinden van k als $f(k)$ gegeven is, komt neer op het omgekeerde, namelijk de logaritme nemen van $f(k)$. Omdat we alleen met gehele (discrete) getallen werken, noemt men dit de *discrete logaritme*.

Net als de (gewone) logaritme noteren we deze functie met log. Voor priem 31 en grondtal 3 (zie weer bovenstaande reeks van machten van 3) kunnen we bijvoorbeeld opzoeken dat $\log(10) = 14$, want $3^{14} \equiv 10$. Voor de discrete logaritme geldt, net als voor de gewone logaritme, dat $\log(ab) = \log(a) + \log(b)$ en $(\log(a))^n = n \log(a)$.

Hoewel de discrete logaritme al honderden jaren bekend was, kwamen Diffie en Hellman pas in 1976 op het idee om dit te gebruiken voor het creëren van een geheime sleutel via een communicatiemiddel dat best afgeluisterd mag worden. Dit gaat als volgt. Stel, Alice en Bob willen veilig met elkaar communiceren. Zij spreken af om priemgetal p en voortbrenger g te gaan gebruiken. Dit kan over een onveilig communicatiekanaal, want iedereen mag p en g weten.

Alice kiest nu een geheim getal a kleiner dan $p - 1$. Haar publieke sleutel wordt $A \equiv g^a \pmod{p}$. Bob doet hetzelfde: hij kiest zijn geheime getal b en berekent zijn publieke sleutel $B \equiv g^b \pmod{p}$. Aangezien A en B openbaar zijn (ze worden bijvoorbeeld op internet gezet) kan Bob beschikken over A en Alice over B. Daardoor kan Bob $A^b \pmod{p}$ berekenen en Alice $B^a \pmod{p}$. En nu de clou: $A^b \equiv B^a \pmod{p}$! Dit zou zelfs gelden als je niet modulo p rekent, ga maar na: $A^b \equiv (g^a)^b \equiv g^{ab} \equiv (g^b)^a \equiv B^a$.

Alice en Bob beschikken nu dus over een gemeenschappelijke geheime sleutel $A^b \equiv B^a \pmod{p}$ die niemand anders kan weten, zonder dat ze informatie naar elkaar hoefden te sturen die geheim moest blijven. Als p 150 cijfers groot is, dan is ook A^b een getal van 150 cijfers. Zo'n getal kan uitstekend worden gebruikt als geheime sleutel voor een ander geheimschrift, bijvoorbeeld triple-DES of AES.

Opdracht. Kies voor $a = 13$ en $b = 23$ en verifieer bovenstaande met de tabel.

ging bij, om een codebericht te kraken dat was vercijferd met een sleutel van 129 decimale cijfers (ongeveer 297 bits). Pas op 16 april 1994, 17 jaar later, kon de Nederlandse wiskundige Arjen Lenstra bekend maken dat hij de boodschap ontcijferd had, door een combinatie van veel computerkracht en geavanceerde wiskunde. Het bedrijf dat RSA exploiteerde stelde daarna een hele lijst van uitdagingen met steeds langere sleutels op. Ze zijn op hun wenken bediend: in 1999 werd een RSA-sleutel van 512 bits gekraakt, in 2009 volgde een RSA-sleutel van 768 bits. Opnieuw waren hierbij Nederlandse wiskundigen nauw betrokken.

Toch kan je nu niet zeggen dat het RSA-systeem als zodanig gekraakt is. Dat zou pas het geval zijn als iemand een efficiënte methode vond om RSA-sleutels van een *willekeurige* lengte te kraken. Waarschijnlijk – banken zeggen daar in het openbaar niets over – gebruikt internetbankieren sleutels van 1024 bits, maar dat kan zonder veel moeite worden uitgebreid tot 2048 bits.

RSA is buitengewoon grondig getest en heeft tot nu toe alle aanvallen weerstaan. Echter, het is lang niet voor alle toepassingen geschikt, omdat het relatief veel rekencapaciteit per vercijferde bit vergt. RSA kan daarom nog niet ingebouwd worden in chipkaarten, en zelfs moderne computers kunnen niet met RSA *real time* spraak of andere omvangrijke datastromen vercijferen.

RSA werd in 1977 direct na de introductie gepatenteerd. Men moest voor elke toepassing waarbij RSA werd gebruikt betalen voor het gebruik. In 2007 verliepen de belangrijkste patenten. Momenteel kan RSA probleemloos worden toegepast.

CHIPKAARTEN Een verhaal apart is de beveiliging van chipkaarten. Op chipkaarten worden vaak *schuifregisters*, zie het kader op pagina 9, als beveiliging gebruikt, omdat ze weinig geheugenruimte en rekencapaciteit vergen. De OV-chipkaart die de laatste tijd telkens in het nieuws komt, is een *Mifare Classic-chip* van de producent NXP. De Classic is een van de simpelste en goedkoopste chips, en het crypto-algoritme is een eenvoudig te kraken schuifregister, Crypto-1.

Vanaf de eerste introductie van de OV-chip werd hier al voor gewaarschuwd, en in 2007 werd de Mifare Classic voor het eerst openlijk gekraakt. Dit jaar is het proces om de chip te kraken dusdanig versimpeld dat het met een PC en op internet te downloaden software te doen is. Je kunt de kaart dan opladen zonder te betalen (dit is overigens wel een strafbaar feit!).

De Mifare Classic wordt tevens gebruikt door talloze bedrijven en overheidsinstanties in toegangspasjes, dus er doemt een serieus veiligheidsprobleem op. Is de Mifare Classic dus een slechte chipkaart? Dat ligt genuanceerder. De chip werd ontwikkeld in 1994, toen Crypto-1 nog veilig was. Doordat er momenteel zoveel toepassingen zijn van de Mifare Classic, is deze het doelwit geworden van heel veel hackers. Er zijn waarschijnlijk legio zwakkere chipkaarten, die alleen maar veilig lijken omdat hackers er weinig belangstelling voor hebben. Je kunt ook zeggen dat de Mifare Classic ten onder is gegaan aan zijn eigen succes.

KWANTUMCRYPTOGRAFIE & KWANTUMCOMPUTER Het volgende stadium in de cryptografie leunt sterker op de fysica dan op de wiskunde. Volgens de kwantumtheorie hebben deeltjes als elektronen en fotonen zulke vreemde eigenschappen, dat ze gebruikt kunnen worden om boodschappen gegarandeerd veilig over te brengen. Twee fotonen kunnen, als ze uit een gemeenschappelijke bron komen, 'verstrengeld' zijn, wat inhoudt dat ze van elkaar weten wat er met ze gebeurt, ook als ze al kilometers (of lichtjaren) van elkaar verwijderd geraakt zijn. Je kunt als verzender dan de fotonen die de ene kant op gaan gebruiken om een boodschap over te brengen (ongeveer als in een Morsecode), terwijl je aan de fotonen die de andere kant op gaan kunt aflezen, of er tussenin niemand met de boodschap knoeit.

Diezelfde kwantumverstrengeling is een potentiële bedreiging voor RSA (en Diffie-Hellman). Het factoriseren van een groot getal m komt voor een flink deel neer op het testen van een gigantisch aantal mogelijke delers van m. Een computer moet zo'n getal als bits in zijn geheugen laden (0, 0, 1, 0, 0, 1, …) en de getallen de een na de ander uitproberen, wat voor veel mogelijkheden langer duurt dan de leeftijd van het heelal.

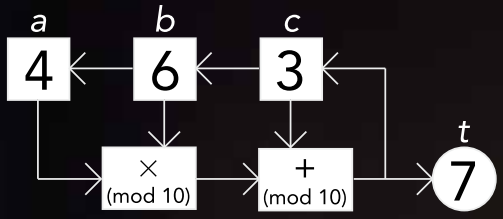
Het bizarre van een kwantumcomputer is dat diens geheugen bestaat uit kwantumbits, die, zolang ze verstrengeld zijn, in zekere zin alle mogelijke toestanden tegelijk verkeren. Dus elke kwantumbit is dan 0 en 1 tegelijk, en N verstrengelde kwantumbits stellen alle getallen van N bits tegelijk voor. Er bestaat daardoor een algoritme op een kwantumcomputer dat enorm grote getallen bliksemsnel kan factoriseren: hij probeert in zekere zin alle mogelijke delers tegelijk uit. Dat zou het einde van RSA en internetbetalingen betekenen.

Is het al bijna tijd om je spaargeld van de bank te halen en het weer in een oude sok te stoppen? In 2007 is men erin geslaagd een kwantumcomputer te bouwen met een handjevol kwantumbits, die het getal 15 correct factoriseerde in 5×3. Verdere vooruitgang is sindsdien niet bekend gemaakt. ■

Schuifregister

Klare tekst:

MIJN PINCODE IS NEGEN ZES ZES NUL



a		b		c					
4	×	6	+	3	≡	7	M	+7	T
6	×	3	+	7	≡	5	I	+5	N
3	×	7	+	5	≡	6	J	+6	P
7	×	5	+	6	≡	1	N	+1	O
5	×	6	+	1	≡	1	P	+1	Q
		⋮				⋮			⋮

Vercijferde tekst:

TNPOQ PVHPE KPVSK HKPHE YFKUV UR

Een schuifregister bevat een aantal registers (hier *a*, *b* en *c*). Deze registers worden bij aanvang gevuld met initiële waarden (hier 4, 6 en 3). Vervolgens gaat het schuifregister stappen. Bij elke stap wordt de terugkoppelwaarde $t \equiv a \times b + c \pmod{10}$ berekend. Hierbij staat 'mod 10' voor 'modulo 10'; dat betekent dat alleen het laatste cijfer van het berekende getal meetelt. De terugkoppelwaarde *t* wordt opgeteld bij de boodschap. Tevens worden de registers *a*, *b* en *c* vervangen door *b*, *c* en *t*.

Een schuifregister met *p* mogelijke waarden per register en *q* registers herhaalt zichzelf na maximaal p^q stappen. Deze heeft maar drie registers met elk 10 toestanden, dus hij herhaalt zich na maximaal 1000 stappen. Maar dit hangt ook van de terugkoppelfunctie en de initiële waarden af: als die niet goed gekozen zijn, herhaalt de output zich al sneller, of hij ontaardt in een serie nullen.

Opdracht: Hoe kan er met dit schuifregister worden ontcijferd?
Om over na te denken: Onderzoek zelf de hier gekozen terugkoppelfunctie: haalt die de maximale periode? Bij welke initiële waarden? Kun je betere bedenken?

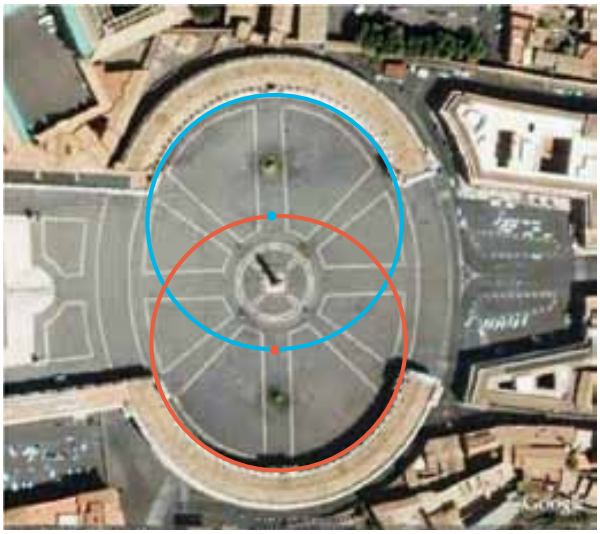
In het septembernummer kon je lezen over de vorm van het Sint-Pietersplein, ontworpen door Bernini, een Italiaanse kunstenaar en architect uit de barok. In dit artikel bekijken we Bernini's constructie nader, en bespreken we het kleinste kerkje van Rome: de San Carlino, een juweeltje van Borromini, tijdgenoot van Bernini.

■ door Alex van den Brandhof

ROMEINSE BAROK

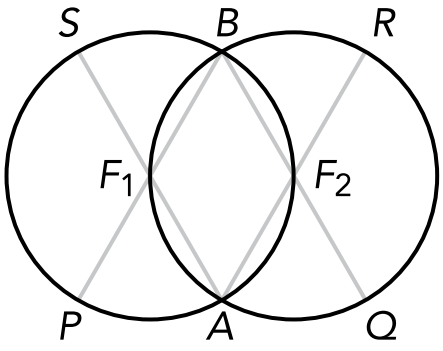
In *Pythagoras* 50-1 (september 2010) schreef ik over de vorm van het Sint-Pietersplein in Rome. De ovale vorm van het plein baseerde de architect Gian Lorenzo Bernini (1598-1680) op *cirkels*, in tegenstelling tot wat in veel toeristenboekjes over Rome vermeld staat: daar wordt meestal over een *ellips* gesproken. Uit enkele reacties van lezers bleek dat er nog wat meer over Bernini's constructie valt te zeggen. Ik werd geattendeerd op het boek *Geometry Civilized: History, Culture, and Technique* van J.L. Heilbron, waarin Bernini's constructie wordt beschreven.

Neem je de cirkels die om de *binnenkant* van de zuilenrijen gaan, dan heb je een zogeheten *vesica piscis*: twee cirkels die door elkaars middelpunt gaan, zoals uit de Google Earth afbeelding (figuur 1) blijkt. In figuur 2 zie je de constructie; de twee cirkels met middelpunten F_1 en F_2 snijden elkaar in A en B. Om de punten P en Q, en ook R en S, met elkaar te verbinden, gebruikte Bernini óók cirkelsegmenten. De boog PQ is een deel van de cirkel met middelpunt B en straal BP. De boog RS is een deel van de cirkel met middelpunt A en straal AR. De ovale vorm die je dan krijgt, zie je in figuur 3.

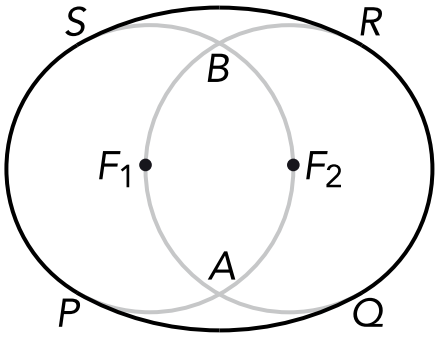


Figuur 1 Google Earth-afbeelding van het Sint-Pietersplein. Het plein is gebaseerd op een zogeheten *vesica piscis*.

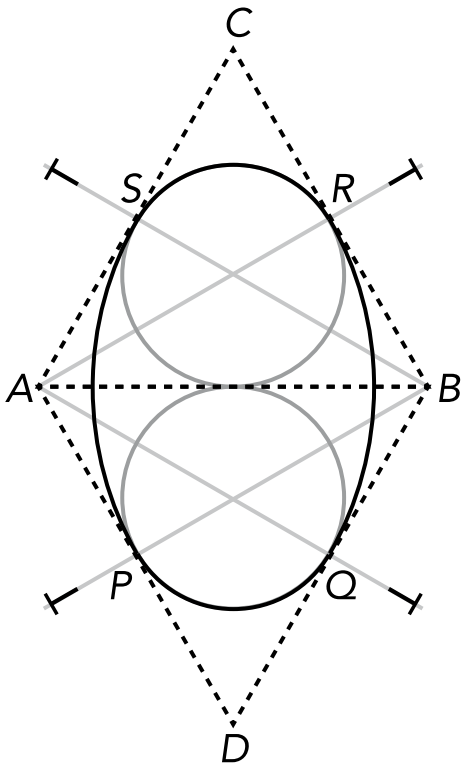
SAN CARLINO Italiaanse architecten uit de zestiende eeuw waren dol op cirkels. Niet alleen Bernini, ook zijn aartsrivaal Francesco Borromini (1599-1667) koos de cirkel vaak als uitgangspunt. Borromini was veel minder succesvol dan Bernini en dat zal eerder met zijn introverte en zwaarmoe-



Figuur 2 De basis van het Sint-Pietersplein; twee cirkels die door elkaars middelpunt gaan.



Figuur 3 De ovale vorm van het Sint-Pietersplein. Ook de bogen PQ en RS zijn delen van cirkels.

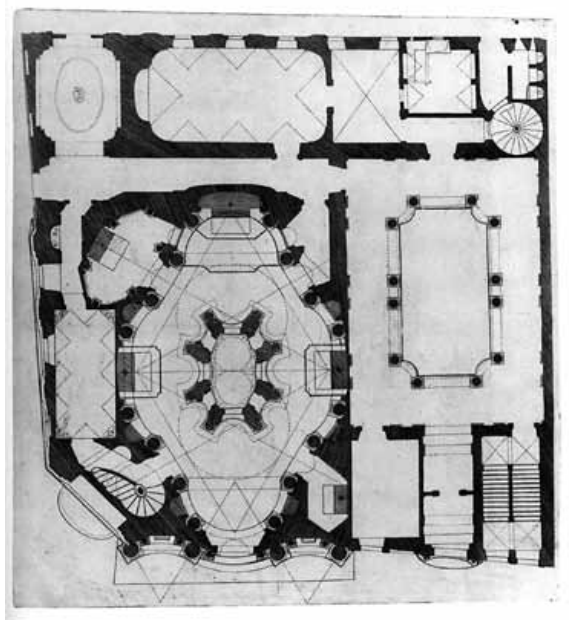


Figuur 4 De ovale vorm van het grondplan en de koepel van Borromini's *San Carlo alle Quattro Fontane*.

dige karakter te maken hebben gehad dan met zijn kwaliteiten: volgens velen had Borromini veel betere papieren dan Bernini, als het om architectuur ging. In Rome zijn een paar echte juweeltjes van Borromini te vinden. Een daarvan is de *San Carlo alle Quattro Fontane*, ook wel *San Carlino* ('Kareltje') genoemd. Gelegen op het kruispunt van de drukke Via del Quirinale en de Via delle Quattro Fontane staat dit prachtige kerkje, waarvan wordt gezegd dat het zó klein is dat het in een pilaar van de Sint-Pieter past. Met zijn convexe en concave vormen is de San Carlino een hoogtepunt van de barokke architectuur.

Net als Bernini bij het Sint-Pietersplein deed, koos Borromini voor de San Carlino voor een ovaal. Hij ging uit van twee even grote gelijkzijdige driehoeken *ABC* en *ABD* (de zijde *AB* hebben ze gemeenschappelijk) met hun ingeschreven cirkels, zie figuur 4. De bogen *PS* en *QR* completeren de ovale vorm. Boog *PS* is een deel van de cirkel met middelpunt *B* en straal *BP*, boog *QR* ligt op de cirkel met middelpunt *A* en straal *AQ*.

Deze ovale vorm is de basis voor het grondplan van de San Carlino, zie figuur 5. De hoekpunten *A*, *B*, *C* en *D* in figuur 4 zijn de middens van de apsissen van het kerkje. En de assen van de kapelletjes liggen op de symmetrieassen van de driehoeken *ABC* en *ABD*.



Figuur 5 Het volledige grondplan van de San Carlino, met diverse geometrische verhoudingen.

Figuur 6 De koepel van de San Carlino.

De ovale vorm die Borromini ontwierp, gebruikte hij tevens als basis voor de prachtige, lichte koepel, zie figuur 6. De decoraties in de koepel zijn magnifiek: Borromini gebruikte een geometrisch patroon dat is gebaseerd op een mozaïek van de kunstenaar Sebastiano Serlio (1475-1554). Borromini wist dit patroon op een ingenieuze wijze op driedimensionale wijze te verwerken. ■

LITERATUUR

J.L. Heilbron, *Geometry civilized: history, culture, and technique*, Oxford University Press (1998)
Anthony Blunt, *Roman Baroque*, Pallas Athene (2001)
Anthony Blunt, *Borromini*, Harvard University Press (1979)

JOURNAAL

■ door Alex van den Brandhof

Abelprijs voor pionier van hogere dimensies

De Amerikaan John Milnor is de winnaar van de Abelprijs 2011. Dit maakte de Noorse Academie van Wetenschappen bekend op 23 maart.

De jury roemt Milnor vanwege zijn 'baanbrekende ontdekkingen in de topologie, meetkunde en algebra'. Wiskundige Timothy Gowers eerde Milnor tijdens zijn speech die via internet live te volgen was. Te zien was hoe hij via de telefoon contact kreeg met de tachtigjarige prijswinnaar. Op Gowers' vraag of hij zichzelf beschouwt als probleemoplosser of theoriebouwer, antwoordde Milnor: 'A problem solver. I never looked for the big theory, but tried to make small steps and ask intriguing questions. But you never know what can come from this.'

Milnors diepzinnige ideeën en fundamentele ontdekkingen zijn van grote invloed geweest op de vorming van het wiskundige landschap van de tweede helft van de twintigste eeuw. Gedurende zes decennia heeft Milnor een belangrijke stempel gedrukt op de moderne wiskunde. Dat blijkt wel uit alle begrippen waar de naam van Milnor aan gehecht is: Milnor-getal, Milnor-afbeelding en Milnor-vermoeden, om er maar een paar te noemen. De zogeheten 'exotische' 7-dimensionale bollen die hij in 1956 construeerde en waarmee hij een opzienbarend resultaat in de topologie boekte, werden onmiddellijk herkend als meesterwerk.

Op 24 mei zal Milnor tijdens een feestelijke ceremonie de prijs – een bedrag van zes miljoen Noorse kronen (ongeveer 760.000 euro) – ontvangen uit handen van koning Harald V.

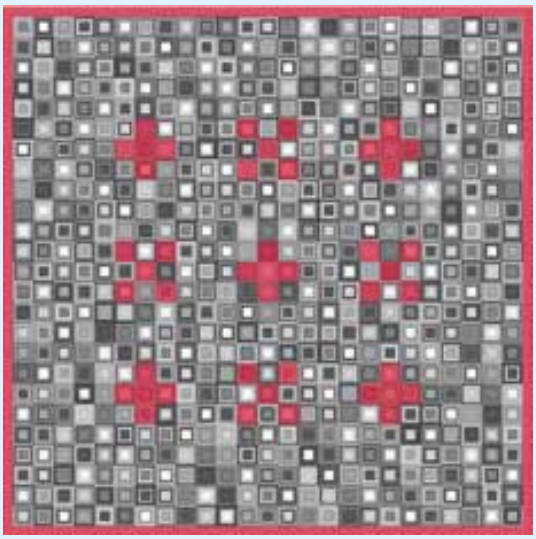
Magisch vierkant: een wiskunstig object

Margaret Kepner won de eerste prijs bij de *Mathematical Art Exhibition Award*, die sinds 2009 jaarlijks wordt uitgereikt. Kepner baseerde haar mathematische kunstwerk, getiteld *Magic Square 25 Study*, op een magisch vierkant.

Een magisch vierkant is een vierkant van n bij n hokjes waarin n^2 getallen zodanig zijn geplaatst, dat de som in elke rij, elke kolom en de beide diagonalen steeds hetzelfde is. Deze som heet de magische constante. In een catalogus van haar werk schrijft Kepner: 'Mijn ontwerp is gebaseerd op een vierkant van 25 bij 25 met de getallen 0 tot en met 624. De magische constante is 7800. De getallen in het vierkant worden gerepresenteerd door een visueel "basis-5-systeem".'

Kepner schreef de getallen 0 tot en met 624 in het vijftallig stelsel. Bijvoorbeeld het getal 8 wordt 13 ($= 1 \times 5^1 + 3 \times 5^0$) en het getal 477 wordt 3402 ($= 3 \times 5^3 + 4 \times 5^2 + 0 \times 5^1 + 2 \times 5^0$). Deze codering leverde een patroon op van 625 unieke, 'geneste vierkanten' in grijstinten.

Het vierkant van Kepner bevat bovendien 25 kleinere vierkanten van 5 bij 5, die ook allemaal magisch zijn met magische constante 1560. Ten slotte zijn er nog andere groepen van 5 vierkantjes die som 1560 hebben. De gekleurde accenten in *Magic Square 25 Study* tonen een paar van deze magische 'substructuren'.



Margaret Kepner, *Magic Square 25 Study* (2010), 32 × 32 cm. Afbeelding: © American Mathematical Society

Wiskunde-T-shirts

Onlangs is de Nederlandstalige website www.lovelymath.com van start gegaan. De site is een webwinkel voor wiskunde-T-shirts én een nieuwsplein dat bericht over wiskundige ontwikkelingen.

De schoonheid, de kracht en de geschiedenis van de wiskunde: dat zijn de drijfveren van lovelymath.com. Deze drie aspecten komen tot uiting in hun fraaie T-shirts. Er is een T-shirt waarop 'de mooiste wiskundevergelijking ooit' – van Leonhard Euler – prijkt, zie ook het artikel op pagina 23. Verder is er een shirt met de kleinste perfecte vierkantverdeling, gevonden door de Nederlandse wiskundige Arie Duijvesteijn. En er is een shirt waarop de stelling van Georg Pick – voor de oppervlaktebepaling van een onregelmatige veelhoek – aanschouwelijk is gemaakt. Op de site staat een uitleg over de wiskunde op de T-shirts. Verder bericht lovelymath.com over wiskundige ontwikkelingen binnen het onderwijs, de wetenschap, het bedrijfsleven en de maatschappij.

Partitiegetallen gedragen zich als fractals

Al eeuwenlang proberen de knapste wiskundekoppen grip te krijgen op de zogeheten *partitiefunctie*. Deze functie geeft aan op hoeveel manieren een aantal knikkers kan worden opgedeeld in groepjes. Amerikaanse wiskundigen hebben nieuwe baanbrekende resultaten op dit gebied geboekt.

Als je 5 knikkers hebt, kun je die bijvoorbeeld verdelen in vier groepjes: één groepje van 2 en drie groepjes van 1. Als som kun je dit schrijven als 5 = 2 + 1 + 1 + 1. Een andere partitie is 5 = 3 + 2 (twee groepjes). Ook 5 = 1 + 1 + 1 + 1 + 1 (vijf groepjes) en 5 = 5 (één groepje) zijn partities. In totaal zijn er 7 partities van 5. We noteren dat als $p(5) = 7$.

In het algemeen geven we het aantal partities van n aan met $p(n)$. De rij partitiegetallen is de rij $p(1), p(2), p(3), \ldots$ Die rij begint zo: 1, 2, 3, 5, 7, 11, 15, 22, … De getallen worden al snel ongelofelijk groot. Zo is $p(20) = 627$ en $p(100)$ is al meer dan 190 miljoen.

Wiskundige Ken Ono heeft met een aantal collega's bewezen dat de partitiegetallen zich in zekere zin gedragen als *fractals*, een resultaat dat niemand eerder voor mogelijk had gehouden. Zij hebben deelbaarheidseigenschappen van partities ontrafeld en een theorie ontwikkeld die de 'oneindig herhalende' structuur verklaart. 'We hebben bewezen dat partitiegetallen een "fractale structuur" hebben voor elk priemgetal vanaf 5. Deze getallen zijn "zelfherhalend" *in a shocking way*', aldus Ono.

Het team van Ono vond de volgende formule die geldt voor het aantal partities van het getal $13^3n + 1007$:

$$p(13^3n + 1007) \equiv 6p(13n + 6) \pmod{13}.$$

Deze formule gaat uit van het priemgetal 13 en genereert een rij van eenvoudige lineaire combinaties van partitiegetallen deelbaar door 13. Het 'fractale' zit hem in het feit dat als je inzoomt op die rij, je een deelrij vindt waarvan lineaire combinaties van partitiegetallen deelbaar zijn door 13^2:

$$p(13^4n + 27371) \equiv 45p(13^2n + 162) \pmod{13^2}.$$

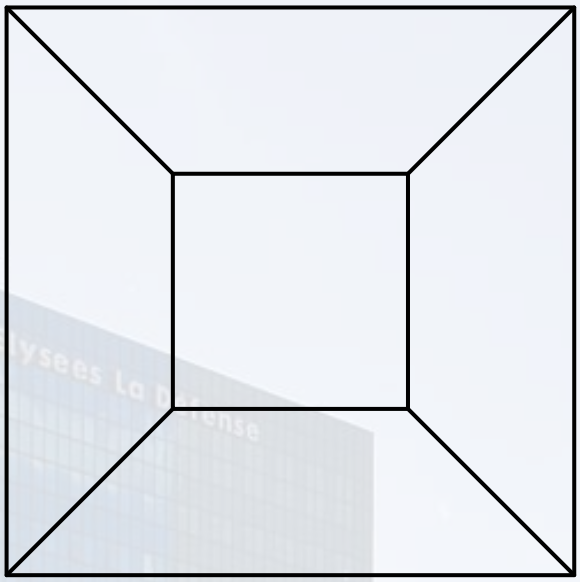
En als je nog verder inzoomt, levert dat iets soortgelijks voor 13^3, enzovoorts. In dit voorbeeld werd een formule met priemgetal 13 genomen. De wiskundigen bewezen een algemene stelling die zegt dat zulke formules bestaan voor élk priemgetal dat groter dan of gelijk is aan 5. Hoewel hun resultaat het *bestaan* van dergelijke formules garandeert, hebben ze geen algoritme gevonden om die formules te genereren. Of zo'n algoritme bestaat, is weer een andere vraag.

Alsof de gevonden fractale structuur nog niet genoeg was, hebben de wiskundigen nog een ander succes geboekt: ze hebben de eerste *eindige* formule opgesteld om partitiegetallen te berekenen. 'We hebben een functie P gevonden, een soort *magical oracle*', zegt Ono. 'Ik kan nu een willekeurig getal nemen; je stopt het in P en na een beetje rekenwerk heb ik het aantal partities van dat getal. De functie P gebruikt geen gruwelijke getallen met oneindig veel decimalen. Het is een eindige, algebraïsche formule. Het is dátgene, waar we al heel lang naar zochten.'

DE VIERDE DIMENSIE

In de serie 'Op reis' nemen we je mee naar een plaats waar wiskundig iets te beleven valt. In Parijs staat een projectie van de vierdimensional kubus: *La Grande Arche*.

■ tekst Klaas Pieter Hart, foto Pete Sieger



Als je in Parijs bent, neem dan lijn 1 van de Métro richting *La Défense*. Als het mooi weer is, stap dan uit bij het voorlaatste station *Esplanade de la Défense* en loop in de richting van het eindstation. Onderweg kun je allerlei fraaie sculpturen bewonderen, maar in de verte kun je het doel van je tocht al zien: een groot wit gebouw dat er uitziet als een holle kubus. Dat is de *Grande Arche*, een kantoorgebouw dat in 1989 geopend is.

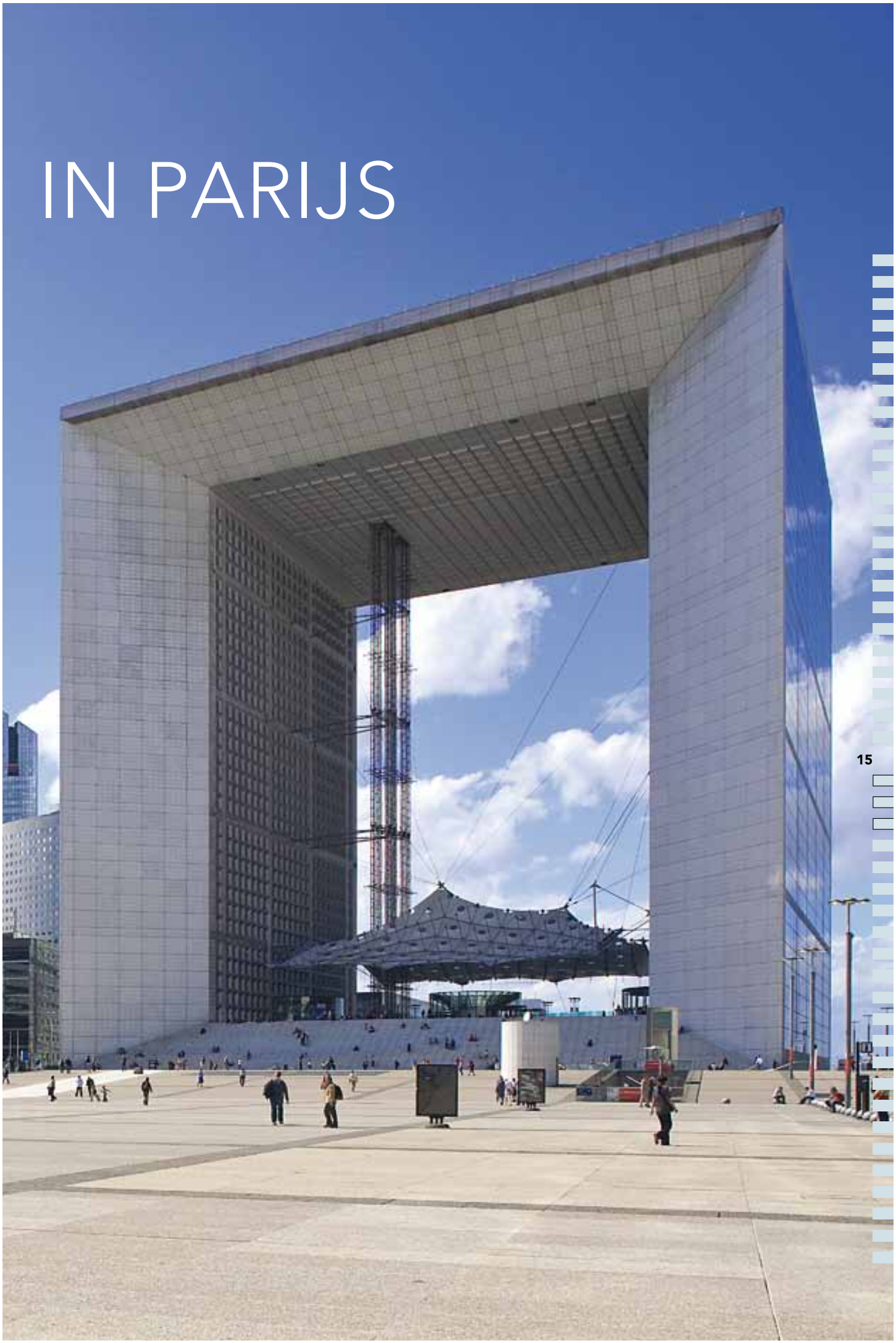
Het gebouw is bedacht door de Deense architect Johan Otto von Spreckelsen en zijn landgenoot Erik Reitzel. Als je goed kijkt, zie je twee kubussen in elkaar met verbindingslijnen tussen overeenkomstige hoekpunten. Zo vormt het gebouw een projectie van de vierdimensionale kubus in onze driedimenionale ruimte.

Om je voor te stellen hoe dat werkt, beginnen we met een nuldimensionale kubus: één punt. Dat punt verdubbelen we en we verbinden die punten met een lijn; zo ontstaat een ééndimensionale kubus, een lijnstuk. Door dat te verdubbelen en de twee kopieën te verbinden, ontstaat een tweedimensionale kubus: een vierkant dus. Een echte, driedimensionale, kubus maken we door dat vierkant te verdubbelen en met zijn evenbeeld te verbinden. In de bovenstaande lijntekening is het tweede vierkant naar achteren geschoven, zodat we als het ware recht de kubus in kijken.

La Grande Arche is gemaakt door een kopie van de buitenste kubus langs de vierde dimensie naar 'achteren' te schuiven en dan weer onze ruimte in te projecteren. De kubus is zó geplaatst dat de *Arc de Triomphe* precies halverwege het *Louvre* en La Grande Arche staat. Hij is een klein beetje gedraaid, 6° 33', ten opzichte van de verbindingslijn met het Louvre. Dat is omdat er spoorlijnen onder het gebouw lopen en ook om het dezelfde afwijking ten opzichte van die lijn als het Louvre te geven.

Jammer genoeg is het dak sinds april 2010 niet meer toegankelijk voor het publiek. Je kon in het restaurant lekker eten en je had een mooi uitzicht over Parijs. ■

IN PARIJS



Deze jaargang staat de prijsvraag van *Pythagoras* in het teken van het vijftigjarig jubileum. In de eerste vijf afleveringen verschijnt telkens een puzzel met het getal 50 als thema. In dit nummer vind je slotaflevering en de oplossing van aflevering 3.

■ door Matthijs Coster

50 POLYOMINO'S

Neem een velletje ruitjespapier en teken een aantal blokjes die steeds met minimaal één zijde aan elkaar grenzen. Een dergelijke figuur heet een *polyomino*. Er zijn bijzondere gevallen: bij twee blokjes praten we over een *domino*, bij drie blokjes over een *triomino*, bij vier blokjes over een *tetromino* (hier is het spelletje *Tetris* van afgeleid). Vijf aaneengesloten blokjes vormen een *pentomino* en zes blokjes een *hexomino*. Het aantal mogelijke domino's, triomino's, tetromino's, pentomino's en hexomino's is achtereenvolgens 1, 2, 5, 12 en 35.

In deze laatste aflevering van de jubileumprijsvraag gaan we uit van vijftig polyomino's. Je ziet ze in figuur 1: 1 domino (groen), 2 triomino's (geel), 12 pentomino's (blauw) en 35 hexomino's (rood). Deze vijftig figuren bestrijken een oppervlak van 278. De polyomino's passen precies in figuur 2, een vierkant van 17 bij 17, met een gat erin dat uit 11 blokjes bestaat.

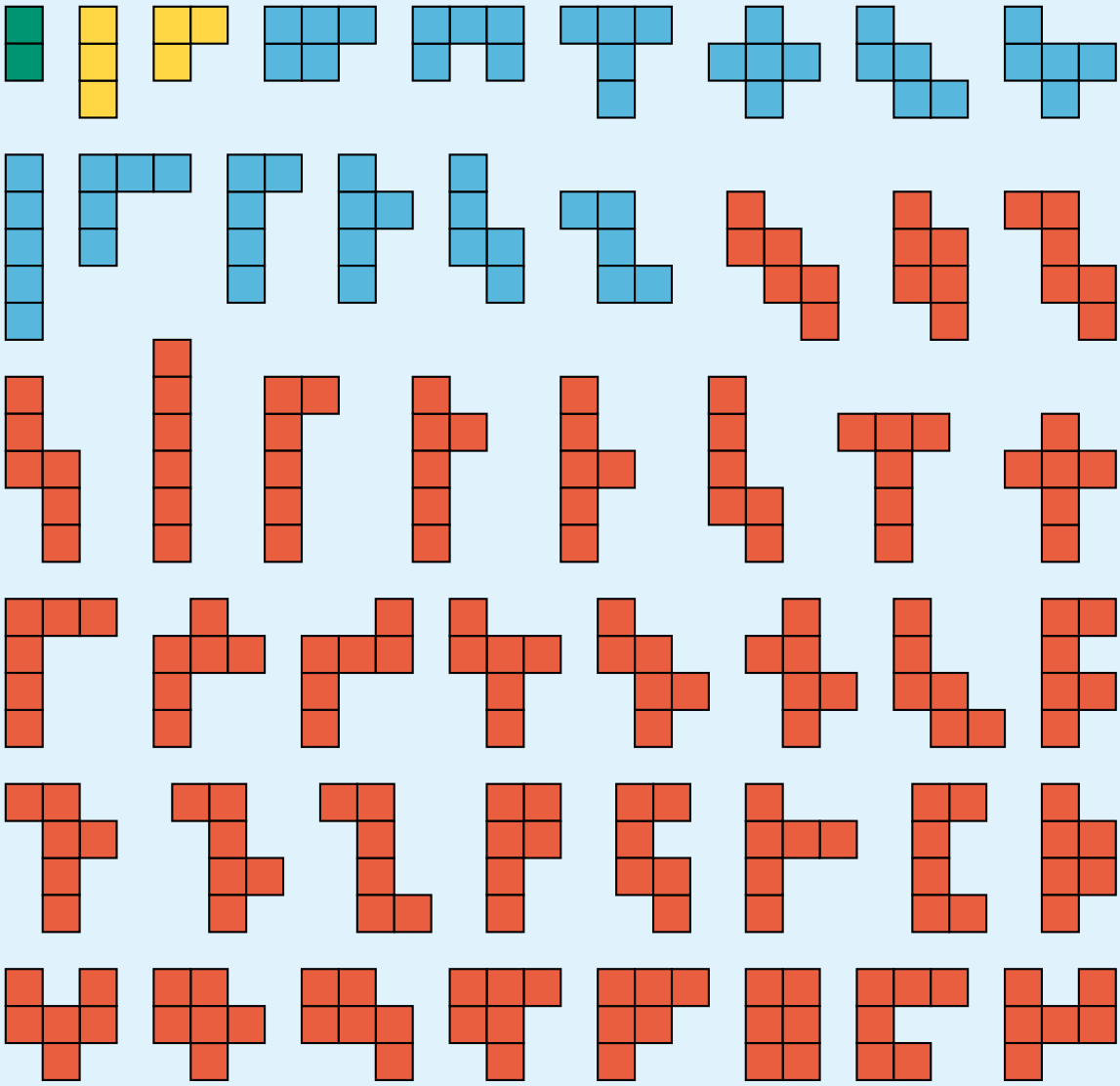
OPGAVE **Rangschik de vijftig polyomino's van figuur 1 zodanig in figuur 2, dat alle grijze blokjes gevuld zijn. Je mag de figuren draaien (roteren) en omdraaien (spiegelen).**

De redactie schat dat er minimaal een miljard oplossingen bestaan voor deze puzzel! Het volstaat om één oplossing in te sturen. Voor onderbouwleerlingen is het vinden van een willekeurige correcte invulling al een hele prestatie. Voor de anderen hebben we een extra uitdaging in petto: probeer de puzzel zo te leggen, dat er zoveel mogelijk *symmetrieën* ontstaan. We onderscheiden twee soorten symmetrieën. Bij de eerste soort verwissel je een deel van de puzzel met een ander deel van dezelfde vorm. Fraaier is natuurlijk als je drie of meer exacte kopieën hebt die met elkaar kunnen worden uitgewisseld (zie figuur 3 op pagina 18 voor een voorbeeld). Bij de tweede soort symmetrie haal je een stuk van de puzzel eruit, en leg je dat stuk met dezelfde polyomino's; op een andere manier, maar met behoud van symmetrieën (zie figuur 4 en 5 op pagina 18 voor een voorbeeld). Wie legt de puzzel met het grootste aantal symmetrieën?

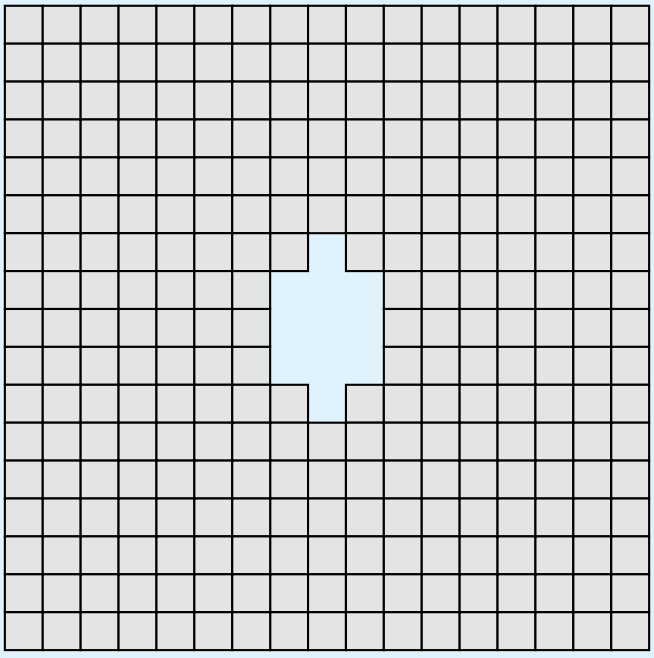
PUZZELEN OP DE COMPUTER Je kunt de polynomino's op pagina 17 uitknippen en daarmee schuiven (dit artikel staat ook in pdf op onze website). Maar je kunt ook digitaal puzzelen. Ga naar www.pythagoras.nu en klik in het linkermenu op 'Prijsvraag'. Je treft daar een Excelbestand aan met de vijftig figuren. Tevens staat er een handleiding hoe je de figuren kunt draaien en spiegelen. Heb je geen Excel? Geen nood! Er staat tevens een bestand dat gebruikt kan worden met Geogebra (een gratis softwarepakket, dat ook als applet te gebruiken is). Met dank aan Odette De Meulemeester, die de applet voor ons maakte.

INZENDEN Stuur je oplossing naar **prijsvraag@pythagoras.nu** of per analoge post naar **K.P. Hart, Faculteit EWI, TU Delft, Postbus 5031, 2600 GA Delft.** Noteer in de linkerbovenhoek van de envelop 'Pythagoras Jubileumprijsvraag'. Vermeld je naam, adres, telefoonnummer, leeftijd en, als je scholier bent, ook je school en je klas. Je kunt ook met je hele klas meedoen; vermeld in dat geval ook de naam van de wiskundedocent. Als je oplossing symmetrieën bevat, stuur dan een beschrijving mee van die symmetrieën. Omdat we al in het volgende nummer de oplossing en prijswinnaars willen publiceren, moet je gauw inzenden: de deadline is **15 mei 2011.** Veel succes met deze slotaflevering van de jubileumprijsvraag!

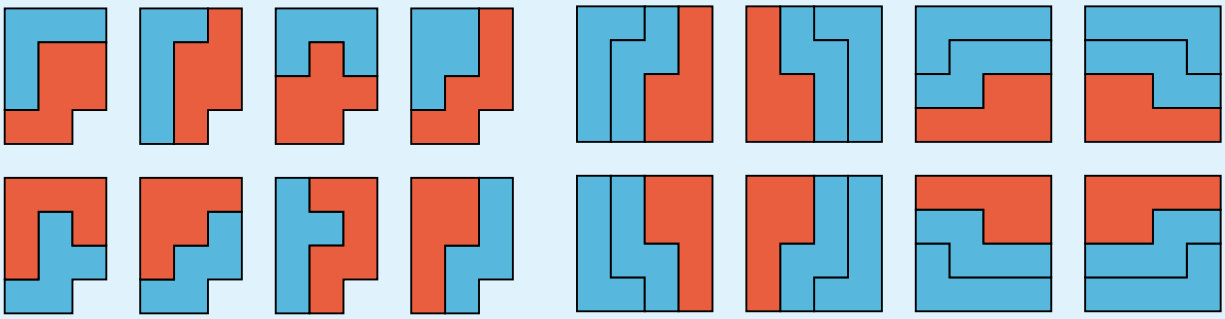
PRIJZEN Per aflevering geven we een Irisbon van 20 euro weg. Na 15 mei maakt de jury de totaalbalans van alle afleveringen op en zijn er de volgende prijzen te winnen: twee eerste prijzen van 100 euro, twee tweede prijzen van 50 euro, vier boekenbonnen van 25 euro en diverse fraaie wiskundeboeken. Bij min of meer gelijkwaardige inzendingen geeft de jury de voorkeur aan leerlingen boven niet-leerlingen.



Figuur 1 De puzzelstukjes: vijftig polyomino's.

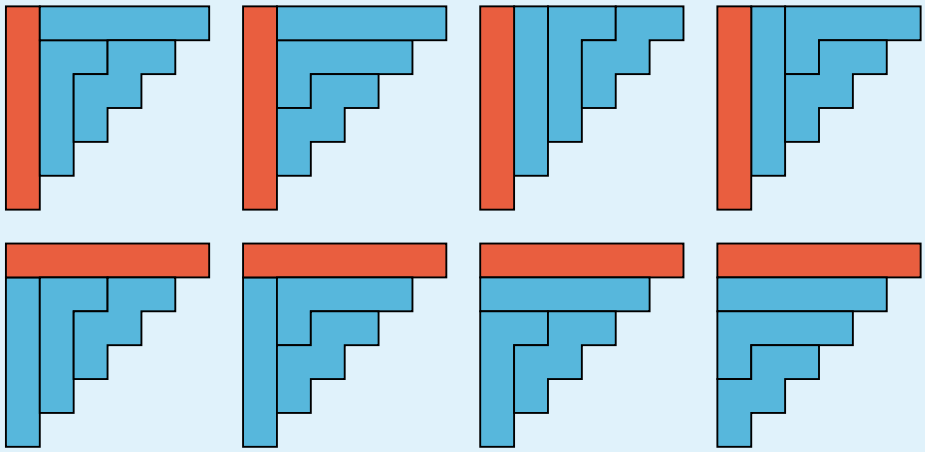


Figuur 2 Het grijze gebied moet geheel worden bedekt met de vijftig polyomino's.



Figuur 3 Deze figuren bestaan steeds uit een combinatie van een pentomino en een hexomino. Als je in de puzzel al deze acht stukken kunt leggen, dan kun je vervolgens op vele manieren de stukken met elkaar uitwisselen.

Figuur 4 Acht verschillende manieren om een vierkant te leggen met drie polyomino's (een hexomino en twee pentomino's), met behoud van symmetrieën: het vierkant kun je (herhaald) 90 graden draaien, en je kunt het vierkant spiegelen over een horizontale as (en vervolgens één keer of vaker draaien).



Figuur 5 Acht verschillende manieren om met vier polyomino's (een hexomino en drie pentomino's) dezelfde vorm te leggen, met behoud van symmetrieën:
- de W en de L vormen een symmetrische figuur die kan worden gespiegeld langs de diagonaal;
- hetzelfde geldt voor de W, de L en de I5;
- hetzelfde geldt ook voor de W, de L, de I5 en de I6.

OPLOSSING AFLEVERING 3 De jubileumprijsvraag van het januarinummer was lastig! Toch hebben diverse lezers er hun tanden in gezet en goede oplossingen gevonden. Veel moest met de hand gebeuren, de opgave was niet bepaald geschikt voor mensen die graag programmeren. Bij de opgave gingen we uit van 21 dagen, waarbij in totaal 50 inzendingen binnenkomen, elke dag minimaal één. De 21 dagen noemen we a, b, c, ..., s, t, u. Een mogelijke *inzendingenreeks* is (2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 29). De vraag is: bestaat er een aantal opeenvolgende dagen waarbij het totale aantal inzendingen k is? Hierbij is $k \in \{1, 2, ..., 50\}$. Je ziet vrij snel dat er bij de genoemde inzendingenreeks geen oplossing is voor bijvoorbeeld $k = 49$.

1. Geef een voorbeeld van een inzendingenreeks waarbij er voor elke waarde van k een oplossing is. De inzendingenreeks moet natuurlijk bestaan uit 21 getallen die bij elkaar opgeteld 50 zijn. Het getal 0 mag er niet in voorkomen.
2. Bestaat er een inzendingenreeks die uit minder dan 21 dagen bestaat waarbij er voor elke waarde van $k \in \{1, 2, ..., 50\}$. een oplossing is? Wat is het kleinste aantal dagen?
3. Neem de inzendingenreeks (2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 29). Zoals gezegd bestaat er voor $k = 49$ geen oplossing. Zoek voor zoveel mogelijk waarden van k een inzendingenreeks (bestaande uit 21 dagen) met de eigenschap dat er *geen* oplossing is voor die waarde van k. Het is niet vanzelfsprekend dat dit voor elke $k < 50$ mogelijk is!

4. Probeer opgave 3 nu met een zo klein mogelijk aantal inzendingenreeksen uit te voeren.

Opgave 1 was goed te doen. De jury ontving meerdere oplossingen, zoals (1, 2, 2, 2, 2, 2, 2, 2, 11, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2).

Om bij opgave 2 de ondergrens te bepalen, moet je het volgende bedenken. Je moet 50 verschillende getallen maken door steeds een aantal opeenvolgende getallen op te tellen. Stel je gaat uit van negen dagen (dag *a* tot en met *i*). Je kunt op negen manieren 1 dag kiezen, op 8 manieren twee opeenvolgende dagen, op 7 manieren drie opeenvolgende dagen, en zo doorgaande tot op 1 manier alle negen dagen. Het totaal aantal getallen dat je zo kunt maken is 9 + 8 + 7 + … + 2 + 1 = 45, maar dat is minder dan 50. De ondergrens ligt op 10 dagen. Niemand vond een oplossing met 10 dagen, maar Ernst van de Kerkhof, Fred Schalekamp, Frank Tinkelenberg, Aad van de Wetering en de Drie Wisketiers (pseudoniem van drie wiskundestudenten) vonden oplossingen in 11 dagen. De Drie Wisketiers hebben alle oplossingen (laten) berekenen. Zij vonden dat er slechts vier oplossingen zijn:

1. (1, 1, 1, 20, 5, 4, 4, 4, 4, 3, 3)
2. (1, 2, 3, 7, 7, 7, 7, 7, 4, 4, 1)
3. (1, 4, 4, 7, 7, 7, 7, 7, 3, 2, 1)
4. (3, 3, 4, 4, 4, 4, 5, 20, 1, 1, 1)

Uiteraard zijn de laatste twee de gespiegelden van de eerste twee.

Bij opgave 3 is eenvoudig in te zien dat als op alle dagen een even aantal oplossingen wordt ontvangen, er dan nooit op een aantal opeenvolgende dagen een oneven aantal oplossingen binnengekomen kan zijn. Dus met (2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 10) zijn de aantallen inzendingen 1, 3, 5, 7, 9, …, 45, 47 en 49 onmogelijk. Het is een heel gepuzzel om voor de even getallen een soortgelijke inzendingenreeks te vinden. De jury had bijvoorbeeld moeite om een serie te vinden voor 10. Een dergelijke serie is (2, 2, 2, 2, 3, 2, 2, 2, 2, 3, 2, 2, 2, 2, 3, 2, 2, 2, 2, 3, 6).

Het kleinste aantal inzendingenreeksen, waarnaar in opgave 4 werd gevraagd, ontvingen we van Ernst van de Kerkhof en Fred Schalekamp, zie onderstaande tabellen. Clara en Jan Willem van Ittersum stuurden een Excel-spreadsheet in die de jury kon gebruiken of de inzendingen correct waren.

Net als vorige keer geven we weer twee Irisbonnen weg. Ze gaan naar Ernst van de Kerkhof, docent van Basisschool De Driesprong (afdeling Leonardo) in Geleen en Marieke van der Wegen (klas 5V3) van het Stedelijk Lyceum Kottenpark in Enschede. ■

Reeks	Inzendingenreeks																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	(1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	30,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1)
2	(4,	4,	2,	2,	2,	2,	2,	2,	2,	2,	2,	2,	2,	2,	2,	2,	2,	2,	2,	4,	4)
3	(1,	4,	4,	4,	1,	3,	1,	3,	1,	3,	1,	3,	4,	4,	1,	3,	1,	3,	1,	3,	1)
4	(1,	6,	1,	5,	1,	1,	5,	1,	1,	1,	5,	1,	1,	5,	1,	1,	5,	1,	1,	5,	1)
5	(1,	1,	1,	12,	1,	1,	1,	1,	1,	9,	1,	1,	1,	1,	1,	1,	11,	1,	1,	1,	1)

Reeks	Oplossing voor *k* (j = ja, n = nee)																				
	1 . . . 5 . . . 10 . . . 15 . . . 20 . . . 25 . . . 30 . . . 35 . . . 40 . . . 45 . . . 50																				
1	j j j j j j j j j j n n n n n n n n n n n n n n n n n n n j j j j j j j j j j j j j j j j j j j																				
2	n j n j n j n j n j n j n j n j n j n j n j n j n j n j n j n j n j n j n j n j n n n j n n n j																				
3	j n j j j n j j j n j j j j j j j j j j j j j j j j j j n j j j n j j j n j j j n j j j n j j j																				
4	j j j n j j j j j j n j j j j j j n j j j j j n j j j j j j n n j j j j n n n j j j j n n n j j j																				
5	j j j j j j n n j j j j j j j j j j j n n n n j j j j j j j j j j n n n n n n n j j j j j j j j																				

Met een paar spijkers en een schilderijtje aan een koord kun je verrassende wiskunde doen. De puzzels in dit artikel zullen je niet loslaten totdat je de oplossing gevonden hebt!

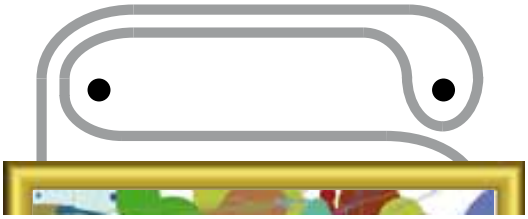
■ door Alex van den Brandhof

EEN LELIJK SCHILDERIJ

Meneer Knoop heeft een schilderij. Een lelijk schilderij. Hij heeft het gekregen van zijn tante Til. Meneer Knoop moet het wel ophangen: als tante Til op bezoek komt, zal zij er zeker naar vragen. Zeggen dat het schilderij is stukgevallen, zal hem niet in dank worden afgenomen. Gelukkig weet meneer Knoop wat van wiskunde en kan hij ervoor zorgen dat tante Til het schilderij zélf stuk laat vallen. Hij hangt het schilderij om meerdere spijkers, tante Til zal opmerken dat zo veel spijkers overbodig zijn en zal direct – want zo is tante Til – een spijker uit de muur trekken, waarna het schilderij naar beneden stort en breekt. Meneer Knoop verheugt zich op de komst van tante Til...

EEN KOORD OM SPIJKERS Een schilderij hangt met een koord aan twee spijkers, zoals in figuur 1. Als je één spijker verwijdert, blijft het schilderij hangen, zij het scheef. Het is ook mogelijk om het koord zó om de twee spijkers te hangen, dat het schilderij blijft hangen als je de linker spijker verwijdert, maar omlaag valt als je de rechter weghaalt. Hoe dat moet, zie je in figuur 2. Met nog een extra lus kun je het koord zó om de spijkers hangen, dat

Figuur 1



Figuur 2

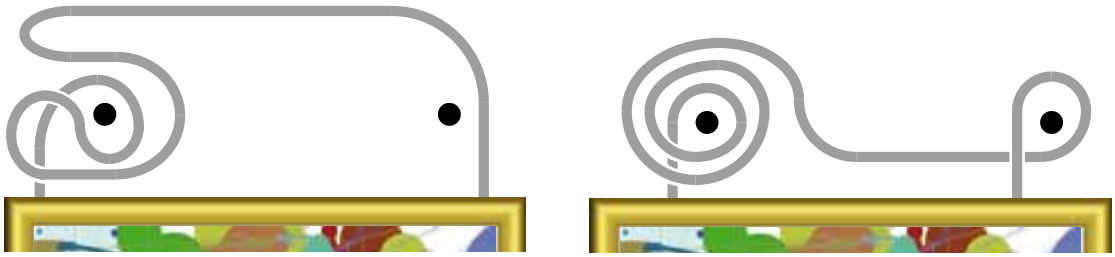
het er niet toe doet welke van de twee spijkers je uit de muur trekt: het schilderij zal altijd vallen. Hoe dat moet, verklappen we niet onmiddellijk, het is veel leuker het zelf te ontdekken!

Opdracht 1. Hoe moet je het koord om twee spijkers hangen, opdat het schilderij valt bij verwijdering van één willekeurige spijker?

Veel lastiger wordt het, als je het schilderij aan *drie* spijkers ophangt. De volgende opdracht is verre van eenvoudig!

Opdracht 2. Hoe moet je het koord om drie spijkers hangen, opdat het schilderij naar beneden valt als je één spijker – het doet er niet toe welke van de drie – verwijdert?

WOORDEN MAKEN Opdracht 1 is je met wat proberen misschien wel gelukt, maar bij opdracht 2 raak je al gauw gefrustreerd als je het koord lukraak om de spijkers wikkelt. Met wiskunde kom je verder! Beginnend bij het uiteinde van het snoer dat links aan het schilderij vastzit, wikkel je het snoer een aantal malen om de spijkers en ten slotte kom je uit bij het rechter uiteinde van het snoer. Bij elke lus kun je het snoer met de klok mee om een spijker draaien, of tegen de klok in. Als je twee spijkers A en B hebt, noteer je met a een lus om spijker A *met de klok mee*, en met a^{-1} een lus om A *tegen de klok in*. En idem dito noteren we met b en b^{-1} een lus om B met de klok mee respectievelijk te-



Figuur 3

gen de klok in. Op die manier kun je 'woorden' maken. Het woord ab komt erop neer dat je het snoer eerst een keer met de klok mee om A draait en vervolgens een keer met de klok mee om B; dit woord hoort dus bij de situatie in figuur 1. Het woord dat hoort bij de situatie in figuur 2 is aba^{-1}. In figuur 3 zie je nog twee situaties: links $aa^{-1}b$ en rechts $aaab^{-1}$.

Wat opvalt aan de linker situatie in figuur 3, is dat je de eerste twee lussen net zo goed weg kunt laten: draai je het snoer één keer met de klok mee om A en ga je vervolgens direct weer terug, dan komt dat erop neer dat je het snoer *helemaal niet* om A draait! We noteren dat als volgt: $aa^{-1} = 1$ (net als in de gewone rekenkunde: $2 \cdot 2^{-1} = 1$, $5 \cdot 5^{-1} = 1$ et cetera). Het woord $aa^{-1}b$ is daarom gelijk aan $1b = b$. Het woord $aaab^{-1}$ kun je niet korter schrijven.

Als je een spijker uit de muur trekt, komt dat erop neer dat alle lussen om die spijker wegvallen. Neem je in figuur 2 de linker spijker weg, dan betekent dat, dat alle letters a in het woord aba^{-1} wegvallen; je houdt dan b over en dat betekent dat het schilderij om de rechter spijker blijft hangen. Neem je echter de rechter spijker weg, dan vervallen alle letters b in het woord aba^{-1} en dan houd je $aa^{-1} = 1$ over: het schilderij hangt aan geen enkele spijker meer en valt dus op de grond.

Opdracht 3. Als je nog niet uit opdracht 1 was gekomen, zoek dan een woord met de letters a en b en zorg ervoor dat dat na het wegstrepen van alle a's gelijk is aan 1, en ook na het wegstrepen van alle b's.

Opdracht 4. In opdracht 2 ging het om drie spijkers. Zoek een woord met de letters a, b en c en zorg ervoor dat dat gelijk is aan 1 als je één soort letter (a, b of c) wegstreept.

ALGEMENER Eén spijker weghalen en het schilderij valt... Lukt dat ook als het schilderij om vier spijkers hangt? Vijf spijkers? Honderd spijkers? Het onwaarschijnlijke antwoord is ja! Voor élk natuurlijk getal n is het mogelijk om het koord zó om n spijkers te hangen, dat het schilderij valt als je ook maar één willekeurige spijker verwijdert! Altijd (altijd!) is het mogelijk om met n verschillende letters een woord te maken (alle letters mogen natuurlijk meerdere keren gebruikt worden) op zo'n manier dat je 1 overhoudt nadat je van één letter alle exemplaren wegstreept. Dit is een resultaat uit de *algebraïsche topologie*.

Het resultaat kunnen we nog verder generaliseren. Een schilderij kun je zodanig om n spijkers hangen, dat het schilderij valt bij verwijdering van k spijkers, maar blijft hangen bij verwijdering van minder dan k spijkers, voor elke $1 \leq k \leq n$. En als je over twee kleuren spijkers beschikt, zeg rood en blauw, geldt zelfs het volgende. Je kunt een schilderij zodanig om n rode en n blauwe spijkers hangen, dat het schilderij valt als je k spijkers van elke kleur weghaalt, maar blijft hangen als je van ten minste één kleur minder dan k spijkers weghaalt.

Opdracht 5. In figuur 4 zie je vier spijkers: links twee rode en rechts twee blauwe. Kun jij uitzoeken hoe je het koord om deze vier spijkers moet hangen, opdat het schilderij valt bij verwijdering van één rode en één blauwe spijker, maar blijft hangen bij verwijdering van twee spijkers van dezelfde kleur?

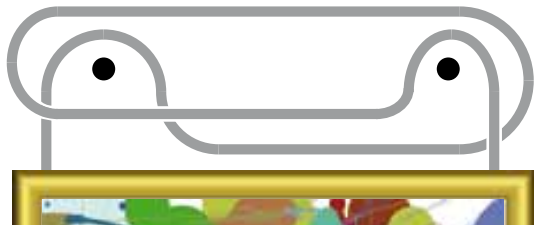
Figuur 4

Sla de pagina nog niet meteen om: op de volgende pagina vind je de antwoorden van de opdrachten.

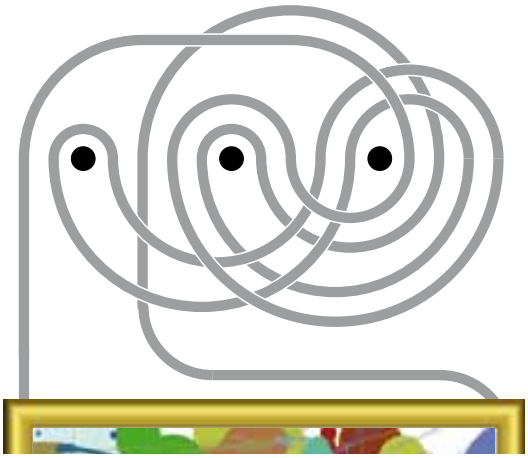
OPLOSSINGEN

EEN LELIJK SCHILDERIJ

Opdracht 1.



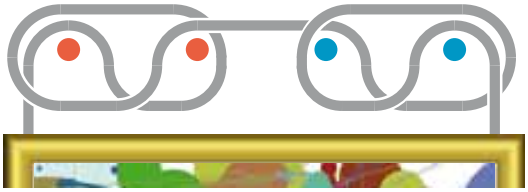
Opdracht 2.



Opdracht 3. Het woord is $ab^{-1}a^{-1}b$. Als je de a's wegstreept, dan houd je $b^{-1}b = 1$ over. Streep je de b's weg, dan houd je $aa^{-1} = 1$ over.

Opdracht 4. Het woord is $abcb^{-1}c^{-1}a^{-1}cbc^{-1}b^{-1}$. Als je de a's wegstreept, dan krijg je $bcb^{-1}c^{-1}cbc^{-1}b^{-1} = bcb^{-1}bc^{-1}b^{-1} = bcc^{-1}b^{-1} = bb^{-1} = 1$. Ook als je de b's of de c's wegstreept, houd je 1 over.

Opdracht 5. De twee rode spijkers noemen we A en B, de twee blauwe spijkers C en D. We zoeken een woord met de letters a, b, c en d. Het ontstane woord na wegstreping van alle a's en c's óf alle a's en d's óf alle b's en c's óf alle b's en d's moet gelijk zijn aan 1. Het ontstane woord na wegstreping van alle a's en b's óf alle c's en d's moet ongelijk zijn aan 1. Met wat gepuzzel vind je het woord $ab^{-1}a^{-1}bcd^{-1}c^{-1}d$. Zie onderstaande figuur. ■



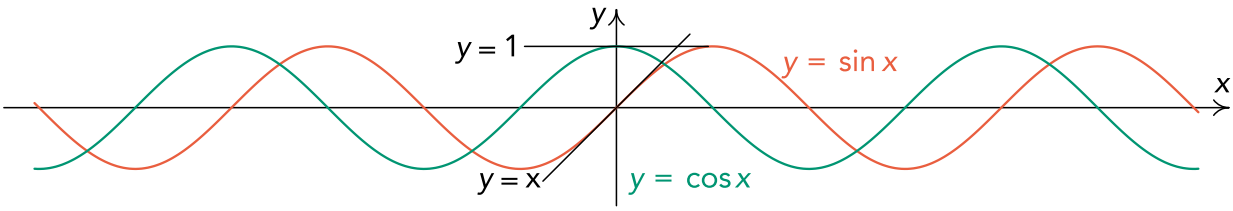
ZELF MAKEN

Bevestig aan de bovenhoeken van een schilderijtje (een eenvoudig latje volstaat natuurlijk ook) een koord. Voor de spijkers kun je goed *deuvels* gebruiken: pinnen waarmee je platen en planken aan elkaar kunt bevestigen (zie de linkerfoto hieronder). Geef de deuvels voor opdracht 5 en soortgelijke opdrachten een kleur. Boor in een plank een aantal gaten. Zorg ervoor dat de diameter van de gaten iets groter is dan de diameter van de deuvels, zodat je de deuvels er makkelijk in kunt steken en er weer uit kunt trekken. Of misschien heb je op zolder nog een deel van een oude kast met voorgeboorde gaten (zie de foto rechts).

Mensen zijn dol op ranglijsten, dus verschijnen met enige regelmaat lijstjes met 'de mooiste formules aller tijden'. In de natuurkunde kan je eigenlijk nooit om $E = mc^2$ heen, maar de wiskundeliefhebbers zijn het er meestal over eens dat $e^{i\pi} + 1 = 0$ de allermooiste formule is. Je kunt hem met wat moeite zelfs met middelbare schoolwiskunde bewijzen.

■ door Paul Levrie en Hilde Missinne

DE MOOISTE FORMULE OOIT,
EN HOE JE HEM ZELF AFLEIDT



Figuur 1 De grafieken van $y = \sin x$ en $y = \cos x$.

In de 'mooiste formule ooit' komen de twee belangrijkste constantes uit de wiskunde, e en π, samen voor met de drie basisgetallen 0, 1 en i waaruit, in zekere zin, alle andere getallen voortkomen. Het getal π ken je natuurlijk als de verhouding tussen de omtrek en de diameter van een cirkel, maar dit irrationale getal 3,1415926... duikt op talloze andere plaatsen in de wiskunde op. Irrationaal wil zeggen: de exacte waarde kun je alleen beschrijven met een oneindig aantal cijfers achter de komma waar geen regelmaat in zit.

Het getal dat we aanduiden met e is het grondtal van de exponentiële functie e^x en van de natuurlijke logaritme ln x. Ook e = 2,71828... is een irrationaal getal. Het getal i ken je misschien nog niet: het getal is gedefinieerd door $i^2 = -1$. Dus i is niet negatief en niet positief (en ook niet nul uiteraard), want van zowel een positief als een negatief getal is het kwadraat positief. Wat is i dan wel? Oorspronkelijk, in de zestiende eeuw, dook i op als een trucje om de oplossingen van sommige derdegraadsvergelijkingen uit te rekenen. Daarbij kwam het zogenoemde imaginaire getal i alleen in de tussenresultaten voor, het was zo vriendelijk om zich niet in de uiteindelijke oplossing te vertonen. Eigenlijk is deze imaginaire i pas in de negentiende eeuw geaccepteerd als een volwaardig getal waarmee gerekend kan worden als met alle andere getallen.

Niettemin wordt het nog steeds als bijna wonderbaarlijk ervaren:

$$\text{irrationaal}^{\text{imaginair} \cdot \text{irrationaal}} = \text{geheel}.$$

Hoe verzint een mens zoiets, en vooral: hoe bewijs je dit? De formule

$$e^{i\pi} + 1 = 0$$

is een speciaal geval van de formule van Leonhard Euler (1707-1783):

$$e^{ix} = \cos x + i \sin x.$$

Als je hier $x = \pi$ invult, krijg je

$$e^{i\pi} = \cos \pi + i \sin \pi = -1.$$

UITGANGSPUNTEN We gaan hieronder deze prachtige formule afleiden, waarvoor we te rade gaan bij Euler zelf, die er verschillende bewijzen voor gegeven heeft (zie bijvoorbeeld het boek *Euler: the Master of us all* van W. Dunham). We zetten eerst enkele vertrekpunten op een rijtje:
a. Het getal i heeft de eigenschap dat $i^2 = -1$, voor de rest kunnen we rekenen met het getal i alsof het een gewoon getal is.
b. Het getal e is het getal dat steeds beter wordt benaderd als we in de uitdrukking $(1+\frac{1}{n})^n$ het natuurlijke getal n steeds groter nemen. (Probeer het maar eens op je rekentoestel, bijvoorbeeld voor $n = 10^{10}$.) Meer nog, voor een getal z hebben we dat

$$\left(1+\frac{z}{n}\right)^n = e^z$$

voor n heel groot.

c. Verbanden tussen hoeken en zijden in een rechthoekige driehoek veronderstellen we bekend.
d. Aan de grafieken van cosinus en sinus, zie figuur 1, zie je dat $\cos x - 1$ en $\sin x - x$ verwaarloosbaar zijn als x heel klein is. (Ook dit kan je checken met je rekentoestel, kies bijvoorbeeld $x = 10^{-10}$.) We doen als Euler en vervangen $\cos x$ door 1 en $\sin x$ door x als x heel klein is. Aan de figuur kan je eveneens zien dat $\cos(-x) = \cos x$ en dat $\sin(-x) = -\sin x$.

DE AFLEIDING Nu kunnen we beginnen. We zullen gebruik maken van de formule van De Moivre, en om die aan te tonen hebben we de somformules van cosinus en sinus nodig. Gelukkig is er hiervoor een grafisch bewijs. Uit figuur 2 kan je afleiden dat

$$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$$

en ook

$$\sin(\alpha + \beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta\,.$$

Hiermee kunnen we het volgende product eenvoudiger schrijven. We werken eerst de haakjes uit:

$$(\cos t + \mathrm{i}\sin t)(\cos u + \mathrm{i}\sin u) = \cos t\cos u + \mathrm{i}\sin t\cos u + \mathrm{i}\cos t\sin u + \mathrm{i}^2\sin t\sin u.$$

We weten dat $\mathrm{i}^2 = -1$, en we herschikken de termen:

$$(\cos t + \mathrm{i}\sin t)(\cos u + \mathrm{i}\sin u) = \cos t\cos u - \sin t\sin u + \mathrm{i}\,(\sin t\cos u + \cos t\sin u).$$

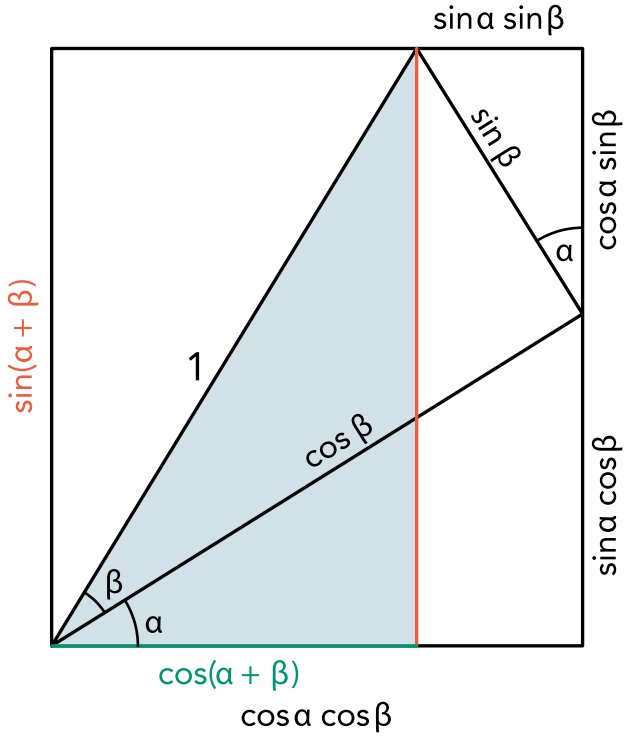
Met de somformules ($\alpha = t$, $\beta = u$) kunnen we hieruit besluiten dat

$$(\cos t + \mathrm{i}\sin t)(\cos u + \mathrm{i}\sin u) = \cos(t+u) + \mathrm{i}\sin(t+u)\,.$$

Kiezen we u gelijk aan t, dan wordt dit

$$(\cos t + \mathrm{i}\sin t)^2 = \cos 2t + \mathrm{i}\sin 2t.$$

Als we dan de beide leden nog eens vermenigvuldigen met $\cos t + \mathrm{i}\sin t$, dan vinden we op dezelfde manier:



Figuur 2 Met dit plaatje kan de formule van De Moivre bewezen worden. Bron: R. Nelsen, *Proofs without Words II: More Exercises in Visual Thinking*, Mathematical Association of America, 2000.

$$(\cos t + \mathrm{i}\sin t)^3 = \cos 3t + \mathrm{i}\sin 3t.$$

In het algemeen vinden we zo de formule van De Moivre:

$$(\cos t + \mathrm{i}\sin t)^n = \cos nt + \mathrm{i}\sin nt. \qquad (1)$$

Vervangen we hierin t door $-t$, dan wordt deze formule (zie uitgangspunt d):

$$(\cos t - \mathrm{i}\sin t)^n = \cos nt - \mathrm{i}\sin nt. \qquad (2)$$

Wat Euler hiermee doet is het volgende. Als je deze laatste twee formules bij elkaar optelt, dan vind je:

$$\cos nt = \frac{(\cos t + \mathrm{i}\sin t)^n + (\cos t - \mathrm{i}\sin t)^n}{2}.$$

We kiezen nu t gelijk aan $\frac{x}{n}$ met n een heel groot natuurlijk getal. Het getal t is dus heel klein, en we kunnen dan (volgens uitgangspunt d) in het rechterlid $\cos t$ vervangen door 1 en $\sin t$ door t. Dit geeft:

$$\cos nt = \cos x = \frac{\left(1 + \frac{\mathrm{i}x}{n}\right)^n + \left(1 + \frac{-\mathrm{i}x}{n}\right)^n}{2}.$$

Maar de termen in de teller van het rechterlid zijn precies de uitdrukkingen die we tegenkomen bij de definitie van het getal e in uitgangspunt b. En om-

De formule van De Moivre (Abraham De Moivre, 1667-1754) zegt dat

$$(\cos x + \mathrm{i}\sin x)^n = \cos(nx) + \mathrm{i}\sin(nx)$$

voor elk geheel getal n. De formule van Euler die we willen bewijzen lijkt een verklaring te geven voor die van De Moivre. Inderdaad: wat tussen de haakjes staat in het linkerlid is volgens Euler gelijk aan e^{ix}, en het rechterlid is om dezelfde reden gelijk aan e^{inx}. We kunnen dus de formule van De Moivre ook schrijven als $(e^{ix})^n = e^{inx}$, wat lijkt te volgen uit eigenschappen van machten.

dat we n heel groot hebben gekozen, hebben we nu:

$$\cos x = \frac{e^{ix} + e^{-ix}}{2}.$$

Uit (1) en (2) kan je ook een formule halen voor sin nt, door ze van elkaar af te trekken. Dit geeft:

$$\sin nt = \frac{(\cos t + \mathrm{i}\sin t)^n - (\cos t - \mathrm{i}\sin t)^n}{2\mathrm{i}}.$$

Op precies dezelfde manier als boven volgt nu

$$\sin x = \frac{e^{ix} - e^{-ix}}{2\mathrm{i}}.$$

We zetten beide resultaten even naast elkaar:

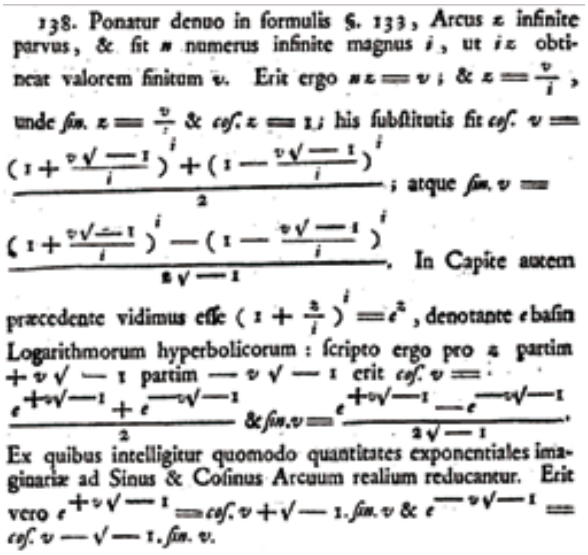
$$\cos x = \frac{e^{ix} + e^{-ix}}{2} \quad \text{en} \quad \sin x = \frac{e^{ix} - e^{-ix}}{2\mathrm{i}}.$$

Je ziet dan dat als je bij de eerste vergelijking i keer de tweede optelt, de volgende formule volgt:

$$\cos x + \mathrm{i}\sin x = e^{ix}.$$

En dit was de formule die we wilden bewijzen. Euler deed het precies op dezelfde manier. In figuur 3 zie je een stukje uit het boek waarin hij het schreef. ■

Figuur 3 Op deze Zwitserse postzegel uit 1957 is Leonhard Euler afgebeeld met links de formule $e^{i\phi} = \cos\phi + i\sin\phi$. Het getal e wordt ook wel het *getal van Euler* genoemd. Euler heeft inderdaad het symbool e ingevoerd (in 1731) voor het getal 2,718281828... Maar hij heeft bij de keuze van die letter zeker niet gedacht aan de eerste letter van zijn naam, daarvoor was hij veel te bescheiden.



138. Ponatur denuo in formulis §. 133, Arcus z infinite parvus, & ſit n numerus infinite magnus i, ut iz obtineat valorem finitum v. Erit ergo $nz = v$; & $z = \frac{v}{i}$, unde $\sin. z = \frac{v}{i}$ & $\mathrm{cof}. z = 1$; his ſubſtitutis fit $\mathrm{cof}. v = \frac{(1 + \frac{v\sqrt{-1}}{i})^i + (1 - \frac{v\sqrt{-1}}{i})^i}{2}$; atque $\sin. v = \frac{(1 + \frac{v\sqrt{-1}}{i})^i - (1 - \frac{v\sqrt{-1}}{i})^i}{2\sqrt{-1}}$. In Capite autem præcedente vidimus eſſe $(1 + \frac{z}{i})^i = e^z$, denotante e baſin Logarithmorum hyperbolicorum: ſcripto ergo pro z partim $+v\sqrt{-1}$ partim $-v\sqrt{-1}$ erit $\mathrm{cof}. v = \frac{e^{+v\sqrt{-1}} + e^{-v\sqrt{-1}}}{2}$ & $\sin. v = \frac{e^{+v\sqrt{-1}} - e^{-v\sqrt{-1}}}{2\sqrt{-1}}$.

Ex quibus intelligitur quomodo quantitates exponentiales imaginariæ ad Sinus & Coſinus Arcuum realium reducantur. Erit vero $e^{+v\sqrt{-1}} = \mathrm{cof}. v + \sqrt{-1}.\sin. v$ & $e^{-v\sqrt{-1}} = \mathrm{cof}. v - \sqrt{-1}.\sin. v$.

Figuur 4 Fragment uit een boek van Leonhard Euler (in het Engels vertaald door John D. Blanton onder de titel *Introduction to Analysis of the Infinite*).

PYTHAGORAS OLYMPIADE

■ door Matthijs Coster, Alexander van Hoorn en Eddie Nijholt

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

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

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

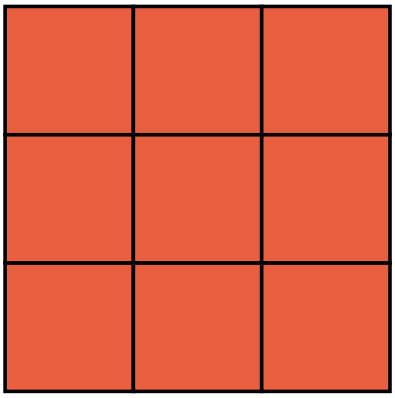
Voorzie het antwoord van een duidelijke toelichting (dat wil zeggen: een berekening of een bewijs). Vermeld je naam en adres; leerlingen moeten ook hun klas en de naam van hun school vermelden.
Je inzending moet bij ons binnen zijn vóór 30 juni 2011.

DE GOEDE INZENDERS VAN JANUARI 2011

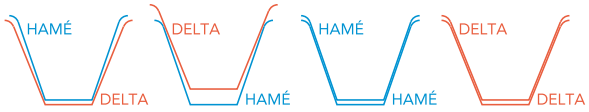
202: Stijn Cambie (klas 5), VTI Poperinge; Birgit Gysbrechts (klas 3), KSO Glorieux, Ronse; Marcel Roggeband, Hoofddorp; Michelle Sweering (klas 3), Erasmiaans Gymnasium, Rotterdam; Djurre Tijsma (klas 4), Christelijk Gymnasium Beyers Naudé, Leeuwarden.
203: Stijn Cambie (klas 5), VTI Poperinge; Thijs van der Gugten (klas 5), GSG Guido de Brès, Amersfoort; Marcel Roggeband, Hoofddorp.
204: Wouter Baar (klas 5), OSG Sevenwolden locatie Fedde Schurerplein, Heerenveen; Jan-Willem van Ittersum (klas 5), Keizer Karel College, Amstelveen; Jolien Kerssens (klas 5), Jac. P. Thijsse College, Castricum; Marcel Roggeband, Hoofddorp; Michelle Sweering (klas 3), Erasmiaans Gymnasium, Rotterdam; Niek Teeuwen (klas 5), Gymnasium Felisenum, Velsen-Zuid; Djurre Tijsma (klas 4), Christelijk Gymnasium Beyers Naudé, Leeuwarden.
205: Stijn Cambie (klas 5), VTI Poperinge; Jan-Willem van Ittersum (klas 5), Keizer Karel College, Amstelveen; Marcel Roggeband, Hoofddorp.
De Irisbonnen gaan naar Birgit Gysbrechts en Niek Teeuwen.

OPGAVE 210

In een rooster van 3 × 3 hokjes zijn in totaal veertien vierkantjes te onderscheiden: negen van 1 × 1, vier van 2 × 2 en één van 3 × 3. Hoeveel vierkantjes zijn er op deze manier te onderscheiden in een rooster van 50 × 50 hokjes?



OPGAVE 211



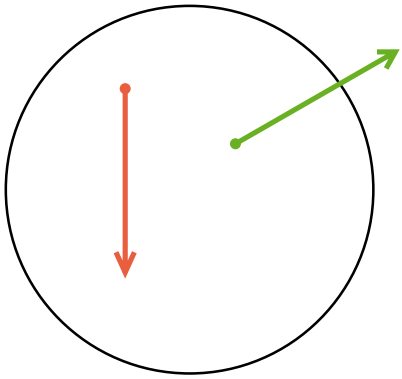
Ernst heeft acht emmers: vier van het merk HAMÉ en vier van het merk DELTA. Hoewel Ernst de emmers niet met het blote oog uit elkaar kan houden, weet hij dat een emmer van HAMÉ in (bovenop) een emmer van DELTA past, maar niet andersom. Bovendien passen twee emmers van dezelfde soort natuurlijk wel in elkaar.

Hoe kan Ernst in zo weinig mogelijk zetten alle emmers identificeren? Een zet bestaat uit het op elkaar zetten van twee emmers (geen stapeltjes); het uit elkaar halen van twee emmers mag zo vaak als je wilt.

OPGAVE 212

Op een ronde tafel met een straal van 1 meter zetten we een muis neer. (De kans dat de muis binnen een gebied G wordt gezet, is *evenredig* met de oppervlakte van G.) De muis loopt in een willekeurige richting 1 meter recht vooruit. Hoe groot is de kans dat de muis van de tafel af loopt?

In onderstaande figuur geeft de groene pijl een situatie weer waarbij de muis van de tafel loopt, bij de rode blijft blijft de muis op tafel.



OPGAVE 213

Plaats in vier kolommen achtereenvolgens de getallen 1, 2, 3 en 5. In elke kolom mag je onbeperkt getallen toevoegen, door het product te nemen van drie getallen uit de drie andere kolommen (uit elke kolom één getal naar keuze). Als voorbeeld is in de meest linkse kolom 30 (= 2 × 3 × 5) toegevoegd.

Komt uiteindelijk het getal 540.000 voor in één van de kolommen en zo ja, in welke kolom(men)?

1	2	3	5
30			

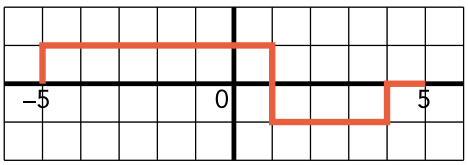
OPLOSSING 202

Op een feestje is nog één glas limonade en één glas prikwater over. Hans en Johan willen allebei de limonade en besluiten de drankjes te mengen. Beide glazen zitten voor $\frac{2}{3}$ vol en ze hebben geen extra glas. Gaat het ze lukken om door middel van overgieten een eerlijk mengsel te maken?

Oplossing. Stel dat Hans en Johan een aantal keren iets hebben overgeschonken, maar de limonadeconcentraties in de glazen nog niet gelijk zijn. Geef de concentraties aan met c_1 en c_2, en de inhouden met i_1 en i_2. Als ze een deel van de inhoud van glas 2, zeg i, overschenken in glas 1, verandert de concentratie in glas 2 niet, maar de nieuwe concentratie in glas 1 wordt $(c_1i_1 + c_2i)/(i_1 + i)$. Omdat voor de schenkactie geldt dat $c_1 \neq c_2$, is $(c_1i_1 + c_2i)/(i_1 + i) \neq (c_2i_1 + c_2i)/(i_1 + i) = c_2$. Met andere woorden: als voor het schenken de concentraties niet gelijk zijn, zijn ze na het schenken ook niet gelijk! Een eerlijk mengsel is dus onmogelijk. (In de praktijk zullen de concentraties natuurlijk wel voldoende bij elkaar in de buurt komen.)

OPLOSSING 203

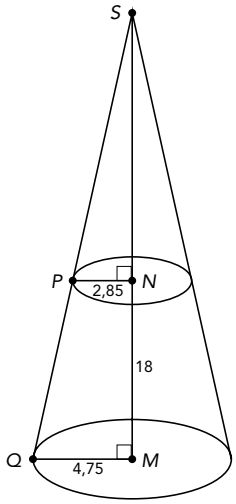
Op hoeveel manieren kun je in een assenstelsel in 14 stappen van het punt (–5, 0) naar het punt (5, 0) lopen? Onder een stap wordt verstaan: van een roosterpunt naar één van de vier naastgelegen roosterpunten (links, rechts, boven of onder). Elk roosterpunt mag je meer dan één keer passeren. Ook is het niet erg als je tijdens de wandeling al een keer langs het eindpunt komt. Een voorbeeld van een route zie je hiernaast.



Oplossing. Geef de totale aantallen stappen in de vier richtingen aan met B(oven), O(nder), L(inks), R(echts). De totale wandeling van 14 stappen moet netto uitkomen op 10R. Een mogelijkheid hiertoe is 10R-2B-2O. We kunnen deze 14 letters nog op $14! = 14 \cdot 13 \cdot 12 \cdots 1$ verschillende volgorden zetten. Maar nu tellen we veel dubbel, want de letters R zijn bijvoorbeeld niet te onderscheiden. Er zijn $(14!)/(10! \cdot 2! \cdot 2!)$ wandelingen die aan 10R-2B-2O voldoen. Op gelijke wijze vinden we $(14!)/(11! \cdot 1! \cdot 1! \cdot 1!)$ wandelingen voor 11R-1B-1O-1L en $(14!)/(12! \cdot 2!)$ wandelingen voor 12R-2L. Opgeteld zijn dit 8281 wandelingen.

OPLOSSING 204

Een vaas heeft de vorm van een afgeknotte kegel (neem aan dat het ondervlak en het bovenvlak evenwijdige schijven zijn met de middelpunten boven elkaar). De hoogte van de vaas is 18 cm en de diameter van de bovenste en die van de onderste schijf zijn respectievelijk 9,5 cm en 5,7 cm. Als de vaas dwars wordt gelegd en er wordt een tikje tegen gegeven, zal hij gaan rollen en zal de bovenste rand daarbij een cirkelbaan over de vloer beschrijven. Geef de straal van deze cirkel.



Oplossing. Zij M het middelpunt van de grote cirkel (bovenzijde van de vaas), N het middelpunt van de kleine cirkel (onderzijde van de vaas) en zij P en Q twee boven elkaar gelegen punten op de twee cirkels, zie bovenstaande tekening. Het snijpunt van MN en PQ noemen we S. De gevraagde straal is $|SQ|$.
De stelling van Pythagoras geeft

$$|PQ| = \sqrt{|MN|^2 + (|MQ| - |NP|)^2} = \sqrt{18^2 + 1{,}9^2} = 18{,}1.$$

Wegens $NP \,//\, MQ$ is $\Delta SNP \sim \Delta SMQ$, zodat $|SP|/|SQ| = |NP|/|MQ| = 2{,}85/4{,}75$ ofwel $|SP| = 0{,}6|SQ|$. Als we dit invullen in $|SQ| - |SP| = 18{,}1$, krijgen we $|SQ|(1 - 0{,}6) = 18{,}1$ zodat $|SQ| = 45{,}25$ cm.

OPLOSSING 205

We bekijken cirkels in een assenstelsel die door precies n punten heen gaan waarvan zowel de x- als y-coördinaat een rationaal getal (breuk) is.
a. Geef een voorbeeld van zo'n cirkel voor $n = 0$, 1 en 2.
b. Bewijs dat er geen voorbeelden bestaan als $n \geq 3$.

Oplossing.
a. $n = 0$: Neem middelpunt $M(0, 0)$ en straal $r = \sqrt[4]{2}$. Dan heeft $x^2 + y^2 = (\sqrt[4]{2})^2 = \sqrt{2}$ geen rationale oplossing (x, y) want $\sqrt{2}$ is irrationaal.
$n = 1$: Neem $M(\sqrt[4]{2}, 0)$ en $r = \sqrt[4]{2}$. Dan volgt uit $(x - \sqrt[4]{2})^2 + y^2 = (\sqrt[4]{2})^2$ dat $x^2 - 2x\sqrt[4]{2} + y^2 = 0$ met als enige rationale oplossing $(x, y) = (0, 0)$.
$n = 2$: Neem $M(\sqrt{3}, 0)$ en $r = 2$. Voor $(x - \sqrt{3})^2 + y^2 = 2^2$ moet gelden $x^2 - 2x\sqrt{3} + y^2 = 1$ met de twee rationale oplossingen $(x, y) = (0, \pm 1)$.
b. Stel dat een cirkel minstens drie rationale punten bevat, zeg P, Q en R. Uit $(x_P - x_M)^2 + (y_P - y_M)^2 = (x_Q - x_M)^2 + (y_Q - y_M)^2 = (x_R - x_M)^2 + (y_R - y_M)^2$ volgen drie lineaire vergelijkingen in x_M en y_M met rationale coëfficiënten, dus M heeft ook rationale coördinaten. Nu mogen we zonder verlies van algemeenheid M op $(0, 0)$ stellen; de rationaliteit van elk punt op de cirkel verandert hierbij immers niet. Zij nu (a, b, c) een *primitief Pythagoreïsch drietal* (drie natuurlijke getallen met $a^2 + b^2 = c^2$ en ggd$(a, b, c) = 1$). We bekijken het punt $S\,(x_P \cdot \frac{a}{c} - y_P \cdot \frac{b}{c}, x_P \cdot \frac{b}{c} + y_P \cdot \frac{a}{c})$. Dan heeft S rationale coördinaten en geldt

$$x_S^2 + y_S^2 = (x_P \cdot \tfrac{a}{c} - y_P \cdot \tfrac{b}{c})^2 + (x_P \cdot \tfrac{b}{c} + y_P \cdot \tfrac{a}{c})^2 = (x_P^2 + y_P^2)((\tfrac{a}{c})^2 + (\tfrac{b}{c})^2) = (x_P^2 + y_P^2) \cdot 1 = r^2,$$

dus ligt S ook op de cirkel. Omdat er oneindig veel primitieve Pythagoreïsche drietallen zijn, bevat de cirkel oneindig veel punten met rationale coördinaten, en dat zijn er dus nooit precies n.

NAAMZOEKER

■ door Matthijs Coster

In het vierkant hiernaast zitten de namen van 24 beroemde wiskundigen verstopt:

Abel	Hilbert
Bernoulli	Jacobi
Brouwer	Klein
Cantor	Lagrange
Descartes	Leibniz
Dirichlet	Lie
Erdos	Newton
Euclides	Ramanujan
Fermat	Riemann
Freudenthal	Stieltjes
Galois	Wiles
Godel	De Witt

Streep alle namen door (horizontaal, verticaal of diagonaal). Met de overgebleven letters (de X'en uitgezonderd) kun je de namen van twee Griekse wiskundigen maken. ■

L	K	X	D	I	B	O	C	A	J	P	T	Y
E	L	Z	I	N	B	I	E	L	T	T	R	N
D	E	H	R	L	I	E	A	A	I	E	N	L
O	I	G	I	S	L	B	O	W	W	A	A	S
G	N	R	C	E	E	U	E	U	M	H	T	E
E	R	A	H	L	T	D	O	E	T	I	S	T
G	O	F	L	I	X	R	I	N	E	X	E	R
N	T	E	E	W	B	R	E	L	R	R	A	A
A	N	R	T	T	O	D	T	B	C	E	S	C
R	A	M	A	N	U	J	A	N	L	U	B	S
G	C	A	T	E	E	R	D	O	S	I	E	E
A	H	T	R	S	N	E	W	T	O	N	H	D
L	E	F	S	I	O	L	A	G	N	E	S	X

De Nederlandse Wiskunde Olympiade wordt in 2011 voor de vijftigste keer gehouden. De eerste editie van deze jaarlijkse wedstrijd was in 1962. Dit was meteen een succes: er deden maar liefst 3346 deelnemers van 284 scholen aan mee. In dit artikel kijken we welke opgaven de leerlingen 'uit grootmoeders tijd' voor hun kiezen kregen.

■ door Birgit van Dalen en Quintijn Puite

50 JAAR WISKUNDE OLYMPIADE

Al sinds het begin van de vorige eeuw werden er in de wereld wiskundewedstrijden voor scholieren gehouden. Met name in Oost-Europa waren ze er erg fanatiek in. Dat leverde niet alleen plezier op voor de deelnemers, maar het had ook als effect dat er steeds meer Oost-Europese wiskundigen doordrongen tot de wereldtop. Vanzelfsprekend wilden andere landen niet achterblijven, dus in steeds meer landen werden wiskundeolympiades georganiseerd.

In Nederland werden er sinds 1805 wel al wiskundige prijsvragen uitgeschreven door het Wiskundig Genootschap, maar het duurde tot 1962 voordat de eerste olympiade een feit was. Het laatste zetje werd gegeven door een nieuw wiskundetijdschrift, namelijk *Pythagoras*, dat voor het eerst uitkwam in 1961 en heel goed werd ontvangen onder scholieren. Dit blad en de olympiade zijn dus vanaf het begin nauw verbonden geweest. Aangemoedigd door dit succes werd besloten om de Nederlandse Wiskunde Olympiade op te richten, met als doel (we citeren letterlijk uit een artikel uit die tijd):

(a) de leerlingen tot wiskundestudie te animeren;
(b) jeugdige talenten tijdig te ontdekken;
(c) topprestaties te honoreren;
(d) de keuze van een wiskundig beroep onder leerlingen van goede aanleg te propageren;
(e) betrouwbare aanwijzingen te verzamelen voor een verantwoorde leerstofkeuze bij het v.h.m.o. (voorbereidend hoger en middelbaar onderwijs), waarmee in het bijzonder de meer begaafde leerlingen zullen zijn gebaat.

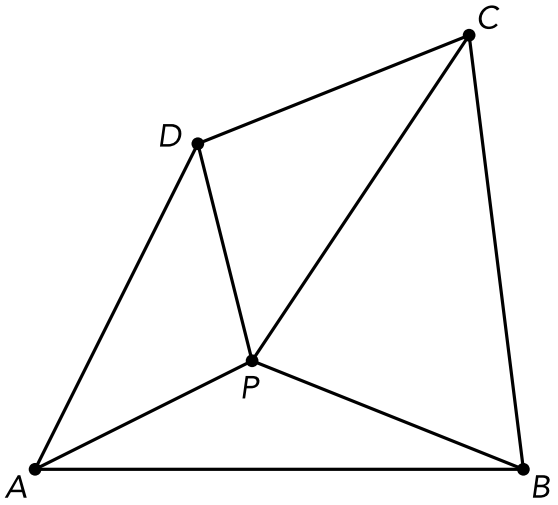
Op woensdag 2 mei 1962 was het zover en werd de eerste ronde van de allereerste Nederlandse Wiskunde Olympiade gehouden. In dit artikel bekijken we de eerste twee opgaven.

Opgave 1 van de eerste ronde 1962:
Gegeven is een vlakke vierhoek, waarvan elke hoek kleiner is dan een gestrekte hoek. Geef het punt aan, waarvoor de som van de afstanden tot de hoekpunten van de vierhoek zo klein mogelijk is. Bewijs dat Uw antwoord goed is.

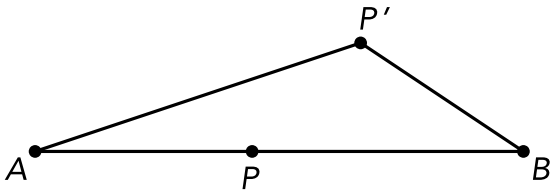
De opgave (hierboven in de oorspronkelijke formulering) gaat over een vierhoek waar geen deuken in zitten (elke hoek is kleiner dan 180°). Laten we de vier hoekpunten van deze vierhoek A, B, C en D noemen, zie figuur 1. Als we nu ergens een punt P in het vlak kiezen, dan kunnen we de afstand van P tot A meten; die schrijven we als $|PA|$. Zo ook kunnen we de afstanden van P tot de andere drie hoekpunten meten. De vraag is nu: voor welke P is $|PA| + |PB| + |PC| + |PD|$ minimaal?

Omdat niet direct duidelijk is wat het antwoord op deze vraag is, gaan we eerst maar eens iets makkelijkers bekijken. Wat als we nou alleen de afstand $|PA|$ zo klein mogelijk willen hebben? Hoe dichter P bij A ligt, hoe kleiner deze afstand wordt. Hij is natuurlijk minimaal als P bovenop A ligt.

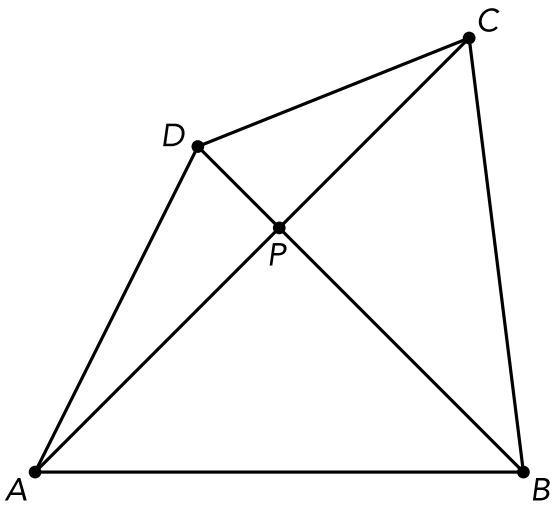
We maken het iets moeilijker: nu willen we $|PA| + |PB|$ zo klein mogelijk hebben. We kunnen P niet tegelijkertijd bovenop A en bovenop B kiezen,



Figuur 1



Figuur 2



Figuur 3

dus de afstand kan deze keer niet 0 worden. Stel dat we een elastiekje spannen van A naar B langs punt P. De lengte van het elastiekje is precies $|PA| + |PB|$. Nu houden elastiekjes ervan om zo kort mogelijk te zijn; dan staat er zo min mogelijk spanning op. Wanneer is dat het geval bij dit elastiekje? Dat is natuurlijk als het elastiekje recht van A naar B loopt. Dus precies als P op het lijnstuk AB ligt.

Kunnen we dit ook wiskundig beargumenteren? Als P op het lijnstuk AB ligt, dan is $|PA| + |PB| = |AB|$. Voor een punt P' dat *niet* op lijnstuk AB ligt, geldt natuurlijk dat $|P'A| + |P'B| > |AB|$, zie figuur 2. Dus inderdaad geldt dat $|PA| + |PB|$ zo klein mogelijk is als P op het lijnstuk AB ligt.

We zouden nu graag willen dat niet alleen $|PA| + |PB|$, maar ook $|PC| + |PD|$ minimaal is. Dan is namelijk ook de som van die twee minimaal. Natuurlijk is $|PC| + |PD|$ minimaal als P op het lijnstuk CD ligt, maar helaas kan dat niet tegelijk met P op het lijnstuk AB, want deze lijnstukken hebben geen punt gemeenschappelijk. Deze strategie werkt dus niet.

We kunnen echter de som $|PA| + |PB| + |PC| + |PD|$ ook op een andere manier in tweeën splitsen, namelijk als $|PA| + |PC|$ en $|PB| + |PD|$. De eerste som is minimaal als P op het lijnstuk AC ligt, de tweede als P op het lijnstuk BD ligt. En dat kan wél tegelijkertijd! Namelijk precies als P het snijpunt van de diagonalen AC en BD van de vierhoek is, zie figuur 3.

Het antwoord op opgave 1 is dus: het snijpunt van de diagonalen, met als bewijs dat zowel $|PA| + |PC|$ als $|PB| + |PD|$ in dat geval minimaal zijn.

Opgave 2 van de eerste ronde 1962:
Los x en y op uit de vergelijking
$(\sin(x - y) + 1)(2\cos(2x - y) + 1) = 6$.

Dit ziet er vreselijk ingewikkeld uit. Om een beetje een idee te krijgen van wat er eigenlijk staat, gaan we maar eens wat waarden voor x en y invullen. De sinus en cosinus van veelvouden van 30° zijn makkelijk uit te rekenen, dus daar kiezen we onze x en y op uit. De laatste kolom in de volgende tabel geeft de waarde aan van $(\sin(x - y) + 1)(2\cos(2x - y) + 1)$ als we x en y invullen. We zoeken dus alle paren (x, y) waarvoor hier 6 uit komt.

x	y	$\sin(x - y)$	$\cos(2x - y)$	uitkomst
30°	60°	$-\frac{1}{2}$	1	$\frac{3}{2}$
60°	30°	$\frac{1}{2}$	0	$\frac{3}{2}$
90°	60°	$\frac{1}{2}$	$-\frac{1}{2}$	0
90°	0°	1	−1	−2
0°	90°	−1	0	0

Het blijkt nog niet zo makkelijk te zijn om 6 in de rechterkolom te krijgen, of zelfs maar om daar in de buurt te komen. Hoe groot kunnen we de waarde

in die kolom eigenlijk krijgen, als we hem zo groot mogelijk proberen te maken? We weten dat $\sin(x-y)$ nooit groter is dan 1, dus $\sin(x-y)+1$ is hoogstens 2. En $\cos(2x-y)$ is ook nooit groter dan 1, dus $2\cos(2x-y)+1$ is hoogstens $2\cdot 1+1=3$. We zien dat zolang de twee factoren links in de vergelijking allebei positief zijn, de rechterkant nooit groter kan worden dan 6. En hij wordt zelfs alleen 6 indien $\sin(x-y)=1$ en ook nog $\cos(2x-y)=1$.

Het kan natuurlijk ook nog zo zijn dat we twee negatieve factoren links hebben, die met elkaar vermenigvuldigd 6 opleveren. Maar $\sin(x-y)\geq -1$, dus $\sin(x-y)+1$ kan helemaal niet negatief zijn.

We hebben nu laten zien dat de vergelijking alleen waar is als $\sin(x-y)=1$ en $\cos(2x-y)=1$. Voor welke x en y geldt $\sin(x-y)=1$? Dat is alleen als

$$x-y=90^\circ+k\cdot 360^\circ,$$

met k geheel (want veelvouden van 360° maken niet uit). En wanneer is $\cos(2x-y)=1$? Dat is precies als

$$2x-y=m\cdot 360^\circ,$$

met m geheel. Nu moeten we hieruit nog x en y bepalen. We kunnen dit bijvoorbeeld doen door de twee gelijkheden van elkaar af te trekken:

$$\begin{aligned}x&=(2x-y)-(x-y)=\\&m\cdot 360^\circ-(90^\circ+k\cdot 360^\circ)=\\&-90^\circ+(m-k)\cdot 360^\circ.\end{aligned}$$

En nu wordt y gelijk aan

$$\begin{aligned}y&=x-(x-y)=\\&(-90^\circ+(m-k)\cdot 360^\circ)-(90^\circ+k\cdot 360^\circ)=\\&-180^\circ+(m-2k)\cdot 360^\circ.\end{aligned}$$

Welke getallen kunnen $m-k$ en $m-2k$ eigenlijk zijn? Als we m vast kiezen en k alle gehele getallen laten aannemen, dan neemt $m-k$ ook alle gehele getallen aan. (Ga maar na: voor willekeurige gehele t kunnen we k zo kiezen dat $m-k=t$, namelijk $k=m-t$.) Dus we kunnen $m-k$ wel vervangen door t, waarbij t weer elk geheel getal kan zijn. Nu wordt $m-2k$ gelijk aan $t-k$. Om precies dezelfde reden kan dit ook weer alle gehele getallen aannemen, welke t we ook kiezen. Dus in plaats van $m-2k$ kunnen we ook wel r schrijven, met r een willekeurig geheel getal.

Omdat veelvouden van 360° toch niet uitmaken, kunnen we −180° ten slotte ook wel schrijven als 180° en −90° als 270°. Al met al vinden we als oplossingen:

$$\begin{cases}x=270^\circ+t\cdot 360^\circ,\\y=180^\circ+r\cdot 360^\circ.\end{cases}$$

Dit is een heel 'rooster' aan oplossingen, met $(x, y)=(270^\circ, 180^\circ)$ als 'oorsprong' en steeds een nieuwe oplossing als we bij de x- of y-coördinaat (of bij allebei) een veelvoud van 360° optellen (of eraf halen).

We controleren nog even of we geen rekenfouten gemaakt hebben door $x=270^\circ$ en $y=180^\circ$ in te vullen. Dan krijgen we $\sin(x-y)=\sin(90^\circ)=1$ en $\cos(2x-y)=\cos(360^\circ)=1$, dus

$$(\sin(x-y)+1)(2\cos(2x-y)+1)=6.$$

TOEN EN NU Deze eerste ronde van 1962 bestond uit negen opgaven. De deelnemers konden hiervoor bij elkaar 120 punten scoren. De gemiddelde score was echter slechts 17 en maar één deelnemer scoorde meer dan 100 punten. De precieze scores op de twee opgaven die we hierboven besproken hebben, zijn onbekend. Tegenwoordig is het met de computer een fluitje van een cent om allerlei statistieken te genereren, maar in 1962 werden de scores van alle 3346 deelnemers met de hand verwerkt. Ook het nakijken was een flinke klus, want zoals je al gezien hebt, bevatte de eerste ronde open vragen, waar een berekening of zelfs een bewijs gevraagd werd. Tegenwoordig komen open vragen pas bij de tweede ronde en is de eerste ronde een mix van meerkeuzevragen en opgaven waar een getal als antwoord moet worden gegeven (maar geen berekening).

Ook de aard van de opgaven is in de loop van de tijd wel wat veranderd. Een bewijsopgave zoals opgave 1 uit 1962 zou nu nooit meer in de eerste ronde terechtkomen. Ook voor de sinussen en cosinussen uit opgave 2 is geen plek meer in de huidige eerste rondes, omdat dat tot de bovenbouwstof behoort, terwijl de olympiade nu ook open staat voor onderbouwleerlingen. In 1962 daarentegen mochten alleen leerlingen uit de op één na hoogste klas van de middelbare school deelnemen.

Maar als we die verschillen tussen toen en nu even vergeten, zien we dat de opgaven van nu toch wel veel weg hebben van de opgaven uit 1962. Ook nu zijn de opgaven wat speelser dan de schoolwiskunde en ook nu heb je vaak een creatieve ingeving nodig om een opgave op te lossen. Die uitdaging en dat puzzelachtige karakter van de opgaven is wat de olympiade zo leuk maakt; daar is sinds 1962 niets aan veranderd! ■

OPLOSSINGEN KLEINE NOOTJES NR. 4

USB-STICK VAN DOBBELSTENEN

De som van tegenover elkaar liggende vlakken op een dobbelsteen is altijd 7. Met twee aan elkaar geplakte dobbelstenen, staan op de vier lange kanten dus de getallen (a, b), (c, d), $(7 - a, 7 - b)$ en $(7 - c, 7 - d)$; je gooit dus gemiddeld de som van deze acht getallen gedeeld door 4: dat is 7. Met drie aan elkaar geplakte dobbelstenen, staan op de vier lange kanten (a, b, c), (d, e, f), $(7 - a, 7 - b, 7 - c)$ en $(7 - d, 7 - e, 7 - f)$; gemiddeld gooi je dan de som van deze twaalf getallen gedeeld door 4: dat is 10,5.

SCHUIFPUZZELS

De bovenste puzzel kan wel, de onderste niet.

LEEFTIJDEN

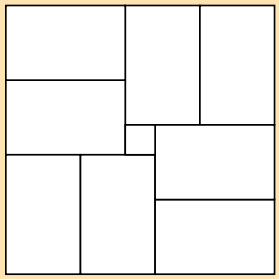
64, 57, 31 en 28 jaar. (Er zijn ook onwaarschijnlijke oplossingen, zoals 87, 56, 23 en 14 jaar.)

KANSWEGEN

Er zijn $2^4 = 16$ volgordes: LLLL, LLLR, …, LRRL, …, RRRR. Zes ervan hebben twee R'en en twee L'en. De kans is dus $\frac{6}{16} = \frac{3}{8}$. De kans met één knikker bij de start op de linkerschaal is natuurlijk ook $\frac{3}{8}$, want in het geval dat beide schalen bij de start leeg zijn, heb je na één knikker ook een situatie met één knikker op één schaal. Er zijn daarna nog acht volgordes waarvan er drie voldoen: RRL, RLR, LRR.

VIERKANTEN ZAGEN

Het vierkant van 36×36 is te verdelen in 4 vierkanten van 18×18; één zo'n vierkant zie je hiernaast. Uit één ervan kunnen 8 rechthoeken van 5×8 gezaagd worden. In totaal dus 32.



PYTHAGORAS 50ste jaargang nummer 5 april 2011
ISSN 0033 4766

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

Internet www.pythagoras.nu

Hoofdredacteur Arnout Jaspers

Eindredacteur Alex van den Brandhof

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

Bladmanager Arnout Jaspers
Mathematisch Instituut
Universiteit Leiden
Postbus 9512, 2300 RA Leiden

Vormgeving Grafisch Team Digipage BV, Leidschendam

Druk Drukkerij Ten Brink, Meppel

Uitgever Koninklijk Wiskundig Genootschap

Verantwoordelijk uitgever Chris Zaal

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

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

Abonnementsprijs
(6 nummers per jaargang)
€ 25,00 (Nederland),
€ 28,00 (België),
€ 32,00 (overig buitenland),
€ 22,00 (leerlingabonnement Nederland),
€ 25,00 (leerlingabonnement België),
€ 15,00 (groepsabonnement Nederland),
€ 16,00 (groepsabonnement België).
Zie www.pythagoras.nu voor toelichtingen.

Aan dit nummer werkten mee
Dick Beekman, auteur van diverse breinbrekerboeken (d.beekman9@chello.nl), Alex van den Brandhof, docent wiskunde op het Vossiusgymnasium te Amsterdam (alex@pythagoras.nu), Matthijs Coster, wetenschappelijk onderzoeker bij het Ministerie van Defensie (matthijs@pythagoras.nu), Jeanine Daems, aio wiskunde aan de UL en docent wiskunde op het Rijnlands Lyceum te Sassenheim (jeanine@pythagoras.nu), Birgit van Dalen, aio wiskunde aan de UL (bevandalen@gmail.com), Jan Guichelaar, wetenschapshistoricus (jan@pythagoras.nu), Klaas Pieter Hart, docent topologie aan de TUD (kp@pythagoras.nu), Alexander van Hoorn, student wiskunde aan de UvA (alexander@pythagoras.nu), Arnout Jaspers, wetenschapsjournalist (arnout@pythagoras.nu), Paul Levrie, hoogleraar wiskunde aan de ingenieursopleiding van de Karel de Grote-Hogeschool in Antwerpen (paul.levrie@kdg.be), Hilde Missinne, docent wiskunde aan het Instituut Spijker in Hoogstraten, België (hilde.missinne@markdal.be), Eddie Nijholt, student wiskunde aan de UvA (eddie@pythagoras.nu), Quintijn Puite, docent wiskunde aan de TUE en de Hogeschool Utrecht (g.w.q.puite@tue.nl).

20 JAAR GELEDEN

Op de achterkanten van deze vijftigste jaargang van *Pythagoras* laten we je zien hoe het tijdschrift in de loop der jaren is veranderd. Hier zie je het omslag en de eerste pagina uit het binnenwerk van het aprilnummer 1991 (jaargang 30 nummer 3).